On Methodologies to Select Systems for Automated Personal Identification

Anthony John Palmer

Thesis submitted to the University of London
for the degree of Doctor of Philosophy

Information Security Group,
School of Mathematics and Information Security,
Royal Holloway, University of London

July 2015

Declaration

Declaration of Authorship

These doctoral studies were conducted under the supervision of Professor Kenneth G. Paterson. The work presented in this thesis is entirely my own, whilst enrolled in the Information Security Group, School of Mathematics and Information Security as a candidate for the degree of Doctor of Philosophy.

I, Anthony John Palmer, hereby declare that the work presented in this thesis is entirely my own. This work has not been submitted for any other degree or award to any other university or educational establishment.

The research follows the recommendations stated in the Royal Holloway Guidelines on Research Governance, Research Ethics and Good Research Practice dated 15th February 2008.

Anthony John Palmer
July 2015

Acknowledgements

It is with immense gratitude that I acknowledge the support and guidance of my supervisor, Professor Kenny Paterson, throughout my research efforts. His enthusiastic attitude and encouragement helped me to overcome the many challenges associated with part-time research study.

I am also indebted to Professor Johannes Zanker for his assistance in scoping the boundaries of this multi-disciplinary research. Also I would like to thank Doctor Lizzie Coles-Kemp for introducing me to qualitative data analysis and the benefits of using a Computer-Aided Qualitative Data Analysis System (CAQDAS).

I am extremely grateful to all the interviewees and their organisations for consenting to participate in the empirical case study research. I thank them sincerely for providing me with their valuable time and efforts to furnish me with their incisive insights, which were paramount to my research inquiry.

Finally, I would like to thank my wife Caroline for her patience over the last seven years so that I may pursue my research ambitions. I fully appreciate the many sacrifices she has made for me in order to achieve my goal.

Abstract

Systems deployed to automatically identify persons operate in diverse application contexts, ranging from border control policing to on-line banking, attract benefits and risks to stakeholder organisations and to their respective user communities. This thesis explores the efficacy of a systematic methodology to select the *optimal* system for a given application context.

We created a systematic methodology in order to ascertain the extent of a systematic methodology's efficacy to select the optimal system for a given application context. We also developed criteria in order to assess the efficacy of such selection methodologies.

Employing the case study research methodology, we conclude that a systematic methodology is reasonably efficacious for selecting the optimal system when the circumstances surrounding the application context necessitate a comprehensive inquiry. An organisation should conduct a comprehensive inquiry when there is a need to establish objectives and requirements for the system in order to evaluate a range of candidate systems, employ repeatable systematic processes in order to reduce their reliance on the capabilities of discipline experts, and/or produce an audit trail of the programme's method which may be used as evidence to justify the system selected.

We ascertained that the scope of a comprehensive inquiry demands a multi-disciplinary approach to evaluate over 240 factors relating to the selection of the optimal system. An evaluation needs to examine the application context itself in order to determine the stakeholders' objectives and requirements for a system. Candidate systems may then be appraised on their capabilities to fulfil stakeholders' requirements.

We used our systematic methodology, in a case study involving the enhancement of an enterprise's user authentication system, to identify contextual exemplars demonstrating when a systematic methodology is efficacious for selecting these systems. Two retrospective case studies served to identify and explain the proficiencies and deficiencies of current approaches pursued by organisations' programmes.

Contents

List of Figures

List of Tables

CHAPTER 1

Introduction

Contents

This chapter gives an overview of this thesis. We describe the research problem, our research questions and the motivation for our research. We also provide a description of our research methodology, our main findings and our contributions to the body of knowledge. We also present the overall structure of the thesis.

1.1 Automated Personal Identification

Automated personal identification is an increasingly important function for government, business and society [247, 307]. The assured identification of persons brings benefits to organisations and user communities that can then rely upon the assertions associated with authentication systems and identification systems [59, 72].

Authentication systems are deployed as part of preventative measures to control users' access to information systems and other resources [11, 271, 287]. Identification systems are often deployed as detection utilities. Woodward cites [323] the use of a biometric system to expose multiple fraudulent social benefit claims in the USA. We use the term *automated personal identification* in this thesis to describe the information system function of automatically identifying persons. We use this term because of the lack of uniformity in the terminology and scope relating to the term *identity management* found in the literature. We explain our reasons for using the generic term *Automated Personal Identification Mechanism* (APIM) to represent an authentication system or an identification system in Chapter 2. We also describe other related concepts in order to clarify the scope of our research in that chapter.

Automated personal identification may bring a range of benefits to stakeholders in various application contexts; however, organisations and their user communities often encounter issues with deployed APIMs.

1.1.1 Issues Associated with Automated Personal Identification

Information systems are constantly under threat from attackers, which affects the management of organisational risks [78]. The impacts of risks are often difficult to predict [3] and the consequences of security breaches are arduous to quantify [282].

The consequences of security breaches relating to an APIM may range from a direct financial loss to an organisation, through fraud, to an exposure of a user community member's private information. On direct losses, for example, the Telegraph newspaper reports that banks in the UK appear to have lost ground to the criminals after figures showed a 71 percent rise in on-line banking fraud, up to £29.3m for the first half of the 2014, despite the increased usage of 'log-in gadgets'.[1]

[1] http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/11091524/Online-banking-fraud-up-71pc-despite-rise-of-log-in-gadgets.html

The UK Information Commissioner's Office (ICO) outlines organisations' obligations, in terms of security controls on passwords, which should be deployed in order to protect individual's private data. The UK ICO has the power to issue monetary penalty notices to organisations for serious breaches of the UK Data Protection Act, and for serious breaches of the UK Privacy and Electronic Communications Regulations.[2]

It is often difficult, however, to acquire evidence to demonstrate that these consequences are a direct result of a defective APIM deployment. Nevertheless, the frequency of reporting identity fraud, through organisations such as CIFAS, the UK's Fraud Prevention Service, is increasing [139]. Publicly available statistics, however, do not often ascribe the losses and costs of security breaches or other impacts directly to an APIM failure, although some surveys, such as the US Department of Homeland Security Science and Technology Directorate and SRI International, report customers' experiences as victims of digital identity fraud [88]. There are some resources, such as Scam Watch[3] which provide countermeasure guidelines to the user community. Reports relating to an APIM's deficiencies, however, may have an adverse impact on a user communities' reliance on the information system and its services which the APIM is designed to protect.

Some deployed APIMs also attract social acceptability issues [317]. For example, the UK Identity Card Programme attracted much criticism in the national press because of potential infringements of civil liberties, as the UK government's proposed to capture UK Citizens' fingerprint data.[4] Organisational handling of individuals' private information, both autobiographical and biometric data, is a growing concern [45, 308, 178], with complex legal implications [196]. Many APIMs also exhibit usability design flaws [67, 2, 167] in that users often have too many passwords or Personal Identification Numbers (PINs) to remember, which may result in the same password or PIN being used to access many different resources.

Some APIMs, particularly biometric systems, are not always accessible to all persons in the user community [162, 214]. For example, a biometric sensor device may fail to capture a signal of sufficiently good quality, e.g. a person's fingerprint, to enable the biometric identification system to encode that data for processing. Physical disabilities may also limit a person's ability to use small devices [250], for example Universal Serial Bus (USB) sticks.

Organisational investment in innovations to automatically identify persons often possess

[2] https://ico.org.uk/enforcement
[3] http://www.scamwatch.gov.au/content/index.phtml/tag/identitytheft
[4] http://news.bbc.co.uk/1/hi/8707355.stm

deficiencies, which may lead to the failure of an APIM deployment to fulfil its intended purpose.[5]

1.1.2 Vulnerabilities Associated with Automated Personal Identification

Deficiently deployed APIMs are exploited through their vulnerabilities, which include:

- technological defects [271, 197, 255]. For example, early fingerprint sensors failed to detect artificial fingers, which prompted biometric device manufacturers to introduce liveness testing;
- erroneous user actions [182, 9]. For example, a text based password to access a laptop computer can be easily written down on a piece of paper which may be attached to that laptop computer for a miscreant to take opportunistic advantage; and
- social engineering attacks [206]. For example, criminals target phishing attacks on individuals in an attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity, such as a bank.

Software vulnerabilities are difficult to identify and eradicate entirely in information systems [318]. APIMs rely on software components and such software implementations are not exempt from possessing vulnerabilities. The Adobe Inc. access control security breach reported in the media [85] describe security breaches where users' identifiers and passwords were captured by miscreants due to a deficient APIM deployment which used cryptographic protection techniques incorrectly. Identifiers and passwords are often protected by injecting a unique seed value and then hashing that result rather than encrypting the related password file. Files containing user identifiers and associated passwords may be attacked using brute force password cracking tools, such as Hydra.[6]

Empirical evidence suggests [8] that users do not always follow organisational security policies on password creation because of users' limited recall capabilities [324]. Also users do not always manage passwords in line with organisational security policies and the authentication data relating to an identifier are often conveyed to other individuals or are

[5] http://www.dailymail.co.uk/news/article-440069/Safest-passport-fit-purpose.html
[6] https://www.udemy.com/blog/hacking-tutorial/

misplaced [9]. Yet, Highland's predictions [130], that passwords are likely to be used for the authentication of persons for the foreseeable future, remain valid.

The deployment of a deficient APIM may be explained by organisations' lack of proper consultation or engagement with the other stakeholders, particularly the user community, during the design phases. Authentication guidelines focus [217, 158] on organisational risks, functionality and performance together with assurance levels of systems despite the need for wider evaluation of human related factors [1, 2], such as, social acceptability, usability, accessibility and subjects' privacy concerns. Some biometric guidelines [38] acknowledge, however, the need to address the human issues surrounding the usability and accessibility of biometric systems.

1.1.3 Advances in Automated Personal Identification

The advances in automated personal identification include technological innovation in the introduction of new biometric modalities [7] and also the use of commonly deployed modalities, e.g. fingerprints, in the latest communication devices. [8] There are also advances in the formation of federated identity management schemes, such as the UK Government Digital Verify Identity Assurance Service [9], which is to become the default way for citizens to access a variety government services using a single account and authentication mechanism through an accredited Identity Provider (IP).

Chauhan et al.'s survey [48] of biometric modalities identifies electrocardiogram and lip prints (cheiloscopy) as emerging means to identify persons, in addition to the more commonly deployed modalities, such as iris scans, retina scans, fingerprint, face and voice, and possibly infrequent deployments of signature, ear, keystroke and gait modalities.

Nandakumar et al. propose [214] a multi-biometric system which fuses the signals from the different biometric modalities in order to improve the implicit upper bound on the accuracy of a biometric system using a single modality. Data from multiple biometric sources may be consolidated at the sensor level, using data from the same biometric trait, or feature level fusion may be used, where the fusion involves different feature sets extracted from multiple biometric sources. The identification or authentication decision is based upon several data sources.

[7] http://www.biometricsinstitute.org/pages/types-of-biometrics.html
[8] https://www.apple.com/uk/iphone-6/touch-id/
[9] https://identityassurance.blog.gov.uk

Similarly, Clarke and Furnell argue [55] that the capabilities of current technologies enables composite, transparent and continuous authentication, using a variety of data relating to a user, e.g. keystrokes, as an alternative to a single Boolean user authentication process. Nevertheless, biometric identification and authentication systems, based on probabilistic calculations, by design do not always yield impeccable identification decisions [311, 86, 214]. Therefore, an APIM's decision relating to the identification of the genuine person or the verification of an owner's claim to a digital identity may not always be precise.

Organisations create and manage digital identities for their user or subject communities. Consumers are often required to set up an account with each transacting entity, which involves the creation of an identifier together with authentication data, e.g. a password. This account and its authentication mechanism then enables consumers to reap the benefits of conducting their purchasing activities on-line. Social networking sites also utilise similar access control measures. The NorSIS Password Survey in 2012 ascertained [285] that the average minimum number of passwords, used by persons for private purposes is 17 per person and 8.5 per person for work-related purposes.

The FIDO (Fast IDentity On-line) Alliance was formed to address the lack of authentication interoperability amongst devices, e.g. smart cards, smart card readers and mobile phones, as well as the problems users face with creating and remembering multiple identifier names and passwords for their accounts, by developing user authentication interoperability specifications.[10] Organisations are introducing digital identity services to customers to enable them to use a single credential at various sites on the Internet which require user authentication. Experian Ltd is an example of an early entrant into the identity provider market in the UK.[11]

Windley argues [321] that user communities' confidence in identification and authentication systems are influenced by economic models, people's attitudes and behaviour, processes surrounding their usage and the management of the systems, tools and technologies deployed, and the governance regimen. Camp concludes [43] that trust in information systems operating in different communities is difficult to assess. Despite the vulnerabilities associated with APIMs Birch contends [29] that the assured automatic identification of individuals can bring benefits to stakeholders by adopting a matured attitude towards the surrounding issues of managing digital identities.

Deployed APIMs may be considered by some stakeholders, as *fit for intended purpose*. Con-

[10] https://fidoalliance.org/specifications
[11] http://www.experian.co.uk/identity-and-fraud/products/authenticate.html

versely, other stakeholders may consider these same APIMs as *unsuitable* for their intended purposes. Notwithstanding potential conflict in stakeholders' views and that APIMs possess vulnerabilities, as well as attracting issues and costs, we consider that the determination of *the optimal* APIM for a given application context is an important and laudable aim. The selection of an optimal APIM and its deployment configuration may then be evaluated in terms of its appropriateness in respect of its intended purpose within the salient factors of the specific application context.

1.2 Determining the Optimal APIM

We believe that it is reasonable to assume that organisations' information system programmes strive to deploy the optimal APIM for a given application context. In practice, however, it is possible that an APIM may be deployed on the basis of its *adequacy* rather than its *optimal fitness for purpose* to address identified risks. Equally, organisations may be aware that an APIM is defective or that it may not be entirely *fit for purpose*, yet choose to prioritise investments into other programmes rather than funding additional security measures to address identified defects.

Irrespective of the terminology employed to depict the desired quality, an APIM cannot be considered to be *fit* or *acceptable* or *adequate* for purpose unless criteria are established and relevant data, from the application context, are acquired to perform an evaluation. An APIM may then be evaluated in respect of addressing stakeholders' objectives, using a range of criteria, relating to its deployment in an application context or as a candidate for deployment. Organisational decision-makers may utilise such evaluations in order to establish whether the APIM is optimal to meet their objectives of sufficiently minimising the uncertainty surrounding the effectiveness and efficiency of security controls [164], but also whether it aligns with organisational investment strategies [77].

1.2.1 Evaluation of an Application Context

Warfel recommends [307] that an evaluation of an application context for automated personal identification should be based on three axioms:

- the degree of identification is consistent with the need;

- the ratio of false accepts and false rejects are compatible with the risk and the customs of the business involved; and
- the costs of the identification are consistent with the need.

Organisations and their respective user communities may have different perspectives on these axioms because each stakeholder may be impacted in different ways, particularly as a consequence of a security compromise. Land observes [180] that information systems, in general, favour particular departments over other parts of an organisation. Stakeholder perspectives in respect of the needs, costs together with the risks and customs of the application context may not only vary within organisations but also externally between the different stakeholder organisations, including the user communities. Gerber and von Solms conclude [118] that the multiplicity of risks and the spectrum of social issues, with political cultural, economic, legislative and social roots, necessitate a multi-disciplinary approach when evaluating security requirements for an organisation and its user community.

Stakeholder organisations focus on managing digital identities in order to address the risks and costs associated with protecting access to enterprise information assets [321]. Conversely, evidence from Weir et al. [314] and Toledano et al. [288] suggest that users are driven by convenience and usability considerations, preferring to avoid cumbersome or intrusive identification and authentication routines. In the specific context of health information systems, in extreme circumstances unreliable authentication mechanisms have a life-threatening impact [99]. Price recognises [242] that there are both benefits and drawbacks to stakeholders involved with using digital identities. Striving for balanced security controls, however, can bring benefits to both organisational and user community stakeholders [246]. The approach to achieving this balance between stakeholders, however, may be complex due to the diverse range of factors which may need to be evaluated in the application context. The approach may also need to incorporate a technique to identify stakeholder compromises for determining the *balanced* security controls for the automated identification of persons in a given application context.

We believe that ascertaining the balanced security controls for the automated identification of persons in an application context requires the establishment of evaluation criteria and also the development of an approach in the form of evaluation processes in a systematic methodology. Criteria need to be established in order to determine, through comprehensive evaluation, the optimal APIM for a given application context. An evaluation also needs to encompass a range of perspectives and values from the various stakeholder groups, including

users, involved in the application context. An evaluation task that aims to strike a balance between stakeholders' objectives, using established criteria to evaluate their perspectives relating to the security, usability and privacy factors for that application context, then raises the question of which methodology to pursue [123, 333].

Checkland explains [49] in his thirty year retrospective review of information system development methodologies, that specific methodologies, irrespective of their hard–soft distinction, are efficacious for certain types of programme and contextual circumstances. Similarly, we believe that some methodologies for deploying APIMs may be efficacious for certain types of programme and contextual circumstances to identify the optimal APIM for a given application context.

1.2.2 Methodological Considerations

Organisations may consider pursuing a range of strategies in order to select the optimal APIM for their various application contexts. Some organisations may opt to use the default APIM provided by an information system, an application program, an operating system or a device.

The Whither Committee's Biometrics Report proposes [230] that:

> *"there are significant opportunities [for researchers] to develop an evaluative model that would guide potential procurers and users of biometric systems. Guidance for potential users of biometric systems on an appropriate initial set of questions to ask before getting into the details of modalities and so forth have proven particularly useful."*

We consider that these significant research opportunities apply not only to biometric systems but to all types of systems that automatically identify persons. We propose that the guidance sought should be in the form of a methodology which evaluates a range of factors, including stakeholders' objectives and requirements for an APIM deployment. We believe that such an evaluation should be specific to an application context so that the optimal APIM for that context may be identified.

We acknowledge that there may be some contextual circumstances when some methodologies may not be as efficacious as other approaches (and vice versa) in ascertaining the optimal

APIM for a given application context. Before attempting to assess the efficacy of various approaches, we need to establish an understanding of the methodological tools available.

1.2.3 Overview of Existing Methodologies

We now provide an overview of the existing methodological tools in order to reveal possible research avenues using Avison and Fitzgerald's methodology era model [18]. Our review of the Information Security (InfoSec) methodological tools and the tools for evaluating APIMs can be found in Section 3.2 and Section 3.3 respectively. We classified the methodological tools found in the literature into guidelines, analytical frameworks, conceptual modelling, heuristic approaches and systematic methodologies. We explain our classification scheme in Section 3.1.3.

Avison and Fitzgerald's methodology era model [18] enabled them to reveal the evolution and development of the methodological tools for information system development methodologies. Their model identifies four methodology eras:

Stage 1 – pre-methodology era which is characterised as a period where systems are developed without the use of an explicit or formalised methodology;

Stage 2 – an early-methodology era, which is characterised by approaches that comprised of phases and stages to enable the management of the discipline of systems development;

Stage 3 – a methodology era, which is characterised by formalised documented methodologies that were developed from practice or theory; and

Stage 4 – an era of methodological assessment, which is characterised by the reappraisal of the philosophy, concepts, processes and practicality of system development methodologies.

We use the same maturity model to illustrate the relative maturity of methodologies applied in the InfoSec discipline and the methodological tools for evaluating APIMs.

We claim that InfoSec methodological tools have reached the methodology era [Stage 3] in that we were able to locate several tools in each of our defined classes. We next provide a high-level description of the recent InfoSec methodologies in order to demonstrate the maturity of the tools to support our claim.

Fléchais' methodology [101], based upon Boehm's software development methodology [33], is an unstructured heuristic approach to incorporate usable security designs into information system (IS) development programmes. Similarly, Faily's collaboration with Fléchais [93, 94] resulted in a meta-model evaluation tool to assist requirements engineering processes in order to design secure and usable information systems. Mouratidis and Giordini's development [208] of Secure TROPOS, a security-oriented extension of the TROPOS Methodology [36], provides an agent-oriented software development methodology. These methodologies tend to concentrate on software development rather than describing the security procedures in a security architecture or the expected user behaviour in an application context.

We did not find any evidence which suggests that these InfoSec methodologies have been validated empirically or that their efficacy has been assessed, which indicates that these tools have not reached the methodological assessment era [Stage 4] in their evolution.

We claim that methodological tools specifically for evaluating APIMs have reached the early-methodology era [Stage 2]. From our review of methodologies in the literature we located several analytical tools and evaluation frameworks which are designed to assist with the selection of systems for the automated identification of persons.

Ashbourn's Pentakis approach [15] is an analytical tool for evaluating biometric deployments only. Similarly, Toledano et al.'s evaluation framework [288] focuses on the evaluation of four different types of biometric modality. Renaud's analytical tool [250, 249] concentrates on assessing authentication systems based upon subject knowledge, e.g. a password. These contributions evaluate authentication systems or identification systems as solutions without having sufficient regard to the intended purpose and the factors surrounding the application context which may influence stakeholders' decisions.

Royer and Meints' evaluation framework [258], however, focuses on modelling the factors relating to the selection of an Enterprise Identity Management System (EIdMS), which may result in the selection of an authentication system or an identification system, with or without the use of biometrics. Royer developed [256] the EIdMS Decision Support System based upon this evaluation framework. It appears that these methodological tools, which we classify as conceptual modelling and heuristic approach tools respectively, have yet to be validated empirically.

From our investigations we were unable to locate systematic methodologies in the scientific literature which are designed specifically to develop or select a system for automated

personal identification of persons for a given application context. We also located systematic methodologies used by professional services companies; however, insufficient detail has been published to enable them to be scientifically assessed. We found the IdMology: Coherent Identity Management Methodology (CITM) [12] and the MMASQ (Model-centric Methodology for Analysis, Specification and Qualification) [13] which appear to be used by practitioners in professional service providers.

The lack of published systematic methodologies for evaluating or selecting APIMs provides us with a research opportunity to develop such a methodology. Also, we found no evidence in our review of the literature that methodological tools for evaluating APIMs have reached the Stage 4 era. This finding provides us with an additional research opportunity to assess our developed systematic methodology and also to reappraise current approaches.

Based on these two identified research opportunities we next explain our motives for conducting research into systematic methodologies for evaluating and selecting APIMs. Our focus is on the assessing the efficacy of systematic methodologies, as tools, to select the optimal APIM for a given application context.

1.2.4 Motivation for Our Research

From the research opportunities identified in the previous section we propose that it is expedient to expend research effort on establishing a systematic methodology, which can identify the optimal APIM for a given application context. Also an investigation into the efficacy of the resulting systematic methodology (and additionally explores the efficacy of current approaches) may not only contribute to the existing body of knowledge but could also enhance the understanding of current practices to deploy APIMs.

As we described in Section 1.1.1, there are many issues associated with deployed APIMs. Similarly, as we identified in Section 1.1.2, there are many vulnerabilities associated with deployed APIMs. These issues and vulnerabilities may stem from the inappropriate usage of the identification technologies, deficiencies in the capabilities of the practitioners and/or the efficacy of the methodology.

The advances in identification technologies, briefly described in Section 1.1.3 and also reviewed in APIMs in Section 2.4.3, suggest that deficiencies in some APIM deployments

[12] http://whitepapers.itbusinessnet.com/whitepaper398
[13] https://www.hjp-consulting.com/consulting/requirements-engineering

might not be confined to the available identification technologies themselves. An examination of the identification technologies should, as Polemi argues [238], consider the characteristics of the application context in which the technology is to be deployed. The vulnerabilities and issues may, therefore, be the result of deploying inappropriate APIMs for some application contexts. Some identification technologies may be considered to be optimal for some application contexts but not for others.

Royer contends [256], from his research involving discipline experts, that the complexity of evaluating interdependent factors to select and deploy the optimal system for automated personal identification necessitates the use of a decision support system. His findings suggest that the selection of the optimal APIM should not rely on discipline experts' capabilities alone and that methodological tools are required to complement their current practices.

The practices described by Windley [321], Williamson et al. [320] and Prasad and Rajbhandari [240] appear to place much reliance on discipline expert practitioners' capabilities to select and deploy the optimal APIM. Discipline experts, however, possess differing competencies and experience and they may pursue different approaches depending upon the circumstances surrounding the application context.

In order to ascertain other causes relating to the issues and vulnerabilities associated with deployed APIMs we believe that an investigation should focus on the problem-solving processes, i.e. the methodologies, which includes the problem-solving processes pursued by practitioners.

A methodology, as a problem-solving process, informs programmes on 'what' steps to take, and 'how' to perform those steps, and importantly the reasons 'why' those steps should be taken in a particular order [165]. Avison and Fitzgerald argue [18] that the tighter, more specific the methodology, the more reproducible are the results, particularly if the methodology specifies the exact techniques and tools to be employed under each circumstance.

Therefore, we aim to develop a systematic methodology to aid discipline experts select the optimal APIM for a given application context. We believe that a discipline expert, as a problem solver, working with a methodical problem solving processes should be more efficacious in selecting the optimal APIM. Our research inquiry aims to gain an initial understanding on the efficacy of our systematic methodology. We also seek to identify the proficiencies and deficiencies of current approaches.

The identified theoretical gaps in the body of knowledge and the apparent deficiencies of current approaches served as valuable motivations for our research effort.

1.3 The Research Problem

Given the gaps identified in the body of knowledge and our motivation, we aim to determine the extent to which a systematic methodology is efficacious in selecting the optimal APIM for a given application context.

Our analysis of the research problem shows that there is a need to be able to ascertain the extent to which an APIM is optimal for a given application context in the first instance. From this understanding an assessment may then be conducted on the efficacy of the methodology pursued which selected that APIM.

The research problem addressed in this thesis is framed as follows:

How efficacious is a systematic methodology in selecting the optimal automated personal identification mechanism for a given application context?

Our research aims to ascertain the efficacy of a systematic methodology to select the optimal APIM for a given application context. We aim to create a systematic methodology and validate its components empirically. We also aim to assess its efficacy by examining the data acquired during its utilisation to select the optimal APIM in a real-world instance. From our acquired empirical data we aim to explain the extent of efficacy of a systematic methodology in a range of circumstances (and possibly not in others) to select the optimal APIM for a given application context.

We exclude the direct comparison of the efficacy of a systematic methodology to that of current practices in the same application contexts because of the research impracticalities, as we explain later in this chapter. Our empirical inquiry, however, seeks to gain an understanding of current practices as well as seeking to identify the circumstances as to when a systematic methodology may be efficacious. We believe that there are circumstances when a systematic methodology may be efficacious for selecting the optimal APIM for a given application context and there are circumstances when other approaches may be more efficacious.

1.3.1 Research Questions

In order to ascertain the efficacy of a methodology the means to identify whether an APIM is optimal for its application context needs to be established at the outset. The identification of the circumstances as to when a systematic methodology is efficacious for selecting the optimal APIM in turn needs to be broken down into several assessments.

Evidence shows [296, 299, 28] that public bodies and the media often criticise the resulting APIM deployments as *unfit for purpose*. We contend, however, that unless the purpose of the APIM for an application context has been defined at the outset and criteria are established to evaluate the optimality of the resulting APIM deployment then such criticisms have scant foundation.

Once the optimality of the APIM deployment is established, the efficacy of the approach pursued to select that APIM may then be examined. Further criteria are thus required to assess the efficacy of methodologies designed to select the optimal APIM for a given application context. The results of the efficacy assessment and the supporting explanations should then assist in the identification of the circumstances when the use of that methodology may be most proficient.

Our inquiry into the above research problem is deconstructed, therefore, into the following research questions:

1. What factors should be evaluated in order to select the optimal APIM for a given application context?
2. How can information pertaining to an application context be acquired and evaluated in a systematic methodology so as to determine the optimal APIM?
3. How can the efficacy of a methodology to select an APIM itself be assessed?
4. When is a systematic methodology efficacious for selecting an APIM and if so, under which scope of circumstances and why or conversely, if not, why not?

1.3.2 Addressing the Research Problem

We adopt a multi-disciplinary research approach to collate, classify and validate a set of factors in order to conduct an evaluation on the utility of a deployed APIM or APIM

candidates for a given application context. Essentially, we argue that stakeholders' objectives and requirements need to be articulated at the outset in order to establish a representation of the desired properties of the APIM for that specific application context so that an evaluation of a deployed APIM or candidate APIMs may be conducted.

We conclude that a systematic methodology is efficacious when the prevailing circumstances of the application context dictate the need for a comprehensive evaluation. We identify several circumstance exemplars and provide explanations as to why a comprehensive evaluation for some application contexts is relevant. We also identify those conditions surrounding the application context that shows when a systematic methodology is not efficacious.

Our research excludes a theoretical comparison of the efficacy of a systematic methodology to that of other methodologies because we were unable to find any such methodologies published with full details in the literature. We, therefore, develop a systematic methodology, for evaluating an application context in order to select the optimal APIM. Our research conclusions may therefore be considered as a *theoretical stake in the methodological ground*.

Our research also excludes a comparison of the efficacy of a systematic methodology to that of current practices. We believe such comparisons with current approaches practised are impracticable because the approach may not have actually been documented or it may be subject to confidentiality protection. We also contend that there are too many real-world complexities and data acquisition impracticalities to make such comparisons a valid research aim. We further justify our reasons for excluding such comparisons later in Section 1.6.2.

In practice, we acknowledge that the underlying power influences, i.e. politics, in and between organisations may negate or reduce the decision-making intentions of our systematic methodology. Our research approach is cognisant that political and commercial interests which influence objective reasoning may impinge upon evaluations and deliberations relating to decision-making on APIM deployments.

1.4 Research Methodology

We used the case study research methodology based upon our critical realist philosophical orientation, the nature of the research problem and the qualitative research strategy formulated to address our four research questions. Chapter 4 elucidates and justifies our research strategy for our research inquiry in detail. Here we, briefly, summarise our research approach, which

involved two distinct lines of inquiry.

1.4.1 Epistemology

Our philosophical orientation leans towards the critical realist paradigm, in that knowledge is grounded in social and historical practises, which may or may not be directly observable [198]. The critical realist paradigm is conducive to retroductive reasoning to discover underlying mechanisms in order to explain observed regularities and also abductive reasoning for iterative theory building [32].

Our explanatory inquiry seeks to apply Pawson and Tilley's generative causal model [233] consisting of a formula of actions in context with intervention mechanisms which produce outcomes. The evaluation of a programme begins with a theory of *causal explanation* based on generative principles, which supposes that regularities in the patterning of social activities are brought about by underlying mechanisms constituted by people's reasoning and the resources that they are able to summon in a particular context [233].

1.4.2 Research Strategy

Our inceptive line of inquiry was to establish a set of factors for evaluating an application context and then validate them using empirical evidence. This inquiry was exploratory in nature. An incremental approach was adopted by reviewing the literature and establishing an initial set of factors. These factors were then validated, using grounded theory qualitative data analysis techniques [47, 259], against the empirical data acquired from three case studies. Data from the case studies were used iteratively in order to identify new factors or refine previously established factors.

We classified our validated factors which acted to inform our efforts to ascertain the requirements of a systematic methodology for selecting an APIM. The development of our systematic methodology commenced with the review of the literature in order to establish an initial evaluation framework and a selection method with discrete steps. The methodology was enhanced iteratively from our analysis of data relating to approaches pursued by programmes in two case studies. These data enabled the identification of methodological lessons from a retrospective analysis of the conditions prevailing at the inception stage of the programme, the events that occurred during the programme and the outcomes of the APIM deployments.

Our main line of inquiry was to assess the efficacy of a systematic methodology to select the optimal APIM for real-world case. This second line of inquiry was explanatory in nature. We used the systematic methodology, as an *intervention mechanism* as described by Pawson and Tilley [233], in a real-world case study. We established criteria to assess the efficacy of our systematic methodology using the data that was acquired during its usage. We also performed a cross-case analysis of methodological efficacy using the data acquired from our three case studies in order to identify patterns in our data.

From this analysis and the circumstances surrounding the programme in each case study we were able to identify the circumstances as to when a systematic methodology is efficacious for selecting the optimal APIM for given application context. The patterns in our data provided us with explanations to support our conclusions on methodological efficacy.

1.4.3 Case Study Research Methodology

Data relating to the two retrospective case studies were acquired from documentary evidence in the public domain and from interviews with participants involved with these APIM deployment programmes. For the intervention case study, data were generated from using the systematic methodology in collaboration with an enterprise's Director of Risks. The data gathering interactions included several interviews, exchanges of correspondence and the production of a Request for Information (RFI) document which was sent to potential suppliers.

Theoretical sampling, as described by Silverman [265], was used to identify three case studies that were collectively representative to develop our theories. Adhering to the authoritative guidance [203, 253, 265] on qualitative data coding, we coded the data acquired from our three data sets. We used Pawson and Tilley's generative causal model [233] as a framework to assess the acquired data on methodological efficacy.

We developed a Decision Support System (DSS) as a representation of our systematic methodology which we used as a repository for the acquired data. The Atlas.ti Computer-Aided Qualitative Data Analysis System (CAQDAS) tool was used to manage the data sets to support of the analysis of our data in respect of our main line of inquiry on methodological efficacy.

1.5 Contributions to Knowledge

From our research efforts our main contribution to the body of knowledge is our initial theory on the efficacy of a systematic methodology in selecting the optimal APIM for a given application context.

We conclude from our research, but we do not prove irrefutably, that a systematic methodology is *reasonably* efficacious when the characteristics surrounding the application context are such that an organisation needs to conduct a comprehensive evaluation in order to select the optimal APIM. Our initial theory is founded upon three explanations which we identified from our analysis of data acquired from using our systematic methodology, **A**pproach to **S**elect the **M**ost **S**uitable **A**PIM (ASMSA) Methodology, in a real-world case study.

An organisation should conduct a comprehensive evaluation when the circumstances surrounding the application context necessitates that its programme needs to:

- establish objectives and requirements for an APIM in order to evaluate a range of candidate APIMs;
- employ repeatable systematic processes in order to reduce their reliance on the capabilities of discipline experts; and/or
- produce an audit trail of the programme's method which may be used as evidence to justify the APIM selected.

The extent of a systematic methodology's efficacy may reach beyond the need to conduct a comprehensive evaluation. Further empirical research should help to build upon our initial theory and also identify other reasons for utilising a systematic methodology to select an APIM.

In answering our research questions our other contributions to the body of knowledge are:

1. a comprehensive range of factors in order to select the optimal APIM for a given application context;
2. an innovative systematic methodology – the ASMSA Methodology comprising an evaluation framework and a method to select an APIM; and

3. a set of criteria to assess the efficacy of a methodology to select the optimal APIM for a given application context.

As a by-product of our research, we developed the ASMSA Decision Support System (ASMSA-DSS), as a tool to represent the processes in the ASMSA Methodology in order to acquire data, store and manipulate data from a case under evaluation.

The establishment of a systematic methodology to evaluate a given application context in order to select the optimal APIM and the establishment of a comprehensive range of factors to evaluate APIMs provides a foundation for further theoretical and empirical research.

From the initial use of the ASMSA Methodology, we found that it has the potential, through further refinement, to become a valuable tool for practitioners. Further research is needed to identify, understand and represent the rules that discipline experts employ, from their in-depth experience, in their approach to select APIMs.

We also conclude that organisations should define the pertinent metrics for their application context and acquire the relevant data in order to evaluate the utility of a deployed automated personal identification system. Our research supports Jaquith's argument [164] that organisations need to enhance the measurement of their security controls. We contend that the absence of such data not only inhibits efforts to evaluate the utility of deployed APIMs, but also impedes efforts to assess the efficacy of methodologies to select such systems.

The material relating to our publication on factors to evaluate APIMs [226] forms the basis of the content of Chapter 7; however, these factors and their associated criteria questions have since been validated and enhanced through our empirical research. The material relating to our publication on the systematic methodology to evaluate and select APIMs [227] also forms the basis of Chapter 7, which describes the ASMSA Methodology comprising an evaluation framework, incorporating factors for evaluating APIMs and associated criteria questions, and a selection method.

1.6 Restrictions on Research Scope and Key Assumptions

The restrictions discussed in this section relate to those aspects of our inquiries that fall within our control. We establish and justify the boundaries of our research field in Chapter 2 by defining key terms, describing the fundamental concepts, and the scope of automated

personal identification. We elected to avoid using the term *identity management* in this thesis so as to ensure that the scope of our research and our findings may be understood within these defined boundaries.

As discussed in Section 1.3, the research problem is framed to restrict our research efforts to determine the extent of a systematic methodology's efficacy to select the optimal APIM for a given context. We exclude research on theoretical and practical comparisons of methodological efficacy for the reasons given in the next two sub-sections.

1.6.1 Boundaries on Theoretical Scope

Essentially, there are no other systematic methodologies for selecting APIMs in the body of knowledge in order for us to conduct a theoretical comparison.

An experimental research methodology using relevant case study data, suitable assessor subjects and different methodologies to select an APIM, is a future possibility; however, we excluded this research option because our aim was to establish a systematic methodology in the first instance and to then investigate the extent of its efficacy. We also assumed that a theoretical research avenue would involve the control of many variables and much of the research work would focus on the subjects' knowledge and capabilities and their interpretation of the data and their understanding of the selection methodology.

The main unit of analysis of our inquiry was to ascertain the extent of a systematic methodology's efficacy to select the optimal APIM for a given application context, as defined in Section 4.5.1. Our secondary unit of analysis focused on the validation of our systematic methodology's components. We believe, however, that future research may enhance the body of knowledge on systematic methodologies provided that the impact of the assessor variable, i.e. the competencies of the methodology user, is minimised.

1.6.2 Boundaries on Practical Scope

Additionally, there is the option to conduct investigations on selecting APIMs using discipline experts and exploring their practices.

Firstly, we had no means to verify an individual's claim to be a discipline expert in the field. We also assumed that it would have been difficult to gain consent and willingness of a

practitioner to participate in our research, particularly to acquire data during an assignment. Our aim was to collect data from using a systematic methodology during an evaluation assignment. We believed that a discipline expert's review of our systematic methodology in isolation of a specific application context would be inadequate for our research purposes. We assumed that pursuing a research strategy that used the systematic methodology would improve the quality of data acquired.

Secondly, we were conscious that some organisations or practitioners may not wish to disclose sensitive data, particularly on reliability, vulnerabilities and costs of the APIM deployments. For this reason we justify our research strategy to use the case study research methodology and selected cases with documentary evidence in the public domain. We also selected our cases on the basis that there were individuals willing to participate in our research under the formal arrangement of a consent agreement.

Our main assumption is that we believed that it would be difficult to compare our systematic methodology with another approach simultaneously in a real-world application context. We assumed that it may be difficult to differentiate the data generated from using the systematic methodology's processes and the data acquired from using a different approach in the same application context. We also assumed, in reality, that it would be difficult to locate two identical application contexts in order to compare different methodologies.

Similarly, if a methodology were assessed retrospectively, i.e. after the APIM selection, then there may be an advantage to the succeeding methodology from having the opportunity to learn from the preceding methodology and its decision outcomes. Most importantly, we were conscious that organisational interests and operational constraints often make it difficult to use controlled scientific intervention, particularly when there is a potential adverse impact on risk countermeasures.

Our research, therefore, concentrates on developing a systematic methodology and assessing its efficacy rather than trying to compare the ASMSA Methodology against current practices directly.

Therefore, our research concentrated upon the efficacy of the systematic methodology as our main unit of analysis without attempting to nullify or reduce the effects of the assessor variable. We also recognised that our interpretation of data gathered from the case studies may also be subject to bias; however, the research methodology was designed to acquire independently produced data, i.e. interviewees' insights, rather than our interpretations and

opinions.

Our research inquiry is based upon our assumption that APIMs are imperfect, in that they have inherent vulnerabilities, attract issues and stakeholders incur costs. We also assumed that stakeholder organisations in each application context define the qualities upon which to evaluate the utility of a deployed APIM.

The significance of our research is that it aims to establish that a systematic methodology is efficacious for selecting the optimal APIM for a given application context under certain circumstances. Shostack and Stewart pose [264] many fundamental questions about the efficacy of some experts' practises to select effective and efficient security controls. The results of our research efforts add a specific methodological instrument to the practitioners' *tool box* and also provide guidance on the circumstances as to when the use of that instrument is efficacious.

1.7 Outline of this Thesis

The thesis is structured into nine chapters with 14 appendices. The contents of each chapter and appendix are as follows:

Chapter 1– Introduction This introductory chapter sets out the research problem addressed in this thesis together with a description of our motivation to conduct research in this field. We also describe our contributions to the body of knowledge and the delimitations of our research efforts;

Chapter 2–Terminology In this chapter we define the terms associated with automated personal identification and also provide a description of the core concepts of identification and authentication used in this thesis;

Chapter 3–Research Issues In this chapter we establish a *tool* classification scheme for reviewing approaches which can be applied within the InfoSec discipline to achieve a desired result. We provide our review on InfoSec approaches in literature based on our classification scheme. We then provide our review of the approaches in the literature on our immediate discipline of the identification and authentication of persons in order to identify research issues. We also explain the development of our four research questions in order to address our research problem on the efficacy of a systematic

methodology to select the optimal APIM for a given application context;

Chapter 4–Research Methodology In this chapter we outline the theoretical foundations upon which we based our decision to use the case study research methodology in order to conduct our research. We also specify our criteria for selecting appropriate case studies and justify the selection of the three case studies used in our empirical research. We then define our main unit of analysis to assess the efficacy of a systematic methodology. We also define our secondary unit of analysis to validate the ASMSA Methodology's factors and criteria questions. We also describe the methods used to gather data from our three case studies and our analytical framework for analysing the acquired data;

Chapter 5–The ASMSA Methodology This chapter opens with a description of the research problem's characteristics which motivated us to develop a systematic methodology to select the optimal APIM for a given application context. We also describe the theoretical principles upon which we designed the ASMSA Methodology. We then provide a description of the ASMSA Methodology's three components comprising the ASMSA Evaluation Framework, its factors for evaluating APIMs and associated criteria questions grouped into evaluation themes, and the ASMSA Selection Method;

Chapter 6–Case Study of an European Union State's eID Card Programme This chapter describes our initial efforts to validate our identified factors and associated criteria questions using data from our first case study. We then examine the approach pursued by the European Union (EU) state's eID Card Programme. We also provide a summary of the methodological insights acquired from members of the programme team in order to identify methodological learnings;

Chapter 7–Case Study of an EU State's eGates Programme This chapter discusses our efforts to validate our identified factors for evaluating APIMs and associated criteria questions using data from this second case study. We then examine the approach pursued by the EU state's eGates Programme. We also provide a summary of the methodological insights acquired from members of the programme team in order to identify methodological learnings. We also conduct a cross-case analysis of our methodological findings from our two retrospective case studies;

Chapter 8–Assessing the Efficacy of the ASMSA Methodology In this chapter we begin by establishing six criteria upon which to assess the efficacy of a methodology to select the optimal APIM for a given application context. We then discuss our efforts to

validate our established methodology using data from the inaugural use of the ASMSA Methodology in the Corporation X's Two Factor Authentication (2FA) Project. We also provide a summary of the methodological insights acquired from Corporation X's Director of Risks in order to identify methodological learnings. We provide the results of our assessment of ASMSA Methodology's efficacy using the data from the Corporation X 2FA Project Case Study and our established efficacy assessment criteria. We then identify circumstances when a systematic methodology may be efficacious for selecting the optimal APIM for a given application context;

Chapter 9–Conclusions and Implications In this final chapter we draw our conclusions on the achievements of our research efforts. We then discuss our conclusions about the research problem and our efforts to answer our four research questions. We then reflect on the research methodology to address our research problem. We summarise the implications of our research to theory and to practice, and then identify avenues for further research;

Appendix A Factors for Evaluating APIMs and Criteria Questions Identified from our Review of the literature;

Appendix B EU State's eID Card Programme Case Study Interview Questions;

Appendix C Factors and Criteria Questions Status Post First Case Study Validation;

Appendix D EU State's eGates Programme Case Study Interview Questions;

Appendix E Factors and Criteria Questions Status Post Second Case Study Validation; and

Appendix F Factors and Criteria Questions Status Post Third Case Study Validation.

1.8 Summary of Chapter

This chapter laid the foundations for this thesis and introduced the research issues, the research problem and its four associated research questions.

Our motivation and a justification for the research were presented and the issue relating to the uniformity of the key terms were highlighted. A description of the research methodology was outlined together with our claims on the contributions to the body of knowledge. The boundaries of our research scope and our main assumptions for the research were discussed.

1.8 Summary of Chapter

Based on these foundations we proceed with a detailed description of this thesis commencing with definitions of the terminology relevant to this research field in the next chapter.

CHAPTER 2

Terminology

Contents

This chapter describes the need to define terms in the automated personal identification research field. We provide descriptions of the underlying theoretical concepts of identification and authentication together with definitions and scope of the term APIM upon which our research is based.

2.1 The Need for Consistency in Scope and Defined Terms

The need for consistency in this research field relates to the differing interpretations of the scope of *identity management* and the lack of uniformity of terms and their definitions relating to its key concepts.

2.1.1 Inconsistencies in the Scope of Identity Management

Bertino and Takahashi acknowledge [27] that researchers and practitioners adopt different interpretations of the scope of the term and the acronym *Identity Management (IdM)*. Some of the literature extends the scope of identity management to cover all types of entities [30, 321, 204]; whereas, other contributions restrict the scope to the automatic identification or automatic authentication of persons [236, 287, 320]. The main difference between identity management and automated personal identification appears to be related to scope. The former term is used to indicate the identification of all types of entity; whereas, the later term is confined to the identification of persons. We use the latter term because of the uncertainty surrounding the definitions and scope of the former term.

The ITU-T Standards Organisation recognises [151] the different interpretations of this term and also the diversity of understandings in respect of its scope. Stevens contends [276] that identity management is the entirely the wrong term, in that organisations are not trying to 'manage' digital identities per se, but to ascertain:

- who an individual is in an information system;
- whether this person is unique in an information system (more than one digital persona); and
- whether a person is who they claim to be.

The International Telecommunications Union defines the scope of the identity management in ITU-T X.1252 Baseline Identity Management Terms and Definitions [151] as:

> A set of functions and capabilities (e.g. administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:
>
> - assurance of identity information (e.g. identifiers, credentials, attributes);
> - assurance of the identity of an entity; and
> - supporting business and security applications.

The following statement appears after the above definition in ITU-T X.1252:

> Please note that this annex does not capture or explain the holistic view of identity management.

This statement leaves the aforementioned scope of identity management open to differing interpretations, as there does not appear to be a definition in the literature on what constitutes *an holistic view of identity management*.

Similarly, ISO/IEC24760 Part 1–A Framework for Identity Management Terminology and Concepts defines [157] identity management as:

> processes and policies involving the life-cycle and value, type, and optional meta data of attributes in identities known in a particular domain

ISO/IEC 24761 Authentication Context for Biometrics [156], published by the same standards working group on identity management, uses the term *biometrics processing unit* instead, which is defined as:

> entity that executes one or more sub-processes that perform a biometric verification at a uniform level of security

We consider the inconsistency in scope of the term *identity management* in the literature and the vagueness of the definitions and scope in these authoritative sources are not suitable foundations upon which to base research and to develop theories. Therefore, we adopt the term *automated personal identification*, as established by Warfel [307] over three decades ago and embraced by Raphael and Young [247] and the U.S. National Institute of Standards and Technology (NIST) [177], as our core generic term which relates to systems that automatically identify or authenticate persons.

Our adopted term may, therefore, be construed to describe the generic requirements for an *Automated Personal Identification Mechanism (APIM)* to automatically identify persons. Those requirements are fulfilled by an identification system or an authentication system.

2.1.2 Lack of Uniformity Relating to Key Terms and Concepts

Clarke states [59] that the practises of identification and authentication have been highly unsatisfactory for the last two decades, mainly, he claims, because the theory and the terms

used, e.g. IdM, for such activities are seriously deficient. Chadwick also recognises [46] the impreciseness of the standards bodies' terminology to describe an IdM system, in his endeavour to explain the scope of federated identity management. ISO/IEC24760 Part 1–A Framework for Identity Management Terminology and Concepts fails [157] to define the term or describe the concept of an identity management system.

Evidence to support Clarke's and Chadwick's observations is exemplified by the standardisation bodies' definitions of IdM terminology in ISO24761 Authentication Context for Biometrics [156], ITU-T X1252 Baseline Identity Management Terms and Definitions [151], The Open Group's Identity Management White Paper and Business Scenarios Report [269, 286], W3C's Workshop on Identity Management [304] and NIST's Special Publication 800-63-2 Electronic Authentication Guideline [217]. The term Personal Identity Verification (PIV), adopted by NIST [98, 215], covers the automatic personal identification of persons accessing government information systems as employees or contractors.

Key terminology relating to biometric systems is also not uniformly used in the literature or in authoritative sources. For example the terms biometric authentication [271], biometric verification [214, 156] and biometric recognition [230] relating to the same concept are further evidence that the terminology and scope of this research field needs to establish consistency. Jain and Li conclude [186] that until consistency in terminology is achieved, by the respective standardisation bodies, there is always a need to define each term in publications in the field of the identification and authentication of persons.

We revert to established theoretical identification and authentication models [95, 58] in order to define the term *Automated Personal Identification Mechanism* and also to describe the scope of automated personal identification in this thesis.

2.2 Identification and Authentication Theory

We describe the concepts of digital identity and the interrelationships in respect of identification and authentication theory in order to then explain the types of usage transactions in an identification system or authentication system.

Clarke's Entity-Relationship of Identity Model [58], shown in Figure 2.1, depicts the concepts and the terms relating to the identification of an entity, in our case a person using their characteristics, and the authentication of an entity that verifies a person's assertion claim to a

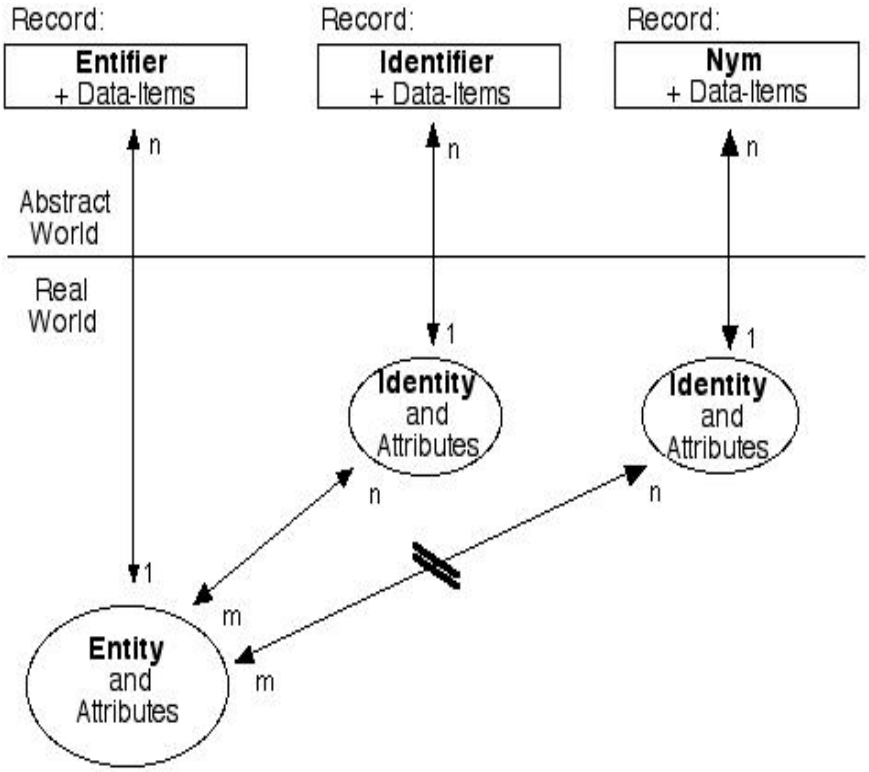

Figure 2.1: Clarke's Identifier Based Authentication Versus Attribute Based Identification Model [58]

user account in an information system. Clark invents [58] the term *entification* to distinguish between an attribute based identification system and an identifier based authentication system. As Clarke acknowledges [58] his term *entification* is not adopted universally; however, we use this term in this thesis for clarification purposes only.

Everett's model [91] of the verification of human users' identity and Fåk's Theoretical User Verification Model [95] provide a foundation upon which to develop an abstract transaction model for automated decisions on the identification or authentication of persons. Figure 2.2, is adapted from Fåk's model, using Clarke's definitions [58], to illustrate an abstract usage model for entification and authentication decisions. The term entification is defined in Table 2.1. The encoded credential signals for making entification or authentication decisions are based on a person's:

- knowledge;
- control of artefacts or tokens;

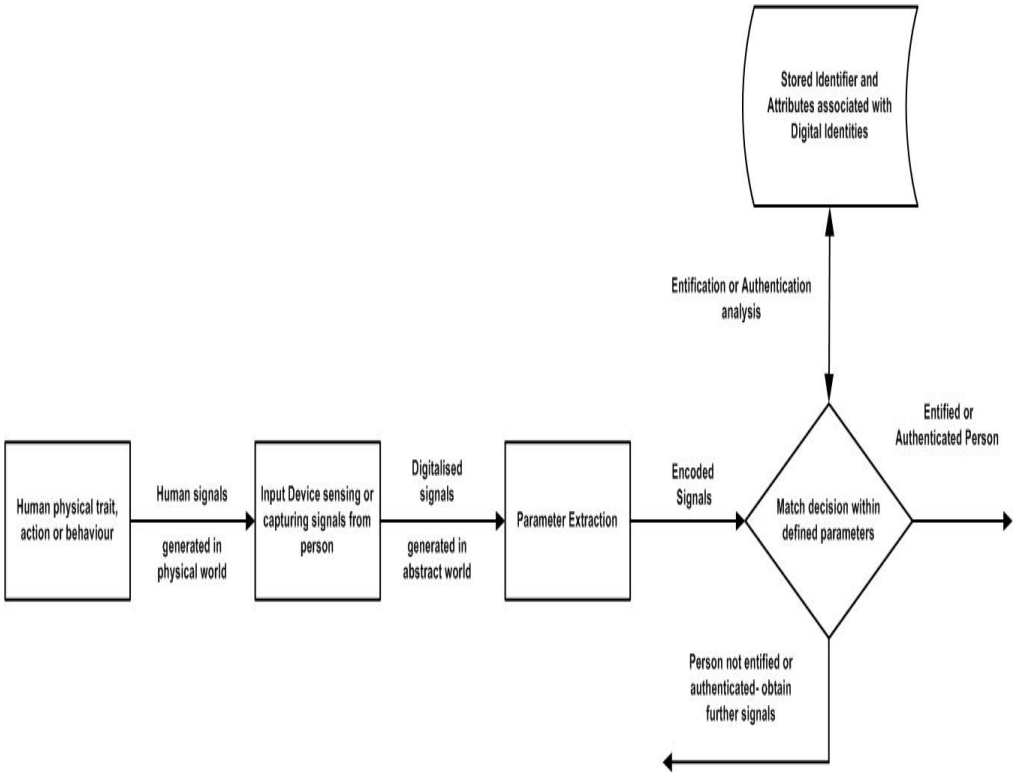

Figure 2.2: Abstract Usage Model of Entification or Authentication adapted from Fåk [95]

- physical features or behavioural characteristics; or
- a combination of these signals.

The type of signal data acquired from a person is either discrete, i.e. exact input data, or a combination of calibrated feature values, i.e. imprecise sensed stream of signals. Credential and other attribute data may be captured during transactional usage in a disconnected and discrete mode, for example a keyboard, possibly involving a token under the subject's control. Alternatively, continuous signals are captured by a sensor device operating in an amalgamated mode, for example, a fingerprint scanner or a camera continually scanning persons' facial images in a moving crowd.

The input signals may be generated naturally by the person or may require cognitive processes to recall knowledge data or may require an artefact or token assigned to the individual to automatically generate additional attributes or alternative encoded signals.

The automated personal identification of a person is accomplished by an authentication

system, using a previously assigned identifier with credential data. Alternatively, an identification system using a person's attribute data, without an identifier, entifies a person. Both systems use the data sensed or captured in order to compare the encoded signal data relating with the attribute data relating to that person in a repository. Some identification systems are designed to establish that a person and their attribute data are not stored in a repository [323].

Some of the literature describes authentication systems as consisting of identification and authentication sub-processes [287]. In these instances the *identification process* provides the person's identifier to the security system and evidence, or credential data, that are supplied as an assertion claim to the account associated with that unique identifier [287]. Identification systems, or in Clarke's terminology *entification*, use attribute data acquired, overtly or covertly, to entify a person.

We differentiate authentication system and identification system transaction decision sub-processes with reference to our established usage model:

- Identification and Authentication: In an authentication system a decision is computed using the identifier to locate the digital identity record of a person and matches the acquired data either discrete data, such as an identifier and its credential which may be a Personal Identification Number (PIN) or sensed data, for example, an encoded facial image relating to that identifier.
- Entification: In an identification system a decision is computed by using the attribute data acquired, from that person, and by searching through a store of attribute data relating to digital identities to locate candidates that match the attribute search data.

Based upon our abstract usage model, in Figure 2.2, the results of the computation decisions which are communicated to an operating system or application's information system is differentiated depending upon the transaction usage type and the type of credential or signal data.

Biometric algorithms match biometric encoded signal data on probabilistic outcomes based upon similarity measurements against stored template data [311] and not exact matches of two discrete values, such as an identifier and authentication data, e.g. a password. This differentiation of transaction usage types and credential data types produces the following usage transaction decision outcomes:

1. Authentication System: Correct identification and authentication of subject; or incorrect identifier or credential data submitted; or malfunctioning token; or malfunctioning authentication system; or incorrect decision or
2. Identification System: No candidate subject entified or one or more candidate subject entified inside the similarity threshold matching search or malfunctioning identification system or incorrect decision.

Decisions on user authentication and biometric verification operate on a one-to-one matching basis [271]. Conversely, entification decisions operate on a one-to-many basis, where the *sensed data* are used to search through a repository containing feature templates belonging to community members [186, 214, 162]. Where entification involves biometric modalities the search involves the interrogation of the modality features of the digital entities stored in the database. Raskin proposes [248] the use of *discrete data* entered by the user, such as a password without the identifier data, for the entification decision process; however, he does not explain how a digital entifier would preserve its uniqueness in an information system containing data acquired from many users.

The decisions relating to these usage models are predicated upon the assurance of other supporting processes, such as activities relating to the enrolment of person relating to a digital identity. These activities which support the transactional use of authentication system and identification systems are defined in sub-section 2.4.

We use *automated personal identification* as a generic term which encapsulates the theory behind Clarke's Entity-Relationship of Identity Model [58] and also entification and authentication usage transactions from our adaption of Fåk's Theoretical User Verification Model [95].

2.3 Definition of Core Terms for Automated Personal Identification

The definitions of the core terms for automated personal identification, shown in Table 2.1, are taken from a variety of sources. The conflicting use of terminology means that our definitions for such terms are drawn mainly from sources with established models of identity and conceptual descriptions of information system processes which automatically identify a person.

2.3 Definition of Core Terms for Automated Personal Identification

TERM	DEFINITION	SOURCE
Automated Personal Identification	Digital processes for automated decisions, by information systems, on the identification or authentication of a person	Raphael and Young [247]
Entification	A rule-based process of associating attribute data values (or combination of values) with a particular person by acquiring the entifier (or entifiers) relating to that person	adapted from Clarke [58]
Identification	A process of associating data with a particular person achieved by acquiring an identifier for that person	adapted from Clarke [58]
Authentication	A process that establishes a level of confidence in an assertion by cross-checking the assertion against one or more credentials	Clarke [58]
Authorisation	The granting of rights and, based on these rights, the granting of access	X1252 ITU-T [151]
Identifier	A representation of one or more attributes used to distinguish that digital identity from others in the same category or domain	Clarke [58]
Entity	In this thesis a human subject or a person	Clarke [58]
Entifier	Unique reference as a means of distinguishing a person in a repository of human entities and their attributes	Clarke [58]
Digital Identity	An abstract representation of a person with one or more attributes to allow that person to be sufficiently distinguishable within context	X1252 ITU-T [151]
Attribute	Information bound to an individual that specifies characteristics of that person.	X1252 ITU-T [151]
Credential	Data with physical or digital existence that serves as evidence to establish the claimed identity of a person.	adapted from ISO9735-1 ISO/TC 154
Subject	The person being identified or authenticated or possibly the *identifyee*	adapted from Warfel [307]
User	The person that directly interacts with the information system, who may or may not be the subject	ISO9241-110 TC173/SC1
Signal	A detectable synchronous event possibly accompanied by descriptive data and parameters	ISO14776-411 JTC1/SC25
Encoded Signals	Characteristic parts of signal that carry extracted data contents for a decision module	Fåk [95]
Input Device	User controlled device that captures signals and transmits information to a system	ISO9241-400 TC159/TC4

Table 2.1: Core Terms for Automated Personal Identification

In this thesis we adopt the term *biometric identification* for entification based biometric systems. We use the term *biometric verification* for identifier based biometric systems. We use the acronym *APIM* generically to denote a biometric identification system, a biometric verification system or an authentication system which uses knowledge, e.g. a password, and possibly other attributes to verify the genuine user.

We adopt our terminology because we consider it to be sufficiently generic and descriptive so as to avoid interpretations that may be construed as meaning a particular type of identification system or authentication system or perceived assurance quality. We append the word *mechanism* to the term *automated personal identification* rather than *system*, in order to differentiate the APIM's purpose from those functions that are performed by the associated information systems, such as an application program or a computer's operating system.

Although, we have defined the term authorisation in Table 2.1 these processes are beyond the scope of automated personal identification. We exclude the authorisation process because it takes place after the entification or the authentication process has completed successfully to a specified level of assurance [159]. We acknowledge, however, that the authorisation of privileges or access rights could relate to the probabilistic degree of assurance in the entification or authentication process [176].

We define an APIM as a system comprising policies, procedures, technology and other resources for maintaining information on digital identities, including attribute data, for the purposes of the entification or the authentication of persons. ISO/IEC 24760 Information Technology: Security Techniques, Part 1 A Framework for Identity Management - Terminology and Concepts [157], as a core international standard, does not include a definition of the term Identity Management System (IdMS). From our review of the literature an IdMS appears to relate to the identification and authentication of all *entities* [30, 151], e.g. an organisation, a process, a device, a person; whereas, we restrict the scope of an APIM to the identification or authentication of *persons*.

Additionally, ISO/IEC 24760 Information Technology: Security Techniques, Part 1 A Framework for Identity Management - Terminology and Concepts [157] extends its scope of identity-based decisions on entities to beyond the functions of identification and authentication. According to this standard identity-based decisions could also include choices relating to the attributes of the entity, e.g. a ruling based upon the age or location of an organisation. We restrict the scope of an APIM to decisions relating to the functions of identification and authentication.

Where we use the term and acronym *Identity Management System (IdMS)* in this thesis we are referring to the entification or authentication of entities or decisions relating to the attributes of entities and the management of those entities' attributes, e.g. identifiers. An entity in IdMS may relate to a person, a device, e.g. a utility smart meter, an organisation or a process in a computer system.

2.4 The Scope of Our Term APIM

Following our definition of core terms and a description of the underlying concepts upon which base our terminology in this thesis we now we describe the scope of our term APIM. We outline an APIM's functional purposes, the life-cycle management of digital identities, the types of APIM deployments and the governance frameworks for APIMs in order to clarify the boundaries of our research.

APIMs operate in both the physical world, e.g. automated border control passenger inspections, and virtual worlds, e.g. Internet banking. Human recognition of other persons is, by inference, out of scope. The inverse process of persons identifying an information system, e.g. a cloud service, is also out of scope. We acknowledge, however, that the automatic mutual authentication of devices, e.g. Transport Layer Security Protocol, may be deployed as part of a solution to remotely authenticate a user's computer system.

2.4.1 Functional Purposes

The scope of the term APIM covers fully automated usage transaction processes utilising devices that measure and decide upon the identification of a person [247].

APIMs are designed to positively entify or authenticate registered subjects to enable access to resources and to prevent misfeasors from gaining unauthorised access to an information system's data and resources. Similarly, an APIM may also, as a separate and dedicated function, enable the entification of a person who is already known to the biometric identification system or alternatively ensures that that person is not already known to that identification system [311].

The scope of the term APIM covers the transactional usage, as described in Section 2.2, for an information system or an operating system or device to request the APIM to automatically

identify a person. We exclude automatic processes relating to attribute based decisions, as described in ISO/IEC 24760 [157], where a relying party may wish to establish that a person is over 18 years old.

We describe the processes to manage digital identities next.

2.4.2 Life-cycle Management of Digital Identities

Bertino and Takahashi state [27] that the life-cycle management of digital identities consists of three main activities:

- registration and enrolment of digital identities ;
- operational maintenance; and
- decommissioning.

The life-cycle management activity of a digital identity or an entity of a person commences with the entitlement checking and registration of that person and it continues throughout transactional usage in the application context until the eventual decommissioning of that digital identity.

2.4.2.1 Registration and Enrolment of Digital Identities

The registration of a digital identity or entity is performed by four distinct tasks, which may not be relevant to all applications.

First, the *entitlement* task ensures that the person is entitled or authorised to have a digital identity to access an information system, e.g. a contractor is given approval to access a client's system resources.

Second, the *identity proofing* task attempts establish the veracity of the claimed identity, possibly using documentary evidence, e.g. individual's national identity card or birth certificate. In some circumstances this process may, where relevant, include background checks on the person's social footprint, e.g. criminal records and bank account information. The identity proofing task is normally performed by a Registration Authority (RA) that captures and verifies the required information from a person's claim to a real-world identity.

This task is in the scope because transactional usage is necessarily predicated, in many contexts, upon the assurance used to verify the claimed identity to be that of the genuine identity [79].

Third, the *registration* task is the creation of a digital identity for a person either by acquiring information from the applicant's registration form, if applicable, or alternatively a person uses an automatic self-registration process.

Lastly, the *enrolment* task involves the personalisation of credentials and attribute data together with the delivery of credential data to the registered subject, for example a PIN value via a PIN mailer through a postal service and, where relevant a token, for example, a bank payment credit card. The enrolment task, depending upon the APIM deployment type, may involve the capturing of biometric data from the registered subject, where the subject is required to visit a registration authority's premises. Alternatively, and possibly additionally, credential data are generated automatically by the APIM, or by the subject, e.g. a password.

2.4.2.2 APIM Operational Maintenance

Operational maintenance consists of tasks to retain the validity of the identifiers or entifiers, credentials and attributes data associated with the digital identities to enable the identification system or authentication system to function as designed.

The operational support functions include the revision of attribute data, for example biometric template updating, and the updating of specific attribute data, for example the renewal of a subject's digital certificates. These maintenance tasks are essential to ensure that a subject's digital identity and its associated data remain valid.

The re-activation of credential data may be manually performed by the APIM's operatives following user notification to a help desk or the process of re-activation may be automatic. For example, resetting forgotten passwords automatically may be achieved through functionality provided by the APIM itself or by an associated information system or by an out-of-bounds method.

2.4.2.3 Decommissioning

In this activity data relating to a person's digital identity are removed from the APIM's subject community repository.

This task may include the removal of data relating to identifiers or entifiers and associated attributes from the centralised repository. The removal of user access to an information system may include the return of a physical token for destruction or the cancellation of a token with a limited validity period, for example a five year expiry date on an ePassport. The decommissioning processes may also involve the revocation of a digital certificate in a case where there is a suspected compromise of a subject's credential. Organisations often overlook this decommissioning process leaving superfluous accounts available which may be attacked by miscreants seeking to gain unauthorised access to data and resources.

The types of activities to manage the digital identities or entities and their associated attribute data and credentials depend upon the type of APIM deployed and its configuration.

2.4.3 APIM Deployment Types

We categorise APIM deployment types by the transaction usage decision process, as described in Section 2.2, as follows:

1. Authentication: The process to determine the authorised subject associated with the identifier by matching exactly the credential authentication data presented by the person.
2. Biometric Identification: The process of entifying a person by capturing a signal or a fusion of signals and conducting a search for candidate entifiers with closely matching characteristics in a repository containing biometric features of an enrolled population.
3. Biometric Verification: The process to authenticate a subject's claim to a digital identity by direct comparison of the similarities of biometric features or signals sensed to those previously extracted during enrolment.

All knowledge based authentication systems which use credentials, e.g. PINs, passwords, graphical passwords and rebus passwords, are included in the term APIM. So too are other forms of credentials such as software and hardware tokens and the use of Short Message

Service (SMS) technologies to deliver one-time authentication codes, which involve an interaction with a person. Biometric technologies are included, whether based upon static physiological attributes, e.g. face, hand geometry, iris biometric modalities, or on dynamic behavioural attributes, e.g. signature, keystroke dynamics and gait biometric modalities. Chemical identification technologies, e.g. latent fingerprints, which involve forensic and biological identification technologies, are excluded because these technologies currently rely on human intervention.

The term APIM includes physical artefacts or logical tokens as credentials that are under the subject's control, which may contain identifiers, authentication data, biographical data, biometric data and digital certificates. Everett classifies [91] artefacts and tokens as either passive, without any test of the holder, or active, with an element of intelligence to test the holder, using knowledge or biometric data. For example, an Integrated Circuit Card (ICC) containing certificates on a bank payment card artefact is inserted into an Europay Mastercard and Visa (EMV) compliant card reader challenge device, and a PIN is required to be entered to authenticate the genuine holder.

Some artefacts and tokens may require the subject to possess a specification compliant reader device or alternatively another device, e.g. a mobile phone to receive an SMS one-time authentication code. Artefacts and tokens have varying processing and protection capabilities to facilitate local or remote authentication of a person. Additionally, tokens together with associated reader devices, e.g. an Integrated Circuit Card reader, are included in the scope. We exclude the pre-personalisation processes of token manufacture because these tokens are not, at that stage, assigned to a digital identity. Persons are normally assigned an identifier during personalisation processes, which may be synchronised with subject enrolment processes.

The spectrum of current APIMs and the emergence of Privacy Enhancing Technologies (PETS), as surveyed by The Meta Group [201] and Fritsch [105], provide an expanding array of potential technologies for the deployment of APIMs. Similarly, infrastructures to preserve privacy and improve digital identity protection in cyberspace, as promoted by Rannenberg et al. [42], play an essential role to support PETS.

There are some applications where the subject must be identified and authenticated to comply with legislation, for example the British Banking Association's know-your-customer rules for UK banks and building societies as part of their obligations under the UK Money Laundering Regulations (2007) [284]. Conversely, there are some application contexts, again to comply

with legislation, where the subject's anonymity must be maintained, for example eVoting.

The spectrum of solution configurations, as shown in Figure 2.3 should not be construed as an exhaustive list of APIM deployment types. It is proffered to explain the scope and subtlety of the various identification technologies and configurations. Importantly, it serves to justify the use of automated personal identification as a more descriptive and generic term for this thesis. It also serves to justify our choice of definitions for the core terms for APIMs, as shown in Table 2.1 and other terms employed relating to APIM deployments, as shown in Table 2.2.

Additional terms associated with APIMs which are used in this thesis are defined in Table 2.2. This table is not intended to be an exhaustive list of terms relating to identity concepts or emerging identification technologies or identity infrastructures.

2.4.4 APIM Governance Frameworks

We adopt the model established in ISO 21188: Public Key Infrastructure for Financial Services–Practices and Policy Framework [153] to distinguish the governance frameworks for APIMs which involve organisations in different roles, either in issuing digital identities (issuing authority) or relying upon digital identities (relying party) or both. We classify these organisations' roles into the following APIM governance framework types:

- Enterprise: The issuing authority and relying party are the same organisational entity, which manages the APIM that issues the identifiers and tokens, where required, to employees, customers and agents;
- Federated: There are multiple relying party organisations that rely on an issuing authority, e.g. a national identity card scheme with an identifier in a token, e.g. public key certificate, or alternatively one relying party may rely on digital identities issued by many issuing authorities, e.g. claims based identity schemes;
- Heterogeneous: There are multiple issuer organisations and multiple relying party organisations involved with the framework or formalised scheme, e.g. in the case of EMV Payment Card issuing authorities and worldwide Automated Teller Machines (ATMs) provided by relying party banks.

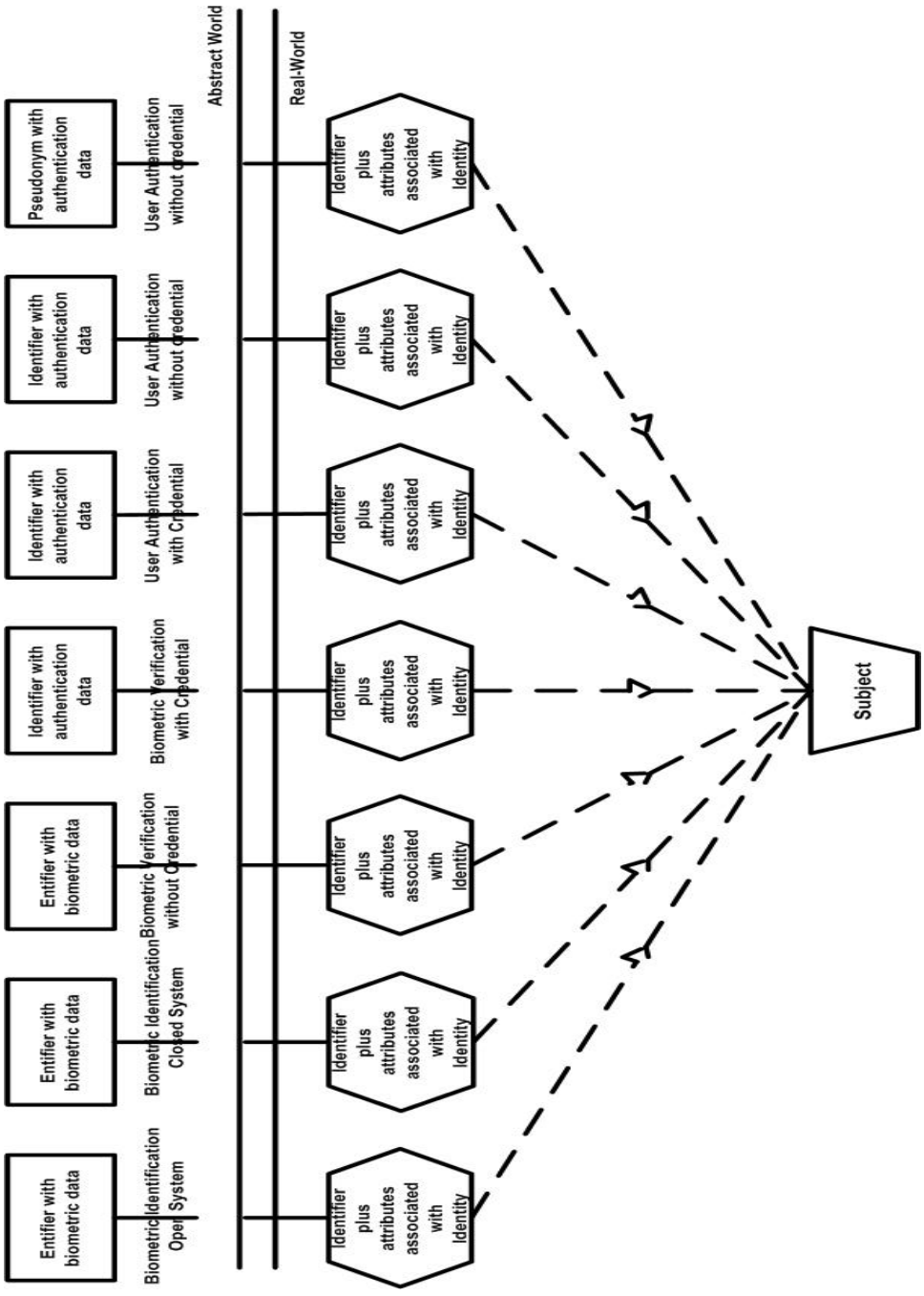

Figure 2.3: Spectrum of APIM Types and Configurations

TERMS	DEFINITION	SOURCE
Identity Proofing Process	Verification process to establish or strengthen confidence in a person's claimed identity from evidence provided	adapted from EOI Standard NZ Government [79]
Registration	A process of making a person's identity known to an APIM, associating a unique identifier with that identity, and collecting and recording the person's relevant attribute data	adapted from ISO24713-2 JTC1/SC37
Application	Set of interrelated components and processes designed to perform a specific function	PAS92 [38] British Standards Institute
Application System	Hardware / software system implemented to satisfy a broad range of requirements in performing a specific task	ISO /IEC 24713-1 SC37
Two Factor Authentication	The identification process is performed using two separate credential data	FIPS PUB 48 [177]
Multiple Factor Authentication	The identification process is performed using multiple credential data	FIPS PUB 48 [177]
Multi-biometric Systems	A system that consolidates evidence presented by multiple biometric sources with attribute data	Ross et al. [214]
Pseudonym	A pseudonym is an identifier of a subject other than one of the individual's real name(s)	Pfitzmann and Hansen [236]
Anonymity	The subject is not identifiable within a set of subjects, the anonymity set	Pfitzmann Hansen [236]
Undetectability	An Item of Interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not	Pfitzmann and Hansen [236]
Unobservability	The Undetectability of the Item of Interest (IOI) against all subjects uninvolved in it and the Anonymity of the Subject(s) involved in the IOI, even against the other Subject(s) involved in that IOI	Pfitzmann and Hansen [236]
Unlinkability	For two or more Items of Interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot distinguish whether these IOIs are related or not	Pfitzmann and Hansen [236]

Table 2.2: Additional Terms relating to Automated Personal Identification

In all of these types the subject is the person to be automatically identified by the application's information system owned by the relying party. Organisations and individuals may place implicit trust in some issuing authorities, e.g. a passport issuing authority, or trust may be expressed formally in a contractual cooperation agreement or through trust scheme rules, e.g. EMV Payment Card Rules [1] or endorsement by an accreditation scheme, e.g. tScheme. [2]

2.5 Summary of Chapter

We have defined the terminology and justified our strategy to formulate a set of definitions relating to automated personal identification. We have also provided an explanation on the scope of the APIM term so that the research issues relating to methodologies to evaluate and select such mechanisms may now be elucidated.

In the next chapter we establish the theoretical foundation of our multi-disciplinary research into methodologies to determine the optimal APIM for a given application context.

[1] https://www.emvco.com/specifications.aspx
[2] www.tscheme.org

CHAPTER 3

Research Issues

Contents

This chapter aims to build the theoretical foundation upon which our research inquiry into systematic methodologies to select APIMs is based. This aim is achieved by creating a new classification model founded on our literature review of the classification of Information Security (InfoSec) methodologies for Information System (IS) development; applying our tools classification model to classify the methodologies in the body of knowledge on security, usability and privacy; reviewing and classifying the specific literature on the selection APIMs, using our InfoSec tools classification model in order to identify gaps in the body of knowledge; summarising the outstanding research issues identified; describing a new paradigm to evaluate an application context; and further elucidation of our four research questions addressed in this thesis.

3.1 Methodology Classification Model

This section reviews the extant literature on the classification of InfoSec methodologies by Baskerville [24], Siponen [266] and Uzunov et al. [302]. We then define a new model which we refer to as our tools classification model. We use this model as our conceptual framework to review the methodological tools which focus on the deployment of secure and usable information systems which offer privacy protection. We also provide our justification for creating our tools classification model.

3.1.1 Five Generations of InfoSec Methodologies

According to Hirschheim et al. [132] as the types of applications, information systems and new technologies continue to grow, so do the number of Information System (IS) development methodologies. They quote Jayaratna's (1994) estimation of over 1,000 development methodologies in existence. The profile of IS development approaches has undergone fundamental changes along with technologies, where each approach, as a single-product based (or configuration) development, a component-based development, or a proprietary development, presents different challenges to designers addressing security concerns [293]. Hirschheim et al. conclude [132] that the research priority is not to introduce new IS development methodologies but to understand the existing stock and the collective knowledge in them.

We justify our initial choice of commencing with Baskerville's conceptual framework to

GENERATION OF METHODOLOGY	SECURITY DEVELOPMENT TOOL CHARACTERISTICS	PRIMARY FEATURES
First InfoSec Generation Check lists	Security checklists and security principles in guidelines, risk analysis	Mapping of limited solutions on to the problem
Second InfoSec Generation Mechanistic Engineering	Control point and exposure analysis matrices, computer questionnaires	A partitioned complex solution that matches functional requirements
Third InfoSec Generation Modelling	Abstract representation and transformation models including logical controls design and data flow diagrams	Highly abstracted design expressing problem and solution space

Table 3.1: Baskerville's Classification of Three Generations of InfoSec Methodologies [24]

review the classification of InfoSec methodologies because his seminal work, published in 1993, has been highly cited and it often acts as the foundation upon which many contributions base their analyses. Siponen recognises [266] that there are many candidate conceptual frameworks available to analyse InfoSec methodologies [citing Dhillion and Backhouse (2001), Hirschheim el al. (1995, 1996) and Iivari et al. (2001)]. Siponen opted in 2005 [266] to extend Baskerville's three generation model as the basis of his efforts to create additional classifications (fourth and fifth generation) of InfoSec methodologies.

Similarly, Uzunov et al. extend [302] Baskerville's three generation model in their construction of a taxonomy for their survey and analysis of model-based InfoSec methodologies, from a distributed systems perspective, in 2012. Uzunov et al. conclude [302] the efforts of recent classification contributions [citing Villarroel et al. (2005), Jayaram and Mathur (2005), Khan and Zulkernine (2009), Jürjens (2009), Fernández-Medina et al. (2009), Talhi et al. (2009) and Kasal et al. (2011)] are deficient. They claim that these classifications, even taken together, do not provide a suitable framework which would allow a comprehensive and fair assessment of the range of the InfoSec methodologies available. We examine these three extant contributions in greater detail in order to identify commonalities, variations and omissions in their classification models. We then develop our own tools classification model based on the results of our examination.

Baskerville's seminal work classifies [24] InfoSec methodologies into three generations which are summarised in Table 3.1. Baskerville elects [24] to use the generation metaphor because he claims that it allows a comparison of otherwise dissimilar approaches by focusing on the intellectual evolution of InfoSec methodologies in response to a changing context, akin to *generations of programming languages*.

Siponen extends [266] Baskerville's classification, using the same generation metaphor, by

GENERATION OF METHODOLOGY	SECURITY DEVELOPMENT TOOL CHARACTERISTICS	TYPICAL TOOLS CITED BY SIPONEN
First InfoSec Generation Checklists	Security checklists and security principles in guidelines, risk analysis	Wood et al. [322] Spruit and Samwel [275]
Second InfoSec Generation Mechanistic Engineering	Control point and exposure analysis matrices, computer questionnaires	BS7799 (replaced by ISO/IEC 27000 series) Common Criteria [64]
Third InfoSec Generation Modelling	Abstract representation and transformation models including logical controls design and data flow diagrams	Hutchinson and Warren [310] Straub and Welke [278]
Fourth Generation Socio-technical Design	Socio-technical design approaches with user participation	Armstrong [14] Karyda et al. [172]
Fifth Generation Social and Adaptable Design	User participation, adaptable to different system development methods, empirically grounded providing evidence on its ease of use and relevance in practice	Author claims no methodologies in existence

Table 3.2: Siponen's Classification of Five Generations of InfoSec Methodologies [266]

introducing a fourth generation of InfoSec methodologies, in recognition of alternative socio-technical design approaches. Table 3.2 shows a summary of the characteristics of Siponen's fourth and fifth generations of InfoSec methodologies together with examples of typical tools available in 2005. Siponen argues [266] that fifth generation of InfoSec methodologies should encompass social, and adaptable methods that are rigourously developed along with practice.

Uzunov et al. argue [302] that activities involved in any InfoSec methodology should include security requirements determination, security modelling, security implementation, and configuration and monitoring. These activities should align to a generic software development life-cycle's stages of requirements engineering, design, implementation, and deployment respectively, as depicted in Figure 3.1.

They also propose that an InfoSec methodology should be designated as either a *comprehensive* methodology (where an InfoSec methodology includes *all* the aforementioned security activities to support an IS development programme) or as a *partial* methodology. Partial methodologies contain security activities to support *parts* of an IS development programme.

Uzunov et al. introduce [302] several classification dimensions in their taxonomy for InfoSec methodologies. These dimensions may be categorised principally as to whether the methodologies' paradigm is code-based or model-based. Code-based methodologies enforce security related activities during a software process without explicit regard for an information system's design or architecture. , Uzunov et al. claim [302] that code-based methodologies

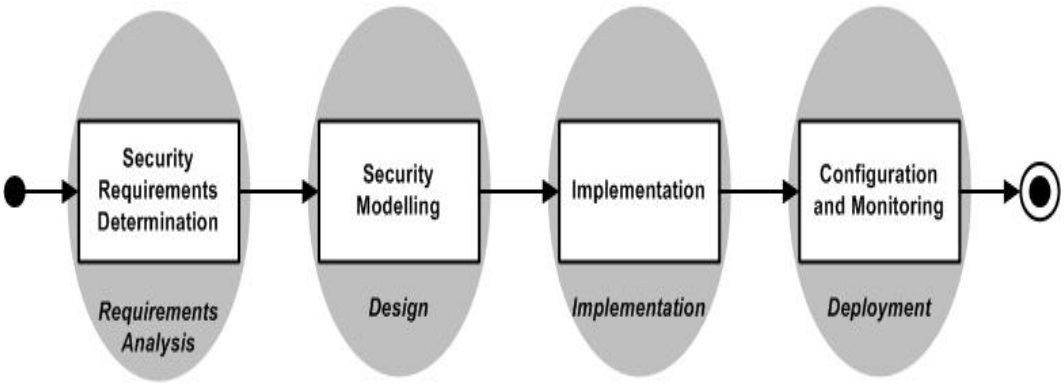

Figure 3.1: Uzunov et al.'s Alignment of an InfoSec Methodology within the Stages of a Generic Software Development Life-cycle [302]

to be analogous to Baskerville's second generation InfoSec classification. Uzunov et al. define [302] model-based methodologies as systematic approaches combining security and modern software engineering that are based on some form of abstract modelling. These models are taken into account during the information system's design activities. Uzunov et al. consider [302] that their model-based classification aligns with Baskerville's third generation of InfoSec methodologies.

While Baskerville's three generation evaluation framework forms the basis for these other two extant contributions there are divergences between Siponen's classification and Uzunov et al.'s classification. Siponen's classification of fourth and fifth generation InfoSec methodologies aligns with Baskerville's intention for the classifications to reflect the intellectual enhancement of InfoSec methodologies in response to the complexities of evolving application contexts.

In contrast, Uzunov et al.'s classification recognises that some InfoSec methodologies contain security activities to support all the phases in a development programme and other methodologies have a specific purpose in certain phases of an IS development programme. For example, risk assessment tools contain security activities which are aimed at establishing the security requirements in the earlier phases of an IS development programme.

While these three extant contributions explain their respective philosophies which underpin their InfoSec classification models neither consider the InfoSec methodology's processes or the impact of these processes on the information system development programme's deliverables in their classifications. Avison and Fitzgerald compare [18] system develop-

ment methodologies primarily according to the methodology's paradigm, its objectives, its processes and the types of products to be delivered.

We believe that InfoSec methodologies should be classified according to a methodology's objectives, as a problem-solving tool, to address the problem encountered by IS programmes to deploy secure and usable information systems. As a problem-solving tool, a methodology's paradigm and its documented processes which describe its security activities, i.e. detailed methods, needs to be incorporated into a classification model.

Our aim is utilise a classification model so as to gain an understanding of the existing stock of InfoSec methodologies and, pertinent to our research problem, to ascertain the methodological tools that are available which are designed to evaluate and select APIMs. The use of an appropriate classification model which reflects our research problem then enables a review the existing methodological tools in the literature.

Next we justify our divergence from the extant InfoSec classification models established by Baskerville [24], Siponen [266] and Uzunov et al. [302] before we describe our alternative classification model.

3.1.2 Justification for an Alternative Classification Model

. Notwithstanding that the scope of these extant InfoSec classifications focus on producing secure information systems outcomes and our scope also includes usability and privacy protection of information systems, we believe that methodologies may be classified according to their functions, processes and intended outcomes. We commence by defining the term *methodology* and then describe a methodology's constituent elements in order justify our deviance from the three aforementioned extant classification models.

From our review of the extant contributions discussed in the previous sections we note that all authors use the terms *method*, *approach* and *methodology* interchangeably, without providing definitions of these core terms. Uzunov et al. define [302] a methodology as a *systematic way of doing things in a particular discipline* is not sufficient for our research purposes. We draw on the extant literature on IS development methodologies [165, 18] in order to provide a definition of a methodology and its constituent components.

According to the Oxford Dictionary a methodology is the system of methods used in a

particular area of study. [1] A methodology is also defined as the branch of philosophy concerned with the science of a method. Concentrating on the first definition, in turn, the Oxford Dictionary defines a method[2] as a particular procedure for accomplishing or approaching something, especially in a systematic or established way.

Checkland contends [49] that while a methodology lacks the precision of a technique (which is undefined) it will be a firmer guide to action than a philosophy. Avison and Fitzgerald argue [18] that a technique tells you *how* and a philosophy tells you *what* and a methodology will contain both elements when applied in the IS development discipline. Jayaratna also disagrees [165] with Checkland's definition in that philosophies assist in making sense of *reality* and are an integral part of a methodology. Jayaratna defines [165] a methodology as:

> *" an explicit way of structuring one's thinking and actions. Methodologies contain models and reflect perspectives of 'reality' based upon a set of paradigms. A methodology should tell you 'what' steps to take and 'how' to perform those steps but most importantly the reasons 'why' those steps should be taken, in that particular order."*

Avison and Fitzgerald's comparison framework aligns [18] with Jayaratna's definition in respect of the constitute elements of a methodology. Avison and Fitzgerald state [18] that a methodology consists of:

- a philosophy, which describes its paradigm, objectives, intended application domain together with the types of target problems;
- models, with various levels of abstraction and orientation;
- techniques and system tools (if any) employed;
- intended scope to address the stages in an IS development programme; and
- outputs in terms of deliverables.

Jayaratna contends [165] that a methodology should be evaluated not only according to its philosophical paradigm, but also the by the structuring of the methodology's stages and steps.

[1] http://www.oxforddictionaries.com/definition/english/methodology
[2] http://www.oxforddictionaries.com/definition/english/method

Avison and Fitzgerald also argue [18] that methodologies should be compared according to their repeatability. They argue that level of granularity in the methodology's documented stages and subordinate steps should be sufficiently well-defined, in a method, so that the methodology's processes are repeatable and its outcomes are reproducible by alternative evaluators.

Some methodologies may only contain high-level process descriptions leaving practitioners to use their skills and competences to interpret the methodology's underlying philosophy for their practices; whereas, other methodologies may contain well-defined prescriptive processes, in a logical sequence. We believe that InfoSec methodologies should be classified primarily according to their underlying paradigms and their steps, described in processes, as problem-solving tools to achieve a programme's desired outcomes. For example, a risk assessment methodology, as a tool, should identify risks in an application context.

We justify our creation of a new model to classify InfoSec methodologies because Baskerville [24], Siponen [266] classification model and review are based upon the generation metaphor, reflecting the intellectual evolution of InfoSec methodologies. In their classification model Uzunov et al. differentiate [302] between methodologies that enforce security-related activities and methodologies which act as modelling tools during IS development programme. The scope of our classification model needs to cover not only security-related activities but also processes in a methodology's steps which assist in the design of usable information systems which offer privacy protection.

We create an alternative classification model based on Jayaratna's definition [165] of a methodology to classify methodological tools according to their function. Our model allows the review of the relevant methodologies based primarily upon the methodology's documented steps, as a problem-solving tool, with objectives of producing secure, usable and privacy protecting information systems as outputs. We use the same model to then review the methodologies for evaluating and selecting APIMs.

3.1.3 Our Tools Classification Model

Our classification model is based upon the type of methodological instrument, the function of the instrument and the desired outcomes from utilising the methodological instrument. In order to further clarify our classification model we provide examples of some InfoSec tools for each of our five classification categories shown in Table 3.3.

METHODOLOGY CATEGORY	METHODOLOGY TOOL EXAMPLES	LOCATED SOURCES
1. Factor Guidance	Security Factor Checklists Codes of Practice Security and Usability Design Principles	Wood [322] ISO27002 Johnston et al. [167]
2. Analytical Frameworks	Evaluation Frameworks Risks Analysis Privacy Impact Assessment	Common Criteria [64] CRAMM [325] NZ PIA Handbook [222]
3. Conceptual Modelling	Capability Maturity Modelling Risks Assessment Expert System Security Architectures	ISO/IEC 21827 [155] Kailay and Jarratt [169] Sherwood et al. [263]
4. Heuristic Approaches	Security Requirements Engineering Approach Socio-technology Privacy Approach	Faily and Fléchais [94] Cavoukian [45]
5. Systematic Methodologies	Iterative InfoSec Methodology Goal-driven Security Requirements Engineering	Fléchais [101] Mouratidis and Jürjens [209]

Table 3.3: Methodology Categories, Tool Examples and their Sources

We use the *tools* metaphor in order to classify InfoSec methodologies because each tool has a functional purpose. The functional purpose should be reflected in its underlying philosophy, as recognised by Uzunov et al. [302], the granularity of detail in its processes [18] and the structuring of its processes [165]. We adopt the tools metaphor because we believe that a methodology, as a problem-solving instrument, may used by discipline experts as problem-solvers to achieve desired outcomes.

The different types of tools may be used to support the development of information systems during all or part of the four main stages of an IS development programme, as proposed by Uzunov et al. [302]. The tools may also be used to perform a review, e.g. a risk assessment, of a deployed information system and/or an appraisal of a deployed APIM.

We now define the five tool types in our tools classification model based upon the function of each type of instrument:

1. Factor Guidance – information on factors to be evaluated in the application context, including the IS, operational procedures and human elements in order to gather relevant data and to inform analytical processes, e.g. check lists and guidance material;

2. Analytical Frameworks – structure to evaluate information acquired from comparison of alternative perspectives;

3. Conceptual Modelling – refers to mapping concepts and their interrelationships at various levels of abstraction to assist semantic understandings and to aid communication;

4. Heuristic Approaches – unstructured processes, based upon a socio-technical research paradigm, and participative design; and

5. Systematic Methodologies – integration of various methodological tools, e.g. a Decision Support System (DSS), into an evaluation framework together with well-defined activities, i.e. documented step-by-step processes in a method.

We proceed with our review of the relevant methodologies now that we have created an appropriate classification model and defined the types of methodological tools.

3.2 Balancing Security, Usability and Privacy

Rannenberg contends [246] that notion of *balanced security* strives to determine acceptable security controls between interacting parties, with their different and possibly conflicting objectives, risks and issues. We adopt Rannenberg's term *balanced* to represent information systems which are designed to be secure and usable and also offer privacy protection.

Information security impinges on a wide range of research disciplines, which are founded upon the interactions between technology, processes and people [11, 120]. The body of knowledge on security, usability and privacy issues draws on research into software engineering, cryptography, biometrics, regulation, and organisational management, which have roots in many scientific disciplines, e.g. computer science, mathematics, business, engineering, law and social sciences.

3.2.1 InfoSec Advisory Tools

This sub-section reviews check list and guidance advisory tools that provide descriptions on factors which *should*, according to their contributors, be considered by organisations' designers when introducing or assessing the security, usability and privacy of a *balanced IS*.

3.2.1.1 Check List Tools

A check list may act as an *aide-mémoire* so that all conceivable controls and configurations can be examined for a balanced IS. A check list tool is primarily aimed at determining a system's functionality, however, these tools do not appear to support all the security activities

for an IS development programme. Some check list tools, however, cover aspects relating to access control, e.g. recommendations on the length and characters in a password. There are elements within these check lists which have the potential, when aggregated with elements from other check lists, to form the basis of a list of factors which require examination in order to select the optimal APIM for a given application context.

Wood's comprehensive list [322] is one of the earliest check list tools which is designed to assist evaluators to assess the appropriateness of a list of security controls for an application context. Bumgarner and Borg's check list offers [40] a comprehensive range of controls to reduce the exploitation of vulnerabilities in an organisation's information security system from cyber-attacks.

Similar types of check lists exist for evaluators considering the introduction of biometrics systems designed to address human identification applications [38, 295]. Pfitzmann and Hansen's repository [236] of privacy terminology with current definitions of the properties of anonymity, unlinkability, undetectability and unobservability, acts as a check list for evaluators and demonstrates the complexities in interpreting privacy terminology.

A check list may be a valuable tool in terms of its comprehensiveness, in that all the possible controls are examined in the security requirements determination phase of an IS programme. Check lists, however, are not incorporated into conceptual frameworks to aid the examination processes. Additionally, check lists are based upon the assumption that all possible controls and configurations, as solutions, are known. We believe that a comprehensive check list, as part of an evaluation framework, should act as the starting point for ascertaining the relevant security controls which an APIM is required to fulfil. In Section 3.3.1 we review the literature which contain factors relating to establishing the requirements for an APIM.

3.2.1.2 Guidance Tools for Evaluating Human Factors

Guidelines may assist in the identification of the human factors and also other factors which need to be examined for the introduction of an APIM for the application context. Additionally, the discussions contained in guidelines help to reveal the interdependencies between the factors and also the complexities surrounding the specification of requirements for an APIM.

Our review of the methodologies is not concerned simply with the usability of security utilities, for example the usability of a cryptographic product [319], but with the security,

usability and privacy of an application and its information system [270]. Nevertheless, the results of Whitten and Tygar's seminal contribution [319] reminds us that individuals either accidentally cause dangerous security errors or are unable to perform a security task or are unable to select the appropriate security object for the task.

Alagar argues [6] that information security is by no means entirely a technical issue and the human aspect of security should play a central role in the design of an information system. The many human factors relating to security are described by Adams and Sasse [2], Yee [328], Adams and Blandford [1], Zurko and Simon [334] and Sasse [261].

Both Grinter and Smetters [270] and Zurko [333] conclude that the greatest challenge in designing secure and usable information systems is one of methodology and not simply to gain an understanding of the pertinent factors. Zurko and Simon conclude [334] that while the identification of these interrelated factors should form the basis of improvement in usable and security of information systems, researchers and practitioners are needed with the competencies to synthesize knowledge from many disciplines in order to progress the design of usable and secure information systems.

Balfanz et al. argue [22] that interface designs should address usability issues by improving the transparency of some security techniques. Ye et al. recommend [326] that security and users' perception of trusted applications need to be built into the application from the beginning rather than added as an after-thought. Trust in an application and, perhaps, the organisation providing that application, is enhanced if the users' experience is satisfactory and the interaction includes specific feedback properties [167].

Factors relating to the protection of users of information systems also require consideration [245]. In many states the protection of individual's private information is covered by regulation; however, citizen privacy is interpreted differently in various jurisdictions [196]. According to Palen and Dourish [225], privacy management is not only about setting rules and enforcing them but also the continual management of boundaries between different spheres of action and degrees of disclosure within those spheres.

Gerber and von Solms argue [118] that there are many complex risks factors that organisations and users face when considering the introduction and usage of information systems, which also attract political, organisational and social issues. According to Anderson [11] many information systems fail not because of technical design mistakes but incorrect incentives for stakeholders.

Over the last three decades, the ISO/IEC Technical Committee JTC1/SC27 IT Security Techniques has issued over 80 security standards, excluding corrigenda, which include standards covering the deployment of security techniques. Working Group 5 of SC27 is tasked to produce standards guidance material on the security and privacy of information systems. Many of these standards incorporate normative instructions, for security compliance purposes, and educational sections, which are advisory in nature.

Guidelines often offer valuable theoretical and practical insights on the factors associated with ascertaining the requirements for an APIM. As advisory tools, guidelines often do not include frameworks to enable the analysis of various pertinent factors from differing perspectives in order to identify the optimal APIM.

3.2.2 Analytical Framework Tools

Next we review analytical instruments which assist in the determination of security controls and security assurance together with those instruments that address human and identity privacy issues as analytical framework tools. The advantages of using such tools is that they often provide benefits expressed as a quantitative monetary value which can be offset against the estimated costs for controls to protect an information system which includes an APIM.

3.2.2.1 Risk Assessment and Security Audit Tools

The risk assessment tool, formulated by Weingart et al. [313] over three decades ago, was designed to evaluate the physical risks to information systems in organisations and seeks to balance the protection of assets and risks using three parameters:

1. The value of the information system and its data (Value);
2. The security of the environment in which the system resides (Environment); and
3. The strength of the protection methods employed (Physical Security Rating).

There are many risks assessment tools available, for example CRAMM[3], which is supported by a risks assessment software application. The Information Risk Analysis Methodology

[3]http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

from the ISF[4] comprises a risks analysis workbench, business impact assessment, threat and vulnerability tools and a control selection tool.

According to Lichtenstein [187] there are so many diverse and imperfect risks assessment methods available, that, in order to select the most suitable tool, organisations should establish usability, credibility, complexity, completeness, adaptability, validity and cost evaluation criteria. Alternatively, Djordjevic et al. argue [81] that risks assessment tools should be designed specifically for certain types of information systems, e.g. the CORAS Risks Framework tool for large-scale distributed and critical information systems. Bernard suggests [26] another strategy of using various risks assessments tools by overlaying several risks assessment outputs at different junctures during the life time of the IS.

Similarly, security governance and audit tools are in abundance. For example, Control Objectives for Information and related Technology (COBIT) is a framework developed by Information Systems Audit and Control Association, now ISACA [5], which has its roots in enterprise governance. COBIT provides [152] a framework that assists enterprises in achieving their objectives for the governance and management of enterprise information systems by maintaining a balance between the realisation of organisational benefits and minimising risk levels.

Nevertheless, despite the wide availability of these tools, Probst and Hunker's observations [243] help to explain why organisations often use economic rationale to invoke only basic controls to counter insider attackers and do not address the more serious external threats. Moore [12] and Dadayan [76] argue that organisations should perform Return On Security Investment (ROSI) evaluations that can demonstrate both tangible and intangible benefits of security controls.

ROSI evaluations do not, however, consider similar values for the intended user community in that they do not address the latter's risks [118], their usability issues[67, 2], their accessibility issues [250] or assess the impact on the user communities' attitudes [23, 280]. User community concerns may be a consequence of or the fear from social engineering attacks, as exemplified by the activities of one particular miscreant [206].

The main advantage of using analytical instruments is that the output results, from the structured analyses, may be traced back to the core source data and the assumptions used

[4]https://www.securityforum.org/
[5]http://www.isaca.org

by the evaluators. We believe, however, that the reliance of analytical instruments on many assumptions, particularly the nature and severity of threats in risks assessment tools, leaves opportunity for subjective manipulation. Nevertheless, assessment tools, e.g. risks assessments and privacy impact assessments, assist in the security requirements definition stage of an IS programme.

3.2.2.2 Security Evaluation Tools

Security evaluation tools are often used by organisations to demonstrate compliance to a security specification.

The common criteria framework [64] retains an organisational and technological focus in evaluating a product's capability Target Of Evaluation (TOE) of meeting a security Protection Profile (PP) for a predetermined application context type.

Anderson contends [11] that the fundamental problem that arises with this type of evaluation, which determines whether an IS meets, or fails to meet, a prescribed assurance target is when the party who implements the protection differs from the party who relies upon it. Given this trust issue, Gollmann concedes [120] that the value of the evaluation effort is questionable, particularly when such evaluations, it is claimed, adds between 10 to 40 percent to the total cost of the IS development.

The Federal Information Technology Security Assessment Framework provides [220] control objectives at five levels, to indicate the degrees of information security compliance across organisations. The IT Infrastructure Library (ITIL) resource, through its ITIL Version 3 publications, incorporate risks management and security controls into IT services life-cycle frameworks [309]. This framework, however, is again focused on organisations and does not encompass the usability and privacy issues of these information systems as they are used in society.

We believe that the focus of these evaluations to obtain security compliance does very little to assist IS programmes to ascertain the security requirements for an APIM to protect access to information systems because the subject communities' risks, privacy issues are not considered sufficiently.

3.2.2.3 Socio-technical Security Evaluation Tools

There is a scarcity of analytical frameworks for evaluating the combined aspects of security, usability and privacy. Although, there are principles for assessing usability of security in IS [327] these are not placed in an analytical framework.

Privacy impact assessment tools ensure that an organisation's and their information systems comply with a state's privacy laws [222, 298]. Warren summarises [308] the key benefits of such tools as:

- the avoidance of loss of trust and reputation;
- the identification and management of risks;
- cost avoidance; and
- meeting and exceeding legal requirements.

Sallhammar et al. propose [260] a real-time evaluation and prediction framework that monitors information system behaviour and unauthorised use and abuse by misfeasors. We believe that this type of tool is an encouraging advancement towards understanding some of the behavioural aspects surrounding user actions (and those of misfeasors) and measuring those impacts on a balanced IS. Achieving such understanding, we believe will aid the requirements definition stage of an IS development programme to ascertain the requirements for an APIM.

These tools tend to base many of their calculations on many assumptions because the primary input data are difficult to gather and data that are acquired also arduous to verify in terms of accuracy. Additionally, we note that the tools have grown in complexity as the basic data matrix is multidimensional representing different perspectives, which has led to many of these tools being supported by software applications. We review the tools in the literature which concentrate on the usability and security of APIMs in Section 3.3.2.

We believe that while these tools have the potential to highlight the main requirements for an APIM, models are required to gain a deeper understanding, through various levels of abstraction, of the interrelationships of the various factors which assist in the design of an APIM or the specifications for an APIM.

3.2.3 Modelling Tools

We review the tools designed to evaluate the security, usability and privacy factors and their interrelationships through architectures, models and expert systems.

3.2.3.1 Architectures

Enterprise IT architectures act as a planning tool to position the deployment issues and act as a problem solving-tool to simplify and isolate factors without losing the complexity of the enterprise [332].

The Zackman architecture [331], which contains a framework to produce a set of abstract models, may be used to represent various perspectives of an information system in order to identify security requirements [129]. TOGAF, produced by the Open Group [6], and other similar enterprise IT architecture tools incorporate security design principles; however, these tools do not provide a method to develop a security architecture [163].

Sherwood et al. [263] developed a tool in order to represent and evaluate enterprise security architectures. Security architectures provide enterprises with a strategic framework for integrating people, process, and technology related controls that address enterprises current and planned business objectives [13]. Security architectures in enterprises may comprise of internal policies and standards, technological controls and educational programmes for the user community, which should be derived from stakeholders' goals [235].

These tools tend to represent the automated personal identification problem from the enterprise perspective and we believe that they do not give sufficient regard to the users' view of the APIM. For example, a user may access many enterprise systems, each with its own APIM, however, these tools fail to represent this issue frequently encountered by users.

3.2.3.2 Models

Tools for modelling information systems and InfoSec representations generally describe three levels of abstraction [268]:

- Organisational Level: defines the organisation role and context of the IS;

[6] http://www.opengroup.org/togaf/

- Conceptual Level: defines the implementation-independent specification for the IS; and
- Technical Level: defines the technical implementation of the IS.

Kokolakis et al. categorise [175] many of these tools using four criteria; namely, conceptual constructs, epistemology, business modelling approach and perspectives. Since the introduction of this categorisation, the efforts by Kim and Lee with their AHP Processes Method [174], Cresswell and Hassan with their Socio-technological IDEF Method [69] and Assel et al. with their Collaborative Working Environment Model [16] are examples of tools which model security and human factors in order to align with business processes.

Grinter and Smetters advocate [123] the use of a user-centred threat model tool, which acts as the initial starting point to identify explicit security requirements. Once this model is established, they claim, the design of the security related components then becomes implicit.

There are also modelling tools designed specifically to assist usable and secure requirements engineering. Faily and Fléchais developed [93] the Integrating Requirements and Information Security tool to model, at the conceptual level, five engineering views consisting of task, goal, risk, responsibility roles and environment. They also developed [94] the Computer-Aided Integration of Requirements and Information Security (CAIRIS) software program, which is used to store elicited case data and is designed to aid requirements analysis. It generates Unified Modelling Language (UML) notation outputs to improve the visualisation of security and usability design.

The use of modelling tools facilitates an abstract description of the application context's problem of automated personal identification and the possibility of abstract descriptions of candidate APIMs, which may address the articulated problem. We believe, however, that insufficient focus is afforded in these tools to understand the *problem* not only from other stakeholders involved with an IS programme but from alternative disciplines, e.g. compliance with privacy legislation on retaining person's biographic and biometric data.

We consider that models, derived from a multi-disciplinary approach, which are an integrated representation of the *automated personal identification problem* are more informative to IS designers than models produced from a single perspective. Such integrated models, however, as Faily concludes [92] which model a diversity of factors relating to the security and usability of an IS in an enterprise necessitates the usage of automated tools.

3.2.3.3 Expert System Tools

The use of expert systems is an alternative way of modelling the complex relationships between many factors to support business decisions on assessments of risks and their management. Implementations of these models, however, appear to have not progressed beyond prototypes.

Dobelis et al. developed [82] an expert system which acquires data for evaluation in the form of business criteria and, based on internal rules, proposes options for security requirements and then evaluates the results according to predefined criteria. Similarly, the Chief Information Security Officer (CISO) Interaction Tool, developed by Parkin et al. [190], ensures that an organisation's security policies are usable from an employee perspective.

Kailay and Jarratt developed [169] the Risk Analysis and Management Expert System (RAMeX) which is a qualitative based expert system which enables small commercial organisations to model risks and also to conduct risk assessments. RAMeX contains an inference engine with functionality to perform forward and backward chaining. It is, therefore, a data-driven knowledge engineering system that uses inference rules.

We believe that their contribution demonstrates that discipline expert's *know-how* may be represented in an expert system and that a knowledge engineering approach may assist in the design and decision-makings in programmes to select APIMs. We review those tools which are designed to model APIMs in Section 3.3.3.

Our review of the literature has so far identified tools which are *partial methodologies* and the main limitation of these tools is that they do not offer IS programmes comprehensive support in all stages of an IS development programme. We believe that InfoSec methodologies should, however, incorporate elements of the tools reviewed so far into an integrated tool, which may be applied in all stages of an IS development programme. A check list of factors integrated into an analytical framework could ensure that data relating to those factors are acquired from an application context. The inclusion of a modelling tool may then represent the security requirements for an APIM for the application context. Similarly, a modelling tool could represent candidate APIMs which may then be evaluated against the requirements of an APIM.

We now review comprehensive InfoSec methodologies which are designed to support all stages of an IS development programme and may include some of the previously described

tools types. We commence with those tools which are based upon principles from various scientific paradigms and describe their approach at high-level only.

3.2.4 Heuristic Approaches

The seminal socio-technical IS development approach, advocated by Mumford [210], takes account of the technical, organisational, economic and social needs of the user community in order to create humanistic and effective information systems. Similarly, Cavoukian recommends [45] a design approach that embeds privacy controls into the design specifications rather than relying of the sufficiency on regulation and policy to safeguard privacy.

Mouratidis and Giordini's development [208] of the Secure TROPOS Methodology, an extension of the TROPOS IS Development Methodology [36], is a knowledge engineering approach that strives to integrate security controls into the IS development stages.

Sasse et al. advocate [262] a holistic design approach to ensure security, usability and privacy factors are integrated into IS development projects. Similarly, Fléchais et al. consider [102] that an approach that models the contexts in which the IS operates, the assets of the IS, and the operatives of the IS, allows for the documenting of both security and usability needs for all stakeholders involved with the IS. Nevertheless, they acknowledge that different stakeholders will have different points of view as to which aspect is most relevant to them.

Alternatively, Siponen et al. consider [267] that their Feature Driven Development (FDD) approach enables security to be integrated into agile development methods at different phases during an IS development project:

1. **Requirements Analysis Phase:**
    - A. Identify the security-relevant objects;
    - B. Identify the security-relevant subjects;
    - C. Determine the security classification of these objects and subjects; and
    - D. Perform a risk analysis and evaluate costs of controls against risks;
2. **Design Phase:**
    - E. Ensure security requirements are included in the design phase;
3. **Implementation Phase:**

- F. Ensure that the *wanted* security features are implemented.

Conversely, Yee warns [328] that:

> *"while it may be easy to write the requirement 'the information system and its security and privacy protection controls must be easy to use' in a requirements document usability elements can't be added to an IS like magic pixie dust."*

Yee argues [328, 327] that conflicts between security and usability goals can be avoided throughout the iterative design processes by addressing users' expectations and users' mental models at an early juncture. Church and Whitten recommend [53], however, that while it is important to articulate the various levels of abstraction to represent usability requirements developers need to be aware of the risks to the overall IS development in doing so.

Many approaches to develop security mechanisms for information systems place unreasonably complex demands on all the stakeholders involved in designing usable and secure information systems [334]. While an IS may possess the desired qualities the behaviour of users has a significant impact on security [195].

The main advantage of this type of comprehensive methodology is that it offers IS designers and discipline experts the flexibility to interpret the processes of the tool for the specific application context in order to select the optimal APIM. We believe that heuristic approaches may not produce reproducible results. Heuristic approaches contain insufficient detail and structuring in their processes descriptions to enable different methodology users to arrive at similar outcomes. Heuristic approaches, therefore, rely on the skills of the methodology user to interpret a heuristic approach's processes in order to specify the requirements for an APIM and their knowledge of candidate APIMs to select the optimal for that application context. In Section 3.3.4 we review those tools which offer a heuristic approach to IS designers and discipline experts in the selection of APIMs.

Finally in this section, we review the tools in the literature which incorporate a detailed description of the stages and steps of the methodology's process in a well-defined method.

3.2.5 Systematic Methodologies

We review two methodologies found in the literature which fulfil, although barely, our classification of a systematic methodology. We review the Mouratidis and Jürjens' approach [209] and Fléchais' approach [101] in greater depth since this type of systematic methodology and its efficacy is the focus of our inquiry. These contributions demonstrate that InfoSec methodologies can offer prescriptive methods based on learning from scientific inquiry and practitioner know-how in order to select the optimal APIM for a given application context.

Both methodologies conform, to a large extent, to Siponen's fifth generation criteria in that they are based on a socio-technological approach and both produce an output, in the form of UML diagrams to describe security requirements. These outputs can be integrated with the other types of design documentation created in an IS development project. Mouratidis and Jürjens' approach [209] also has the capability to translate its TROPOS secure models into UML security models for testing [168]. Fléchais' approach [101] has a UML meta-object facility which provides designers with a means of building models to assist with the integration of InfoSec models into other information system models. While both methodologies do not specifically include privacy aspects we consider that these methodologies may be extended to do so.

Mouratidis and Jürjens' methodology [209], which builds on earlier work on Secure TROPOS [208], is an integration of the Goal-driven Security Requirements Engineering (GDSRE) Methodology and Model-Based Security Engineering (MBSE) Method. Their main aims of the tool are to:

1. Provide a structured process to translate the results of the GDSRE methodology to a design that satisfies requirements;
2. Allow simultaneous elicitation and analysis of the security requirements and functional requirements of an IS;
3. Allow consideration of both the social and the technical dimension of the information systems' security; and
4. Guide software engineers towards a design that is amenable to formal verification with the aid of automated tools.

Fléchais' Appropriate and Effective Guidance for Information Security (AEGIS) approach

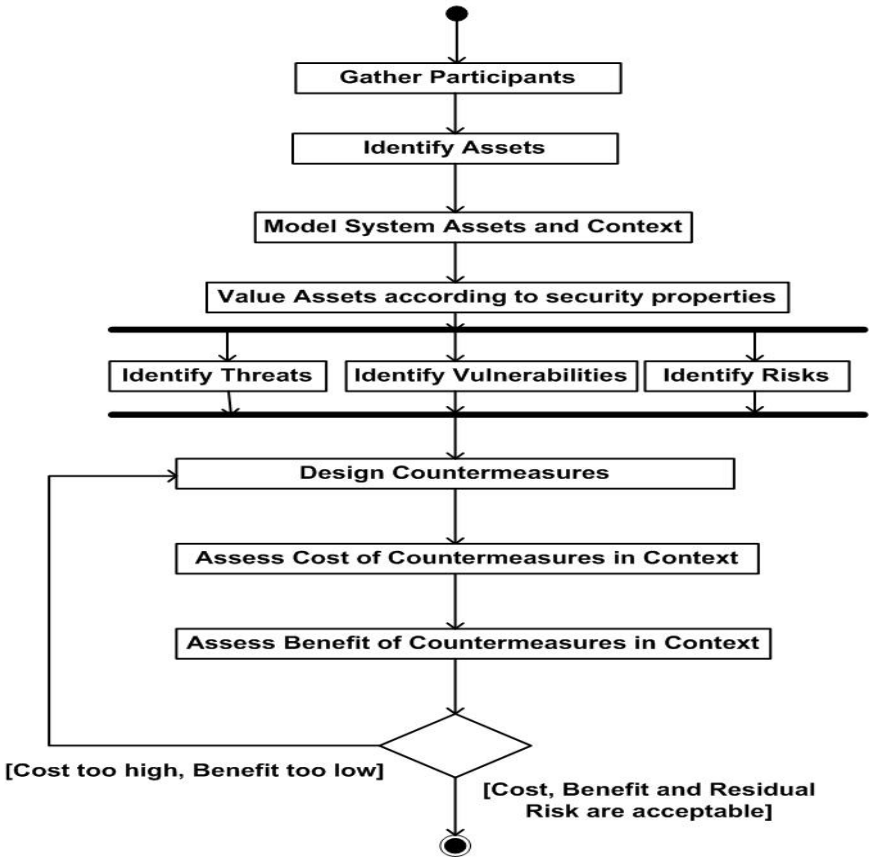

Figure 3.2: Fléchais' AEGIS Activity Diagram [101]

[101] is a socio-technical systematic methodology designed to assist with the difficulty of reconciling technical requirements and human factors in establishing secure and usable information systems. AEGIS offers a risk-based approach for security designers that focuses on acquiring and enhancing contextual knowledge surrounding an IS development project. This methodology is based upon Boehm's iterative IS development principles [33]. AEGIS' principle aim is to improve information quality relating to security decisions for organisational stakeholders by incorporating and better reflecting users' needs, as indirect stakeholders.

The AEGIS Methodology, shown in Figure 3.2, is a meta-process model representing discrete stages of the methodology' activities.

The AEGIS Risk Analysis and Security Design processes are shown in Figure 3.3, which are designed to evaluate the attributes of security properties, using both quantitative and

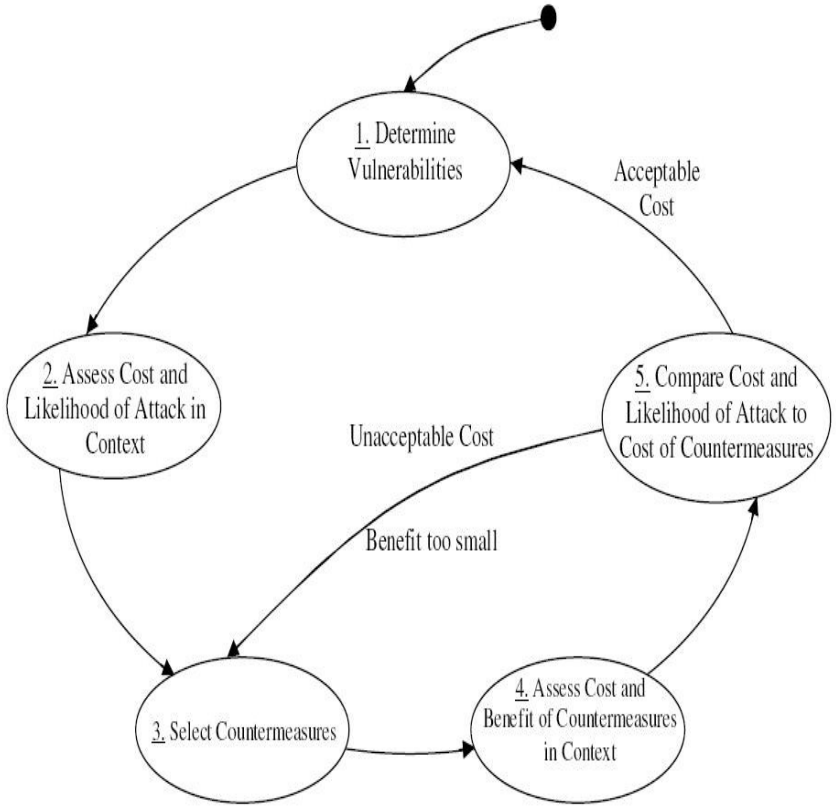

Figure 3.3: Fléchais' AEGIS Risk Analysis and Security Design Process [101]

qualitative data inputs, to capture stakeholders' judgments directly. A comparison of the security properties is used to ascertain which security aspects of the IS are of greatest important to the different stakeholders.

Fléchais concedes [101] that the main limitation of the AEGIS Methodology is that it does not provide a formal decision process. Nevertheless, the AEGIS Methodology provides evidence that the use of prototyping or simulation tools may be employed to facilitate improved end-user participation in setting security requirements through iterative design activities, such as interaction observations, group discussions, analysis of logged data and the revision of designs. The AEGIS Methodology also demonstrates progress in developing a methodology that evaluates alternative viewpoints. Fléchais does not, however, explain how conflicting ideological perspectives are resolved in his case study research, or how different stakeholders' objectives, which were in conflict, were actually reconciled.

Although we classified these contributions as systematic methodologies, in that they contained a description of their methods, we identified two main research issues relating to the selection of APIMs.

3.2.6 Identified Research Issues

We discuss methodological risks and practitioner competency influences on the selection of APIMs from our review of these two systematic methodologies.

3.2.6.1 Methodological Risks

A major limitation of these systematic methodologies is that both describe their processes at a high-level only which attract methodological risks. For example, neither appears to have a mechanism for handling conflicts of interest between the stakeholders, as discovered in practice by Al-Khouri in his case study of the United Arab Emirates (UAE) Identity Card Programme [4]. The decision-making structures in organisations are often complex and security, and particularly APIM, designs may have to be constructed within an organisation's strategic objectives, policies and constraints. We believe that a systematic methodology's processes should seek to understand the stakeholders' interests, as well as the operational requirements, in terms of functionality and performance, for an APIM in a given application context.

Hull et al. argue [138] that the design of an IS *should* be in response to operational requirements for that IS. Agile methodologies are valuable to review implementation interaction designs and features, with periods of reflection and introspection, to facilitate collaborative decision-making with stakeholders [267]. Agile methodologies, in providing such flexibility, rely on individuals and their creativity rather than processes, which are used to drive traditional IS development methodologies [218]. Boehm recognises [34] that the advantages of agile methodologies and the reliance on individuals in a project team attract risks, stemming from individuals' incomplete or incorrect knowledge. Boehm suggests [34] these methodological risks are minimised by plan driven approaches designed specifically to produce architectures and models for external expert review.

The research issue identified relates to whether plan driven systematic methodologies, described by well-defined methods, reduce the risks associated with practitioner's creativity and

competences to select the optimal APIM for a given application context. We consider that inquiry is needed to understand the extent to which systematic methodologies, incorporating plan driven processes, i.e. described in a method, are efficacious in countering these identified methodological risks for selecting the optimal APIM for a given application context.

3.2.6.2 Practitioner Capability Influences

Fléchais states [101] *"the main weakness for accommodating human factors lies in the design processes of a secure technical system"*.

Neither of the reviewed systematic methodologies describes how data are acquired from the stakeholders and the application context so that security designs for the IS may be formulated. Fléchais et al. acknowledge [102] the importance of the facilitator's capabilities and their training requirements from the use of AEGIS in a case study. Therefore, we assume that both these systematic methodologies implicitly incorporate elements of practitioner know-how into their respective methods. The practitioner competencies needed to use these systematic methodologies, including the gathering of information from the application context, are not made clear in these contributions.

Baskerville suggests [24] in his analysis of practitioner usage of third generation InfoSec methods (i.e. analytical tools) that while practitioners broadly aspire to use such tools, they are unable to apply their use in practice. Equally, he points out, that practitioners may intuitively deviate from such methodologies and, therefore, making it difficult to determine whether the InfoSec methodology is flawed or incomplete. Nevertheless, despite these difficulties, we believe that there is theoretical and practical benefit in validating InfoSec methodologies for selecting APIMs

We consider that if such an approach is open to practitioner interpretation, with deviance from intended usage, then inconsistencies in output may result when such a flexible approach is utilised by various practitioners. Conversely, we believe that if a systematic methodology, incorporating a repeatable method and practitioner know-how, is utilised then that approach may increase the consistency of selecting the optimal APIM for that application context. The research issue then becomes the determination of the extent of that systematic methodology's efficacy to articulate the requirements for an APIM for the application context and then select the optimal APIM from several candidate designs.

Research inquiry is needed, therefore, to understand the viability of integrating practitioner know-how into a systematic methodology with well-defined prescriptive processes and the extent of that systematic methodology's efficacy to select the optimal APIM for a given application context.

We reviewed InfoSec methodologies which are applicable to determining security controls in general. The focus of our review now concentrates upon specific methodologies relating to the selection of APIMs, using our tools classification model, as defined in Section 3.1.3.

3.3 Methodological Tools to Select APIMs

In this section we review the methodologies used to select APIMs. We exclude a review of the literature which describe APIMs or the issues associated with APIMs because the focus of our inquiry relates to methodological efficacy.

We review the methodologies in the literature in terms of their function to evaluate and select an APIM during the four stages of an IS development programme:

APIM Requirements Determination evaluating an automated personal identification problem in its application context;

APIM Modelling producing a design or a specification for an APIM, which is pertinent for its intended usage environments;

APIM Implementation comparing candidate APIMs in order to select the optimal identification system or authentication system for a given application context; and/or

APIM Configuration and Monitoring reviewing a deployed APIM.

We consider that the methodologies classified in our first three classifications are *partial methodological tools*, according to the definition provided by Uzunov et al. [302]. Additionally, the absence of descriptions of the methods to use these methodological tools makes scientific review problematical. Our research focuses on methodologies which are applicable across all four stages of an IS development programme which contain descriptions, if only brief, of their method. We concentrate our analysis, therefore, on heuristic approaches and systematic methodologies.

We conclude this section by discussing the identified research issues based on our review of these methodological tools.

3.3.1 APIM Factor Guidance Tools

There is a large body of guidance documents on factors surrounding the evaluation of APIMs. Table 3.4 provides, in a compact form, the located guidance tools specific to evaluating APIMs.

From our review of these tools we ascertained that there is a diversity of factors which require evaluation in order to select the optimal APIM for a given application context. We ascertained, however, that there is not a comprehensive check list of factors in the literature integrating these different perspectives. A consolidated list of factors could be used by an IS development programme to evaluate and to select the optimal APIM for a given application context.

Many sets of guidelines contain a list of technological factors [223, 271, 217] for evaluating APIMs. These guidelines, however, do not evaluate the factors associated with the application context in which the APIMs are to be deployed. Similarly, recommendations on particular identification and authentication systems' configurations, to counter different types of threat, are often based upon an evaluation of a restricted set of technical factors [287].

We believe that while these types of technical examinations are useful in evaluating APIM implementation factors, they do not give sufficient regard to other security activities which take place during an IS development programme, e.g. the macro task of determining the requirements for an APIM. Polemi recommends [238] that the suitability of biometric modalities should follow on from gaining an understanding of the requirements for biometric systems which are applicable to various types of application contexts. Table 3.4 shows the range of factors which are evaluated by each tool; however, none of these contributions provide factors which support all the APIM selection tasks, as defined earlier in Section 3.3.

From our review of those sets of guidelines which extended beyond technical considerations, we note that these guidelines tend to evaluate security, usability and privacy factors (and also many other factors) relating to APIMs from an organisational slant or from a user-centred orientation, as reflected in Table 3.4. We identified, however, that there are many common factors, such as security, usability, accessibility, data capture and privacy protection, which

GUIDELINE'S PERSPECTIVE	PUBLICATION TITLE AUTHOR AND CITATION	FACTORS EVALUATED
Organisational View	1. Use of Biometrics for Identification and Authentication - Advice on Product Selection. UK Biometrics Working Group [295]	Legislative compliance, user attitude, acceptability, technical resources, systems functionality, enrolment policies, cost, positive/negative identification, user cooperation, frequency of use, supervised/ unsupervised application, open/closed system, standard/non-standardised environment, overt/ covert usage and performance accuracy/speed
	2. Guidelines on the Evaluation of Automated Personal Identification. NIST J. Kreps and B. Ancker-Johnston [177]	Resistance to deceit, counterfeit of artefact, susceptibility to circumvention, time to achieve recognition, convenience to user, recognition device cost, device interfacing, time and effort in updating recognition data, reliability, maintainability, cost of protecting device, cost of distribution and logical support
	3. PAS92-Code of Practice for the implementation of biometric systems. British Standards Institute [38]	Security, usability, accessibility, data capture, exception handling, privacy protection and data protection
	4. Biometric techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, including an appraisal where they are most applicable. Polemi [238]	Operational convenience, social acceptability, discrimination, uniqueness, exclusivity, device size, error tolerance, environmental conditions, flexibility of thresholds, cost of software/hardware, effort to update template, data size and device interoperability
User-centred View	1. Evaluating Authentication Systems. Renaud [250]	Security, accessibility, password memorability, special hardware and software requirements, convenience, inclusivity, cost, control of environment, user community's characteristics frequency of use, trust between stakeholders, users' security motivation, unbreakability and auditing requirements
	2. Automated Personal Identification. Raphael and Young [247]	Uniqueness, performance, ubiquity, availability, indispensability, brevity, reliability, security and acceptability
	3. Human Factors Considerations for Passwords and other User Identification Techniques, Part 2: Field Study, Results and Analysis. Allendoerfer [9]	Reliability, accuracy, technology maintenance, recovery, cost effectiveness, usability, accessibility and privacy
	4. Usability evaluation of multi-modal biometric verification systems. Toledano et al. [288]	Effectiveness, efficiency, user satisfaction, privacy and usability

Table 3.4: Factors Related to APIMs which are Evaluated in Guidance Tools

are common objectives to both perspectives. The guidance material produced by Kreps and Ancker-Johnston [177], however, attempt to take an objective stance in evaluating the factors associated with evaluating an APIM.

We believe that the factors for evaluating APIMs in these tools could act as a starting point to produce an objective and comprehensive check list for use by an IS programme as an aid to select the optimal APIM for a given application context. The research issue identified is to determine which factors need to be evaluated by an IS programme in order to select the optimal APIM. This identified research issue together with others identified during our review of the methodologies in the literature are developed into research questions in Section 3.4.

Next we assess the tools that are designed to analyse the many and diverse factors involved with the evaluation and selection of an APIM.

3.3.2 APIM Analytical Frameworks

We review the analytical tools identified in the literature which are based on quantitative or qualitative data models.

3.3.2.1 APIM Quantitative Analytical Frameworks

Mansfield and Wayman provide [194] a *best practices framework* for testing the performance, in terms of accuracy, of biometric systems. The framework includes guidance for technical analysis and comparison of different biometric modalities from measuring key parameters, such as False Match Rate (FMR), False Non-match Rate (FNMR), Failure To Enrol Rate (FTER) and Failure To Acquire Rate (FTAR). These guidelines specifically exclude other factors, such as reliability, availability, maintainability, vulnerability, security, user acceptance, human factors, cost benefit and privacy regulation compliance.

The NIST Human Evaluation Framework [202] is a tool for the quantitative testing of different types of biometric modalities for biometric identification systems. The tool provides a common evaluation framework for the biometrics community so that a complete set of standard quality tests can be applied to data sets from different types of matching algorithms. While these contributions are valuable for testing under laboratory conditions to give general indications on potential capabilities, the real-life performance of biometric systems depend

very much upon how and where they are deployed [193].

Renaud's quantitative analytical framework focuses [249] on web based authentication from a user's perspective; however, it excludes factors relating to the protection of subjects' privacy. All forms of credentials are covered; namely, biometrics and various types of password schemes, including graphical position based systems. Renaud seeks [249] to ascertain the quality of an authentication mechanism by establishing its *quality co-efficient*, through measuring a solution's deficiencies, based on the assumption that all web authentication mechanisms contain deficiencies.

The calculated coefficients are subject to an environment and context factorisation to make adjustments for the degree to which the environment may or may not be controlled by the user. Each factor has a simple scalar measurement unit, e.g. zero denoting absence of a quality, 0.5 denoting quality partially exhibited or one denoting the presence of the quality. Exactly how the task is performed to set numerical values, based upon qualitative data and other evidence, is not presented. Furthermore, the transformation from qualitative data to quantitative data values for analysis, often using subjective opinions, may attract criticisms of biased interpretations.

Toledano et al. evaluate [288] the effectiveness, efficiency and user satisfaction of a biometric modality, from a user's perspective, also using a quantitative approach. They claim that it is difficult to link some factor variables, as they found with the subjective measurements of *ease of use* and *overall preference* data gathered from users of biometric systems with three different types of modalities.

Toledano et al. suggest [288] that the factor interrelationships vary according to the application context. Nevertheless, they have established some relationships, with both positive and negative influences, of different biometric modalities between these factor variables. Conversely, Renaud's analytical framework assumes that the relationships between the factors are constant irrespective of application context. Toledano et al. also claim [288] that the efficiency and the security of a biometric authentication system are not strongly related. Their analytical framework focuses on the subject perspective only and organisations may want to use alternative measurements for evaluating effectiveness and efficiency.

These contributions suggest that it is extremely difficult to model the interrelationships between the factors quantitatively. A qualitative analytical framework which examines the nature of the influences between the factors may reveal further understandings on the

complexities involved with the selection of an APIM.

3.3.2.2 APIM Qualitative Analytical Frameworks

There are many tools in this category which use mixed data types to evaluate factors relating to APIMs from various perspectives.

There are frameworks to evaluate factors that are designed to assist with the selection of biometric modalities and biometric products [295, 63]. There are frameworks designed to measure the effectiveness of APIMs, from an organisational perspective [177, 217], a technical perspective [125, 306, 188] and from a social perspective [244].

Grijpink's assessment framework evaluates [122] each new identification and authentication technology in terms of its *spoiler* effect. A spoiler is defined as an obstacle imposing difficulties on the deployment of an IdM system. The evaluation of the spoiling factors from alternative perspectives, e.g. legal and regulatory, acts to identify possible alternative enhancements to the original proposed IdM system.

Importantly, the benefits of exploring alternative perspectives leads to the proposition that inquiry into the evaluation of APIMs may benefit from multiple perspectives within a meta-evaluation framework. The identified research issue is how such a framework can represent these different perspectives in order to evaluate mixed data types. We consider that the classification of such factors may then be modelled, at varying levels of abstraction, to support decision-makers.

3.3.3 APIM Modelling Tools

The modelling tools found in the literature use mixed data types which are designed to represent the organisational capabilities to manage digital identities in deployed IdM systems.

Capability maturity models evaluate the effectiveness of deployed IdM systems to protect an organisation's information assets and determine the degree of achieving legal compliance by assessing the maturity of organisational processes to manage digital identities [39, 17, 321].

Hughes proposes [137] dashboard indicators to evaluate IdM deployments as an alternative model to the linear processes used in capability maturity models. He suggests [137] that an

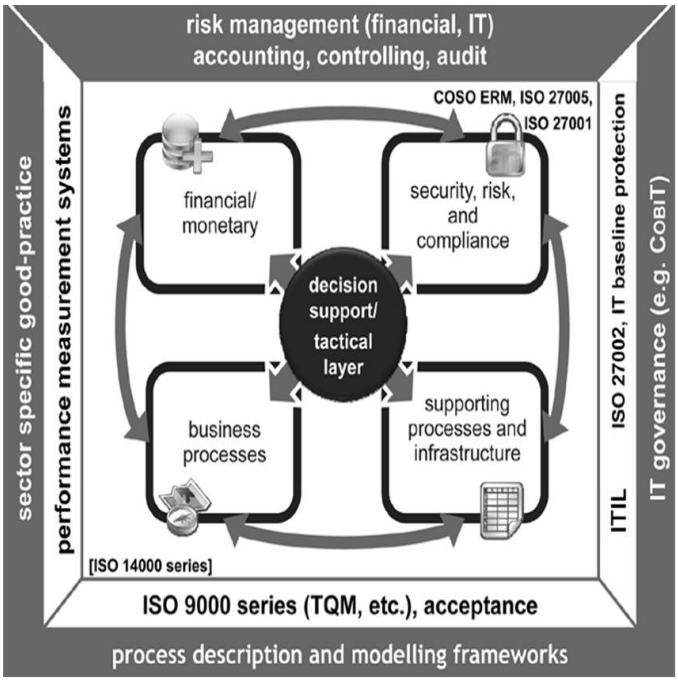

Figure 3.4: Royer and Meints' EIdM Decision Support Model [258]

evaluation of the organisational drivers and information systems' functionality is required in the first instance. From that point the evaluation should then review the organisational processes in terms of their importance and fulfilment of requirements within predetermined acceptability ranges. Each process is evaluated to determine whether the outcomes are within stated acceptability range. The acceptability of the process may fail because of *over fulfilment* or *under fulfilment* to the stated acceptability range.

None of the capability maturity modelling tools identified evaluate factors relating to issues surrounding the usability or accessibility of the IdM systems to the user community. The capability of an IdM system may exhibit mature processes; however, a mature IdM deployment may not necessarily achieve a balance of security, usability and privacy for all of its stakeholders.

Royer and Meints propose [258] a meta-evaluation decision model, based on the business balanced scorecard approach, to aid decisions on evaluating Enterprise Identity Management Systems (EIdMSs). Their model captures data from a variety of assessment outputs which include cash flows, budget, data on the information systems in the enterprise, maturity of process documentation, authentication and authorisation requirements, and physical access

requirements. The model, shown in Figure 3.4, represents the qualitative and quantitative data acquired from a financial, a business process, a security risks and compliance requirements, and an information system and IS support process perspectives.

Royer and Meints acknowledge [258] that the functionality of a Decision Support System (DSS) should extend beyond that of a single matrix, as the EIdM model places a high demand on the automated processing of data relating to the underlying complexities between their identified factors and the aggregation of various data types.

Royer's development [257] of a prototype DSS, as part of his thesis, is an implementation of the model established [258] with Meints. The DSS is designed to assist enterprise decision-makers to select the optimal IdM system given the data acquired from the various input data sources. His model acquires primary data from the application context to enable a meta-evaluation of candidate EIdM systems. He identifies six key factors; namely,

1. Organisational operational processes;
2. Monetary aspects;
3. Quality;
4. Existing information systems;
5. Compliance, risks and security; and
6. Acceptance by users.

He also describes 15 relationships, both single and bi-directional, between these six factors. A factor's value has a direct or indirectly measurable, positive or negative, influence on other factors represented in the model. While Royer proposes [257] the use of Microsoft Excel spreadsheets to store acquired data relating to the six factors, he does not explain the interrelationship computations between these data elements in order to arrive at a prediction in respect of identifying the optimal EIdM system for an enterprise.

The creation of his DSS prototype was achieved by conducting proof of concept interviews with several IdM expert practitioners from six German consultancy organisations. His inquiry into *"How decision-making on IdMs are taking place in practice?"* and also *"Identifying the relevant factors and their linkages which need to be taken into consideration?"* reveal that there is a lack of decision support methods and tools for selecting EIdM systems.

Additionally, Royer ascertains [257] that decision-makers in organisations have a perceived lack of understanding in respect of the organisational impacts resulting from their EIdM system decisions.

While it appears that Royer's model and DSS have not been validated by using either in a real-world evaluation it reveals the complexities of the interrelationships between the factors. Leaving aside that the model and the DSS may be relevant only to enterprise IdM deployments, his research demonstrates that an IdM practitioner's know-how may be acquired and represented in an expert system which models complex decision processes. The identified research issue is how to represent practitioner's know-how in a series of processes as an integral element of a methodology or within an expert system.

We consider that further research is apposite to explore how expert practitioners evaluate the multiple factors associated with selecting APIMs from various perspectives. This inquiry should aim to understand the methods that practitioners employ and also the models that they use to evaluate the multiple interrelated factors associated with selecting an APIM.

Next, we review heuristic approaches as tools to select APIMs.

3.3.4 APIM Heuristic Approaches

There is a scarceness of tools in the literature that describe heuristic approaches to select APIMs.

Vanamali recommends [303] a business driven evaluation approach where the evaluation of solutions extends beyond the resolution of technical issues to enable businesses to perform effectively and efficiently, particularly in the business environments where IT budgets are ever shrinking. Parkin et al. suggest [228] that predicting the effects of amending security policies on identification and authentication mechanisms, e.g. increasing password minimum length, is a better starting point for conducting such evaluations. They propose the use of a mock-up prototype tool to predict the impact, particularly on end users, before trade-offs between financial costs and benefits are even considered.

These strategies identify the need to understand the effect, in terms of its nature and extent of impact, which a particular factor has on other factors during the evaluation of an application context and the appraisal of candidate APIMs. A lack of understanding of these impacts may result in the inappropriate APIM selection. Heuristic approaches, however, are dependent

upon practitioners' interpretation of the approach and their skills and competencies. As the approaches are not documented, i.e. its method, it is, therefore, difficult to differentiate between an approach's proficiencies and deficiencies with the skills of the expert practitioner.

Some approaches may be more efficacious in particular application contexts by adopting a strategic perspective and commence with stipulating organisational objectives and measurable outcomes at the outset. Alternatively, some iterative approaches may be more efficacious when a deployed APIM requires enhancement.

We believe that a tool is required to evaluate the many factors in an application context systematically in order to minimise decision-making risks on the selection of an APIM. We acknowledge, however, that application contexts may vary considerably and the systematic methodology needs to designed to accommodate such variations. The research issue identified then becomes an inquiry into the extent of a methodology's efficacy to select the optimal for certain IS programme development situations. A methodology, therefore, needs to be assessed in terms of the extent of its efficacy to address specific types of automated identification problems of various application contexts each which possess their own distinct range of circumstances.

Lastly, in this section, we review the methodological tools, which possess systematic processes, i.e. a method, to evaluate the factors relating to the selection of APIMs.

3.3.5 Systematic Methodologies for Selecting APIMs

There are no systematic methodologies, incorporating well-defined processes, in the body of knowledge which are designed, as a tool, to select the optimal APIM for a given application context.

We found evidence that systematic methodologies exist to aid the selection of biometric systems with some of these tools being employed by professional services companies during their evaluation assignments. The properties of these systematic methodologies, specifically their methods' processes, have not been published with sufficient descriptive detail to enable repeatable usage by other evaluators. The lack of well-defined processes in these methodologies also inhibits a review to assess their efficacy. We categorise these methodologies based upon whether the evaluation processes are quantitative or qualitative.

3.3.5.1 Quantitative Methodology

Ashbourn designed [15] the Pentakis Methodology in order to assist organisations to evaluate the factors surrounding biometric system deployments. The accompanying Pentakis Expert System has a knowledge base module, in which an evaluator may store data collected from the case under evaluation and produce a calculated solution preference.

The Pentakis tool evaluates user attitudes, transaction timings, scalability possibilities, population profile and costs analysis of a biometric system with various configurations. Pentakis appears to be designed to conduct evaluations without consideration of the application context's operational environment, stakeholders' objectives and their requirements. We believe that the risks associated with this type of methodology all too frequently result in stakeholders' objectives being unfulfilled.

The majority of subject data are quantitative, e.g. costs and performance timings; however, an evaluator may use scalar units to represent their evaluation of a biometric system's qualitative attributes, e.g. usability. Ashbourn fails [15] to explain the methods' processes and the underlying evaluation computations in the Pentakis Expert System in order to review the efficacy of this systematic methodology. There is no evidence that Pentakis has been validated by using it for selecting a biometric system in a real-world application context. Importantly, the Pentakis Methodology reveals the type of know-how that practitioners apply in evaluating biometric system deployments.

3.3.5.2 Qualitative Methodologies

There appear to be three qualitative methodologies used by consulting organisations; however, the details that describe these tools remain commercially confidential.

IdMology is a tool designed to evaluate IdM systems based upon the experiences of expert practitioners in IDFocus LLC [10]. The details of the discipline experts' practises and the scientific foundations of the methodology are not publicly available. The sales literature published by IDFocus LLC provides an overview of IdMology and does not describe the experts' practises or scientific foundations upon which it is designed sufficiently for an objective review.

HJP Consulting GmBH [7] developed, in conjunction with the Software Quality Lab of the University of Paderborn, the Model Centric Methodology for Analysis, Specification and Qualification (MMASQ) for developing IdM systems. This methodology is based on the V-Modell IS development approach [199].

The MMASQ/V Model contains a series of systematic processes and models to represent the design components from a systems engineering perspective and produces UML based requirement descriptions. It is difficult, however, in the absence of any detailed scientific publication, to conduct a review of this systematic methodology. Despite the lack of descriptive detail in the publication domain this methodology further demonstrates, however, that practitioners' methodological know-how may be codified into a systematic methodology.

Al-Khouri claims [4] in his thesis on programme management that the vendor in the United Arab Emirates (UAE) eID Card Programme refused to disclose their systematic methodology to the UAE eID Card stakeholders' representatives. Al-Khouri's findings [4] are further evidence that systematic methodologies exist and are employed by technology suppliers. His findings also suggest that requirements engineering for APIMs need a means to address a variety of stakeholder conflicts which appear to occur during programmes of this nature.

Despite the lack of details on the vendor's methodology, Al-Khouri's thesis provides [4] valuable insights into the dynamics of a national eID Card programme. The UAE eID Card Programme established criteria [5], based upon ISO9126 Software Engineering - Product Quality - Quality Model, to evaluate the quality of the technology deliverables. The programme considered the task to establish such criteria as a critical activity. Most relevant to our inquiry Al-Khouri recognises [5] that such methodologies need to be proportional to the size and importance of the business goals.

Importantly, our review reveals again that practitioner methodological know-how has been codified into methodologies for the evaluation of application contexts in order to select the optimal APIM. We do not, however, have an understanding of the methods used by practitioners in those systematic methodologies. This gap in the body of knowledge presents a research opportunity to formulate the craft of practitioners into a scientific methodology in an important and emerging field of study. The research issue identified is to determine how to represent the practitioner's craft into a selection method, with well-defined processes, within a systematic methodology.

[7] http://www.hjp-consulting.com/consulting/requirements-engineering

The efficacy of the reviewed methodologies remain largely unknown and there are potential real-world benefits in gaining an understanding as to when a particular methodology is more efficacious than other methodologies in order to select the optimal APIM for a given application context. This identified research issue forms the basis of our research problem to determine the extent of a methodology's efficacy for certain types of IS development programmes.

3.4 Development of Research Questions

We develop our four research questions based on the research issues identified in our review of the methodological tools in the literature and our analysis of our research problem.

3.4.1 First Research Question

In Section 3.3.1 we identified the research issue of identifying which factors need to be evaluated by an IS programme in order to select the optimal APIM. Additionally, our review of the guidelines also suggests that we need to a means to ascertain whether an APIM is optimal for a given application context in the first instance before an assessment on the efficacy of the methodology pursued which selected that APIM.

We found, however, that these methodological tools tend to evaluate an APIM in isolation, as a technology, rather than evaluate the application context in which the APIM will be deployed. We also identified that many factors affecting the selection of an APIM are often viewed from a single perspective, either factors that impact largely on organisations' stakeholders or factors that impact the user community in the application context. Also, we ascertained that the relationships between the factors for evaluating APIMs are complex and largely unknown. We believe that a research inquiry to consolidate the factors in these tools into a comprehensive check list in an evaluation framework would be beneficial both theoretically and in practice. These identified factors should be validated using data acquired from empirical inquiry.

We also identified in Section 3.3.2, that analytical frameworks could represent stakeholders' perspectives of an optimal APIM. Similarly, such a framework has the potential to evaluate mixed data types. As we indicated in our review of analytical frameworks, the complexities of mapping factor relationships directly are theoretically prohibitive. We believe it is difficult

because factor interdependencies are driven by the contextual circumstances and that each application context is unique. There are, however, analytical models in the literature which could form a starting point to develop an evaluation framework to represent the characteristics of the application context and the APIM selection processes. Also, we recognise that there is a need for varying levels of abstraction and representations of multiple perspectives in such an evaluation framework.

While the creation of a comprehensive check list of factors, incorporated into an evaluation framework, would address the identified gap in the knowledge, we believe that such a tool could be of importance to an IS programme seeking to select the optimal APIM for an application context. We believe that the availability of such a tool, which may be used to assist IS programmes to ensure that it evaluates a pertinent range of factors, tackle the complexities of selecting the optimal APIM, is worthy of research effort. We formulate our first research question based upon our identified research issue and the decomposition of our research problem to identify which factors need to be evaluated in order to select the optimal APIM.

What factors should be evaluated in order to select the optimal APIM for a given application context?

3.4.2 Second Research Question

As identified in Section 3.3.5, there are no systematic methodologies, with well-defined processes, to select APIMs in the body of knowledge. We consider it apposite to fill this gap in the knowledge by developing a systematic methodology for selecting an APIM and then, as a separate research question in line with our research problem, investigate the extent of its efficacy to select the optimal APIM.

While our review identified the potential for practitioner methodological know-how to be codified into a systematic methodology, the identified research issue is to establish how to represent the practitioner's craft in well-defined processes of a selection method. We suggest that practitioner's know-how could be represented in a series of processes of a method as an integral element of a systematic methodology. The method's processes would acquire information which describe the characteristics of an application context, with its information system and envisaged usage settings. Acquired data would then be evaluated systematically in order to support decision-making on APIMs.

Our second research question seeks to establish a systematic methodology, based upon our suppositions, to acquire data from the application context in order select the optimal system from a range of candidate APIMs.

How can information pertaining to an application context be acquired and evaluated in a systematic methodology so as to determine the optimal APIM?

We believe that a systematic methodology, with well-defined processes, has the potential to assist IS programmes to select the optimal APIM. We acknowledge, however, that the methodology's data acquisition and its evaluation processes requires scientific validation. The use of the systematic methodology in a real-world application context will not only provide empirical data for validation purposes but also to generate relevant data to enable an efficacy assessment. The results from this efficacy assessment are important as they could help inform current practice.

We aim primarily to create a systematic methodology which incorporates security activity processes to support all the stages in an IS development programme. Our secondary aim is to develop a systematic methodology for selecting APIMs which align's with Siponen's fifth generation of InfoSec methodologies. He proposes that such methodologies should encompass user participation, be adaptable to different information system development methodologies and should also be validated through empirical grounding.

We believe that methodology's properties, such as ease of use and its usefulness to practice, are efficacy considerations. These properties should be assessed using data generated during a methodology's utilisation in a real-world application context. Therefore, there is a research need to define a means to assess the efficacy of a systematic methodology to select the optimal APIM for a given application context.

3.4.3 Third Research Question

In Section 3.3.4 we identified the research issue of the need to ascertain the extent of a methodology's efficacy to select the optimal for a given application context. Additionally, the decomposition of our research problem suggests that we need to establish a means to assess the efficacy of methodologies to select the optimal APIM for a given application context. We formulate our third research question so that we establish a means to assess the efficacy of different methodologies, including heuristic approaches, to select an APIM.

How can the efficacy of a methodology to select an APIM itself be assessed?

We recognise that some methodologies may be more efficacious than other approaches in certain application context circumstances. We aim to develop a set of criteria, therefore, to assess the efficacy of methodologies or approaches used in the selection of an APIM. Also from using these efficacy assessment criteria and the data acquired, it may be possible to identify the circumstances and to explain why a systematic methodology is efficacious for selecting APIMs in certain situations.

3.4.4 Fourth Research Question

From our review of the methodological tools, we note that the extent of systematic methodologies' efficacy, and also heuristic approaches, to select the optimal APIM for a given application context have not been investigated scientifically. The aim of our research effort is to improve understandings on systematic methodologies, as problem-solving processes, rather than to seek understandings relating to the competencies and strategies pursued by discipline experts, as methodology users. We, therefore exclude heuristic approaches from our inquiry.

The Whither Committee Report identifies [230] a significant research opportunity to develop an evaluative framework that would guide potential stakeholders who are considering deployment of biometrics. We believe that this identified research opportunity should be extended to a systematic methodology containing an evaluative framework. The systematic methodology should also contain incisive questions to acquire data from the application context and also a method to assist stakeholders to evaluate the application context in which the biometric solution will be deployed. The committee concludes [230], from their survey of biometric deployments, that *failures in biometric systems* are often rooted in:

- the lack of clarity about problem being addressed;
- lack of a viable business case;
- inappropriate application of biometrics where other technologies would work better;
- inappropriate choice of biometrics;
- insensitivity to user perceptions and usability requirements;

- inadequate support processes and infrastructures; and
- poor understanding of population issues.

The issues and vulnerabilities associated with some APIM deployments as identified in Section 1.1.1 and 1.1.2 respectively together with the results from the Whither Committee's survey [230] suggests that some methodological tools might be of benefit to IS programmes. We consider that research to establish the extent of a systematic methodology's efficacy is not only a worthwhile theoretical pursuit but the results of our investigations could also help to inform practice in the real-world. We acknowledge, however, that different methodologies may be more efficacious for some application contexts under certain circumstances and less so for others. We seek to understand the circumstances under which the utilisation of a systematic methodology is efficacious and, conversely, when, by implication, it might not be together with explanatory reasons.

Our fourth research question is framed to explore the contextual circumstances surrounding programmes tasked with deploying APIMs. We also seek to provide explanations as to why a systematic methodology may be efficacious in some situations and not so in other situations.

When is a systematic methodology efficacious for selecting an APIM and if so, under which scope of circumstances and why or conversely, if not, why not?

While some commercial systematic methodologies may exist in the marketplace, organisations often encounter the problem of determining which methodology or approach is most suitable for them to select the optimal APIM for their application context. Stakeholders' programmes will have difficulty in determining which methodology to pursue unless an understanding of the circumstances most relevant for a particular methodology is identified through empirical inquiry.

We believe that there are significant benefits to IS programmes in gaining an understanding on the proficiencies and deficiencies of different methodologies to select APIMs. This understanding may then be used in choose an appropriate methodology for the circumstances surrounding their IS programme. It appears from our review of the methodological tools that few of them have been empirically validated or assessed in terms of their efficacy for their intended purpose.

Our research questions are based upon our main assumption that APIMs are imperfect, in that such deployments possess inherent vulnerabilities and attract issues, and stakeholders

incur costs. Nevertheless, we aim to develop a systematic methodology to select the optimal APIM and then validate it using empirical data. We also aim to answer our research problem by generating the relevant data, for an efficacy assessment, from the use our methodology in a real-world application context.

In summary, our main unit of analysis is to inquire into the efficacy of a systematic methodology in order to identify and explain the circumstances when the use of such a methodology by an IS programme might be beneficial. Our secondary unit of analysis is the validation our systematic methodology and its components. We discuss the selection of the case study research methodology to conduct our empirical inquiry in Section 4.1 and the framing of our two units of analysis in Section 4.5.

3.5 A New Evaluation Paradigm for Selecting APIMs

Based on the issues research issues identified from our review of the methodologies in Section 3.3, we consider that a new paradigm is required to construct scientific theories in respect of the efficacy of systematic methodologies to select APIMs.

Our review of the methodological tools suggests that greater research emphasis is needed on methodologies' processes which aid complex decisions on APIMs. We believe that scientific effort should be diverted away from the search for the panacea APIM because all identification systems and authentications systems possess vulnerabilities, attract issues and incur costs [226].

The efficacy of the systematic methodology should be assessed to ascertain the viability, as defined by Kalfoglou et al. [170], of a systematic methodology to evaluate real-life automated identification problems. From our research inquiry, we aim to develop theories concerning the circumstances under which a systematic methodology may be more efficacious than other decision-making approaches. We also aim to gather explanatory reasons to support our theories by establishing efficacy criteria to model the properties of a methodology to select an APIM.

The next sub-sections justify our reasons to construct a new paradigm in order to develop our theories.

3.5.1 Problem Analysis

Researchers to date have largely studied IdMs and biometrics using a solution based perspective. There is overwhelming evidence [295, 230] that inquiry should be directed at evaluating the application context, together with its identification problem, and not the APIM itself in isolation. Our supposition is that the application context, in which the APIM operates, in turn, influences stakeholders' decision-making processes to select the optimal APIM.

So where do the real-world problems of establishing the optimal APIM for an application context lie because there are many advisory tools, as reviewed, in the literature? Do these problems emanate from stakeholders' difficulties to understand, analyse and articulate their business objectives and requirements for an APIM? Do decision-makers focus on candidate solutions only? Alternatively, could these identified problems lie in the methodology or the methods used by practitioners in order to select the APIM? Fundamentally, are the methodology's processes sufficiently robust to articulate the complexities relating to stakeholder's interests and concomitant issues surrounding the application context?

We propose to address the identified research problem through empirical inquiry using the four composite research questions stated in the previous section. We classified APIMs into three governance frameworks types in Section 2.4.4 in order to model the different stakeholder roles and trust relationships in each deployment type. We aim to conduct empirical research using case study research with cases from each context type, being enterprise, federated and heterogeneous, in order to reveal insights into the trust issues in this problem space.

We believe that the optimal APIM may only be determined if the basis upon which it will be evaluated are articulated at the outset and empirical data are gathered for subsequent comparison with other candidate APIM. The assessment of a systematic methodology's efficacy to conduct that evaluation, in order to determine the optimal APIM, therefore, becomes our main research problem.

3.5.2 The Need for Assessments

We identify the need for assessment at two levels. Firstly, we need to evaluate the application context and its identification problem in order to evaluate whether the APIM selected is optimal. Secondly we need to assess the efficacy of the methodology used to select the optimal APIM.

Information security needs suitable metrics to inform practical decisions, which are often complex [277]. Jaquith recommends [164] cascading technique for measuring the effectiveness of an IdM in an enterprise. Effectiveness of an APIM and other quality properties identified in Section 3.3.1, such as acceptability and maintainability, therefore, need to be modelled to enable evaluation of factors relating to the application context.

For efficacy assessments we need to establish efficacy criteria and then acquire relevant data to conduct an efficacy assessment of our systematic methodology. We also need to ascertain the desirable properties of a systematic methodology to select an APIM.

3.5.3 Desirable Properties of a Systematic Methodology

Siponen argues [266] that future InfoSec tools should not only be created from the socio-technical scientific paradigm, encompassing social factors, but also be rigorously developed in alignment with practices. His argument is based upon the need to incorporate social techniques so as to ensure the social acceptance of security controls and procedures. Similarly, Hitching considers [133] that the lack of consideration of human factors is one of the main deficiencies of traditional InfoSec approaches.

Our inquiry to establish a systematic methodology for selecting an APIM, therefore, attempts to align with these proposed development strategies through empirical research. From our analysis of the research issues, the establishment of our four research questions and our proposed paradigm, we consider that we are ready to select the most appropriate research methodology in order to conduct our empirical inquiry.

3.6 Summary of Chapter

This chapter reviewed the background parent discipline which describe the methodological tools in the body of knowledge which assist in the evaluation of security, usability and privacy issues surrounding the development of information systems. We used our *tools* classification scheme in order to review the methodological tools in the parent InfoSec discipline. We also reviewed the methodological tools which we found in our immediate research field of automated personal identification.

We highlighted some of the limitations of the tools in the parent disciplines used to evaluate

the issues surrounding the security, usability and privacy of information systems. The limitations of the tools available in our immediate discipline were also revealed and major research issues were identified and explained in order to formulate our four research questions.

We identified that research is needed to establish a set of factors upon which to evaluate an application context in order to determine the optimal APIM for a given application context. We justified our arguments that there is also a need for a systematic methodology for such evaluations to aid decisions on selecting the optimal APIM for a given application context. The properties of a systematic methodology were highlighted and we also identified the need to establish criteria in order to assess the efficacy of a methodology used to select an APIM.

We concluded that empirical research is needed to determine the circumstances as to when and why a systematic methodology is efficacious to select an APIM in order to address our research problem.

CHAPTER 4

Research Methodology

Contents

This chapter discusses the characteristics of our research inquiry and our epistemological standpoint in order to justify the selection of the case study research methodology. We provide an overview of the case study research methodology and then justify the selection of our three case studies. We then describe our data collection techniques and our qualitative data analysis procedures. A discussion on the units of analysis is provided, together with criteria to assess the quality of our research inquiry and to validate our claims of contributing to the body of knowledge. Finally, we describe the ethical considerations that governed our research inquiry.

4.1 Selecting a Suitable Research Methodology

In this section we justify our selection of the case study research methodology to conduct our empirical inquiry into the extent of a systematic methodology's efficacy to select an APIM. We use the term *research methodology* in respect of our approach to conduct our investigations to distinguish it from *systematic methodology* which is the subject of our inquiry.

We first discuss the characteristics of our research problem and our four research questions. Next, we discuss the degree of uncertainty surrounding the phenomenon of our inquiry. We then consider the ontological and the epistemological positions of different research paradigms before describing the basis of our adoption of the critical realist research paradigm and its influence on our choice of research methodology. We compare candidate research methodologies and then justify our choice of the case study research strategy. We also identify some constraints and limitations of the case study research methodology.

4.1.1 Methodological Choices for Research

While methodological choices for research are sometimes made unconsciously or through default [52], the awareness of the influences of such choices is critical to the contribution of

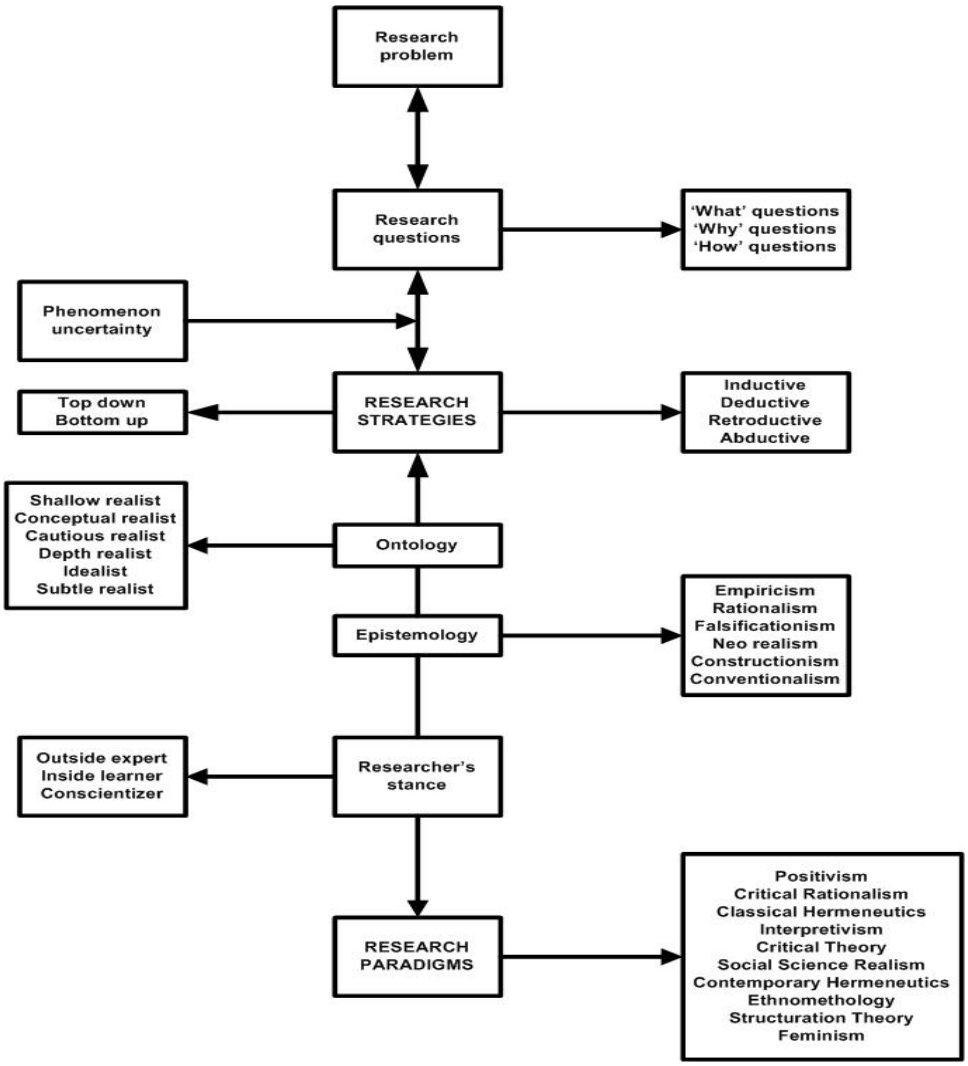

Figure 4.1: Research Design Choices adapted from Blaikie [32]

knowledge and understanding of a particular field [213]. There is also the need to examine the underlying philosophical assumptions and constructs upon which such understandings are based [241].

We examine such research design choices for our inquiry by considering the research strategy questions posed by Blaikie [32] and Trauth's recommendation [291] to also take into account the degree of uncertainty surrounding the phenomenon under investigation. We have added Trauth's phenomenon question to Blaikie's questions [32], which are represented in Figure 4.1. We commence with a discussion on the characteristics of the research problem.

4.1.2 Our Research Problem's Characteristics

The characteristics of our research problem requires the inquiry into the extent of a systematic methodology's efficacy to select the optimal APIM for a given application context. Our research effort is not aimed at establishing an indubitable reality or, conversely, a falsehood of a proposed hypothesis.

We believe the nature of the research problem of establishing the extent of methodological efficacy is context dependent and that the construction of generalisable theories is demanding because there are so many uncontrollable variables which influence our inquiry. Therefore, based on our critical realist beliefs, we aim to build plausible theories regarding the efficacy of systematic methodologies to select APIMs using evidence acquired through empirical research inquiry.

We aim to establish an understanding of how APIMs are currently selected in practice. We refrain, however, from comparing our systematic selection methodology with approaches currently practised by programmes' practitioners because we believe that it would be difficult to employ both methodologies simultaneously in the same inquiry. We assume that it would be a complex task to differentiate between the impacts of each methodology on a programme's efforts to select the optimal APIM. This research strategy may also be viewed as impractical by the stakeholders involved in that inquiry.

The use of a systematic selection methodology on past decisions in the real-world may also be viewed as impractical and of little benefit to stakeholders. We aim, however, to identify methodological learnings by examining approaches pursued by IS programmes in order to inform the design of our methodology. We also aim to use our systematic methodology in a real-world case so that data are acquired for our two units of analysis, which are discussed in Section 4.5.1.

4.1.3 Characteristics of Our Research Questions

According to Blaikie [31] scientific research includes starting from observed regularities, which are produced by hidden mechanisms. From these observed regularities models of these mechanisms may then be created. Empirical research involves searching in the real-world for evidence of these mechanisms in existence. We aim to start our inquiry by observing regularities in current methodological practices as our starting point to gain an understanding

of these underlying mechanisms and methodological learnings relating to discipline experts' practises for selecting APIMs.

Our inquiry seeks to build a model of the regularities of programmes and their practitioners' activities which are tasked by stakeholders to introduce or revise an APIM. We aim to model the regularities of such a programme that represent the surrounding circumstances at the programme's inception, the events and strategies which took place during a programme, the resulting outcomes and hindsight observations from practitioners involved in the programme.

Avison et al. recommend [19] that researchers should try out their theories with practitioners in real-life situations and real organisations. We heed their recommendations by employing our systematic methodology in order to assess its efficacy in selecting the optimal APIM for a real-world application context.

Next, we review the type of inquiry involved for each of our following research questions.

1. What factors should be evaluated in order to select the optimal APIM for a given application context?
2. How can information pertaining to an application context be acquired and evaluated in a systematic methodology so as to determine the optimal APIM?
3. How can the efficacy of a methodology to select an APIM itself be assessed?
4. When is a systematic methodology efficacious for selecting an APIM and if so, under which scope of circumstances and why or conversely, if not, why not?

4.1.3.1 Research Question 1

We consider that our first research question is exploratory in nature.

Our aim is to identify the relevant factors which should be evaluated by programmes in order to select the optimal APIM. Such a comprehensive range of factors should incorporate aspects relating to the application context, the characteristics of user community and their tasks as well as technology deployment, security, usability and privacy issues.

We aim to consolidate the factors in the literature and then validate them by seeking their existence in real-world cases using empirical grounding [47] in the data acquired. We also seek to identify other factors in the acquired data from our empirical research.

4.1.3.2 Research Question 2

Our second research question is both exploratory and explanatory.

Our initial aim to establish how information pertaining to a case under evaluation may be systematically acquired, represented and analysed in order to support decision-making on APIMs is exploratory. Therefore, we aim to create systematic selection methodology that incorporates factors for evaluating APIM which we have identified in our inquiry to answer our first research question.

We aim to adhere to Siponen's criteria [266], for producing a fifth-generation InfoSec tool, by building our systematic selection methodology based upon the identification of methodological learnings. These learnings are to be identified by investigating programmes involved in the selection or revision of an APIM. This empirical research is explanatory in that we aim to understand practitioner's practises during programmes to introduce or revise an APIM. From these understandings we may then incorporate the relevant processes into our systematic selection methodology.

4.1.3.3 Research Question 3

Our third research question is exploratory in nature.

Our aim is to create a set of criteria which may be utilised to assess the efficacy of a methodology or an approach to select an APIM for a given application context. Our inquiry necessitates research into existing decision-making strategies in programme which determine that the APIM selected or revised is optimal for that application context.

We also seek to understand the methods and the data required by organisations in order conduct such evaluations for deployed APIMs.

4.1.3.4 Research Question 4

Our aim is to ascertain the extent to which a systematic selection methodology is efficacious for selecting an APIM is explanatory in nature.

Through empirical inquiry we aim to identify the circumstances surrounding a programme

that suggest that the use of a systematic methodology is an efficacious strategy to select the optimal APIM. We also seek to explain the reasons behind the identified circumstances which support the use of a systematic selection methodology by a programme to select the optimal APIM. Additionally, we aim to explain the reasons why a systematic selection methodology might not be efficacious at all for some situations.

Fundamentally, our aim here is to explain the reasons why a systematic methodology might or might not be efficacious for selecting the optimal APIM for differing application contexts. From the patterns recognised in our explanations we aim to establish plausible theories on the phenomenon of methodological efficacy.

4.1.4 Uncertainty Surrounding the Phenomenon

We define our research phenomenon as the efficacy of a systematic methodology to select an APIM for a given application context.

The impreciseness of terminology that describes the APIM field of study and its scope, as we discussed in Chapter 2, the vagueness in the approaches and data required relating to decisions on APIMs and the lack of information on methodological efficacy collectively adds much ambiguity to the phenomenon of inquiry. We consider the problem of assessing the efficacy of approaches currently practiced and also systematic selection methodologies is difficult because efficacy should be assessed, for its *fitness for purpose*, according to the case under evaluation. We believe, therefore, that a methodology's efficacy is context dependent; however, we assume that the characteristics of some cases are sufficiently similar to build plausible theories about systematic methodologies' efficacy.

Our research inquires into the efficaciousness of a systematic methodology to evaluate an application context in order to select the optimal APIM. Put simply, the extent to which the phenomenon produces the desired effect of selecting the optimal identification system or optimal authentication system for a given context.

Our research, including the development of a systematic selection methodology, aims to improve understandings of this efficacy phenomenon. Little is known about how APIMs are selected in practice and similarly there are no theories about the efficacy of such approaches. Equally, the extent to which a systematic methodology might or might not be efficacious for selecting APIMs is also unknown.

Next we discuss the research paradigms for conducting information system inquiries that influence the design of our research strategy.

4.1.5 Research Paradigms

Guba and Lincoln consider [124] that research paradigms, as basic belief systems, are based on ontological, epistemological and research methodological assumptions. Blaikie asserts [32] that ontology relates to the nature of what exists whereas epistemology is a theory or science of how knowledge is known, what can be known, together with criteria for judging the legitimacy of that knowledge. Ontological assumptions deal with questions about the form and the nature of reality, and, therefore, what is there that can be known about a phenomenon [71]. Epistemological assumptions relate to questions about the relationship between *the knower*, *the inquirer* and *what can be known* [71].

In general, research methodological assumptions relate to how the researcher can go about finding out whatever he or she believes can be known [124]. From the critical realist research paradigm, Dobson advises [83] that research inquiry needs to differentiate between the primary ontological assumptions and secondary epistemological assumptions, the former being intransitive and the latter being transitive in nature. Trauth argues [290] that epistemological assumptions for qualitative research in information systems should be separated from the research methodology pursued. Additionally, Hirschheim concludes [131] that all philosophical assumptions need to be exposed irrespective of qualitative or quantitative methodological base to support claims of valid research and valid research methodologies.

4.1.5.1 Research Paradigms for Information System Inquiries

The spectrum of philosophical assumptions shown in Table 4.1, adapted from Fitzgerald and Howcroft's *hard* versus *soft* treatise [100] using Creswell's definitions [70], represents the dichotomies of positivist and interpretive research paradigms. Quantitative and qualitative approaches, however, should not be construed as polar opposites but represent the extreme ends of the research design continuum [71].

Fitzgerald and Howcroft offer [100] four strategies for resolving these competing philosophical dichotomies in IS research:

HARD PERSPECTIVE	PHILOSOPHICAL QUESTIONS	SOFT PERSPECTIVE
Ontological Level	What is the nature of reality?	
Realist Belief that external world consists of pre-existing tangible structures, which exists independently of an individual's cognition.	versus	***Relativist*** Belief that multiple realities exist as subjective constructions of the mind. Socially transmitted terms direct how reality is perceived, which varies across languages and cultures.
Axiological Level	What is the role of values?	
Rigour Research characterised by hypothetico-deductive testing according to the positivist paradigm, with emphasis on internal validity through tight experimental control and quantitative techniques.	versus	***Relevance*** External validity of actual research question and its relevance to practice is vital, rather than constraining the focus to that by rigorous methods.
Epistemological Level	What is the criteria for constructing and evaluating knowledge?	
Objectivist Both possible and essential that researcher remains detached from the research situation. Neutral observation of reality must take place in the absence of any contaminating researcher values or biases.	versus	***Subjectivist*** Situation between the researcher and the research situation is collapsed. Research findings emerge from interaction between the researcher and research situation. The values and beliefs of researcher are central mediators.
Etic-Outsider-Objective Research orientation outside of researcher who is seen as objective and the appropriate analyst of research.	versus	***Emic-Insider-Subjective*** Research orientation centred on native insider's view, with the latter as the best judge of adequacy of research.
Methodological Level	What are the processes of research?	
Quantitative	versus	***Qualitative***
Confirmatory	versus	***Exploratory***
Laboratory	versus	***Field***
Deduction	versus	***Induction***
Nomothetic	versus	***Ideographic***

Table 4.1: Spectrum of Philosophical Assumptions adapted from Fitzgerald and Howcroft [100] and Creswell [70]

RESEARCH PHILOSOPHY	ONTOLOGICAL ASSUMPTIONS	EPISTEMOLOGICAL ASSUMPTIONS
Positivist	Assumes an objective physical and social world that exists independently of humans, and whose nature can be relatively unproblematically apprehended, characterised and measured.	Empirical testability of theories to be verified or falsified. The relationship between theory and practice is primarily technical and *value free*.
Interpretive	Emphasises the importance of subjective meanings and social-political as well as symbolic action in the processes through which humans construct and reconstruct their reality.	Understanding the social world involves getting inside the world of those generating it. The researchers, with their assumptions, beliefs, values and interests can never assume a *value-neutral* free stance.
Critical Realism	Social reality is historically constituted. Humans, organisations, and societies are not confined to existing in a particular state.	Knowledge is grounded in social and historical practices. There can be no theory independent collection and interpretation of data to conclusively prove or disprove a theory.

Table 4.2: Research Paradigms for IS Compared, adapted from Orlikowski and Baroudi [224] and Myers [213]

1. Isolationist strategy – operating strictly to a particular paradigm, which is mutually exclusive and exhaustive; or

2. Supremacy strategy – each research paradigm striving for supremacy; however, different approaches have strengths and weaknesses with usefulness being related to the nature of the inquiry; or

3. Integration strategy – merging of paradigms; however, this is problematical due to paradigm incommensurability. Merging paradigms may result in diluting a paradigm's particular strengths; or

4. Pluralist strategy – different paradigms are applied in a research situation allowing for a tool box approach where different methods could be used as appropriate.

Conversely, Orlikowski and Baroudi [224] refine the dichotomy of these philosophical assumptions, depicted Table 4.1, for IS research into the positivist, interpretive and critical realist paradigms. Their seminal work is based largely on the Chua's deliberations [51] into researching accounting problems. Table 4.2, adapted from Orlikowski and Baroudi's work [224] and Myers subsequent efforts [213], represents the diversity in research design and the philosophical questions for IS researchers to consider in order to establish their methodological base.

Positivists believe that reality is *value free* whereas interpretive paradigm assumes that reality is *value laden* [71, 100]. The *value aware* critical realist stance is that there is a real-world to discover even though it is imperfectly apprehensible [198]. The positivist research paradigm is appropriate for inquiries where researchers typically formulate propositions that portray the subject matter in terms of independent variables, dependent variables and the relationships between them [213]. The development and use of IS in and by organisations, however, are intrinsically embedded in social contexts [7].

The aim of all interpretive research is to understand how members of a social group, through their participation in social processes, enact their particular realities and endow them with meaning, and to show how these meanings, beliefs and intentions of the members help to constitute their social action [224].

Critical realists believe that a participant's perception is just one window through to the picture of reality, which can be formulated with other participants' perceptions and other forms of evidence [127]. The positivist and interpretive paradigms aim to predict and explain the phenomenon, whereas the critical realist researcher aims to critically evaluate, model and possibly transform the social reality under investigation [224].

Trauth and Howcroft consider [292] the critical research paradigm in IS is useful for inquiries that seek to reveal in-depth insights of power dynamics and underlying politics between stakeholders. Critical realism is relevant for constructing theories with the aim of explaining how and why events happened as they did, for example on a failed IT project [211]. Gregor warns [121], however, any ascriptions of causality have to be made with extreme caution.

Publications from the IS research community are predominantly positivist [116, 292, 213]; however, there are calls to increase qualitative research to obtain scientific knowledge to account for the subject matter in the real-world [50, 117]. Alavi and Carlson believe [7] the progress in the IS research field is enhanced by adopting a plurality of research perspectives in order to gain insight into complex information systems. An understanding of the way we can constitute the phenomenon in different ways, on the basis of alternative paradigms, provides one means through which we can make sense of the phenomenon [181].

Mingers suggests [205] that for any piece of research, even one in which a tightly drawn research question implies a particular method, thought should be given to a range of factors in the situation (including the predilections and experience of the researcher) and the extent to which other methods may add to the richness and validity of the results. Niehaves argues

[219] that in order to answer questions regarding the combining of research methods in the context of multi-method research, it is important to analyse the epistemological assumptions of the research methods themselves.

Myers concludes [213], referencing Lee's observations [183], that while the research epistemologies are philosophically distinct, as ideal types, the practice of research in these distinctions is not so clear-cut. He suggests [213] that there is considerable disagreement as to whether these *research paradigms* are necessarily opposed or can be accommodated within one study.

4.1.5.2 Research Paradigms in InfoSec Inquiries

Coles-Kemp argues [61] that the paradigmatic foundations of what constitutes *valid knowledge* for the InfoSec discipline, through lack of organisational and social theories, is in need of further research effort. InfoSec research needs to extend beyond technological considerations into understanding the socio-organisational perspectives surrounding the secure use of information systems [80].

As the InfoSec community's interest in philosophical and methodological assumptions does not seem to have kept pace with that of the IS community [61], we draw, therefore, on InfoSec's parent IS discipline and the work of Orlikowski and Baroudi as our philosophical base. We believe, however, that InfoSec research could adopt alternative philosophies from other parent disciplines.

4.1.6 Our Philosophical Orientation

Our philosophical orientation leans towards the *critical realism research paradigm*, which is commensurate with our inquiry to gain an *in-depth* insight into the decision-making on APIMs. Nevertheless, we are not so entrenched in our philosophical stance, with strong positive or negative dogma, so as to discard the contributions to knowledge from other philosophical paradigms. We recognise that we need a pluralist strategy and to accommodate different *research paradigms* in order to address our four research questions. We employ a pluralist strategy by adopting two different research paradigms.

We employ the interpretive paradigm in order to construct our systematic methodology to represent discipline experts' *know-how* to primarily answer our second research question.

Our research strategy also employs the interpretative *emic* research paradigm in order to answer our first and third research questions, which are exploratory in nature.

For the final research question we employ a critical realist research paradigm in order to gain *in-depth* insights on underlying power mechanisms that influence organisational approaches to selecting APIMs. Here, we adopt an *etic* outsider objective stance as we are interested in the participant's perceptions of the methodological regularities to select APIMs. Epistemologically, our main inquiry is inclined towards the critical realist scientific paradigm to develop explanations and to build theories relating to the research problem.

Maxwell explains [198] that qualitative study, adopting a critical realist perspective, seeks to understand the processes, the meanings and local contextual influences involved with the phenomenon of interest, for the specific setting or individuals studied. In general, a critical realist evaluation approach in IS attends to how and why an IS initiative has the potential to cause the (desired) changes and seeks to understand for whom and in what circumstances (contexts) an IS initiative works through the study of contextual conditioning [44].

We adopted the critical realist research paradigm because we aimed to critically evaluate the processes in a programme and the extent of their efficacy to select the optimal APIM for a given application context.

4.1.7 Research Strategy

Blaikie advises [32] that the choice of research strategy depends primarily upon the different ways to answer research questions through introductive, deductive, retroductive, and abductive logical reasoning.

We chose to adopt a retroductive research strategy based upon our review of Blaikie's explanations [32], as categorised in Table 4.3, and our analysis of our research questions. We commenced our inquiry into methodological efficacy by observing the regularities of processes in programmes to select APIMs. We used Pawson and Tilley's causal model [233] as a framework to analyse our acquired data in order to assist us to locate the real underlying mechanisms or *causal powers* responsible for a programme's selection of a particular APIM. We describe their causal model in the next sub-section.

Our inquiry, in line with the retroductive research strategy, was to search for consequences as a result of a mechanism's existence in a programme's selection of an APIM. These

	Inductive	**Deductive**	**Retroductive**	**Abductive**
Aim:	To establish universal generalisations to be used as pattern explanations	To test theories, to eliminate false ones and corroborate the survivor	To discover underlying mechanisms to explain observed regularities	To describe and understand social life in terms of social actors' motives and understanding
Start:	Accumulate data or observations	Identify a regularity to be explained	Document and model a regularity	Discover everyday lay concepts, meanings and motives
Goal:	Produce generalisations	Construct a theory and deduce hypotheses	Construct a hypothetical model of a mechanism	Produce a technical account from lay accounts
Finish:	Use these *laws* as patterns to explain further observations	Test the hypotheses by matching them with data	Find the real mechanism by observation and/or experiment	Develop a theory and test it iteratively

Table 4.3: The Logics of the Four Research Strategies Blaikie [31]

consequences were identified in our data which came primarily from observations made by individuals involved with these programmes. We aimed to acquire qualitative data which could assist us to observe the regularities in the programmes' approaches to introduce or revise an APIM. Retroductive reasoning differs from inductive logic in that it is used to work back from observations towards explanations [32]. We also aimed to discover and explain the underlying mechanisms that influence the programmes' decisions on APIMs.

We aimed to build plausible theories on the efficacy of methodologies to select APIMs based upon from our analysis of the data acquired, in line with our philosophical stance and research strategy. We believe there can be no data or application context that will either conclusively prove or disprove resulting theories on the efficacy of a methodology to select the optimal APIM for a given application context.

4.1.8 Analytical Framework

We utilised Pawson and Tilley's evaluation causal model [233], shown in Figure 4.2, as our framework to analyse the data acquired from our research inquiry. Pawson and Tilley explain [233] the logic of realistic evaluation research as:

> *"The task of inquiry is to explain interesting, puzzling, socially significant Regularities (R). Explanation takes the form of positing some underlying Mechanism (M), which generates regularity and thus consists of propositions about how the*

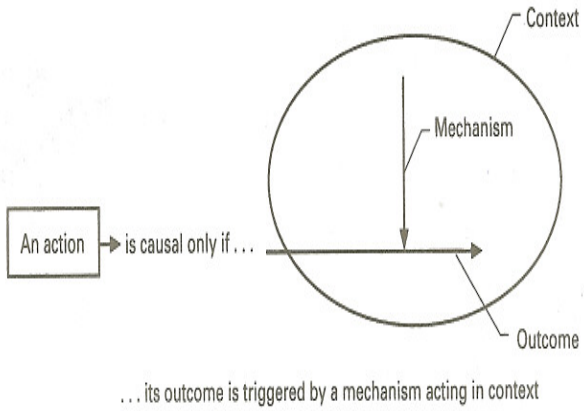

Figure 4.2: Pawson and Tilley's Generative Causation Model [233]

> *interplay between structure and agency has constituted the regularity. Within the realist investigation there is also investigation of how such mechanisms are contingent and conditional, and thus only fired in particular local, historical or institutional Contexts (C).*"

We use the term *underlying mechanism* to mean the underlying 'generative causation structures' that work in generating patterns of behaviour, during programmes to select or revise an APIM.

Our research task was to identify the nature of these *underlying mechanisms* which produce APIM deployment outcomes, within the contextual conditions investigated. We also introduced our systematic methodology as an *intervention mechanism*, to determine the impact on observed regularities and effects in terms (if any) on these underlying mechanisms and the eventual outcomes.

This analytical framework enabled us to identify surrounding circumstances when a systematic methodology is efficacious and also to explain the extent of that efficacy.

4.1.9 Justification for the Case Study Research Methodology

The nature of our empirical inquiry led us to set two preconditions, related to the types of cases and the data collection method, in order to reduce the candidate research methodologies for our qualitative inquiry.

Firstly, we wanted to gather data on cases where decisions on an APIM had already taken place. Therefore, we would not be able to record our observations of events as they happened in an IS programme. We would rely on documentary evidence and interviews as our data collection sources to analyse an IS programme retrospectively. Secondly, we were not interested in using participant observation as a method of collecting data because we were not interested in people's behaviour or interactions in a social group.

Ethnographical research is suited to providing IS researchers with rich insights into the human, social and organisational aspects of an IS through gaining a deep understanding of what people do and say what they are doing, over an extended period of time [212]. We, therefore, discounted research approaches to study social life and cultural practices of communities, such as ethnographical, phenomenological or narrative research, as the focus of our inquiry concentrates on processes and organisational decision-making. Our preconditions led us to consider case study, grounded theory and action research as candidate research methodologies to conduct our empirical inquiry.

Lee argues [183] that case studies can be used as natural experiments, to demonstrate both subjectivist and objectivist schools of thought and multiple tests of a theory. He suggests that case studies can be performed through either natural experiments or other types of experiments, to enhance *degrees of freedom* and, hence generalisation. We recognised that we could use the case study methodology for inquiring into decisions on deployed APIMs and also as a natural experiment in a case using our systematic methodology. Our selection of the case study research methodology in order to conduct our empirical research was a reasonably straightforward decision.

While our preference was to use one research methodology we borrowed techniques, such as qualitative data coding method [259, 104, 253] from the grounded theory research methodology [47], to analyse our data. We also borrowed some of the research protocols that are applied when conducting action research methodology for our case study involving the use of our systematic methodology.

The characteristics of the two other short-listed research methodology candidates are also described in this sub-section for completeness.

4.1.9.1 Case Study Candidate

Case study research methodology involves the researcher exploring the depth of a programme, event, activity, or one or more individuals, which are bounded by time and activity [71].

Yin advises [330] that case study research methodology is most relevant when:

- the research inquiry is posed in the form of *how* or *why* questions;
- the researcher has no control over actual behaviour or events; and
- the focus is on contemporary events rather than historical events.

We considered that our inquiry met all of Yin's criteria [330] and that it involved several organisations and their representatives to acquire data relating to the phenomenon. Myers recommends [213] that for case study research in the business environment that empirical evidence are acquired from one or more organisations. Multiple sources of evidence should be explored, although most of the evidence, he acknowledges [213], comes from interviews and documents.

We adopted the case study research methodology mainly because; as Maxwell argues [198], the unique context of each case is retained and data are interpreted within that context provides an account of a particular instance or event. Our inquiry was event driven in that we sought cases where decisions on APIMs had already been made, in order to take a retrospective view on the programmes' processes and practitioners' activities to ascertain the outcomes of the APIM deployments. We also needed a case study where we could utilise our systematic methodology in order to validate it using empirical data and to acquire data relating to the extent of its methodological efficacy.

Case study research, therefore, not only enabled us to validate the systematic methodology but most importantly to generate data on the efficacy of the approaches adopted, the underlying mechanisms at play and their impact upon the deployment outcomes. We were also conscious of the limitations of case study research to produce generalisations; however, our aim was to produce plausible theories rather than irrefutable generalisations.

Case study research concentrates on the quality of theoretical analysis and intensive investigation of a few cases, i.e. analytical generalisation, rather than statistical generalisation of many cases [305, 198]. Our in-depth inquiry into the phenomenon of interest was studied using three cases in context. We adhered to Cunningham's principles [73] by conducting intensive inquiry which aimed to develop plausible theories from contextualised evidence rather than trying to identify generalisations through excessive internal or external validation sampling. We developed our theoretical case sampling strategy based upon our classification of the APIM's application context, as defined in Section 2.4.4.

We explain our reasons for discounting two other research methodologies.

4.1.9.2 Grounded Theory Candidate

Grounded theory is a strategy of inquiry in which the researcher derives a general, abstract theory of a process, action or interaction grounded in the views of participants [71].

Grounded theory is particularly suitable for researching unfamiliar situations where there has been little previous research on which to develop a theory [305]. Myers proposes [213] two criteria by which grounded theory may be considered as an applicable approach, which relate to the rigour and validity of the data analysis and also the extent to which the researcher may produce a theory.

We considered grounded theory to be an inappropriate research methodology for our research inquiry because the literature provides a foundation upon which we are able to address our exploratory research questions. Nevertheless, we used the qualitative coding methods of grounded theory in our data analysis to develop our theories on our research problem.

Also, our planned use of the systematic methodology in one real-world scenario meant that while claims of plausibility could be argued, from one critical case study, we wanted to be able to counter possible challenges of validity and reliability, due to insufficient sample size, by using theoretical sampling from other case studies using alternatives approaches.

4.1.9.3 Action Research Candidate

Action Research combines theory and practice through cyclical diagnosis, action intervention and change reflection in an immediate problematic situation, with practitioners, in a mutually

acceptable framework [19]. Action research requires the researcher to immerse themselves with the case subject matter being studied and liaising with the participants to analyse what practitioners say what they will do and what is actually done and then analysing data acquired using several reflective modes [200].

The dangers of using action research are often that researchers can become too embroiled in the problem setting. The interactions with practitioners may become complex, with the researcher possibly being viewed or utilised inappropriately as a consultant [265]. Consequently, the research aims become blurred, with the result that the researcher often falls short of meeting their research aims to develop knowledge and create theories [25, 213]. We also identified the risk that our systematic methodology could be flawed or deficient to be used in a real-world context and, therefore, it needed prior empirical validation.

4.1.10 Research Project Constraints

Empirical research into information security in organisations often encounter constraints relating to the access to confidential documentary evidence, due to their commercial sensitivity, and also to conduct interviews with practitioners, due to their limited availability. Equally, a new systematic methodology is unlikely to be used by an organisation to make real decisions, until such times that the efficacy of that methodology is validated or demonstrated in practice.

For these reasons and with possibly other contextual constraints, the opportunities for researchers to try out their theories or inventions in real-world contexts with organisations are often few and far between. The use of a systematic methodology could affect the organisation's security controls, adversely impact resource costs and possibly damage personal reputations. While a researcher may learn from errors by applying a theory or methodology in real-world contexts, the benefits to organisations may not be so rewarding. Such interventions may cause unintended deleterious consequences for both parties.

Organisations with intractable business problems and the absence of systematic methodologies to address their APIM selection problems, however, may be willing to explore the use of an innovative methodology, even if it is to demonstrate transparency or due diligence in their attempt to identify the optimal APIM for their intended business purpose.

4.1.11 Our Research Implementation Plan

In view of the constraints identified above, we developed a research implementation plan for conducting our inquiry into two contemporary case studies initially, where decisions on APIMs had already been made, before finally using our systematic selection methodology in a real-world situation. Our research implementation plan, with its four stages, is shown in Figure 4.3. Stage A involved the identification of the factors for evaluating APIMs and the creation of the criteria questions to acquire the relevant data from the application context. This stage also involved the initial design of an evaluative framework and the steps in our method to select the optimal APIM.

Stage B involved the acquisition of data from our first retrospective case study which was used to validate our identified factors. These data were also used to identify the proficiencies and deficiencies of the approach pursued by the IS programme.

Stage C involved the acquisition of data from our second retrospective case study which was used to further validate our identified factors. These data were also used to identify the proficiencies and deficiencies of the approach pursued by the IS programme.

These retrospective case studies involved the analysis of historical accounts of the events that happened during a programme which lead to the selection of the APIM. The data acquired enabled us to identify the explanatory reasons as to why a particular APIM was selected.

Stage D involved the inaugural use of our systematic methodology during a real-world project to select the optimal APIM. The data gathered in this third case study enabled us to validate the components, including our factors, of our systematic methodology. The data acquired enabled us to identify the circumstances when a systematic methodology may be efficacious for selecting the optimal APIM.

We developed a means to determine whether a candidate case study was appropriate for our empirical research, as framed by our research questions. We justify our selection of our case studies in Section 4.3.

4.1.12 Criteria for Selecting Appropriate Case Studies

Yin advises [330] that it is important to have sufficient access to potential data, whether to interview people, review documents, or make observations in the field and select cases that

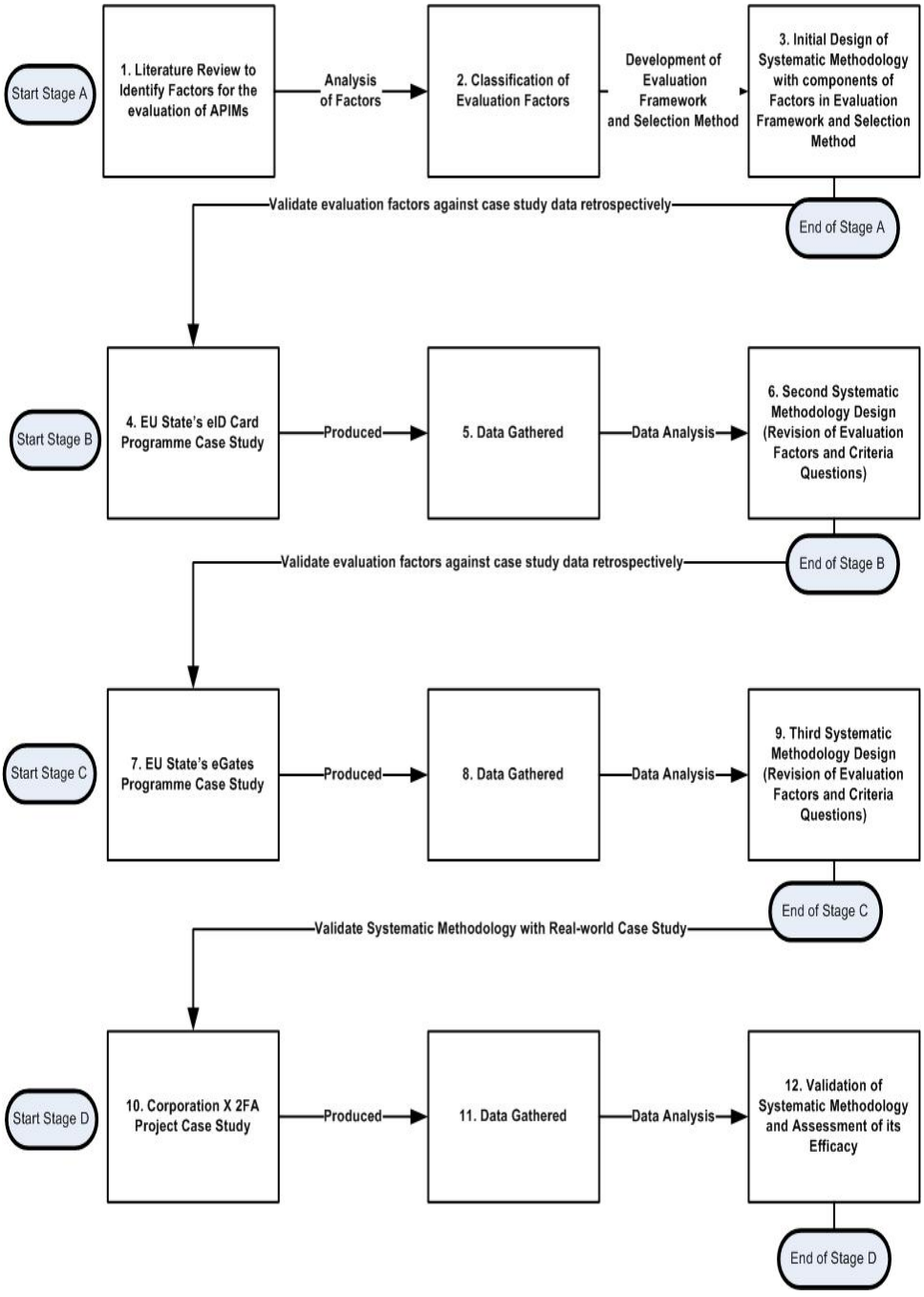

Figure 4.3: Our Research Implementation Plan

will most likely illuminate the research questions.

We consider that access to data, particularly sensitive information relating to major decisions and stakeholders' risks, is fundamental to our empirical research inquiry. In line with our research implementation plan we needed to select two retrospective case studies and also to identify an organisation which would be prepared to use our systematic methodology to select their APIM.

We examined the suitability of retrospective case studies, involving the selection of an APIM, based upon the following criteria:

1. Documentary evidence of adequate depth and breadth on the IS programme was available in the public domain which had been generated by the IS programme's stakeholder sources and also review publications from the indigenous scientific community;
2. Individuals involved in the IS programme who were willing to explain their role, describe their programme deliverables and provide their retrospective insights on the outcomes of the programme during an interview; and
3. Individuals who were willing to share their experiences of using the deployed APIM in an interview.

Different criteria were applied for selecting the case study involving an organisation's use our systematic methodology to select their APIM. McNiff and Whitehead recommend [200] that conditions for research interventions in the real-world should be articulated and agreed, with formal consent, by both parties at the outset. These conditions ensure the rationale of the intervention is fully understood and, where possible, knowledge of the possible consequences of the course of actions pursued is acknowledged in advance.

Our primary criterion was to obtain an organisation's consent for our research intervention. Secondly, we needed to ensure that we would be able to comply with the terms of that consent for our research inquiry. We needed provisions in the agreement to ensure that we could interview and correspond with programme team members and also be allowed access to data relevant for our inquiry. We discuss the consent issues relating to our investigations in Section 4.6.2.

Our theoretical case sampling strategy aimed to study one case from each of the three governance frameworks types (enterprise, federated and heterogeneous) described in Section

2.4.4. We believed that stakeholder trust relationships in the different type of governance frameworks played a significant part in the selection of an APIM.

In order to illuminate our research questions, we identified three case studies which had the potential to generate rich sets of data for our analysis. We justify the selection of our three case studies in Section 4.3.

4.2 Utilising the Case Study Research Methodology

In this section we provide an overview of the risks and limitations associated with conducting inquiries using the case study research methodology. We also outline our actions to ensure validity and reliability of our qualitative research inquiry. Finally, we provide a justification for the case studies chosen for our inquiry.

4.2.1 Risks of Case Study Research Methodology

Yin warns [330] that while contemporary behaviours and events can be advantageous to generate *natural* empirical data there are risks and limitations in selecting case study, as a research methodology.

There is a risk that potential interviewees may change their minds regarding their consent to participate in research or documentary evidence may not be released by organisations for inquiry [265]. We also identified the need to obtain commitment from an organisation and their representatives to use our systematic methodology for selecting an APIM for their application context. We also identified a significant risk that the organisation may curtail the use of our systematic methodology if the period of study became protracted. We reduced these research risks by assessing each candidate case study against three considerations:-

- The probability of gaining access to documentary evidence not only in terms of breadth but depth of coverage, e.g. specifications or official tender notices.
- The probability of recruiting a sufficient number of practitioners who were prepared *to agree in principle* to be interviewed.
- The probability of gaining organisation approval to use the systematic methodology for a programme to introduce or revise an APIM from the project's inception until its

completion.

For the case study involving the real-world usage of our systematic selection methodology we thought it necessary to search for a gatekeeper, as defined by Silverman [265], who had experience of managing processes relating to decisions on an identification system or an authentication system.

4.2.2 Assessing Case Study Research Quality

This sub-section describes the criteria by which we assessed the quality of the case study research. Case study research may be performed using the positivist, the interpretive and the critical realist approach. Each research paradigm adopts different approaches to assess the quality of case study research; therefore, we limit our discussion on the reliability and validity of our research design to the critical realist research paradigm.

Yin's primary criterion [330] for judging the reliability of research designs for case studies stipulates that the inquiry needs to demonstrate that the operations of the study, such as data collection processes, can be repeated, with the same results. The goal of the reliability criterion is to minimise errors and biases in a study [330]. Reliability may be enhanced by researchers using tactics, such as documenting their procedures during data collection and also developing a case study database in order to analyse acquired data.

Maxwell argues [198] that qualitative research from a critical realist approach should use the following criteria upon which to assess its validity:

1. Descriptive Validity – absence of fabrication or distortion of personal accounts or errors in interview transcriptions;
2. Interpretive Validity – comprehend the phenomenon not on the basis of the researcher's perspective but that of the participants within the context; and
3. Theoretical Validity – refers to an account's function as a theory, comprising concepts and their interrelationships, of some phenomenon.

Healy and Perry [127] offer similar criteria, shown in Table 4.4, to assess the applicability and the quality of the case study research methodology for inquiries based upon the critical realist paradigm. Based upon the above recommendations for judging the quality of our

Criteria	**Description of Criteria**	**Case Study Techniques**
1. Ontology Ontological Appropriateness	Research problem deals with complex social science phenomenon involving reflective people.	Selection of research problem, for example, is a how and why problem.
2. Ontology Contingent Validity	Open fuzzy boundary systems involving generative mechanisms rather than direct cause-and-effect.	Theoretical and literal replication, with *in-depth* questions, emphasis on *why* issues, contextual description of the cases.
1. Epistemology Multiple perceptions of participants and of peer researchers	Neither value free nor value laden, rather value aware.	Multiple interviews, supporting evidence, broad questions before probes and data triangulation. Self-description and awareness of own values. Published reports for peer reviews.
1. Methodological Trustworthiness	Extent to which research can be audited. It is consistent and data are reliable.	Case study database, use in the report of relevant quotations and matrices that can summarise data, and of descriptions of procedures, e.g. case study selection and interview procedures.
2. Methodological Analytic Generalisation	Analytic generalisation (that is, theory building) before statistical generalisation (theory testing).	Identify research issues before data collection, to formulate an interview protocol that will provide data.
3. Methodological Construct Validity	How well the information about constructs in the theory being built are measured.	Use of prior theory, case study database, and triangulation.

Table 4.4: Applicability of Case Study Inquiry within the Critical Realist Paradigm Healy and Perry [127]

research design, we introduced tactics, described in the following sub-sections, into our data collection methods and data analysis techniques in order to ensure the reliability and validity of our research.

4.2.2.1 Reliability Tactics

We documented our processes and protocols for the collection of our data from our three case studies. The two retrospective case studies involved the recording of semi-structured interviews where the interviewees were briefed in advanced in respect of the purpose of the interviews and the intended research questions. We also documented our processes for locating documentary evidence in the public domain.

We developed a DSS which was used as a database to store acquired data from each of our three case studies.

4.2.2.2 Descriptive Validity Tactics

In order to ensure descriptive validity, we collected data from published material from genuine sources and from information in official web sites. Interviewees also furnished us with internal programme material, which was authorised for disclosure to us for our research but not made public. As far as we could ascertain the documentary evidence which originated from official sources was considered to be authentic.

We also conducted semi-structured interviews with participants involved in the programmes to select an APIM. The questions were posed in such a way so that interviewees described the events which occurred during the programme, recounted the programme's outcomes and explained their views on the approach pursued by the programme.

Questionnaires containing a briefing on our research were provided to most interviewees in advance of the interview session. This tactic was intended to ensure that the interviewee understood the question in the manner intended in relationship to their role in the programme. All interview transcripts were returned to interviewees to obtain their agreement as to the accuracy of our interview transcriptions. The data collection techniques and case study protocols are described in detail later in this chapter.

4.2.2.3 Interpretative Validity Tactics

For interpretative validity, the analytical codes relating to the factors for evaluating application contexts were formulated from our review of the literature. These codes were validated by searching for their existence in the data, i.e. 'grounded', acquired from our three case studies. We identified further analytical codes in our case study data which were not contained in the literature. Our data coding activities also enabled us to identify new factors for evaluating APIMs.

We could not use the *inter-appraiser* reliability check, as recommended by Silverman [265], to ensure validity of our interpretation of these codes, because we were unable to recruit other willing researchers familiar with coding qualitative data.

As critical realism relies upon the participants' views and not those of the researcher interviewer's comprehension to demonstrate interpretative validity, we needed to adopt an approach to ensure that our bias was minimal. It was important that the interviewee was aware that their opinion was paramount. Therefore, the interviewee was informed, during the consent negotiation, about the purpose and the complete data gathering and transcript validation processes prior to the interview. The interviewees were also informed that the interview would be recorded and transcribed for their review.

We informed the interviewees that they could delete parts of the transcript, if it might possibly reveal their identity or expose confidential information inadvertently. Importantly, to assist interpretative validity, we advised the interviewees that they could amend the transcript to reduce the ambiguities of their utterances during the recorded interview session. They were also advised that they could add further information to the transcript to clarify points made or if they subsequently remembered other pertinent details relating to their comments.

This strategy not only reduced the difficulties associated with interviewees' recall capabilities but also ensured the accuracy of their account and minimised the risk of our misunderstanding their comments. Where relevant, we also reviewed the data from documentary sources to further validate the data gathered from interviewees.

4.2.2.4 Theoretical Generalisation Tactics

Yin argues [330] that case study designs should aim towards analytical generalisation, to align with the theoretical propositions, rather than statistical generalisation involving *sampling units* where inference is made about a population or universe. In turn, theoretically defined purposive sampling demands that researchers think critically about the parameters of the candidate case study against the research questions, the theoretical propositions and the explanations which are under development [265].

We selected theoretically driven case studies rather than inquiring into random or representative samples. Our supposition was that methodological efficacy is influenced by the type of APIM governance framework and the nature of the trust relationships between the stakeholders. Our aim, therefore, was to study at least one case in each of the three APIM governance framework types, e.g. enterprise, federated and heterogeneous, as defined in Section 2.4.4. This strategy of pursuing theoretically driven sampling enabled us to conduct *in context analyses* and also *cross-case analyses* in order for us to build our theories.

4.2.2.5 Improving Construct Validity

Construct validity refers to how well information about the constructs in a theory are assessed in the research [127].

Yin argues [330] that potential problems with construct validity can be minimised by using multiple sources of evidence to provide multiple measures, e.g. data triangulation of the same phenomenon. Silverman warns [265], however, that even using a single analytical model can be tricky in arriving at an overall 'truth'.

While we used multiple data sources and validation procedures our strategy was to ensure that we had a variety of views to compare and contrast as to how each individual experienced the processes in selecting an APIM. Therefore, we were not trying to improve the accuracy of data collected in order to construct *one correct picture of reality*.

Maxwell argues [198] that declarations of contributions to knowledge, based on empirical research context related evidence, depend on:

1. how the fact was obtained;

2. its plausibility for alternative claims; and
3. that there must be an explanatory connection between the fact and the claim.

We aimed to not only interpret the documentary evidences' content in literal terms but also discover the meanings and intentions of the data evidence gathered. Where possible we used multiple sources of data to construct various views of the phenomenon under investigation in order to discover alternative interpretations of the data acquired. This strategy in turn helped us to construct our understandings of the underlying mechanisms that influenced stakeholders' decisions. From the case study data sets we developed explanations on the efficacy of approaches practiced together with that from using a systematic methodology in order for us to build plausible theories.

In line with Yin's recommendations [330], the key informant in the third case study, in which we employed our systematic methodology, reviewed a draft of our case study report in order to improve research construct validity.

Gallier's conclusion [116] on attitudes towards contributions to knowledge is succinctly expressed as follows:

> *"We are thus led to the conclusion that the proper attitude for the creation of knowledge is neither of dogmatism of apprehension or comprehension nor of utter scepticism, but an attitude of partial scepticism in which the knowledge is held provisionally to be tested against apprehensions, and vice versa."*

Our modest expectations were to build initial plausible theories on the efficacy of systematic methodologies based upon our tentative suppositions.

4.3 Justification for the Case Studies Selected

Our case study selection criteria, defined in Section 4.1.12, and our research quality criteria, specified in Section 4.2.2, meant that we were required to review many IS programmes involving APIMs when selecting our case studies. These IS programmes ranged from national identification schemes to university campus cards for students.

Our search principally involved networking amongst colleagues in the security industry in order to approach organisations to seek their interest in participating in our research. As

expected, there were a number of programmes where our attempt to get formal approval from the appropriate organisational authorities to undertake a case study was not forthcoming. Equally, serendipity played an important part in our final selection; however, this fact should not be interpreted as meaning that these cases were 'inferior'.

The next sub-sections provide our justification for the three selected case studies. We refrain from explicitly identifying our case studies and the participants in order to protect the identity of the individuals and the organisations that contributed to our research. Ethical considerations relating to our research are discussed later in Section 4.6.

4.3.1 Case Study of an EU State's Electronic Identity Card Programme

We selected this case study because there were significant documentary evidence in the public domain relating to the issues surrounding this EU state's Electronic Identity (eID) card programme. These documents were mainly published by the state, through its Ministry of the Interior and regional governments, and by the indigenous academic community.

We also justify the selection of this case study because we were able to obtain consent to interview two prominent members of the programme team who were involved with the major decisions in the critical phases of the programme. Although we initially believed that it would relatively easy to locate and interview citizens who had gained experience of using their eID card for transactions, this assumption was erroneous. We later discovered, as we explain in Chapter 6 on the efficacy of the programmes's approach, that the on-line functionality of the eID card was under-utilised by citizens.

The programme was being publicly hailed by the state's representatives, particularly at the Security Document World and Biometrics Conference conventions during 2009 and 2010, as a *successful* deployment of a state eID card for its citizens. Presentations given by these representatives, responsible for managing the eID Card Programme, explained the business and technical issues that had been encountered and described how these problems were overcome by the programme.

We designated this case study as a federated governance framework type in that the state's Ministry of the Interior (MOI) was the sole issuing authority of the eID card, with many other organisations relying on the authentication capabilities of the eID card and its associated processes.

Our initial efforts using empirical data to validate our identified factors for evaluating APIMs and also our findings relating to the efficacy of the EU state's eID Card Programme's approach are described in Chapter 6.

4.3.2 Case Study of an EU State's eGates Border Control Programme

This second case study was selected because we were able interview several individuals who were involved in the eGates programme (either directly or indirectly, as an employee of a supplier of eGates). We were also able to interview passengers who used the eGates on a regular basis other types of automated border control facilities in other states. Additionally, there were several specifications relating to electronic passports and automated border control systems in the public domain.

From our preliminary investigations we located pertinent documentary evidence from the International Civil Aviation Organization (ICAO) relating to improving passenger facilitation and the use of Electronic Passports (ePassports) at border control crossings. We also found case study documentation on the use of ePassports in other EU states, which was published by the EU border control coordination agency Frontex. This state's border control agency also maintained a website containing general advice on the availability of the eGates to the travelling public.

We designated this case study as a heterogeneous governance framework type in that many EU member states issued ePassports to their citizens and equally there were many potential border control authority relying parties in the EU. There were immigration control authorities in other EU member states involved in automatically inspecting passengers' ePassports using eGates' systems. These authorities relied on the electronic authentication of these EU ePassports as part of their manual passenger inspection procedures.

Our efforts to further validate our factors for evaluating APIMs and also our findings relating to the efficacy of the eGates Programme's approach are described in Chapter 7.

4.3.3 Case Study of Corporation X's Two Factor Authentication Project

We considered this project to be a suitable case study candidate primarily because we gained formal consent from Corporation X's Director of Risks (DoR) in Asia to use our ASMSA Methodology for his project. Additionally, his commitment to collaborate in our research

and his interests in InfoSec methods were the key reasons for us to select this case to study. The 2FA Project was established to review Two Factor Authentication (2FA) solutions for verifying employees and agents of Corporation X.

The consent agreement contained clauses regarding the protection of Corporation X's commercially sensitive and confidential information. There was very little documentary data in the public domain; however, the DoR was enthusiastic to employ our systematic methodology because he claimed *"there was no in house IdM expertise"*. He confirmed that he was willing to commit his time and effort to interviews, reviews and exchange correspondence with us over the anticipated project period.

The terms of the consent agreement also described the case study protocol which restricted all communication to be channelled through a single point of contact between Corporation X's DoR and us. This communication restriction was considered necessary by Corporation X because the DoR wanted to ensure that all information was aggregated and approved in Corporation X before it was released to us. We considered, however, that the data released to us represented the organisation's consolidated views. The release of data from alternatives sources, particularly from other departments in Corporation X, would have enabled us to identify differences between the internal stakeholders perspective for an APIM. The terms of our consent agreement, however, meant that we were not afforded that opportunity. Notwithstanding this constraint, we considered that Corporation X's APIM project gave us a valuable opportunity to use our systematic methodology for a real-world problem.

The data acquired was mainly gathered through structured and semi-structured interviews and exchanges of emails, which also included corrections of documents produced by our ASMSA Decision Support System (ASMSA-DSS). Several semi-structured interviews were also employed to ascertain the DoR's reflective views from using our systematic methodology, particularly its efficacy in addressing the corporation's business problem.

We designated this case study as an enterprise governance framework type as Corporation X was the sole issuing authority and the only relying party.

This case study was used to further validate and refine the factors previously validated using the two retrospective case studies. This case study also generated data which enabled us to assess the efficacy of our systematic methodology from its *use* to select the optimal APIM in a real-world application context.

Our efforts to validate our systematic methodology and its components and also our findings relating to the efficacy of our methodology are described in Chapter 8.

4.4 Data Collection

This section describes the data collection strategy adopted for our inquiry and the rationale behind the strategy to meet the requirements of our two units of analysis to validate our systematic methodology and, most importantly to assess its efficacy. We also describe the data collection techniques used in our inquiry.

4.4.1 Data Collection Strategy

Our data collection strategy was formulated to acquire pertinent information from the literature and then use the data from each case study research iteratively as described in our research implementation plan.

Our examination of the literature assisted our efforts to:

1. identify the factors relating to the evaluation of an application context and candidate APIMs;
2. establish an initial systematic methodology comprising factors, with associated criteria questions, in an evaluation framework and a selection method; and
3. establish a set of criteria for assessing the efficacy of a methodology to select an APIM.

Our strategy was designed to commence with an examination of pertinent literature in order to acquire data to assist our efforts and understanding to answer our first three research questions. From our examination of the literature, we formulated an initial list of factors for evaluating APIMs [226] and we also created the inaugural version of our systematic methodology [227]. Our strategy was then to use the data from each case study iteratively for our two units of analysis.

We commenced with the EU state eID Card Programme Case Study, then continued with the EU state's eGates Programme Case Study and finally used the systematic methodology in the Corporation X's 2FA Project Case Study. The strategy was designed to validate our

factors in each retrospective case study and to then aggregate the learnings, iteratively, into the systematic methodology and our DSS. Our systematic methodology and its associated DSS were also refined following our analysis of its use in the Corporation X 2FA Project Case Study.

Empirical data from the case studies were used to validate and refine the factors to answer our first research question. These empirical data were also used to further the development of the systematic methodology so that we could answer our second research question. Data from the literature review and the retrospective case studies were used to establish the criteria to assess the efficacy of a methodology to select an APIM in order to answer our third research question.

Data from the Corporation X 2FA Project Case Study were used primarily to answer our fourth research question by assessing the efficacy of our systematic methodology to select an APIM. Our empirical data corpus was also analysed to identify patterns in application contexts so as to identify the circumstances as to when a systematic methodology is efficacious for selecting an APIM together with supporting reasons. Our data corpus also enabled us to identify those circumstances when a systematic methodology is not efficacious for selecting the optimal APIM.

4.4.2 Justification for Our Data Collection Strategy

We justify our data collection strategy on our anticipation that cumulating learnings from each case study iteratively would maximise the value of our research effort.

We also justify our data collection strategy because we considered that our systematic methodology needed to be validated, using the two retrospective case studies, in preparation for its use with a real-world case study. Our strategy was to validate the systematic methodology as far as possible with data from each retrospective case study before it would be used with a real-world evaluation.

The validation tasks mainly included verifying relevancy of the factors for evaluating APIMs, the criteria questions for acquiring data relating to factors and our methodology's selection method. This strategy was designed to minimise both the risks to the organisation arising from the systematic methodology being insufficiently robust for the intended evaluation and selection purposes. We also wanted to minimise the risk that an immature methodological

tool may have also jeopardised our research inquiry and our personal reputation.

4.4.3 Examination of the Literature

We examined the literature specifically covering issues surrounding identification and authentication deployments and also biometric deployments, from both theoretical and empirical sources, to identify an initial set of factors for evaluating APIMs.

In order to establish an initial systematic methodology we reviewed the general literature on evaluation frameworks, methodologies and methods. We also reviewed literature on decision-making, particularly, where there are multiple stakeholders' objectives and multiple criteria are to be used in the evaluation of candidate solution options. The guidance contained in the literature enabled us to establish criteria to assess the efficacy of decision-making strategies for APIMs.

We also examined the literature to gain a broad understanding on the IS development methodology issues, which we assumed would also be encountered in APIM programmes, e.g. agile methodology versus waterfall approach. We also reviewed literature on the management of stakeholder consultation processes, particularly Hemmati's Multiple Stakeholder Processes (MSPs) [128], designed to address conflicting stakeholders' objectives, as may be the case with APIMs.

4.4.4 Documentary Data

Documentary data, which included archival records, for the two retrospective case studies were gathered from multiple sources, including official government or quasi government agencies, academic sources, national and specialist industry press, and business related social networks to get a wide range of views.

There was much documentary evidence in the public domain relating to our two retrospective case studies. The types of documents included technical specifications, official public announcements, deployment progress reports, decrees and other legislation.

The strengths of using documentary evidence are that the data are stable allowing repeat analysis; unobtrusive in that data are not normally created for the case study; exact with intended references and the detail of coverage [330, 265]. We were aware, however, that our

inability to access confidential documents could potentially hinder our attempts to gain an understanding of any underlying mechanisms potentially influencing stakeholders' selection of an APIM. We were also conscious that some documentary evidence may be written with a bias for a particular purpose in order to manipulate audience perception.

4.4.5 Interviews

We briefly describe the types of interview, the number of interviews and how the interviewees were recruited.

We conducted three semi-structured interviews in our eID Card Programme Case Study. Two of our interviewees were introduced to us through mutual professional colleagues and the other interviewee was introduced through contacts in the academic community. We conducted eight semi-structured interviews in our eGates Programme Case Study. One of the interviewees who was working in the programme was known to us professionally and he introduced us to five other colleagues involved with that programme. The other two interviewees were our friends who had used the eGates recently as passengers.

We used semi-structured and structured interviews with the DoR in the Corporation X 2FA Project Case Study. The DoR was a professional colleague and friend, over several years, who asked us to assist him with his real-world business problem.

The strengths of undertaking interviews is that the research can focus directly on the research questions, through the case study, in order to gain insight and explanations from different perspectives [330]. The risks to gathering data through interviews include bias due to poorly articulated questions including leading questions, response bias, inaccuracies due to poor recall and reflectivity, with the interviewee attempting to provide answers that the interviewer wants to hear [330].

Our *in-depth* semi-structured interviews with practitioners normally lasted for a maximum period of one hour. Our interview questions were open-ended and we tried to follow the line of inquiry in a natural way by posing questions in a non-threatening manner. Our questions were posed carefully, as part of the case study protocol to avoid posing leading questions, in an attempt to allow the interviewee to provide their own respective narrative from their perspective of events and to give their personal opinion. Our questions were furnished to the interviewees in advance. During the interview, however, we had to slightly amend some

of the questions actually posed to correspond to the interviewee's role, previous answers supplied, and the dynamic nature of the dialogue.

The interviews on the Corporation X Case Study required a different approach. Questions from the established systematic methodology were used in a methodical, structured manner to acquire information about the application context from the interviewee. In contrast, semi-structured interviews were used to acquire the interviewee's opinion on the systematic methodology's efficacy and to elicit other thoughts on its processes in an open manner. We supplied the interviewee with an agenda that showed the types of questions and issues that would be discussed in the scheduled interview. Our initial interviews with the DoR were mainly conducted face-to-face. The Skype teleconference facility was used on all other occasions as the DoR was based in Malaysia.

We were conscious that the interviewees' responses in all three cases may be a reflection of their respective organisations' official policy or approved communication on matters relating to the case study rather than an expression of personal reflection or opinion. We assumed that our analysis of the transcripts would help to identify such biases. The removal of certain recorded utterances from the transcripts, by the interviewee, also suggested that the interviewee may have expressed their insights too frankly. As recommended by Coffey and Atkinson [60], we inspected the literal meaning of the interviewee's verbal utterances and also evaluated the function of that communication, as a chronicle of events, influences, decisions and their justifications.

The data contained in the interview transcripts formed the majority of our evidence for our data analysis.

4.4.6 Our Memos and Reflective Notes

In line with Richard's recommendations [253] we created memos based on our observations during the interview dialogue. We also wrote reflective notes to record our insights following the analysis of our acquired data. The memos acted as spontaneous informal records of thought as these ideas occurred. Conversely, reflective notes were created after careful deliberation of an issue or factual claim during our analysis.

Memos written during data collection activities serve as a significant source of information, as part of the data making process, in which the researcher records accounts of changes and

discoveries [253]. We used memos to record how we acquired our data, indicating possible influences that may have skewed the data, which should be taken into account when the data are being analysed. We also created memos about documents, particularly those documents that were not in the public domain. We also created reflective notes relating to contradictions between interviewee's accounts and documentary evidence.

These data provided us with the means to record identified disparities in evidence gathered in order to make independent judgments about the reliability of data gathered. These data also helped us to recognise power relationships amongst stakeholders in our case studies.

Next we discuss how the data collected were handled to facilitate analysis and to protect the integrity of the data acquired.

4.4.7 Special Treatment of Data Before Analysis

Several documents in the EU state's eID Card Programme Case Study were translated into English language using the Google translation facility. Where relevant, clarification on some phrases in the text was sought from fluent French speakers.

We used the AVS Audio Recorder Software version 3.9, running on our laptop computer with its integral microphone, to record all interviews in a variety of locations and environments. These recordings were saved into the MPEG-2 Audio Layer III (MP3) standard audio format, which we considered to be an adequate audio recording quality for our research purposes.

We also used the F4 Audio Transcription application software, freeware licensed by Dr. Dresing and Pehl GmBH [1] to assist in the production of the textual transcripts in Rich Text Formatted (RTF) files from audio recorded interviews in MP3 format. These transcription files were imported and saved in Microsoft Office Word 2007 file format.

The translations together with other documentary evidence, including the interview transcripts, were converted into the Portable Document Format (PDF) in order to protect the integrity of the data collected.

[1] http://www.audiotranskription.de

4.5 Data Analysis

In this section we describe our two units of analysis and the methods used to analyse our acquired data. We also describe the software tools that we employed to conduct our qualitative data analysis.

4.5.1 Units of Analysis

Patton defines [232] a unit of analysis as the main object being studied, which in social science includes processes, individuals and organisations (groups of individuals).

Our main unit of analysis was to *determine the extent to which a systematic methodology is efficacious for selecting the optimal APIM for a given application context*. The focus of our analysis is explanatory in that the analysis aimed to recognise patterns in our empirical data which identified the circumstances as to when, together with supporting reasons, a systematic methodology to select or revise an APIM is efficacious, and when it is not, for selecting the optimal APIM for an application context. We also reviewed the literature on information system development methodologies and decision-making strategies in order to not only establish criteria to assess efficacy of our systematic methodology in order to answer our third research question, but also to provide an analytical framework to answer our fourth and main research question.

This analysis necessitated the recognition of patterns in our data not only within each case study but also across our three data sets. The use of cross-case data analysis is not only useful for reassurance that events and processes are not idiosyncratic but also to assists to understand how they can be qualified by contextual conditions [203]. We used cross-case data analysis to identify common contextual conditions surrounding each case in order to identify when a systematic methodology is efficacious together with the contributory reasons. We developed our theories based upon the exemplary reasons identified.

Our secondary unit of analysis was *to establish and validate a systematic methodology designed to determine the optimal APIM for a given application context*. This unit of analysis addressed our first two research questions. Our research commenced by identifying and validating factors which should be evaluated in order to select the optimal APIM for a given application context. The validated factors formed the basis of our inquiry to address our second research question to establish how information pertaining to an application

context could be acquired and evaluated, using a systematic methodology, for the purpose of selecting the optimal APIM. This research question led us to review the literature on evaluation frameworks for our identified factors and also decision-making processes in methods in order to develop our systematic methodology.

4.5.2 Methods of Analysis

This sub-section describes our qualitative methods to analyse the case study data collected for our two main units of analysis.

Miles and Huberman argue [203] that qualitative data analysis comes down to three concurrent flows of activities consisting of:

1. data reduction;
2. data display; and
3. conclusion drawing and verification.

For our main unit of analysis in order to analyse our data we employed the qualitative data coding method, as defined by Richards [253] and Saldaña [259], which form the basis for grounded theory research [47]. The goal of qualitative data coding is to learn from the data collected, return repeatedly to extracts, until there is an identification of patterns, which can aid understanding and build explanations [253].

Friese describes [104] qualitative data coding in terms of descriptive level analysis and conceptual level analysis, the latter acting as input information into developing theories. Saldaña encourages [259] the commingling of the different types of coding, using a code weaving technique, to form analytical models relative to the research inquiry. Charmaz argues [47] that theoretical coding should follow descriptive and conceptual focused coding, which not only conceptualises the codes established but also moves the analytical story in a theoretical direction. She recommends [47] the use of memos, which we have labelled reflective notes to differentiate with data collection activities, to analyse data and record ideas to help develop concepts and theories.

We produced descriptive codes and process codes in our first analytical cycle in order to reduce our data. We then identified and labelled our conceptual codes in our second analytical

cycle. We used theoretical coding in our final analytical cycle to identify patterns in our conceptual codes in order to develop our theories.

4.5.2.1 Data Reduction

We commenced by coding the data for each case into descriptive and process codes in order to produce causal network diagrams. The causal network diagrams represented the dynamic nature of the programmes.

Our analysis involved producing a list of descriptive codes from analysing our data, as recommended by Friese [104], and then *grounding our factors* by comparing to the descriptive codes produced. We were not interested in establishing the frequency that these descriptive codes were mentioned in our data, as in content analysis. These analytical processes required a degree of interpretation because of the use of different terminology and meanings in our data corpus.

4.5.2.2 Data Modelling

We followed Saldaña's recommendations [259] by grouping our descriptive codes into categorises of conceptual codes. The analytical framework represented these conceptual codes as antecedent variables, intervening variables and outcomes variables. We decomposed Pawson and Tilley's causal model [233] and developed an analytical framework to represent these conceptual codes and the dynamics of a programme to select an APIM.

Miles and Huberman contend [203] that a causal network is a powerful instrument to display the most important independent and dependent variables, with the plot of the relationships being directional, rather than solely correlational, between these variables. As our analytical framework, we created a casual network diagram for each case study to represent the conditions surrounding a programme at its inception, the events that occurred and strategies pursued during the programme, the deployment outcomes from the programme's approach, and retrospective methodological insights from interviewees.

These representations assisted us to identify the underlying mechanisms which were mainly responsible for a programme's selection of a particular APIM.

4.5.2.3 Drawing and Verifying Conclusions

Charmaz contends [47] that coding is the pivotal link between collecting the data and developing an emergent theory to explain the acquired data. Myers defines [213] theoretical coding as the formulation of a theory, which is achieved by specifying explicit causal or correlational links between individual interpretative constructs.

The conceptual codes assisted us in identifying patterns within context and across context. The causal network diagrams also aided visibility of our data. From these patterns, we were able to identify explanations as to why certain circumstances and events in the programme produced certain output deployment patterns. We used our interviewees' retrospective insights as a means to verify the identified concepts and their linkages, which were represented in the causal network diagram produced for each case.

We used cross-case analysis on our three data sets using our causal network diagrams from each case study to identify patterns and links in our data. This cross-case analysis also included the use of our proposed efficacy criteria to compare and contrast the proficiencies and deficiencies of a systematic methodology with other approaches. We also used our reflective notes containing themes describing the patterns that we had identified during our coding of our data sets.

We then compared these patterns and explanations against the criteria developed to assess the efficacy of methodology to select an APIM. The exemplars recognised in the data helped formulate our initial theories on methodologies, their efficacy and the prevailing contextual conditions at the time of the programme's inception. Our conclusions and development of theories were established using theoretical coding in order to develop plausible explanations based upon the patterns recognised in our data.

For our secondary unit of analysis we needed a different approach in order to verify our systematic methodology using our acquired empirical data. We divided the textual data acquired which influenced the decisions on the deployment of the respective APIM into descriptive codes. We then validated our factors, identified originally from our review of the literature, by searching for their existence in the descriptive codes which we produced from analysing our case study data. We also used these descriptive code to identify new factors, to identify redundant factors and to validate our classification of that factor in its evaluation theme. These descriptive codes also assisted us in our efforts to validate the factors in terms of their descriptive label, their relevancy, their consistency and their completeness. We then

used our descriptive codes to identify *common factor themes* which we then compared to our existing evaluation themes.

We used the data from our third case study not only to validate our factors in the systematic methodology's evaluation framework but also to validate the systematic methodology itself. The data produced from its usage acted as input into our main unit of analysis.

4.5.3 Qualitative Research Tools Utilised

The nature of our inquiry required the following specialist application tools to store, to manipulate and categorise data and to generate various reports and diagrams:

1. Atlas.ti Computer-Aided Qualitative Data Analysis System (CAQDAS) application software version 6.2;
2. Our systematic methodology's Decision Support System prototype (ASMSA-DSS);

CAQDAS tools assist [274] qualitative researchers in the complexities of managing large data sets of mixed data types. These data support tools are designed specifically for researchers to assist them with the discovery and management of unrecognised ideas and concepts; the construction and exploration of explanatory links between the data and emergent ideas; and to create the fabric of argument and understanding [254]. Friese clarifies [104] that a CAQDAS tool does not, however, perform the analysis itself!

Following our consideration of the features of the main CAQDAS tools available, we selected the Atlas.ti tool to support our analytical coding tasks. We selected Atlas.ti tool drawing on Lewins and Silver's guidance [184] and also Lewis' assessment [185] of NVivo version 2.0 and Atlas.ti version 5.0. The conceptual underpinning of the Atlas.ti application is based upon the 'paper and pencil paradigm' and its intuitive design and many of its processes are based upon this analogy [104]. Atlas.ti's search facility and network diagram functionalities were the key deciding factors. This software tool was used primarily to address our main unit of analysis and to construct our causal network diagrams.

Our ASMSA-DSS was implemented as a representation of our systematic methodology. The system was developed using Microsoft Office Access 2007 version which contained a series of databases. Each table represented a conceptual theme and the fields within that table

represented the factors for evaluating APIMs. The interactive processes representing the steps in our systematic methodology's selection method are described briefly in Section 5.7.

Our DSS proved a useful instrument in validating our systematic methodology and also for analysing the large volume of data acquired from our three case studies.

4.6 Research Ethical Considerations

This section discusses our adherence to the research recommendations contained in the Royal Holloway, University of London's guidelines [229], which covers the ethical considerations and our responsibilities to the subjects involved in our research inquiry.

4.6.1 Protecting Subjects' Identity

We formulated a strategy to manage the ethical issues consistently for all our interactions with interviewee subjects and their organisations across all case studies. This strategy included the basis and terms of gaining informed consent from our interviewees, the acquisition of data, the use data of collected, and the subsequent disclosure of information.

Our strategy here was influenced by Royal Holloway's Open Access Publications Policy (OAPP) for research, which includes the publication of doctoral theses. We needed to establish a strategy that adhered to the Royal Holloway's policies yet protected the identity of the subjects involved in our inquiry.

Protection of the interviewees and their organisations' identity formed the basis of the consent obtained enabling us to engage with subjects in our three case studies. Therefore, in line with the consents established with the interviewees, we undertook to protect the confidentiality and integrity of all interview data gathered, all documentation furnished to us, and any reports produced from our inquiry, i.e. this thesis. Therefore, we anonymise the names of our interviewees and their organisations together with the case studies themselves in this thesis.

4.6.2 Informed Consent

Most subjects involved with the case studies were and remain our professional colleagues, or were introduced to us through a professional contact.

Informed consents were gained through email dialogue where we furnished the interviewee with the following information (where appropriate):

- a background to our research, the nature of assistance required and its purpose;
- an outline of how the interview would be conducted and the procedure for the interviewee to change the transcript for their final approval;
- a commitment to protect the identity of the interviewees and their organisations;
- an understanding that the interviewee would obtain authorisation for participating in the interview and to release documentary material that was not in the public domain;
- an expectation that we might need to communicate directly with the organisation to sign a Non-Disclosure Agreement;
- an expectation that permission to interview a subject may only be granted on the basis that any published transcript would need to be vetted, our agreement to anonymise the subjects' identities and to protect organisations' interests;
- a request that documentary evidence not in the public domain may be made available to us only in order to reduce the demands upon the interviewee's time; and
- a commitment to protect the confidentiality and integrity of the transcript data or other materials released by the interviewee.

There were several occasions in the two retrospective case studies where the interviewee did not seek their organisation's consent, in spite of our repeated requests. Despite the absence of consent the interviewees were content to be interviewed on the understanding that we protected their identity and that of their organisation. The interviewees were made explicitly aware that the data was to be used for our research purposes only. We also reaffirmed our commitment to protect their identity and the confidentiality of data gathered. This commitment formed the basis of mutual trust with our interviewees.

Our interviewees were furnished with an explanation of our inquiry, the motivation behind our research and our proposed interview questions in email correspondence several days in advance of the interview. We signed a NDA with the DoR of Corporation X after several amendments to their standard NDA's draft text. We were conscious that a balance needed to be struck between providing sufficient information to enable interviewees to understand the

purpose of the interview and influencing the interviewees to utter comments that supported our suppositions. We believe that interviewees were honest and were sufficiently comfortable to express themselves openly during our interview sessions. Our interview transcripts were compared to documentary data acquired and also examined against data acquired from other interview transcripts in order for us to corroborate each interview's account.

No financial rewards or inducements were offered to interviewees; however, several interviewees demonstrated their interest in the prototype DSS as a means of improving their own organisational information security review processes.

4.7 Summary of Chapter

In this chapter, we have described and justified our research methodology to address our research aims.

We have described the characteristics of the research problem and the research questions. We have also described the uncertainty surrounding the phenomenon of our inquiry. We have explained our leaning towards the critical realist research paradigm to conduct our inquiry. We have justified our selection of the case study research methodology. We have also described and justified our research strategy and outlined our research implementation plan.

We have set out criteria upon which we assessed and protected the quality of our research and the basis of our contributions to the body of knowledge which align with the realist evaluation paradigm. Descriptions of the data collection strategy and the case studies selected together with their justification have also been provided, together with a description of our procedures for gathering information. We have described our main and secondary units of analysis and the methods used to conduct our qualitative data analysis.

We have also provided a discussion on our endeavours to conduct our research and to report our findings ethically, not only to comply with the university's policies, but also to maintain our personal integrity amongst fellow researchers, colleagues and practitioners.

CHAPTER 5

The ASMSA Methodology

Contents

This chapter opens with our analysis of the problems to select the optimal APIM for a given application context. These problems motivated us to develop a systematic methodology to assist the decision-making processes. We describe our method to identify factors in order to evaluate APIMs and also provide the results of our efforts. We then describe how we used these identified factors as our basis upon which to develop our systematic methodology. We continue by providing an overview of the ASMSA Methodology, definitions of its terminology and a description of its concepts. We then describe the ASMSA Methodology's three components comprising ASMSA Evaluation Framework, factors in their evaluation themes, and the ASMSA Selection Method. We conclude by briefly describing the ASMSA Decision Support System which was developed to aid our empirical research.

5.1 Exploring Methodologies to Select APIMs

From our review of methodologies in the literature many contributions suggest [230, 38, 63, 27] that there is a need to explore alternative approaches for selecting APIMs. We consider that empirical inquiry is also needed to gain an understanding of current approaches and their efficacy to select the optimal APIM. Current approaches appear to rely on the skills and competencies of discipline experts rather than well-defined processes of a methodology. Exploration into approaches which contain well-defined processes, however, may help to inform current practices.

Our supposition is that a systematic methodology, providing structure and repeatable processes, may be more efficacious, in some circumstances, to select an APIM than other approaches. Systematic processes have the potential to help reduce inconsistencies due to variations in discipline experts' interpretations.

We believe that employing a systematic methodology with a selection method and a comprehensive range of criteria questions, in an evaluation framework, ensures that required data

are acquired from the application context and that data are evaluated methodically so that the optimal APIM can be identified. A systematic methodology may improve the consistency of evaluations and the accuracy of current practices to select the optimal APIM.

We consider the characteristics of the problems to evaluate and select an APIM for a given application context before we focus on our method to develop the ASMSA Methodology.

5.1.1 APIM Selection Problem Characteristics

Smithson and Hirschheim state [272] that Information System (IS) assessments are complex and demanding. We believe that the selection and configuration of APIMs are equally problematical because stakeholders' objectives are often driven by conflicting interests, incentives or motivations and the diversity of factors relating to an application context which require evaluation.

IS development programmes may not always be able to determine an agreed set of requirements for an APIM due to stakeholders' conflicting objectives. Additionally, we consider that the evaluation of an APIM is also complex, as highlighted by Farbey et al. [97] for evaluating information systems generally, because of the difficulties in measuring intangible benefits within Return On Investment (ROI) decisions.

Keeney et al. conclude [173] that decisions on information systems necessitate a single decision point which should attempt to accommodate conflicting objectives by establishing stakeholders' preferences. Some APIM programmes, such as the ID Card Programme in the United Arab Emirates [4], set up communication processes and structures in order to resolve conflict and disputes within a generic IS programme methodology. Royer concludes [257] that the complexities of decisions to select enterprise IdM systems necessitates the use of decision support tools.

An APIM may be considered as part of a security architecture to control risks associated with accessing organisation assets and resources. Organisational management of risks, in turn, attracts political, organisational and social issues [118]. Rannenberg proposes [245] that the use of evaluation criteria assists organisations to evaluate whether information systems fulfil a range of requirements, not only in terms of functionality, but also their security and usability effectiveness. These evaluation complexities may also be exacerbated because IS programmes are often forced to make many assumptions in respect of the application context,

the purpose for the APIM and the capabilities of various APIMs. We believe that decisions based on a diverse range of stakeholders' objectives and evaluation criteria may reduce some of these evaluation complexities, particularly where the data are imprecise due to incomplete, conflicting or non-accessible information.

Fuzzy decision-making methods for multiple objective decision-making are categorised by Lai and Hwang [179] according to the availability of preference information to the decision-maker:

1. no articulation of preference information;
2. a priori articulation of preference information;
3. progressive articulation of preference information; and
4. posterior articulation of preference information reached by an interactive method.

We consider that the APIM selection problem falls into Lai and Hwang's third category, in that the progressive articulation of preference information is required for decisions involving multiple stakeholders' objectives and multiple evaluation criteria. We believe that decisions on APIMs are founded upon too many assumptions and the lack of clear objectives and requirements for an APIM. We believe that a methodology should systematically acquire and record pertinent information relating to an application context, together with stakeholders' objectives and requirements for an APIM, in order to select the optimal APIM.

5.1.2 A Systematic Methodology for Selecting APIMs

We believe that the nature of the APIM selection problem suggests that a methodology, progressively obtaining stakeholders' preference information and data to reduce assumptions, within well-structured processes, is a valid decision strategy. Such a strategy should include iterative stages of evaluation with stakeholders in order to progressively gain sufficient insight into the personal automated identification problem for the application context.

White recommends [316] that methodologies should always incorporate feedback from stakeholders to validate any assumptions made in the decision-making processes. We believe that stakeholder feedback on articulated stakeholders' objectives and requirements for an APIM should assist IS programmes to produce unambiguous requirement specifications and explanatory statements to justify assumptions.

Patton advises [231] that qualitative evaluation methods are well-suited for disciplines that are developing, innovative or changing. We believe that automated personal identification is an emergent discipline which necessitates a systematic methodology to evaluate qualitative and qualitative data acquired from the application context and the candidate APIMs.

Our research plan was to identify which factors needed to be evaluated in order to select the optimal APIM for a given application before we commenced the construction of other components in our systematic methodology. We now describe our effort to address our first research question.

5.2 Identifying and Classifying Factors

This section describes our research method to identify an initial set of factors for evaluating and selecting an APIM. These research activities relate to the first two steps of our research implementation plan shown in Figure 4.3 on page 124. We then describe the results from our research efforts in this subsection. Our research method to classify these identified factors is then described in Section 5.2.2.

5.2.1 Method for Identifying Factors

Our method commenced by noting the factors expressed explicitly in methodological tools in the literature, some of which are reviewed in Section 3.3. We then identified factors contained in publications from standardisation bodies, e.g. NIST. We supplemented these identified factors by reviewing the security, usability and privacy literature relating to automated personal identification. We provide a discussion on these further identified factors in the next subsection.

We assigned a descriptive label to each identified factor and also constructed a criterion question for each factor. The purpose of a criterion question is to acquire subject data related to an identified factor. We elucidate on the relationship between these two concepts in Section 5.3.4.

We then examined the literature relating to a prominent, and often considered as controversial, programme to introduce an APIM for employees and contractors into United States of America (US) government departments. We scrutinized the issues raised by Karger

[171], surrounding the US Homeland Security Presidential Directive [300] and the Federal Employee Personal Identity Verification (PIV) Programme's Specification [98] in order to identify further factors. We chose to examine the literature relating to this programme because there were, at the time, many articles appearing in scientific publications, in professional community discussion forums and in the international press, which discussed the merits and drawbacks of introducing such an APIM into US government departments.

Our review of the literature relating to this programme helped to identify some of the implementation factors and issues encountered when an APIM is introduced into a particular user community. We concluded our method by reviewing Allendoerfer's comprehensive field surveys [8, 9]. These surveys assisted us to identify factors relating to usability issues that arise as a consequence of imposing multiple APIMs upon a user community.

5.2.2 Method for Classifying our Identified Factors

We collated these identified factors into a master list which we then classified into 18 factor groups. These 18 groups were then classified into three perspectives.

Each factor group represented a conceptual theme, e.g. reliability, for evaluating APIMs. The factor groups were further classified into perspectives (risk management, requirements and solutions' attributes) to align broadly with Warfel's three axioms [307] for evaluating identification technologies. Each factor group was then assigned an evaluation theme label, e.g. Reliability Testing Evaluation Theme. The concepts relating to each evaluation theme within our three perspectives are elucidated in Sections 5.2.6 to 5.2.8.

We used the qualitative data conceptual coding technique, as advocated by Richard [253], in order to recognise the evaluation themes in our identified factors. The conceptual coding technique functions as a way to categorise a set of data into an implicit topic that organises a group of similar repeating ideas or concepts [259]. This data coding technique allowed us to amalgamate factors, from diverse perspectives, in order to create a theoretical list to begin to address our first research question. The additional review of relevant standards and guidelines ensured that sufficient breadth was covered to formulate an inaugural list of factors for evaluating APIMs. This inaugural list could be then validated through our empirical inquiry.

We labelled each of our identified factors and evaluation themes in order to minimise

ambiguity. The grouping of the identified factors into evaluation themes assisted us to identify and to eliminate redundant factors. Our classification also helped to ensure the integrity and consistency of our research method to identify these factors in the literature.

5.2.3 Identified Factors for Evaluating APIMs

We identified 207 factors for evaluating APIMs from our examination of the literature, which are detailed in tables contained in Appendix A. The majority of our identified factors originate from the literature produced by government agencies [295, 177, 98, 252].

We found that contributions in the literature that evaluate security, usability and privacy factors (and also many other factors) relating to APIMs adopt an organisational slant [295, 252] or emanate from a user-centred leaning [334, 126]. We identified, however, from our literature review that there are some factors, such as assurance, trust and confidence, that appear to be common aims for all perspectives. From our review of this literature, in particular, we found that the following issues on automated personal identification are discussed frequently:

1. Acceptability Issues – the benefits, social acceptability, risks, control, usefulness and the costs of the APIM to the respective stakeholders [247, 56];
2. Usability and Maintainability Issues – the ability of users to perform their tasks and the ability of the system owners to manage the APIM [288, 15, 125]; and
3. Accessibility Issues – inclusiveness in terms of human physical capabilities, knowledge and equipment (hardware and/or software) [250, 238].

The discussions surrounding these issues assisted us to identify further factors. These discussions also assisted us to formulate our criteria questions relating to a factor.

5.2.4 Purpose of Factors and Criteria Questions

We explain the purpose and relationship of our identified factors and their associated criteria questions before presenting our classification of the factors identified in the literature.

A factor is an element that requires evaluation, together with other elements, for the purposes of enabling the informed selection of an APIM for a given application context. Essentially,

a factor serves as an **aide-mémoire** to remind an IS programme that a particular aspect needs sagacious consideration because that factor, e.g. cost, has the potential to influence the selection of the optimal APIM for the application context.

Subject data for a factor are acquired by using its associated criterion question to extract the relevant data from the application context in question. Data acquired may be contained in an assessment report or information may be acquired from other primary sources. Each factor is assigned a descriptive label in order to identify that factor in an evaluation theme. Each evaluation factor has at least one criterion question to acquire data corresponding to that factor.

The close inspection of the factor entries in the tables in the appendices reveals that some factors have similar identification labels. These apparent similarities, however, are not erroneous replications. We found that there are common factors where such considerations are evaluated from different perspectives.

5.2.5 Results of our Classification of Identified Factors into Evaluation Themes

In this section we present the results of our factor classification effort. The factors and evaluation themes shown in tables contained in Appendix A also appear in our paper *Criteria to Evaluate Automated Personal Identification Mechanisms* [226]. Many factors, notably costs, often had multiple sources in the literature. We opted to cite only one source reference for each factor in Appendix A because these identified factors were to be validated empirically.

We classified our identified factors into 18 evaluation themes. These themes were further classified into the following three perspectives, as shown in Table 5.1, to align broadly with Warfel's three axioms [307] to evaluate identification technologies. We assigned the following labels and definitions to our identified perspectives:

- Risks Management Perspective – Factors in this category are designed to evaluate stakeholders' information on the rationale and extent to which an APIM should protect an asset, or allow entitlement, commensurate with the risks and customs of the subject community;
- Requirements Perspective – Factors in this category are designed to evaluate informa-

RISK MANAGEMENT FACTORS PERSPECTIVE	REQUIREMENTS FACTORS PERSPECTIVE	SOLUTIONS' ATTRIBUTES FACTORS PERSPECTIVE
1. Strategic Issues	6. Functionality	12. Security Architecture
2. Risks Assessment	7. Community and Usability	13. Identifier Credential
3. Social Acceptability	8. Privacy Compliance	14. Reliability Testing
4. Risks Controls	9. Credential Registration	15. Usability Testing
5. Business Case	10. Controls' Performance	16. Technology
	11. Assurance Requirements	17. User Accessibility
		18. Owners' Costs

Table 5.1: Factor Perspectives and Evaluation Themes

tion regarding the degree of the identification assurance required for the APIM which should be consistent with the stakeholders' objectives; and

- Solutions' Attributes Perspective – Factors in this category are designed to evaluate data relating to a candidate APIM's capability to fulfil the articulated requirements for an APIM, e.g. does the candidate APIM authenticate users within the required time of one second.

We believe that our criteria questions, when applied to an application context, have the potential to produce a plethora of data for evaluation which may also reveal conflicting requirements, issues and constraints. We consider that the evaluation of these factors are best tackled within an evaluation framework. For now we simply present our factors and their associated criteria questions in their respective evaluation themes and perspectives. We explain how these evaluation themes are incorporated in our methodology in Section 5.3.5.

5.2.6 Evaluation Themes in the Risks Management Perspective

The five factor evaluation themes in this perspective are the Strategic Issues Evaluation Theme, the Risks Assessment Evaluation Theme, Social Acceptability Evaluation Theme, the Risks Controls Evaluation Theme, and the Business Case Evaluation Theme.

The factor themes in this perspective relate to the strategic considerations to introduce or to revise a deployed APIM, the issues surrounding the risk assessment process to determine the need for an APIM, which may fulfil an identification problem. The factor themes also cover issues surrounding the social acceptability of an APIM in the application context and the objectives for an APIM as a control mechanism. The factor themes also cover the issues surrounding the creation of a business case in order to obtain investment for the APIM for

the application context.

We now describe the thematic concepts which we recognised in our analysis of the identified factors.

5.2.6.1 Strategic Issues Evaluation Theme

We recognised a theme in the identified factors relating to strategic issues surrounding the selection of APIMs, which concerns the stakeholders' objectives for introducing or revising an APIM and its intended purposes.

Gerber and von Solms argue [118] that organisations should form their security objectives within the regulatory, political and economic boundaries, with due consideration of the community's cultural and historic background. We believe that their argument applies equally to selecting an APIM. The factors grouped into this theme relate to the need for an APIM, the benefits derived from investment in an APIM, the purpose of an APIM within the organisational objectives, and any political or legal imperatives which impact the selection of the APIM. Such considerations and decisions are often undertaken at a strategic level in an organisation.

The factors which relate to our strategic issues evaluation theme, together with their criteria questions, are shown in Table 1A of Appendix A.

5.2.6.2 Risks Assessment Evaluation Theme

This evaluation theme relates to issues surrounding the stakeholders' risks in using the APIM for its intended purposes in its envisaged usage environments. These issues are often considered during a risks assessment.

The factors grouped into this theme relate to the attack likelihood or compromise probability on an asset or resource, the threat motivation for misfeasors, the vulnerabilities in the organisation's operational context, and the organisation's general strategy for managing risks.

As a control measure, an APIM often forms part of security architecture to minimise risks to assets. A risk assessment should, as a minimum, specify the information assets,

their estimated value, identify vulnerabilities, acquire threat intelligence, ascertain incident probabilities and likely impact on those assets in the event of a successful attack in order to determine risk controls [234].

Our identified factors do not relate to project risks here; however, an IS programme's failure to specify sufficient controls to protect the assets could impact upon the effectiveness of the APIM deployed. While security controls may improve risk management, development and operating costs, as well as political and other economic interests, should be accommodated to achieve an acceptable balance for organisations and their intended user community [252].

The factors which relate to risks assessments, together with their criteria questions, are shown in Table 1.B of Appendix A.

5.2.6.3 Social Acceptability Evaluation Theme

The evaluation theme recognised in the identified factors relate to acceptability of the APIM to the intended user community.

The factors grouped into this theme relate to the relationship between the user community and the APIM organisation, the obligations placed on the user in using the APIM, the general social attitudes towards the use of APIMs in the application context and the users' costs of using the APIM.

Adams and Blandford recognise [1] the gaps which exist between organisational approaches to securing systems and the user's role in operating security mechanisms within *communities of practice*. They argue that the degree of trust between organisations and their users, particularly where an affiliation has not been established, appears to influence the social acceptability of some security mechanisms.

Dourish et al. contend [84] that users' perception of security has an important role to play in helping communities understand the purposes and benefits of security mechanisms. Some organisations attempt to manage their user community's perception of security [9]. Nevertheless, users may still become disillusioned with an APIM as a result of bad experiences from deceptive interactions [326].

The factors which relate to issues surrounding the social acceptability of the APIM, together with their criteria questions, are shown in Table 1.C of Appendix A.

5.2.6.4 Risks Controls Evaluation Theme

The theme recognised in the identified factors relate to risks controls for the application in its context and the need for an APIM as a control mechanism.

The factors grouped into this theme relate to the countermeasures risks, the objectives of the controls, the budget allocated for the controls and the security policies and privacy policies which influence the APIM as a control mechanism.

The need to introduce or revise a deployed APIM could be an organisational response to an identification of increased or decreased risks. The need may also be a response to an APIM which is attracting many usability problems or the need for an organisation to comply with regulation. It appears in practice, however, that changes in policy, covering the protection of assets, are often only brought about as a response to significant security breaches [300]. An organisation may need to revise security policies or privacy policies, which include references to standards or guidelines on deploying information security controls, e.g. ISO/IEC 27002 Information Technology – Security Techniques - Code of Practice for Information Security Controls.

The factors which relate to risks controls and the implementation of security policies, together with their criteria questions, are shown in Table 1.D of Appendix A.

5.2.6.5 Business Case Evaluation Theme

The identified factors which relate to business case to the evaluation theme to introduce an APIM or to revise a deployed APIM.

The factors grouped into this theme relate to understanding the business problem, the rationale for stakeholders to introduce or revise an APIM, notably the sponsoring stakeholders, the constraints which may impact a project to introduce or revise an APIM, the standards which the APIM must align with, particularly for interoperability purposes, and the acquisition of information relating to similar deployments to the application context in question. Also, we identified a factor which relates to methodology for gathering the business requirements for the APIM.

An organisation may decide to minimise the risks to assets by instigating a change programme. Usually, a feasibility study estimates the costs and benefits to implement these business

strategies and to sustain the controls over an acceptable lifetime. The analysis of similar identification challenges, contexts or user community characteristics may help reveal the type of solutions previously implemented, the resulting issues, the major project risks, the investment effort, and elapsed time necessary to allow benefits to be realised.

The factors which relate to business case for an APIM evaluation theme, together with their criteria questions, are shown in Table 1.E of Appendix A.

5.2.7 Evaluation Themes in the Requirements Perspective

The six factor evaluation themes in this perspective are the Functionality Evaluation Theme, the Community and Usability Evaluation Theme, the Privacy Compliance Evaluation Theme, the Registration and Credential Issuance Evaluation Theme, the Controls' Performance Evaluation Theme, and the Assurance Requirements Evaluation Theme.

The factors in this perspective relate to the requirements for an APIM, compliance with privacy legislation, the registration and enrolment of subjects including identity proofing, and the distribution credential (if relevant) to users. These factors also cover the functional requirements for the APIM in the application context including the design issues surrounding usability and accessibility. The factors also cover performance and assurance requirements for the APIM.

Experience in deploying biometric system suggests that the analysis of the application context's human identification problem and the statement of business requirements are fundamental before any consideration of technical solutions [295]. Objectives to resolve problems or transform operations should be expressed as requirements (at least at a high-level) for a service or business control or enabling process and should not be solution driven [295]. The elicitation, analysis and specification of these business requirements are critical success factors for APIMs [295]. Operational requirements, including the APIM's interactive design, may best be achieved through a prototype or pilot in a live environment to validate the security specification and configurations requested [65].

There is a range of vulnerabilities associated with all existing APIMs and the efforts to articulate requirements should concentrate how stated objectives should be met and not a description of possible solutions [63]. Statements on performance requirements also need to be expressed as an assurance rating, capable of measurement, and not in abstract terms [98],

e.g. a ‘secure system’.

5.2.7.1 Functionality Evaluation Theme

The factors in this evaluation theme relate to the functional requirements for the APIM in the application context’s usage environments.

The factors grouped into this theme relate to the functional requirements for the APIM surrounding:

- positive or negative identification;
- overt or covert identification;
- structured or random identifier data;
- the types of data available which may be used for identification purposes;
- the users’ tasks dynamics;
- the degree of supervision, if any; and
- the degree of control over the physical and logical environments.

The functions contained in authentication systems and identification systems offer biometric solution types to various business problems [295]. There are, however, a multitude of local and remote device configurations which impact the functional requirements for APIM. The issues relating to APIM deployment not only complicates the articulation of functional requirements but also affects the degree of control that organisations and users have over these mechanisms in both networked and physical environments [271].

The factors which relate to the functionality for the APIM, together with their criteria questions, are shown in Table 1.F of Appendix A.

5.2.7.2 Community and Usability Evaluation Theme

The factors grouped into this theme describe the characteristics of the subjects in the community and their required interactions with the APIM so as to complete their intended tasks.

An APIM's design impacts upon users' tasks to achieve their desired goals [194]. Sasse argues [261] that designers should be encouraged to be more empathetic towards users' goals and should accommodate users' security motivation in relationship to the application context. Yee also argues [327] that designers should develop interfaces that consider the users' tasks and the pressures of their environments. He also contends [328] that gaining an insight into users' security awareness would certainly assist with the design of a security mechanism, particularly when to invoke the security interactions within the users' tasks structures. Leech contends [182] that employers should instigate well-structured training programmes focused on improving user security; however, we believe that education should supplement intuitive design and not replace it.

The factors which relate to the community and usability requirements for the APIM, together with their criteria questions, are shown in Table 1.G of Appendix A.

5.2.7.3 Privacy Compliance Evaluation Theme

The factors in this evaluation theme relate to the legal compliance of the specified APIM with the privacy legislation and other similar regulation. The theme also includes the processes which are required for the APIM to be able to demonstrate such compliance with provisions of the legislation.

The factors grouped into this theme relate to the requirements for the APIM to enable the system owner to demonstrate compliance with privacy, social accessibility and discrimination legislation. We acknowledge, however, that similar compliance factors could be relevant to other laws, regulations and corporate governance policies.

Some organisations may diligently perform their responsibilities to protect users' private data, by incorporating appropriate processes into their governance structure [98]. Conversely, some heterogeneous implementations need the direction of a central or scheme body to set out the governance rules and security policies for using private data to identify individuals [41].

User privacy management requirements have a significant impact on the APIM's interactive design and security architecture, which must choose between two distinct architectures for preserving private data [283]. Organisations may maintain control of private data by technical enforcement [41], possibly supplemented by legal protection. Alternatively, the

APIM's security architecture could delegate the control of private data to the user, as the data owner, together with the tools to manage consent operations [283].

The factors which relate to privacy compliance requirements for the APIM, together with their criteria questions, are shown in Table 1.H of Appendix A.

5.2.7.4 Credential Registration Evaluation Theme

The factors in this evaluation theme relate to requirements for the registration and enrolment of subjects from the intended user community.

The factors grouped into this theme relate to the requirements for verifying the identity of a subject, i.e. identity proofing, registering that subject in the APIM, acquiring or generating data for identification or authentication, the issuing and distribution of credentials to a subject and the distribution of devices or artefacts (if required) to users.

Where risks dictate, additional controls are introduced to identify applicants in order to minimise attacks designed to subvert the subject registration process for the APIM [79]. The consequential risks from failure to detect falsified or counterfeit seed identity documents, e.g. a birth certificate, in order to steal or invent an identity, are minimised by incorporating stringent identity checking controls [79].

Individuals appearing in person with their identity evidence, to register for an APIM, provide the opportunity to undertake biometric enrolment and also to distribute credentials, such as an ePassport. The registration process, however, is often undertaken as a remote activity with the system owner accepting the veracity of the user's claim to an identity.

The factors which relate to registration requirements for the APIM, together with their criteria questions, are shown in Table 1.I of Appendix A.

5.2.7.5 Controls' Performance Evaluation Theme

The factors in this evaluation theme relate to the performance requirements for the APIM in terms of acceptable speed and accuracy for identifying persons.

Our analysis of the factors in the literature suggests that organisations need to balance the performance practicalities associated with application context and the capabilities of the

different types of APIMs. Although this recommendation is directed mainly at deploying biometric systems [63], we consider that this advice applies to all types of APIMs.

Performance may be crudely expressed as the decision trade-off between the APIM's speed and accuracy to identity or to authenticate a person. This trade-off decision is particularly relevant where a biometric identification system operates in a very large community [119]. While biometrics may strive to meet tough acceptable impostor rate thresholds the true accuracy of user authentication is often masked [230]. Authentication data, e.g. passwords, may be passed to colleagues or captured by masqueraders, thereby casting doubts over the effective performance of an authentication system [9]. Conversely, user authentication systems, using password data, often have better response times than biometric authentication systems.

Requirements analysis should determine acceptable and realistic accuracy targets, based upon the practical experience of testing the performance of biometric systems in similar environments [194]. Evidence suggests that for some biometric projects insufficient thought has been given to setting acceptable performance in relation to risk [63]. The inevitable result is the performance of some biometric solutions often falling short of expectations. An excessive accuracy expectation applies equally to authentication mechanisms, as the user should be the only individual to know the authentication data [9], but increasingly this condition is not the case, e.g. phishing attacks.

The factors which relate to control performance requirements for the APIM, together with their criteria questions, are shown in Table 1.J of Appendix A.

5.2.7.6 Assurance Requirements Evaluation Theme

The factors in this evaluation theme relate to the assurance requirements for the APIM in terms of the APIM's capability to resist attack and the capability to detect that an APIM has been compromised. The factors also include the requirements for conducting assurance tests and the testing methods in order to ensure that it is possible to demonstrate than an APIM conforms to a specified assurance quality.

The Biometric Working Group recommend [63] that it is important to stipulate the assurance tests requirements at the outset so that relevant data may be generated in order to assess a system's assurance effectiveness. They also state that it is equally important to describe the

framework and conditions in order to produce substantiated evidence for evaluation.

The Common Methodology for Information Technology Security Evaluation provides [64] a universally available evaluation framework for organisations to describe their assurance requirements for an APIM in the form of a protection profile for a specific system or product or Target Of Evaluation (TOE). Weingart et al. suggest [313] that the assurance sought in a system should, in theory, match those controls stipulated in order to reduce identified risks to an acceptable level.

Commonly, system assurance testing takes place in controlled environments before such implementations are released to users [221]. The UK Biometrics Working Group recommends [295] that assurance testing should also involve subjects from the intended user community in their operating environment as this additional data may augment assurance evidence gained in the laboratory.

The factors which relate to the assurance requirements for the APIM, together with their criteria questions, are shown in Table 1.K of Appendix A.

5.2.8 Evaluation Themes in the Solutions' Attributes Perspectives

The seven factor evaluation themes in this perspective are the Security Architecture Evaluation Theme, the Identifier Credential Evaluation Theme, the Reliability Testing Evaluation Theme, the Usability Testing Evaluation Theme, the Technology Evaluation Theme, the User Accessibility Evaluation Theme and the Owners' Costs Evaluation Theme.

The evaluation themes in this perspective relate to the attributes of an APIM, as a candidate solution, which may fulfil the requirements for an APIM to address an identification problem. The evaluation themes which describes the APIM's attributes includes the solution's security architecture, its technical components and the processes describing how subjects are registered and enrolled, how subjects and possibly other entities may use the APIM (with or without a credential), and how a subject's entitlement to access an asset or resource using that APIM is terminated. The factors also cover the mechanism's attributes relating to reliability testing, usability testing and accessibility testing of the APIM. There are also factors relating to the various types of costs associated with designing, developing, deploying, operating and maintaining an APIM.

5.2.8.1 Security Architecture Evaluation Theme

The factors in this evaluation theme relate to security architecture attributes of a candidate APIM or a deployed APIM in an application context. These attributes include a description of the data used to identify subjects and the protection of that identification data.

The main factor relates to the type of data, e.g. user knowledge, biometric modality or code generated from an artefact, which is used to identify the subject. There are also factors relating to the modes of operation for the APIM's identification data. The other factors grouped into this theme relate to the attributes describing the technological components, the infrastructure, the processes surrounding the acquisition of subjects' identification data and the processes to maintain the confidentiality and integrity of that data during usage and storage.

From our analysis of these factors we identified that an APIM may be an integral element in an security architecture which contains other complimentary risks controls. We also recognised that a security architecture may support a system with the dedicated purpose of identifying persons, i.e. a biometric identification system which utilises bespoke sensing devices and software. Cotroneo et al. recommend [65] that authentication systems should utilise ubiquitous devices and software elements in order to improve technical interoperability and usability for users; however, this advice is often difficult to embrace.

The factors which relate to the security architecture attributes, together with their criteria questions, are shown in Table 1.L of Appendix A.

5.2.8.2 Identifier Credential Management Evaluation Theme

The factors in this evaluation theme relate to the description of the APIM's credential management processes associated with identifiers assigned to users. An identifier is datum, e.g. an email address, X500 distinguished name or a Globally Unique Identifier (GUID), which uniquely identifies the subject of this digital identity within a given application context. Credentials are data associated with a subject, e.g. possession of a password or a private key, which serve as evidence to assert the claimed digital identity of a person.

The key factors associated with credentials relate to distinguishing goals of the credential, the data model of the credential, the physical (if relevant) and logical data structure of the

credential and the design limitations of the credential [216]. The other factors grouped into this theme relate to the credential's lifetime, the credential's authenticity, the credential integrity, the processes for maintaining the credentials, the delivery of the credential to the user, the credential use locations and the requirements for credential accreditation (if applicable).

Biometric identification requires a person's biometric data credential and their associated identifier to be stored in a central repository [162]. Data used in an authentication system may be stored in a central database and/or on an Integrated Circuit Card (ICC) or other types of storage device. Credentials embedded in ICCs provide the capability for users to be verified locally without the need for host connections [271].

The distribution of credentials, e.g. payment cards and PIN mailers to account holders, by the APIM's issuing authorities often brings logistical challenges. Credentials, e.g. User Identifiers and passwords, both initial and re-issued, may be sent, possibly separately, to users through the postal system or across open networks. The controls for credential distribution should be directly correlated to the risks and costs for both the system owner and user [79].

The factors which relate to the attributes of an APIM's credentials, together with their criteria questions, are shown in Table 1.M of Appendix A.

5.2.8.3 Reliability Testing Evaluation Theme

The factors in this evaluation theme relate to the reliability test results of a candidate APIM or deployed APIM for the application context.

The factors grouped into this theme relate to test result information on the APIM's performance, in terms of accuracy and speed to identify or authenticate authorised users and to detect unauthorised users, its resistance to attack, the difficulty of producing a counterfeit artefact and/or credential data to circumvent the identification system or authentication system.

Tests planned for an appraisal regime or evaluation framework should produce substantiated data for reliability assessments [64]. Gathering information on APIMs, as they are used in practice, also provides data to validate reliability indications [63, 324]. While formal security evaluation helps to form independent opinion the real challenge appears to be to reassure organisations to rely upon access control security mechanisms and other parties to trust that protection [11].

The factors which relate to the reliability of an APIM evaluation theme, together with their criteria questions, are shown in Table 1.N of Appendix A.

5.2.8.4 Usability Testing Evaluation Theme

The factors in this evaluation theme relate to the usability test results of a candidate APIM or deployed APIM for the application context.

The factors grouped into this theme relate to tests results from users' utilisation of the APIM's Human Computer Interface (HCI), the visibility of the security status, the alignment of the APIM with the user's tasks, and the users' satisfaction of the APIM gained from their usage experiences.

The inadequacies of HCI security design often dilute the effectiveness of preventative controls [68]. Even with usability design deficiencies, security effectiveness is improved by enabling users to make informed decisions from having a better understanding of a device's security operations [237].

Knowledge based authentication systems mainly attract user password management problems [9]. Increasing the number of password attempts could help users' chances of recollection success; however, this strategy may marginally increase the opportunity of an external adversary obtaining that authentication data [262]. While aids to improve password recall may assist in some contexts, e.g. rebus passwords [189], effort should be focused on improving authentication system security designs [2, 261, 315].

The factors which relate to the usability of an APIM evaluation theme, together with their criteria questions, are shown in Table 1.O of Appendix A.

5.2.8.5 Technology Evaluation Theme

The factors in this evaluation theme relate to the technology and the resources, in terms of systems, personnel and skills, to support the APIM for the application context.

The factors grouped into this theme relate to the computer systems, networks, devices and other components for the APIM, the anticipated life time of these technologies, how the identification data and infrastructure are protected and the competencies of the personnel

required to support the APIM.

APIMs rely upon many technological components that include system servers, networks, personal computers, user input devices and supporting application software. Some of these components are ubiquitous while many are bespoke to a specific type of APIM. Some biometric solutions use proprietary algorithms, e.g. facial recognition, although international effort has agreed common biometric data exchange formats in order to improve interoperability [160].

Technological components should respond with inferred protective actions from users' intentions [123] and reflect the state of those trusted interactions [328]. Operating System designs that permit an application program to use one of several identification security agents running concurrently, in a layer between the security tasks layer and the operating system containing security data objects, is a possible research direction [289].

The factors relating to an APIM's technological components and associated criteria questions are shown in Table 1.P of Appendix A.

5.2.8.6 User Accessibility Evaluation Theme

The factors in this evaluation theme relate to the accessibility test results of a candidate APIM or deployed APIM for the application context.

The factors grouped into this theme relate to the results of conducting sensory, skills and/or cognitive tests, which may prohibit users from using the APIM as designed. This theme also includes factors relating to the need for users to possess artefacts, devices or special software to use the APIM. It also contains factors relating to the measurement of user confidence in using the APIM and the user efforts required to maintain the devices and credentials associated with the APIM.

Some individuals may fail to enrol on some biometric systems because they are unable to provide the minimum distinctive user input signals required, e.g. capturing fingerprint minutiae [311], to sensory devices. In some countries there are regulations to ensure organisations provide alternative arrangements to individuals with disabilities that may impinge upon their ability to use devices or systems effectively.

User access exclusion may also relate to technological constraints or interoperability issues,

such as bespoke devices or type of operating system or application. The need for individuals to purchase devices, e.g. smart card readers, may also impact upon user accessibility to use the APIM purely on affordability grounds. A system owner often has to consider the benefits and the adverse impact of utilising proprietary technology or adopting the use of ubiquitous technology or a configuration of both.

The factors which relate to the user accessibility of an APIM for the application context, together with their criteria questions, are shown in Table 1.Q of Appendix A.

5.2.8.7 Owner's Costs Evaluation Theme

The factors in this evaluation theme relate to the costs associated with a candidate APIM or deployed APIM for the application context over the required operational period.

The factors grouped into this theme relate to that various types of costs associated with the implementation, deployment and maintenance of the APIM in the application context. The cost elements also include the costs of input devices, artefacts, infrastructure costs and recovery costs.

These cost elements to deploy an APIM in an application context are required for return on investment and budget considerations. Some contingency should also be planned as poorly designed security interfaces often lead to user errors and the system owner incurring unbudgeted costs, e.g. administrators reissuing tokens to users. The type of costs relating to APIM deployments may be designated either as capital investments or revenue expenditure; however, without delving into the complexities of accounting practices, the provision of precise costs will assist organisational investment decisions.

The factors which relate to the costs associated with an APIM for the application context, together with their criteria questions, are shown in Table 1.R of Appendix A.

In accordance with our research implementation plan, we aimed to validate our identified factors by *grounding* their existence in data acquired from our three case studies. We also aimed to identify new factors for evaluation from our qualitative analysis of data acquired from these case studies.

From applying our criteria, potential candidate APIMs may now be compared objectively with the risk management objectives and stated requirements for the APIM in its target

application context. We believe that this comparison is best undertaken within an evaluation framework, using a well-defined method, within a systematic methodology.

5.3 Development of the ASMSA Methodology

We developed the ASMSA Methodology based upon our supposition that a systematic methodology is efficacious for selecting the optimal APIM for *some* application contexts.

We pursued our aims to develop a systematic methodology by building upon our efforts to identify factors for evaluating APIMs as described in Section 5.2. While our identified factors and their criteria questions were grouped into common themes [226], we recognised that an evaluation framework was necessary to serve as a way of modelling the data acquired and representing the attribute interrelationships from an application context. This model is designed to assist with gaining an understanding of the APIM selection problem from three perspectives.

Additionally, we recognised that we needed to develop a selection method to acquire data from the application context in question and to synthesize that data systematically in order to demonstrate objectivity. We also recognised the need to create well-defined processes so that the selection method is repeatable by other methodology users.

5.3.1 Method for Developing the ASMSA Methodology

This section explains how we utilised our factors and their associated criteria questions in order to develop a methodology to answer our second research question.

Our research method for developing the ASMSA Methodology's components commenced by undertaking a high-level review of literature covering IS evaluation, modelling concepts and their relationships, decision-making, and multiple stakeholder consultation process management. We then analysed the characteristics of the APIM selection problem, as described in Section 5.1.1, and developed a model which could represent the factors and their interdependencies. We also reviewed commercially available IdMS assessment methods in order to consider their applicability for evaluating APIMs.

We developed the ASMSA Evaluation Framework iteratively by creating a provisional model to represent the concepts identified in the classification of our identified factors. This model

was then revised to reflect the purpose of the evaluation and the problems associated with selecting the optimal APIM for a given application context. We discuss the general problems of selecting information technologies in the next sub-section.

We developed the ASMSA Selection Method by creating a series of processes, based upon the requirements engineering processes, as specified by Hull et al. [138], and then decomposed each process into discrete steps. These discrete steps were designed to acquire data from the application context using the criteria questions associated with our identified factors. We then integrated data manipulation steps into our method which draws on Keeney et al.'s Multiple Objective Multiple Criteria (MOMC) technique [173] for decision-making situations involving multiple stakeholder objectives and multiple criteria. We next elucidate on our choice of this technique which has been applied to investments decisions on IT.

5.3.2 Decisions on Information Technology

We reviewed literature covering IT evaluations [97, 272, 251, 76] to enable us to understand how different factors impact upon information technology selection problems. We also reviewed literature on Multiple Stakeholder Processes (MSPs) [128], as we recognised from our factor classification work that APIMs are often implemented in situations where there are many stakeholders with similar, and often conflicting, objectives.

We also needed to understand qualitative decision-making approaches and methods applied in qualitative selection processes [316, 231]. We recognised that there was a need to incorporate techniques which are designed for decisions involving multiple stakeholders with multiple objectives, as described by Keeney et al. [173] and Homburg [134] into our methodology. We also needed to incorporate techniques into our methodology which, according to Ehtamo et al. [87], attempt to address persistent conflicting issues between stakeholders.

We also reviewed literature specifically covering the general study of evaluation frameworks [165, 281] in order to assist with the construction of a model to represent acquired data and the interrelations of the factors involved in selecting APIMs. After constructing this abstract framework we were then positioned to develop a corresponding method for evaluating and selecting APIMs.

There are many types of IT assessments that provide analytical information from a range of subjective and objective inputs [272]. We considered it appropriate to design an approach

that exploited these various IT assessment types in order to acquire a rich set of data from the application context to be evaluated in ASMSA's evaluation framework. Our exploratory research led us to construct an evaluation framework and meta-evaluation selection method, to use secondary data, as defined by Stufflebeam [279], in our evaluation framework which draws information from a combination of several types of primary assessment. In this sense, the ASMSA Evaluation Framework may be regarded as a high-level evaluation of several evaluations.

5.3.3 Methodological Design Choices

This section describes our design choices in the creation of our systematic methodology, **A**pproach for **S**electing the **M**ost **S**uitable **A**PIM (ASMSA) Methodology.

From our review of our identified factors, we observed that the factors were of mixed data types, ranging from factors on political considerations for an APIM to the costs for deploying an APIM. The methodology's design, therefore, needed to evaluate both qualitative data and quantitative data acquired for the purposes of selecting the optimal APIM. For the design of our methodology, we considered the strategy of using quantitative analysis techniques by evaluating qualitative data quantitatively. For example, the usability of an APIM could be expressed as a scalar measurement, as reflected in the design of Ashbourn's Pentakis Methodology [15] for selecting biometric systems. We discounted assigning a numerical value to indicate the usability of an APIM because, as we found from our classification of our factors, the attributes relating to usability are expressed in qualitative terms, for example an intuitive interface [167].

We recognised that the attributes of some of our factors needed to be expressed qualitatively while the attributes of other attributes, e.g. False Acceptance Rates must be expressed quantitatively. We needed to design a methodology which accommodated mixed data types and processes that incorporated quantitative data and qualitative data analysis techniques. Keeney et al. argue [173] that complex decisions involving multiple objectives and multiple criteria with a rich set of mixed data requires a qualitative approach to enable value based compromises. While Royer adopts a quantitative approach [257] for selecting enterprise APIMs, we adhere to the qualitative approach recommended by Keeney et al .[173].

We concede, however, when there may be two candidate APIMs exhibiting the necessary capabilities and attributes to fulfil the requirements for an APIM, then the comparison of

numerical values, e.g. impostor detection rates and costs, should be incorporated into our methodology. We incorporated qualitative and quantitative analytical techniques into our methodology's design in order to evaluate mixed data types.

We developed the ASMSA Methodology to support complex decision-making by incorporating:

- discrete actions in our selection method;
- structured criteria questions to acquire data relating to our factors;
- techniques to manipulate acquired data; and
- processes to evaluate acquired data in an evaluation framework.

Therefore, we created the ASMSA Methodology, comprising of a tentative evaluation framework in order to represent mixed data types based upon our identified factors and our classification of these factors into evaluation themes within three perspectives. We also constructed a provisional selection method with detailed steps in three stages and criteria questions to acquire data from an application context relating to our identified factors. Essentially, we constructed and published our systematic methodology **before** we commenced our empirical research. Our aim was to use the empirical data gathered from our three case studies, described in Chapters 6, 7 and 8, to validate our identified factors and also to refine the ASMSA Methodology's components.

5.3.4 Development of the ASMSA Evaluation Framework

Jayaratna states [165] that frameworks improve the understanding of a range of concepts, models, techniques and methods that aid decision-making. The construction of a well-articulated model which defines the concepts and describes the interrelationships between the concepts then allows for solution options to be derived and also to be evaluated.

We created the ASMSA Evaluation Framework to correspond to our three perspectives, our evaluation themes and the factors located in the literature. We recognised the need to revise the labels of our three perspectives, during our efforts to create our evaluation framework, from Risks Management, Requirements and Solutions' Attributes to Understanding, Effectiveness and Efficiency Perspectives respectively, as now shown in Figure 5.2. The titles of

the evaluation themes and the identified factors, however, remained the same during this stage of our implementation plan.

We reference Table 5.2 in our explanation of the concepts which underpin our methodology in Section 5.4.3 and also our description of our evaluation framework in Section 5.5. We describe our rationale for renaming our three perspectives in Section 5.4.3.1.

UNDERSTANDING PERSPECTIVE	**EFFECTIVENESS PERSPECTIVE**	**EFFICIENCY PERSPECTIVE**
1. Strategic Issues	6. Functionality	12. Security Architecture
2. Risks Assessment	7. Community and Usability	13. Identifier Credential
3. Social Acceptability	8. Privacy Compliance	14. Reliability Testing
4. Risks Controls	9. Credential Registration	15. Usability Testing
5. Business Case	10. Controls' Performance	16. Technology
	11. Assurance Requirements	17. User Accessibility
		18. Owners' Costs

Table 5.2: Evaluation Perspectives and Factor Evaluation Themes

5.3.5 Development of the ASMSA Selection Method

The ASMSA Selection Method is constructed to align with the decision analysis path recommended by White [316], consisting of:

- problem formulation;
- constructing and testing a model;
- deriving a solution;
- implementation; and
- monitoring issues and risks.

From our analysis of the characteristics of the APIM selection problem in Section 5.1.1, we considered that the Multiple Objective Multiple Criteria (MOMC) decision-making technique, as described by Keeney et al. [173], is a relevant strategy upon which to base a method for selecting APIMs.

Keeney et al. recommend [173] the MOMC decision-making approach is pertinent for extracting order from the morass of diverse, generally conflicting, uncertain and often evolving attitudes in complex decision-making cases. According to Farbey and Finkelstein

[96], MOMC explicitly recognises contrasting viewpoints and uses more than one set of values to facilitate objective decision-making.

The MOMC decision-making approach incorporates an iterative approach to data acquisition so that it may be employed from the conceptual phase of a development project onwards, where assumptions require investigation, to help identify stakeholders' objectives together with compromise options and preferences. According to Homburg [134], the more objectives are sub-divided into a hierarchy, the easier it usually is to identify attribute scales that can be objectively assessed. Establishing a decision hierarchy of objectives for an IT selection process, as illustrated by Sylla and Wen [281], also helps to identify the benefits and other intangible decision factors.

We developed ASMSA's Selection Method and its processes based upon the principles of MOMC decision-making approach, in order that it possessed the capability to systematically identify similarities and conflicts in stakeholders' objectives and requirement preferences. We also recognised, however, the need for separate processes in our method to reconcile conflicting objectives for an APIM with stakeholders.

Hemmati defines [128] Multiple Stakeholder Processes (MSPs) as *"methods which aim to bring together all major stakeholders in a new form of communication for decision-finding and (possibly decision-making) on a particular issue"*. We consider that MSPs, as advocated by Hemmati [128], are relevant techniques to engage stakeholders in a dialogue in order to reconcile potential conflicts in stakeholders' objectives and for addressing any assumptions made regarding the requirements for an APIM. We embedded the principles of MSPs into the processes of our selection method so that stakeholders' objectives and preferences may be reconciled methodically.

5.3.6 Methodological Efficacy Considerations

Avison and Fitzgerald contend [18] that unless a methodology contains a specification of a method or a plan of discrete actions, then its processes cannot be easily repeated and may be open to various interpretations by methodology users, e.g. programme managers or discipline experts.

We acknowledge, however, that unless a methodology is adhered to then it will be difficult to gather the relevant data in order to assess the methodology's efficacy. Additionally, for such

an assessment there is a need to segregate data that represents discipline experts' skills and other competencies developed from data generated from the use of the methodology. Avison and Fitzgerald concede [18] that the comparison of development methodologies, whether theoretical or in practice, is a very difficult task. We also believe that comparing approaches to select the optimal APIM for an application context is not a trivial task.

The efficacy of our methodology (and other approaches) to select the optimal APIM for *certain* application contexts, therefore, requires a means to assess the efficacy of their problem-solving processes. We define criteria specifically to assess the efficacy of a methodology to select an APIM in Section 8.1. We developed these criteria from Lai and Hwang's criteria [179], designed for assessing fuzzy decision-making methods, and our methodological learnings based upon our two retrospective case studies.

We recognise that there may be situations when a systematic methodology may not be the most efficacious approach to select an APIM, for example when the circumstances demand expediency. Nevertheless, we believe that unless a methodology in an IS development programme incorporates the means to evaluate the effectiveness and efficiency of APIM candidate solutions, then stakeholders cannot objectively determine the potential and actual utility of their investment. Similarly, the effectiveness and efficiency of a deployed APIM cannot be determined objectively for the specific application context, unless there is the means to determine such utility.

5.4 Overview of the ASMSA Methodology

This section provides an overview of the ASMSA Methodology. The succeeding sections describe the ASMSA Evaluation Framework and the ASMSA Selection Method in detail. Our systematic methodology is also described in the publication 'Approach for Selecting the Most Suitable Automated Personal Identification Mechanism (ASMSA)' [227].

5.4.1 ASMSA Methodology's Philosophy

Avison and Fitzgerald argue [18] that the philosophy of IS development methodologies comprise of:

- the underlying paradigm underpinning the approach;

- the objectives of the methodology;
- the domain of situations that the methodology addresses; and
- the applicability of the methodology (whether targeted at specific types of problem or general purpose).

The ASMSA Methodology is based upon our belief that a multi-disciplinary approach is required to address the problem of selecting an APIM. Our belief is based upon the range of evaluation themes, e.g. risk management, regulation, security assurance, privacy protection, usability, costs, demonstrated in our identified factors for evaluating APIMs. The range of evaluation themes suggests that an evaluation based on a single perspective, e.g. cost, may not necessarily lead to the identification of the optimal APIM. We believe that the optimal APIM can be identified by evaluating a range of factors from our three perspectives in order to determine its *fitness for purpose*.

Howell contends [135] that critical thinking is only possible when the judgments of others are brought into the equation; when the standpoints of each and all are open to inspection. We believe that a methodology based upon the examination of differing standpoints, e.g. legal, operational, risk, financial, within an evaluation framework which employs systematic well-defined processes has the potential to improve decision-making for APIMs.

The ASMSA Methodology is designed as a process-oriented methodology in that we lay out its processing steps in significant detail. Its functions are designed to:

- acquire data relating to the background of the application context and evaluate the stakeholders' objectives for the APIM;
- acquire data relating to the requirements for the APIM for the application context and evaluate the effectiveness of the articulated requirements which aim to fulfil the stakeholders' objectives for the APIM; and
- acquire data relating to the candidate APIMs and evaluate the efficiency with which each solution fulfils the requirements for the APIM.

We designed the ASMSA Methodology to address a specific pre-identified problem, in that some stakeholders in the application context may claim that a deployed APIM is ineffective or inefficient. Our methodology acquires data to evaluate the effectiveness and efficiency of

a deployed APIM in order to provide evidence to corroborate or contradict such claims. We also designed our methodology to address the problem of selecting the optimal APIM for situations when new information systems are being introduced.

The ASMSA Methodology is applicable for determining the optimal APIM to authenticate persons wishing to access information or resources. It is also applicable for determining the optimal APIM where the sole function of the information system is the identification of a person, as a known member of the subject community.

5.4.2 Overview of ASMSA Methodology's Components

The ASMSA Methodology consists of:

- the ASMSA Evaluation Framework;
- identified factors for evaluating APIMs and associated criteria questions to acquire relevant data; and
- the ASMSA Selection Method.

The ASMSA Evaluation Framework is designed to represent the current state of the application context and its *APIM selection problem*. The framework also models the objectives and requirements for a desired state, which relates to the introduction or revision of an APIM. The ASMSA Method is designed to systematically acquire data, using criteria questions, relating to the application context and the candidate APIMs. There are also techniques in our method to reconcile, manipulate and evaluate data acquired. Our method aims to gain an understanding of the application context. It then aims to ascertain whether the description of the requirements for an APIM are effective. The comparison of the candidate APIMs' are then compared against the stipulated requirements in order to identify the optimal APIM for that application context.

The ASMSA Evaluation Framework component evaluates the application context and candidate APIMs to be deployed (or that have been deployed) from three perspectives:

1. Understanding Perspective – an **understanding** of the application context which includes the articulation of stakeholders' objectives for the APIM;

2. Effectiveness Perspective – the **effectiveness** of the articulated requirements for the APIM which aim to fulfil stakeholders' objectives; and

3. Efficiency Perspective – the **efficiency** with which each candidate APIM or deployed APIM satisfies those stipulated requirements.

For brevity, we use Understanding Perspective; Effectiveness Perspective; and Efficiency Perspective as defined terms in this thesis. The ASMSA Evaluation Framework is a meta-evaluation framework that uses information from other evaluations, e.g. risk analysis, privacy impact assessment, and other primary information related to the application context as its subject data. We describe the ASMSA Evaluation Framework in Section 5.5.

The identified factors for evaluating APIMs and the associated criteria questions are the second component in our methodology. A criterion question is designed to acquire data about a particular factor in a perspective's evaluation theme. Each factor is assigned at least one criterion question to acquire the relevant data. The acquired data, in response to the criterion question posed, is then represented as an attribute value associated with the respective factor.

As an illustration of our factor classification structure, a criterion question with the factor entitled 'Overt or Covert Identification' seeks to acquire information on whether the APIM is to automatically identify persons transparently and the legal and/or technical issues which may apply to covert identification. This factor falls under the Functionality Evaluation Theme within the Effectiveness Perspective which is located in Table A.6 of Appendix A. The criteria questions are used to acquire subject data at discrete steps in the ASMSA Selection Method's three stages.

The ASMSA Selection Method is the third component of the ASMSA Methodology. Our selection method's processes are contained in discrete steps within three stages as represented in Figure 5.3 on page 197. The ASMSA Selection Method processing steps are explained in Section 5.6. The processing steps in our method are represented in the ASMSA Decision Support System.

The ASMSA Decision Support System (ASMSA-DSS), described in Section 5.7, is a representation of the ASMSA Methodology's components. The system was originally designed to assist us with the management of the data acquired from our three case studies. We enhanced this system to represent the logical flow of processing steps in our selection method. The ASMSA-DSS guides the user sequentially through the processing steps of our

TERM	DEFINITION
Objective	Aim that is pursued to its fullest extent.
Goal	Priority value or level of aspiration that are achieved, suppressed or not exceeded.
Factor for Evaluation	Aspect of an application context that requires evaluation by a stakeholder organisation's programme in order to select the optimal APIM.
Factor Explanation	Description of the reasons for evaluating a particular factor for selecting the optimal APIM.
Evaluation Theme	Organised category of conceptually congruent factors that form the basis of an evaluation in the ASMSA Evaluation Framework.
Criterion Question	Interrogative query designed to acquire attribute values from the application context under investigation, which relate to a specific factor.
Attribute Values	Qualitative or quantitative data properties of factors that provide a means to evaluate an application context.
Stage	One of the three phases in ASMSA's Selection Method.
Step	One of the series of processes employed within a Stage of ASMSA's Selection Method

Table 5.3: Definitions of ASMSA Methodology's Terminology

selection method. In our third case study the DoR used the ASMSA-DSS to guide his efforts to evaluate and select an APIM.

We define our terms and describe the concepts which underpin our methodology in order to explain these aforementioned components in greater detail.

5.4.3 ASMSA Methodology's Terminology and Concepts

We define the terminology used in the ASMSA Methodology and its concepts in Table 5.3 and also provide a description of the concepts and their relationships which underpin our methodology.

The ASMSA Evaluation Framework models the characteristics of the application context so that the selection problem is evaluated from three *perspectives*; namely, the Understanding Perspective, the Effectiveness Perspective and the Efficiency Perspective. Data acquired, represented in evaluation themes, of each perspective *influences* factors in succeeding perspectives. Subject data are acquired using *tools* in the ASMSA Selection Method. Subject data are manipulated and synthesized by *techniques* in the ASMSA Selection Method.

The concepts in the ASMSA Methodology are defined as:

- Perspectives – Data which describe a view of the APIM selection problem;
- Influencers – Effects of data in a perspective on a succeeding perspective;

- Tools – Assessment instruments which acquire subject data from multiple primary sources; and
- Techniques – Subject data that are validated, manipulated or categorised in our selection method's processes.

We now provide a description of the function of these defined concepts in the ASMSA Methodology.

5.4.3.1 Perspective Concept

A perspective represents, through data acquired, a view of the application context and its selection problem.

We adopt a 'fitness for purpose' philosophy to address *the selection problem* which is similar to Sherwood et al. [263] business driven approach for designing security architectures. The three perspectives in our evaluation framework do not, however, represent the different views of technology specialists, e.g. an architect, designer or developer. We believe that the commingling of technological viewpoints may not determine the effectiveness or efficiency of candidate APIMs to fulfil stakeholders' objectives because the utility of an APIM should include factors from broader perspectives, such as regulatory compliance and financial management.

Our evaluation framework explicitly recognises that enterprise stakeholders may have similar or conflicting views, internally between departments, and externally with other enterprises or governments or customers or citizens, which need to be reconciled. Those views need to be captured and represented in a model for evaluation. We equate our three perspectives to White's recommendations [316], as follows:

1. Understanding Perspective equates to problem formulation of the application context in its current state;
2. Effectiveness Perspective equates to constructing and testing a model to represent the desired state; and
3. Efficiency Perspective equates to deriving a solution together with the identification and monitoring of issues and risks.

Each perspective is elucidated in respect of our evaluation framework as follows:

Understanding Perspective We formulate the problem by articulating an understanding of the application context's background, the stakeholder participants and their objectives for an APIM, together with legal, regulatory and other constraints. The understanding data are represented in attributes of the evaluation themes in the left column of Table 5.2. Importantly, this perspective includes data on the business case so that the benefits of the APIM are articulated at the outset.

Effectiveness Perspective We construct and test a model of requirements by specifying the functional, performance and assurance attributes for the APIM. This model also includes the processes to register and enrol subjects, the automated identification task's dialogue in the intended usage environments and privacy compliance regulations. The effectiveness data are represented in attributes of the evaluation themes in the middle column of Table 5.2.

Efficiency Perspective We derive a solution by modelling the properties of each candidate APIM or APIM deployment in terms of its identifier management characteristics, proposed security architecture, and its technical properties. The perspective also represents data relating to testing the usability, reliability, and accessibility of an APIM. We also include properties relating to identified vulnerabilities, issues and stakeholders' costs associated with an APIM. The efficiency data are represented in the attributes of the evaluation themes in the right column of Table 5.2. We equate the monitoring of issues, vulnerabilities, and also stakeholders' costs as outputs from the evaluation of candidate APIMs or a deployed APIM.

These three perspectives in the ASMSA Evaluation Framework are represented by the bold rectangular boxes in the centre of Figure 5.1 shown on page 188

5.4.3.2 Influencer Concept

The influencer concept describes how data, represented in a perspective, effects data in succeeding perspectives in the ASMSA Evaluation Framework. The influencer concepts are depicted by the broad solid patterned dark grey arrows in Figure 5.1. The influencer concept is not bi-directional.

ASSESSMENT TYPE	EXAMPLE ASSESSMENTS
Type A – Understanding Assessments	Privacy Impact Assessment, Risks Assessment, Organisational Policies, Feasibility Study, Business Case, Use Cases, Data Protection Legislation, Return On Security Investment, Social Studies, Threat Analysis
Type B Effectiveness Assessments	Business Requirements Analysis, Costs Benefits Analysis, Review of Simulation, Conceptual Prototype Review, Case Studies, Pilot Deployment Assessment, International Standards, Scheme Specifications
Type C – Efficiency Assessments	IT Architectural Review, Functional Tests, Supplier Product Specifications, Performance Test Results, Vulnerability Assessment, Device Specifications, Usability Testing Results, Software Code Analysis

Table 5.4: Assessment Types and some Example Assessments

An example of an influencer may be social norms relating to citizen's views on the protection of their private information which constrain the functional requirements for the APIM. Similarly, a deployed APIM which possesses vulnerabilities, attracts various issues and incurs costs may influence stakeholders' objectives to revise an APIM.

The ASMSA Evaluation Framework is designed, as a meta-model, to represent the persistent tensions between these three perspectives and the iterative nature of setting objectives, evaluating effectiveness of the requirements for an APIM, and also evaluating the efficiency of candidate APIMs or an APIM deployment against articulated requirements. We describe the influences in ASMSA's Evaluation Framework in Section 5.5.3.

5.4.3.3 Tools Concept

Tools are used by the ASMSA Selection Method to *acquire* subject data relating to the three perspectives from primary data sources. The data acquisition flows are represented by the three narrow horizontal patterned dashed arrows on the right hand side of Figure 5.1. We categorise the data acquired based on the types of assessment tool, as shown in Table 5.4, to correspond to ASMSA's three perspectives.

5.4.3.4 Technique Concept

We use the term *techniques* to describe other procedures in ASMSA's Selection Method that manipulate, reconcile or transform subject data and the processes to manage the dialogue with stakeholders.

The main technique used in our method is a process to prioritise stakeholders' objectives, which is based upon Keeney et al.'s MOMC guidelines [173]. We adapt the MOMC decision-

making technique in order to enable the establishment of a preference of stakeholders' objectives. A secondary technique reconciles stakeholders' objectives with operational requirements by employing Homburg's Hierarchical Objectives Mapping Technique [134], which deconstructs stakeholders' objectives into sub-objectives in order to identify high-level requirements. We use this technique in order to provide a link between an objective and at least one requirement for the APIM. This reconciliation technique ensures that all objectives link to at least one corresponding requirement and that all requirements link to at least one objective. An objective that is not linked to a requirement suggests that the requirements gathering activities are not complete. The presence of a requirement that does not link to an objective suggests that there is either an objective omitted or the requirement is beyond the scope of the programme, i.e. the identification of scope creep.

Our third technique uses Hemmati's MSP methods [128] to manage the stakeholder consultation processes with the aim of resolving differences in stakeholders' objectives for the APIM. Hemmati provides [128] guidance on how to identify stakeholders, both direct and indirect, and to communicate information, articulate stakeholders' objectives and preferences, and to resolve conflict between stakeholders. Our use of the MSP technique should also assist with the identification of compromise positions on stakeholders' objectives for an APIM.

In the next two sections we provide further explanations of how these *concepts* are used in our evaluation framework and in our selection method.

5.5 The ASMSA Evaluation Framework

We now describe the ASMSA Evaluation Framework in detail by explaining its three evaluation perspectives based upon the concepts defined in the previous section. We also explain the interrelationships between the perspectives in our framework, with our factors and criteria questions, and also with the ASMSA Selection Method. The ASMSA Evaluation Framework is represented in Figure 5.1.

The ASMSA Evaluation Framework is a meta-evaluation framework operating at a second order level, aggregating and manipulating data, from primary evaluations, such as a privacy assessment impact. Data acquired from primary evaluations are the subject data of meta-evaluations [279]. Subject data acquired are applied against the criteria questions associated with the factors in the ASMSA Evaluation Framework.

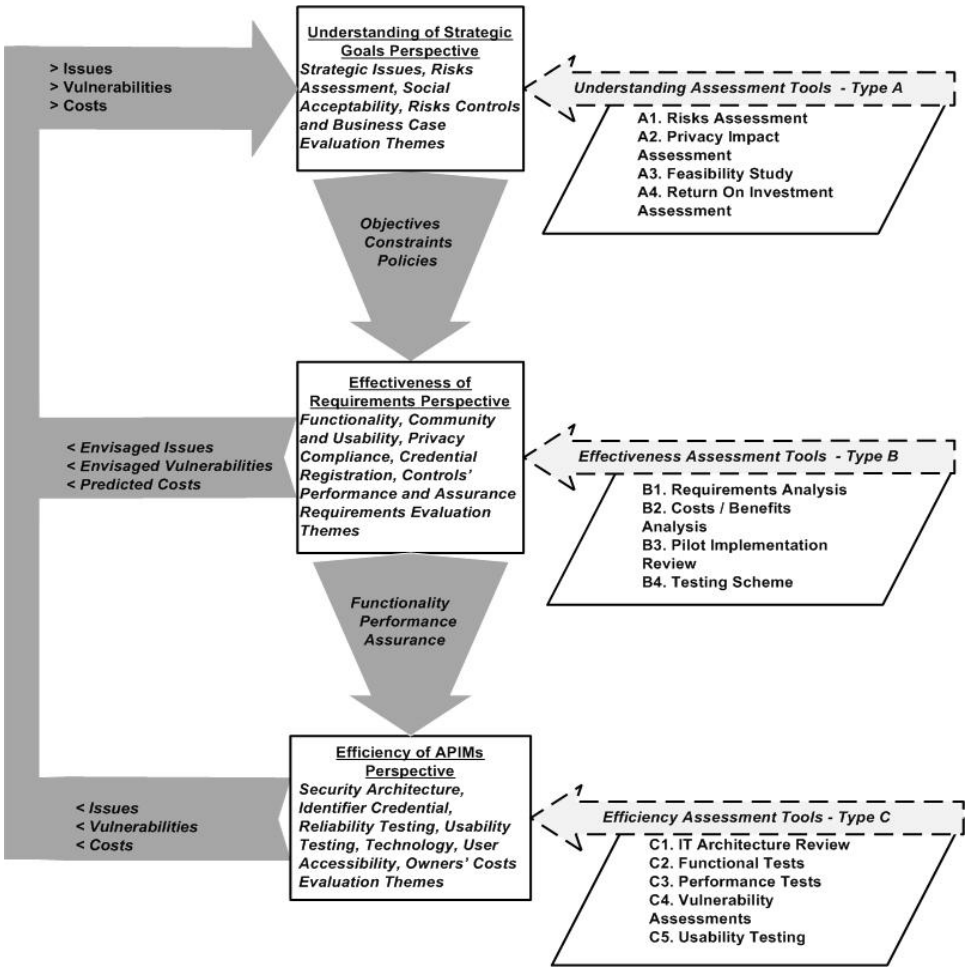

Figure 5.1: The ASMSA Evaluation Framework

The evaluation framework is not a simulation of an APIM. It represents a particular application context under evaluation, where an APIM has been deployed or an APIM may be introduced. This model is designed to represent our three identified evaluation perspectives, which relate to the characteristics of the application context in its current state, the objectives and requirements for the APIM in a desired state, and the attributes of candidate APIMs or a deployed APIM.

5.5.1 Aims of the ASMSA Evaluation Framework

The ASMSA Evaluation Framework aims to identify discrepancies in acquired data to introduce an APIM or to review a deployed APIM. The discrepancies are identified by comparing the acquired data in the evaluation themes of each perspective. The identification of the discrepancies in the acquired subject data help to inform decision-makers as an IS programme progresses from its inception stage, where purpose and incentives require sagacious consideration, through to eventual deployment and operation.

Data acquired relating to the application context, in the inception stages of an IS programme, may need to be expressed in broad terms. It may also be necessary to make many assumptions regarding the requirements for the APIM. As more information becomes available, from the use of our selection method with its criteria questions, data relating to these assumptions are refined, recalibrated or eliminated. Previously acquired data should then be compared in order to identify discrepancies between the existing data set and the additional acquired data set. The framework is designed to allow for iterative refinement of acquired subject data, i.e. revision of stakeholders' objectives and requirements, as further data are acquired from various primary sources as the IS programme progresses.

Subject data are gathered from primary data sources, categorised into assessment tools types, as shown on the three dashed horizontal patterned arrows on the right hand side in Figure 5.1. We describe the types of primary data sources later in Section 5.5.4. Data gathered from these sources are then used to respond to the criteria questions and are represented as subject data attributes in the evaluation themes of our evaluation framework.

5.5.2 ASMSA's Evaluation Perspectives

We elucidate on ASMSA Evaluation Framework's three perspectives.

Understanding of the Strategic Goals This perspective represents data relating to the strategic goals for application context in which the APIM will be introduced or has been deployed. This perspective aims, through using the criteria questions in the relevant evaluation themes, to acquire data so as to gain a thorough understanding of the application context, its stakeholders and their objectives for the APIM, particularly its main usage purpose and its intended subject community.

Data are acquired for this perspective using the criteria questions from the evaluation themes in the left column of Table 5.2 on page 177. The term *understanding* is preferred to the term *acceptability* because we believe that acceptance of an APIM may only be achieved through gaining an understanding of all stakeholders' views and their motivations related to application context in question.

Effectiveness of the Requirements This perspective is designed to acquire and represent the requirements for the APIM in order to determine whether the stipulated requirements fulfil stakeholders' articulated objectives.

Data are acquired for this perspective using the criteria questions from the evaluation themes in the middle column of Table 5.2. The requirements are expressed as functional requirements, performance requirements and assurance requirements. This perspective also represents information regarding the nature of the user's interactions to use the APIM. It also represents information about the assurance test plan or test scheme describing as to how, and the extent to which, the assurance properties of the APIM need to be tested.

Criteria questions in the Effectiveness of Requirements Perspective also seek to help define the Key Performance Indicators (KPIs) in order to measure the effectiveness and efficiency of each candidate APIM as a solution to the identification problem. The criteria questions also seek explanations on how the defined KPIs are to be evaluated and the data to be acquired in order to measure the effectiveness and efficiency of a candidate APIM.

Efficiency of APIM Solutions The efficiency of solutions perspective is designed to represent the attributes of candidate APIMs or a deployed APIM in order to determine the extent to which a candidate APIM or deployed APIM satisfies the stipulated requirements for an APIM. Data are acquired for this perspective using the criteria questions from the evaluation themes in the right column of Table 5.2.

This perspective also represents the vulnerabilities, issues and costs associated with the candidate APIM or deployed APIM. We observed through our classification of factors that all deployed APIMs possess vulnerabilities, attract issues and incur costs; however, this statement requires empirical grounding using data from our case studies. The selection of an APIM is identified on the basis of its efficiency to satisfy the stipulated requirements for the APIM together with the evaluation of the APIM's associated vulnerabilities, issues and costs.

5.5.3 Interrelationships Between ASMSA's Components

ASMSA's Evaluation Framework, as illustrated in Figure 5.1, is designed to work in conjunction with ASMSA's Selection Method, as represented in Figure 5.3. The 18 evaluation themes identified are incorporated into the respective perspectives of the evaluation framework as shown in Table 5.2. The types of tools to acquire subject data for each perspective are represented by the dashed arrows on the right hand side of Figure 5.1.

The data acquired for the factors in their evaluation themes, using the criteria questions, collectively represent the three perspectives in the ASMSA Evaluation Framework. The ASMSA Selection Method comprise three phases which uses the criteria questions to acquire data for the ASMSA Evaluation Framework's three perspectives.

The influence relationships between the data recorded in the three perspectives of the ASMSA Evaluation Framework are:

1. Output Data from the Understanding Perspective The influencer data outputs from the Understanding Perspective are the stakeholders' objectives for the APIM; the constraints, e.g. legal, legacy infrastructures and budgetary; and broad organisational and social policies. The term *policy* should be construed as consisting of general principles rather than low-level implementation security policies, e.g. minimum number of characters in a user's password. The constraints set the scope of the APIM and its boundaries in which the requirements are determined.

Output data represented in the Stakeholders' Objectives, Policies and Constraints evaluation themes from the preceding Understanding Perspective as shown in Figure 5.1, forms part of the input data into in the Effectiveness Perspective. Subject data acquired from Type B Effectiveness Assessments are the alternative data source.

2. Output Data from the Effectiveness Perspective The data outputs from the evaluation themes of the Effectiveness Perspective form data inputs into the Understanding Perspective. The data outputs in the Functional Requirements, Performance Requirements and Assurance Requirements evaluation themes of the Effectiveness Perspective also form the data inputs into the Efficiency Perspective.

The effectiveness attribute data in the Functional Requirements, Performance Requirements and Assurance Requirements evaluation themes of the Effectiveness Perspective form the basis upon which candidate APIMs or an APIM deployment are to be evaluated in terms of their capability and efficiency to fulfil the stipulated requirements.

The influencer data output from the Effectiveness Perspective, as represented by the return arrow, form the influences into the Understanding Perspective, which may require stakeholders to revise their objectives or review identified constraints and policy directives. These data act as feedback validation of stakeholders' objectives to the Understanding Perspective. This review activity enables the identification of discrepancies between the data represented in the Understanding Perspective and the Effectiveness Perspective.

3. Output Data from the Efficiency Perspective The output data from the preceding Effectiveness Perspective forms part of the input data for the Efficiency Perspective. Subject data acquired from Type C Efficiency Assessments are the alternative data source.

The return arrow from the Effectiveness Perspective, as illustrated in Figure 5.1, representing the identified issues; identified vulnerabilities and actual stakeholders' costs in the respective evaluation themes influence the data in the Understanding Perspective. The identification of discrepancies between the Understanding Perspective, representing the objectives for the APIM, and the Efficiency Perspective, representing a candidate APIM or a deployed APIM, acts as feedback to stakeholders to enable them to review their objectives. Our evaluation framework is designed to enable evaluation at any juncture in an IS programme or upon demand following the deployment of an APIM.

The reconsideration of the data in the Understanding Perspective, from data outputs from the Effectiveness and Efficiency Perspectives, and Type A Understanding Assessments may bring about changes in stakeholders' objectives or revision of some constraints. An APIM may also be granted exemption from certain organisational policies. Any amendments are then reflected in the respective evaluation themes in the Understanding Perspective.

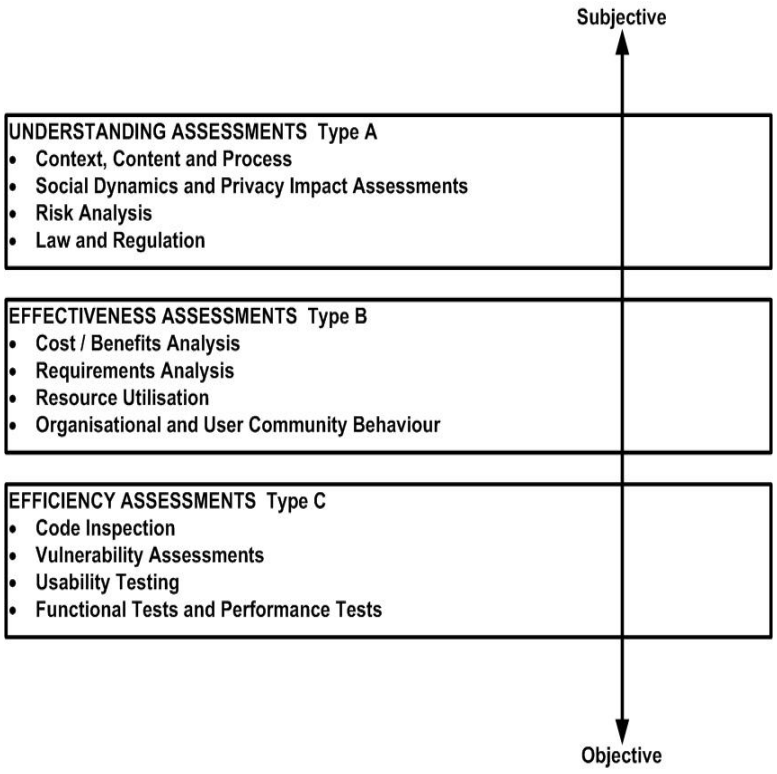

Figure 5.2: Spectrum of Assessment Tools for Acquiring Subject Data

5.5.4 Categorisation of Primary Data Sources

We used Smithson and Hirschheim's comprehensive review of IT assessments [272] as our basis to formulate our categorisation of the types of assessment tools containing primary data. IT assessments fall across the spectrum between objective and rational analysis to subjective and political considerations [97]. Additionally, we also recognise that assessments may report their findings with varying degrees of granularity and scope, from high-level macro assessments through to micro interrogations, e.g. program coding reviews, as represented in Figure 5.2.

We categorise the primary data sources into three broad types to correspond with the ASMSA Evaluation Framework's three perspectives. The assessment tool examples shown in Figure 5.2 are indicative only, based upon our review of the literature, and these representations should not be construed as an exhaustive list of primary data sources.

Subject data are acquired from the primary data contained in the following assessment tool

types:

Type A – Understanding Assessments Subject data for the Understanding Perspective are acquired from primary data contained in understanding type assessments, which have investigated the characteristics of the personal automated identification problem in the application context and have ascertained stakeholders' objectives.

The purpose of an APIM may be part of an organisation's security architecture which controls employees' access to enterprise data and resources. Alternatively, the introduction of a business application may require an APIM as an enabling technology. For example, an Internet banking service must, in accordance with financial regulations in some jurisdictions, identify and authenticate its customers.

Subject data are designed to be acquired from primary data contained in understanding assessments data during a programme's inception stages to introduce an APIM or during the initial stages to review a deployed APIM.

Type B–Effectiveness Assessments Subject data for the Effectiveness Perspective are acquired from primary data contained in effectiveness type assessments, which focus on the stipulation of requirements for the APIM.

Effective requirements engineering is fundamental to an organisation's ability to develop products and services in order to keep pace with change and increasing complexity [138]. The form of the primary data describing requirements for the APIM information may be contained in documentation, expressed in natural language, or in UML notation, or may be represented by a prototype APIM implementation.

The requirements in the ASMSA Evaluation Framework need to be expressed in natural language, however, to enable direct comparisons with data acquired in other perspectives. Requirements expressed in different forms which use different communication protocols, irrespective of their levels of abstraction, serve as subject data for the Effectiveness Perspective.

Subject data are acquired from effectiveness type assessments during a programme's requirements development stages *after* stakeholders' objectives have been identified and articulated to introduce or to review an APIM.

Type C–Efficiency Assessments Subject data for the Efficiency Perspective are acquired from primary data contained in efficiency type assessments, which occur during the activities to evaluate candidate APIMs or to evaluate a deployed APIM against stipulated requirements for the APIM.

The primary data for a candidate APIM may be generated by potential APIM suppliers, possibly in the form of a bid response to an organisation's Request For Product (RFP) notice, which describes the functionality and performance capabilities of their offering. Alternatively, data may emanate from supplier's technical specifications.

The data for a deployed APIM may come from a variety of sources, both internal and external. An organisation may seek data from performance tests to ascertain availability statistics, throughput rates, and failure rates from an internal laboratory deployment. These types of statistics from deployed APIM may be derived from event entries collated in audit logs. Alternatively, data may originate from other sources where the APIM technology has been deployed in similar application contexts or may originate from independent accredited assurance sources.

Subject data are acquired by using the criteria questions and extracting the relevant data evidence from the primary source material available.

5.6 The ASMSA Selection Method

In his framework for evaluating methodologies Jayaratna defines [165] ill-structured contextual situations as circumstances when stakeholders' objectives are vague or conflict, the identification problems are not understood, the subjects' attitudes are uncooperative, and the relationships between the stakeholders are complex and highly political. The circumstances surrounding decisions on APIMs often appear to meet for Jayaratna's criteria for ill-structured situations. For example, the introduction of an electronic identity card for UK citizens attracted much criticism because the objectives for the card were not made clear by the UK Government [317, 21].

We believe that the selection of the optimal APIM for ill-structured situations necessitate the use of well-defined systematic processes in order to formulate an understanding of the problem in its current state, a representation of the desired state to address the defined problem. In turn, candidate APIMs, or a deployed APIM, should be evaluated on the basis

of their capabilities to achieve that desired state. The ASMSA Selection Method is a meta-method, operating at a second order level, which aggregates and manipulates data acquired from primary evaluations, such as a risks assessment or a coding review. Data acquired from primary evaluations are the subject data of the processes and steps in our method. Our method consists of systematic processes segregated into three stages as represented in Figure 5.3. Each stage is deconstructed into discrete steps, to acquire and evaluate data for the selection of the optimal APIM for a given application context. Some steps are designed to acquire subject data from the application context while the remaining steps involve the manipulation, validation and reconciliation of that acquired subject data.

The ASMSA Selection Method's processes acquire subject data, using the criteria questions, systematically in order to extend the breadth of coverage and the granularity of data acquired for evaluation.

The ASMSA Selection Method's processes, using the criteria questions, are designed to remove misunderstandings that may arise from vague or implicit interpretations of primary data. As supplemental information are acquired during the use of our selection method then previous responses to criteria questions may need to be reconsidered or outstanding assumptions revisited. We acknowledge that there may be some assumptions, however, that cannot be eliminated entirely. For example, assumptions relating to threats are inevitable as miscreants' underlying motives are ephemeral and speculative by nature [78].

The ASMSA Selection Method consists of three stages which aims to inform decision-makers continuously. The purpose of each stage is to ascertain:

- Stage 1 - an understanding of the application context in order to identify and articulate stakeholders' objectives for the APIM and a hierarchy of stakeholders' preferences;
- Stage 2 - the effectiveness of the stipulated requirements for the APIM to fulfil stakeholders' objectives by reconciling requirement statements with stakeholders' objectives; and
- Stage 3 - the efficiency with which a candidate APIM or a deployed APIM satisfies the stipulated requirements.

The ASMSA Selection Method identified and articulates stakeholders' objectives at the outset so that requirements for the APIM may be reconciled against those stated objectives.

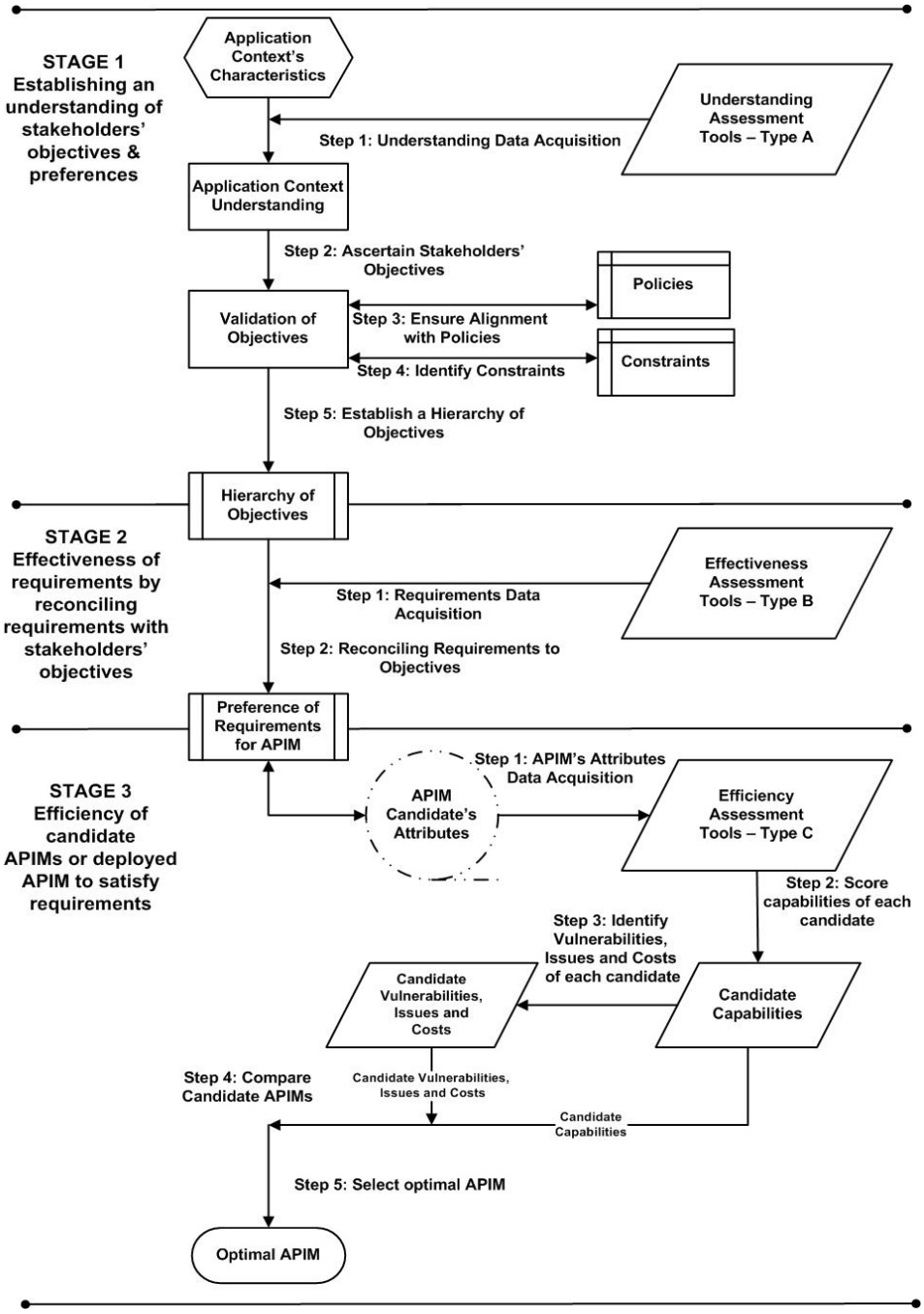

Figure 5.3: Overview of the ASMSA Selection Method

Similarly, our method requires candidate APIMs or a deployed APIM to be described comprehensively so that their capabilities may be evaluated against the stipulated requirements. This evaluation includes a task to rate the capabilities of candidate APIMs or a deployed APIM quantitatively. Our method also contains processes to identify the APIM's issues, vulnerabilities and costs associated with deploying an APIM in the application context. The ASMSA Selection Method analyses several key variables with mixed data types in order to select the optimal APIM.

Our selection method incorporates a parallel task, throughout all stages, to manage stakeholder consultation processes, as advocated by Hemmati [128], for reconciling conflicting stakeholders' objectives. The use of this technique in our methodology relies upon collaborative dialogue between stakeholders' representatives, including subjects and users, in order to acquire data on stakeholders' objectives and also to coordinate effort to facilitate stakeholder trade-off compromises and preferences for the APIM.

Our method is designed to ensure that data are acquired, reconciled and manipulated in a systematic manner, in order to bring regularity to the programmatic processes of selecting the optimal APIM for a given application context. We now describe the steps in each of the ASMSA Selection Method's three stages.

5.6.1 Stage 1–Establishing an Understanding of Stakeholders' Objectives

The purpose of this initial stage of our selection method is to identify and articulate stakeholders' objectives for the APIM and a produce a hierarchy of preferences from an understanding of the application context.

The five steps in Stage 1 of our method are designed to acquire subject data relating the application context from the information contained in outputs produced from Type A Understanding Assessments. The stakeholders' objectives based upon contextual information, together with assumptions, policy directives and constraints influence the evaluations in Stage 2 of our method. The ASMSA Selection Method incorporates the principles of the MOMC decision-making technique [173, 96] to identify and articulate stakeholders' objectives and to prioritise their preferential values for the APIM. The stakeholders' objectives are then deconstructed in order to produce a hierarchy of objectives and preferences.

The primary data sources may include a business case for the APIM, feasibility study for

the APIM and project initiation documentation that describe the purpose for the APIM, the intended subject community, and the environment, both physical and logical, in which the APIM will operate. Primary data from assessments, such as risks assessments, privacy impact assessments are also used to acquire data in order to respond to the criteria questions. The method depends upon the output of a risks assessment, however rudimentary, in order to determine the extent to which identification assurance is needed for the APIM.

While the output in these assessments may contain factual impact data, e.g. actual losses, much of these types of assessment rely on probability predictions and assumptions. Probabilities, which are based upon individuals' beliefs, preferences and utility judgments, influence subsequent analysis and decision-making [179]. The method is designed so that probability predictions may be recalibrated following the acquisition of further relevant data. The method is also designed to reduce the impact of assumptions by ensuring that all assumptions are reviewed at the end of each stage in our method.

5.6.1.1 Step 1–Understand the Application Context

An understanding of the application context is achieved by acquiring subject data, using the criteria questions in the Strategic Issues, Risks Assessment, Social Acceptability, Risks Controls and Business Case evaluation themes from the application context's primary data sources.

This step requires that the rationality for introducing or revising an APIM is articulated concisely by the sponsor stakeholder, in order to avoid misinterpretation, irrespective of the underlying political or commercial drivers. Clarity of the APIM's purpose assists the processes in our selection method to acquire the relevant data and the evaluation of that acquired data in its succeeding steps.

We anticipate that a substantial amount of data acquired in this step may be based on assumptions; however, our method allows for data to be added or revised following corroboration with other data acquired during later steps of our method. The design of our selection method enables an iterative approach in that an evaluation may return to any previous step.

5.6.1.2 Step 2–Ascertain Stakeholders' Objectives

This step is one of the most critical in our method because stakeholders' willingness and commitment to use an APIM should be determined at the outset. The criteria questions in the Business Case Evaluation Theme are used to acquire data on the stakeholders' objectives for the introducing or revising an APIM.

Subject data are acquired from all relevant stakeholders so that a diversity of viewpoints help to reduce the risks of specifying incomplete objectives for the APIM. There may be circumstances, however, which prohibit the involvement of the subject or user community or there may be monetary or time constraints that inhibit efforts to establish all stakeholders' objectives, given the core purpose for the APIM.

This step requires managed consultation with the stakeholders in order to obtain their views and degree of commitment for introducing or revising a deployed APIM for the application context. The initial task of stakeholder identification is important, so that interested parties, both direct and indirect entities, engage in the consultation processes.

In some application contexts the objectives of indirect stakeholders, not operating in the application context, are also identified and included within the consultation processes. Indirect stakeholders may be impacted adversely by the failure of an APIM to identify genuine subjects to a predetermined level of assurance.

The data acquired representing the stakeholders' objectives are then compared for alignment with the sponsor stakeholder's purpose for the APIM. Depending upon the outcome of the processes to align stakeholders' objectives, with the stated purpose of the APIM, this step may require the re-evaluation of the stated purpose for the APIM or further clarification of some of the stakeholders' objectives.

The sponsor stakeholder may, however, opt to cancel or postpone the introduction of an APIM where significant conflict between stakeholders may not be resolved satisfactorily for all interested parties. In such cases our method should be aborted at this step.

5.6.1.3 Step 3–Ensure Alignment with Policies

This step requires the acquired stakeholders' objectives for the APIM to be checked for their alignment with stakeholders' organisational policies. These policies may include ethical

policies and environmental directives together with security policies. The criteria questions in the Risks Controls and Social Acceptability Evaluation Themes should be used to acquire data to ensure alignment with stakeholders' organisational policies.

From the result of these comparisons, it may be necessary for some organisations, particularly the sponsor, to seek exemption or refine policies in order to accommodate all the stakeholders' objectives. Alternatively, some objectives may need to be re-evaluated and possibly revised or removed where the results of comparing the objectives for the APIM contradict a policy that may not be revised.

5.6.1.4 Step 4–Identify Constraints

This step requires the identification of constraints to introduce an APIM or revise a deployed APIM for the application context. The criteria questions in the Business Case, Social Acceptability and Strategic Issues Evaluation Themes are used to acquire data in order to identify the constraints relating to introducing or revising an APIM.

Information system development effort together with associated budgetary restrictions and delivery timescales are often recognised as constraints on APIM deployments. Nevertheless, other constraints need to be identified, such as international interoperability, social norms, infrastructure limitations and legacy system restrictions, which may impact the stakeholders' objectives.

5.6.1.5 Step 5–Establish a Hierarchy of Objectives

In this step we draw heavily on Homburg's technique [134] to create a hierarchy of objectives and preferences for the APIM. The hierarchy of stakeholders' objectives articulated are to be mapped to requirements in Stage 2 Step 2, which we describe later in Stage 2. The tasks in this step are as follows:

A. Review Articulation of Objectives Review the stakeholders' objectives data acquired in order to determine whether the objectives have been described sufficiently to reflect the purpose for the APIM. This task also ensures that implied objectives are stated explicitly. Also the review determines whether the stated objectives for the APIM have the potential to be achieved within the identified policies and constraints. The result of

this review may require a revision of some stakeholders' objectives.

B. Rank Objectives through Consultation Consult the stakeholders to rank the stated objectives, using the MSP technique, as a continuation of their engagement that was established in Stage 1. This prioritisation task is geared to demonstrate the sponsor or decision authority's accommodation of the stakeholder's preferences and to provide documentary evidence where trade-offs have been conceded. Each high-level objective is assigned to a preference category, e.g. *must* have, *should* have, and *desirable*, to indicate its agreed priority with stakeholders. There may be a point where a judgment has to be made regarding stakeholders' expectations. The engagement of an acceptable independent mediator, using MSP consultation processes, has the potential to identify compromises, with advantages for all, thereby overcoming disputants' tensions and antagonisms [87]. Failure to obtain stakeholder acceptance may result in stakeholder actions that hinder progress to realise the stated purpose or goal for the APIM.

C. Decompose the Objectives Decompose the APIM's objectives until the sub-objectives become broad high-level requirement statements. This task results in a description of the sub-objectives to fulfil the prime stakeholders' objectives for the APIM. Homburg advises [134] that the more the objectives in the hierarchy are sub-divided the easier it becomes to recognise the attributes for measurement and their appropriate scale. These attributes, i.e. requirements, are acquired and validated in the next stage of our method.

5.6.2 Stage 2–Reconciling Requirements to Stakeholders' Objectives

The main aim of our method in Stage 2 is to identify and articulate the requirements for the APIM. The secondary aim is to identify potential issues and deficiencies in the requirement statements to fulfil the stakeholders' objectives.

The steps in Stage 2 of our method acquire subject data using the Type B Effectiveness Assessments in order to document the requirements for the APIM. The stipulated requirements for the APIM are then reconciled against the stakeholders' objectives and preferences, as represented in the hierarchy of objectives. This reconciliation task determines whether the stipulated requirements effectively fulfil the stakeholders' objectives and preferences for the APIM.

The functional, performance and assurance requirements statements together with the pro-

posed assurance test plan, as outputs from Stage 2 of our method, represent a requirements specification for the APIM. This specification may be used to engage with potential suppliers of APIM technologies or services; however, such procurement processes are beyond the scope of our research.

5.6.2.1 Step 1–Requirements Data Acquisition

This step uses the criteria questions in the Functionality, Community and Usability, Privacy Compliance, Credential Registration, Controls' Performance and Assurance Requirements evaluation themes in order to acquire the data to specify the requirements for the APIM.

Information system requirements are captured from a variety of primary sources which include interviews with stakeholders, scenario exploitation in workshops, appraisals of existing systems, prototyping and studies [138]. Our method is designed to utilise these primary data sources and also outputs from participative design tools in order to acquire subject data relating to the requirements for the APIM. Avison suggests [20] that the advantages of using a participative design approach, not only includes output covering the design of the information system and identification of its required technological components, but also the deliverables expected during the various stages of the IS development project, e.g. requirements specification.

The following tasks in this step are also designed to review the acquired requirement statements in Stage 2 against the objectives in acquired in Stage 1 in order to identify discrepancies in the data for the APIM:

A. Validation of Requirements A review of stipulated requirements is required to identify contradictory and vague expressions which may result in misinterpretations. This activity also involves checking the alignment between the APIM's user interaction dialogue and the users' operational tasks. This activity is also designed to identify potential vulnerabilities in the functional and non-functional requirements for the APIM. The output from using of prototypes, simulations, or where possible, pilot APIMs in live operational environments is used to validate stipulated requirements and also to identify refinements.

B. Costs Estimations Cost estimations are performed to determine whether the proposed requirements for the APIM, as stipulated at this juncture, have the potential to fulfil the

benefits, as stated in the business case, within the budget, as estimated in the feasibility study. The main output from this task is to estimate the costs for the APIM and to identify issues which may impact stakeholders' objectives.

C. Test Methodology and Assurance Resources The test methodology is employed to assess the assurance attributes of the candidate APIM or deployed APIM. The aim here is to state how data test evidence to substantiate claimed capabilities are to be collated and represented. Criteria questions are designed to acquire data on test plans and corresponding test specifications of the functional and non-functional requirements for the APIM. The APIM may also need to be tested to meet assurance requirements set by external governance parties to a commonly recognised assurance scheme, e.g. common criteria protection profile, to demonstrate specific assurance capabilities.

D. Reduce Assumptions This task is designed to eliminate assumptions made in response to the criteria questions, during the data acquisition processes of Stage 1 and Stage 2. Where it is not possible to eliminate assumptions then the basis upon which those assumptions need to be reviewed. Where data acquired include calibrated estimations, based on Hubbard's measurement rules [136], then the basis for these projections also need to be reconsidered. The aim of this task is to reduce uncertainties for the APIM by minimising the risks associated with assumptions.

5.6.2.2 Step 2–Matching Requirements to Objectives

In this step, the requirements specified are reconciled against the agreed stakeholders' objectives in order to identify any discrepancies in the acquired data. Essentially, the effectiveness of requirements is determined by the extent to which they fulfil stakeholders' objectives for the APIM, within the limitation of identified constraints and policies.

The first task in this step is to reconcile stakeholders' objectives and requirements to ensure that all stakeholders' objectives have at least one statement of requirement. A requirement may fulfil one or more stakeholder objective. Where a requirement cannot be reconciled to a stakeholder objective investigation is needed to ascertain whether there is a missing stakeholder objective or the requirement is spurious.

The aim of this reconciliation task is to ensure the requirements are complete, appropriate and consistent with the stakeholders' objectives. It also provides a means to identify redundant requirements. Depending upon the results of this step the objectives may need to be reviewed

with the stakeholders or the requirements for the APIM may require further examination.

The second task in this step is to evaluate envisaged issues and vulnerabilities together with estimated costs of introducing an APIM or revising a deployed APIM against the stakeholders' objectives. The outcome of this evaluation is to be communicated to the stakeholders to ensure that these envisaged issues, vulnerabilities and costs are acceptable to them in terms of fulfilling their respective objectives. The outcome of this evaluation may identify the need for some stakeholders to reconsider their objectives.

The task to ensure that envisaged issues and vulnerabilities together with estimated costs are acceptable to the stakeholders, therefore, is a critical activity in the ASMSA Selection Method.

The outcome of consultations between the stakeholders may result in the dilution or re-prioritisation of some of the stakeholders' objectives or alternatively it may indicate the need to increase the budget for the APIM or the termination of the IS programme. Apart from termination, if other options are chosen then the processes in Stage 2 of our selection method are to be repeated.

The data acquired and reconciled successfully, as a result of the two tasks in this stage, represent the qualities of APIM, i.e. requirement statements, which need to be evaluated against the attributes of candidate APIMs or deployed APIM. The steps for evaluating candidate APIMs or a deployed APIM are performed in Stage 3 of our selection method.

5.6.3 Stage 3–Efficiency of Candidate APIMs or Deployed APIM

The aim of our method in Stage 3 is to evaluate the subject data describing the capabilities of candidate APIMs or a deployed APIM against the stipulated requirements for the APIM in order to identify the optimal APIM for selection.

The initial processes in this stage evaluate the capabilities and the efficiency with which an APIM candidate fulfils the requirements for the APIM. Our method allows for several candidate APIMs to be evaluated against the requirements in order to perform comparisons between the candidates. This stage is also designed to identify vulnerabilities, issues and costs associated with each candidate APIM or deployed APIM.

The steps in Stage 3 of our method acquires subject data from primary data contained

in outputs from Type C Efficiency Assessments in order to represent the attributes and capabilities of the APIM. The extent to which an APIM's capability fulfils a requirement may be rated by an evaluator or, alternatively, an evaluation panel. A deployed APIM's capabilities are rated in respect to which its attributes currently fulfils the stated requirements. These rating values are generated in Step 2 and used in Step 4 and Step 5 in processes to ascertain the optimal APIM.

5.6.3.1 Step 1–Candidate APIM Data Acquisition

This step uses the criteria questions in the Security Architecture, Identifier Credential and Technology evaluation themes to acquire data in order to articulate the attributes of the APIM and its proposed configuration for the application context. The criteria questions in the Reliability Testing, Usability Testing and Accessibility testing evaluation themes are used to acquire data regarding an APIM's reliability, usability and accessibility capabilities respectively.

The primary data for these four evaluation themes may be acquired from a supplier, testing the candidate APIMs using trial deployments in a controlled environment, e.g. laboratory, and/or in the production environment, where possible. The application context may require specific tests to be performed in order to acquire data relating to an APIM's potential performance in a specific production environment. Performance testing in the laboratory or simulated use cases may also provide data on the accuracy and speed of an APIM to identify a person. These activities and subsequent analysis help to highlight the issues and vulnerabilities, if any, between requirements set and a candidate APIM's actual performance, later in Step 2.

Vulnerability assessments by the IS programme may be undertaken to determine the effort, i.e. the resources and knowledge, required to exploit possible attack vectors in the APIM for that application context. Additionally, a code inspection may also reveal lower level software flaws that could, potentially be exploited by miscreants. Vulnerabilities in APIM designs may not only stem from technological attack vectors but also those flaws emanating from user erroneous misuse of the APIM.

Usability tests and user accessibility tests may be undertaken by the IS programme to identify any interaction design deficiencies in the proposed APIM. These tests are user-focused to validate that the user is not only able to undertake their task efficiently, but also, as Yee advises [329], to assess the extent to which the user has confidence in the system to protect

their interests. These data are used to identify issues relating to the APIM later in Step 3.

5.6.3.2 Step 2–Rate the Capabilities of Each Candidate APIM

This step uses the data acquired in the previous step to evaluate a candidate or deployed APIM's capabilities against the stipulated requirements. The data acquired are used to rate an APIM's capabilities in respect of the extent to which it satisfies the stipulated requirements for the APIM.

This step requires a rating value for an APIM's capability to be entered against the factors in the Functionality, Privacy Compliance, Credential Registration, Controls' Performance and Assurance Requirements evaluation themes. This evaluation depends upon the sufficiency of data acquired in the previous step. Inadequacies in data acquired may require an evaluator to make assumptions, which need to be recorded.

The method uses a rating scheme based upon percentage fulfilment of the requirement. The rating scheme also employs adjusted weightings for either an evaluation theme or a specific factor. We have opted for a quantitative evaluation scheme rather than a qualitative scheme in order to provide greater granularity of grading an APIMs' capabilities to satisfy specific requirements. The use of quantitative evaluation scheme enables direct comparisons of fulfilment, for each evaluation theme, between the candidate APIMs' capabilities.

The data acquired from the previous step may contain specific values, e.g. false accept rates, or mixed data types from appraisals that use opinion based evidence. APIMs that fully satisfy all the requirements for APIMs are strong candidates for selection; however, the aim of this activity is to articulate the extent in terms of the proficiencies and also the deficiencies of each APIM to fulfil the stated requirements.

5.6.3.3 Step 3–Identify Issues, Vulnerabilities and Costs of Each Candidate APIM

The aim of the evaluation in this step is to identify issues, vulnerabilities and to clarify the costs associated with each candidate APIM or deployed APIM.

Subject data for this step are acquired from the tests results data using the criteria questions in the Reliability Testing, Usability Testing, User Accessibility Testing evaluation themes. Data from the remaining evaluation themes are also reviewed in order to identify issues and

vulnerabilities and to clarify the costs associated with each candidate APIM or deployed APIM. Subject data may also be acquired from deployments using the APIM in other similar application contexts.

The issues associated with an APIM may range from the need for users to purchase equipment, e.g. smart card readers, to the limitations of biometric identification technologies to acquire biometric data to an acceptable quality, e.g. fingerprint minutiae, for some subjects in the community. The vulnerabilities associated with an APIM may range from the identification of software coding errors to the distribution of users' authentication data, e.g. a PIN value, to the users through an open mail network.

The issues and vulnerabilities identified may be capable of being fully resolved, partially resolved or may be regarded by stakeholders as intractable. This step, however, is to identify and record those issues and not to address them at this juncture. Some issues relating to technological limitations of deployed APIMs suggest that stakeholders may need to re-examine their objectives or requirements. Some identified vulnerabilities may require additional security controls to minimise the impact of their exploitation.

A stakeholder may choose to accept some identified vulnerabilities and manage the residual risks associated with the identified vulnerabilities; however, at this juncture subject data are required on the estimated costs related to managing identified issues and the costs of additional controls to minimise the impact of an identified vulnerability.

Subject data for the APIM costs may be acquired from suppliers and also from internal reviews of the impacts of the APIM on existing information systems, infrastructures and resources. Our criteria questions are posed to acquire data on various costs elements from the capital cost elements, e.g. purchase of technology, technology development and integration, and maintenance costs relating to the effort to support the APIM continually.

The completion of this step enables the cross-case evaluation of candidate APIMs for a new application context and also the evaluation of candidate APIMs to replace or to enhance a deployed APIM.

5.6.3.4 Step 4–Comparison of Candidate APIMs

This step differs depending upon whether the evaluation relates to the *introduction* of an APIM or a *deployed* APIM.

For those circumstances that require to *introduce* an APIM then our method compares the data acquired for each candidate APIM. This step involves the cross evaluation of the candidate APIMs against four main constructs:

1. The capability ratings of the candidate APIM against the stated requirements.
2. The issues associated with the candidate APIM.
3. The vulnerabilities associated with the candidate APIM.
4. The level of investment required by the sponsor and other stakeholders to deploy and operate the APIM.

There may be several candidate APIMs that possess the required capabilities, possess vulnerabilities with minimal impact, attract issues that may be resolved or managed with reasonable effort, and require a level of investment that falls within the budget to introduce and operate the APIM over its expected life time.

The method, at this juncture, requires the elimination of some of the candidate APIMs, using the capability and investment constructs in order to produce a short-list so that selection effort is concentrated on two or three candidate APIMs.

The initial task involves the elimination of candidate APIMs with capabilities that that do not satisfy the stipulated requirements for the APIM, in that their assigned scores fall below the 50 per cent threshold, i.e. denoting that their capabilities are insufficient.

Next the remaining candidate APIMs are eliminated from the selection process if a candidate APIM possesses vulnerabilities which are not capable of being remedied or accepted by stakeholders. Similarly, a candidate APIM that could potentially attract intractable issues, which may be impractical to manage, e.g. large proportion of subject community unable to produce a specific biometric modality, is also eliminated from the selection process. Where stakeholders opt to include a candidate APIM with issues and vulnerabilities then the costs of compensating for these two elements need to be ascertained by the evaluator.

The total cost of an APIM is derived by aggregating the investment required for the candidate APIM together with the costs related to managing the identified issues and the costs of controls to reduce the risks related with identified vulnerabilities which are associated with the candidate APIM. Candidate APIMs with total costs that exceed the budget for the APIM,

over its expected life time, are eliminated from the selection process. We eliminate these candidate APIMs on the assumption that it would be difficult to justify the deployment of an APIM if its total costs exceed stakeholders' loss expectancies or the claimed stakeholders' benefits for the APIM were exceeded by the total costs for the APIM.

The candidate APIM with the highest capability score is evaluated as being *the optimal APIM* for the application context provided that the total cost of that candidate APIM falls within the budget allocated by stakeholders.

If no candidate APIM remains within the budget allocated then our method requires the stakeholders to review the original budget against the stakeholders' objectives and the requirements for the APIM. Stakeholders may decide to refine their objectives or revise their requirements for the APIM. Stakeholders may also decide to terminate the introduction of an APIM. Our selection method is then invoked at the appropriate juncture and the evaluation continues with the modified data, depending upon the outcome of stakeholders' deliberations on increasing the budget and/or revising the requirements for the APIM.

In order to determine the effectiveness and efficiency of a *deployed APIM*, then this step requires a gap analysis to be performed between stipulated requirements and the APIM's actual performance together with an evaluation of the identified issues, vulnerabilities and total costs. The system owner or stakeholder decision authority may, depending upon the outcome of the gap analysis, choose to remain with the deployed APIM or may decide to investigate possible changes to the deployed APIM.

Data acquired from candidate APIMs to replace or enhance a deployed APIM may then be evaluated against the stipulated requirements using the steps in Stage 3 of our selection method. Based upon the results of these evaluations stakeholders may select to remain with the deployed APIM or may decide to enhance or replace the existing APIM.

5.6.3.5 Step 5–Select Optimal APIM

This step uses the extrapolations in the previous step to select the candidate optimal APIM with the *highest scored capabilities exhibiting manageable issues and vulnerabilities together with acceptable costs* to fulfil the requirements for the APIM. An optional task in this step is to formulate a justification for the selected APIM.

Where the results of these evaluations produce are two candidate APIMs with the identical

capabilities then the weightings for critical factors are adjusted according to stakeholders' preferences. It may also be necessary to review the rating values allocated to these factors for other candidate APIMs which were eliminated from selection in the previous step. The resulting scores for candidate APIMs with identical capabilities should then reveal the more favourable candidate APIM; however, the variation between weighted scores may only be marginal.

Each candidate APIM possesses capabilities to fulfil the stipulated requirements and also some deleterious properties. Where a situation demands demonstrable impartiality or decision transparency, it may be appropriate to engage an independent authority to oversee some of the processes in our selection method. An independent authority may also need to communicate the justification of their decision to select a particular APIM to stakeholders and other interested parties.

Essentially, the data acquired and data manipulation activities in ASMSA Selection Method's processes form an audit trail which provides substantiated evidence to justify the selection of a particular APIM. We recognised, from the development of our selection method, that further data, in addition to data relating to our initially identified factors, needed to be acquired from the application context, e.g. stakeholder's objectives and predictions on costs for the APIM. The data acquired from our three case studies not only enabled us to validate our initially identified factors but also assisted us to identify further factors for evaluating APIMs.

5.7 The ASMSA Decision Support System

This section describes the ASMSA Decision Support System (ASMSA-DSS) which is our implementation of the ASMSA Methodology. We did not set out to develop a decision support system per se; however, we recognised that we needed a software tool to support our research activities.

A Decision Support System (DSS) is an interactive computer-based system or subsystem intended to help decision-makers use communications technologies, data, documents, knowledge and/or models to identify and solve problems, complete decision process tasks, and make decisions [239]. A DSS is a type of expert system which is often used to solve or to provide a software support tool in order to solve problems that are normally encountered by

human experts, or practitioners, in given situational contexts [294].

Royer argues [257], based upon interviews with several IdM discipline experts, that a DSS is necessary, due to the contextual complexities, to support decision-makers in selecting the appropriate enterprise IdM system. We developed the ASMSA-DSS prototype to assist our research effort to validate our methodology and to manage our large data sets (mainly in text form) acquired from our three case studies.

5.7.1 Design of the ASMSA-DSS

The design of our DSS draws on Sowa's knowledge representation principles [273] to represent discipline experts' knowledge in an expert system.

The ASMSA-DSS prototype is designed to mirror the stages and steps of the ASMSA Selection Method, which include the factors and the criteria questions in the evaluation themes of the ASMSA Evaluation Framework. The steps in the ASMSA-DSS involve data acquisition, using the criteria questions or data manipulation tasks to align with the ASMSA Selection Method. The ASMSA-DSS is designed to aid the evaluation of qualitative acquired data, in a series of processes, in order to identify the optimal APIM.

The ASMSA-DSS prototype possesses functional utilities to search for textual elements in the acquired data sets and to generate standard reports, which include tables and graphs. These utilities proved a valuable tool in our analysis of our three case study data sets. The ASMSA-DSS also contains a program function to differentiate candidate APIM capability rating scores quantitatively. The ASMSA-DSS prototype does not determine the optimal APIM for the application context in question by using fuzzy logic or similar mathematical decision modelling techniques. Its main purpose is to manage large data sets in order to evaluate data qualitatively.

Makowski and Wierzbicki argue [192] that the key design question for decision support systems is about separating the representation of objective knowledge and subjective information in the decision context. Objective knowledge relates the external physical, technical and environment characteristics of the application context. Subjective information includes the individual knowledge and preferences of stakeholder organisations' decision-makers.

We adopt an integrated approach in that some of our criteria questions seek factual knowledge from the application context while other criteria questions demand sagacious consideration,

particularly information relating to a contemplation of values and expression of preferences. An example of a criterion question requiring a careful contemplation of values could relate to a trade-off between increased investment levels versus marginal system performance in terms of identification throughput speeds.

The ASMSA-DSS prototype system allowed us to segregate our efforts to manage our acquired case study data from our activities of amending, creating and removing factors as a result of our factor validation efforts. Our DSS is essentially a software application in which we could manipulate its processes and content to align with the ASMSA Methodology's components as they evolved during the implementation of our research plan.

The ASMSA-DSS prototype is designed to be utilised by an evaluator user or discipline expert user to acquire data from an application context in order to identify the optimal APIM. The interface is menu-driven in that the user may choose when to insert data acquired relating to a specific factor rather than being forced to answer the criteria questions in the prototype sequentially. We provide screen shots samples of an evaluator's tasks to input data into the ASMSA-DSS prototype and also to manipulate that data.

Figure 5.4 shows the ASMSA-DSS' user interface for the evaluator user's task to enter acquired data, in this case a requirement for covert or overt identification. This figure shows the factor of '6. Overt or Covert Identification' followed by two criteria questions underneath and the acquired data 'The identifier / password is overt identification ..... ' in the dialogue input box below.

Figure 5.5 shows the ASMSA-DSS prototype's user interface for the evaluator user's task involving a data manipulation activity, where the objectives for an APIM are reconciled against the detailed requirements for an APIM. This figure shows 'Objective 1 of 66' with the objective of 'Minimise any learning.....' in the dialogue box below, which has been reconciled against the requirements listed in the 'Matched requirements' dialogue box. The list of requirements in the dialogue box below 'Available requirements' may be selected by the evaluator user to fulfil the stated objective of 'minimising any learning'.

One of the key functionalities of the ASMSA-DSS prototype, in order to align with Homburg's objectives deconstruction technique [134], is to ensure that all objectives possess subordinate requirements and all requirements are linked to one or more parent objective. The ASMSA-DSS prototype provides screen warnings if these conditions, as shown in the top right quadrant of Figure 5.5, are not met.

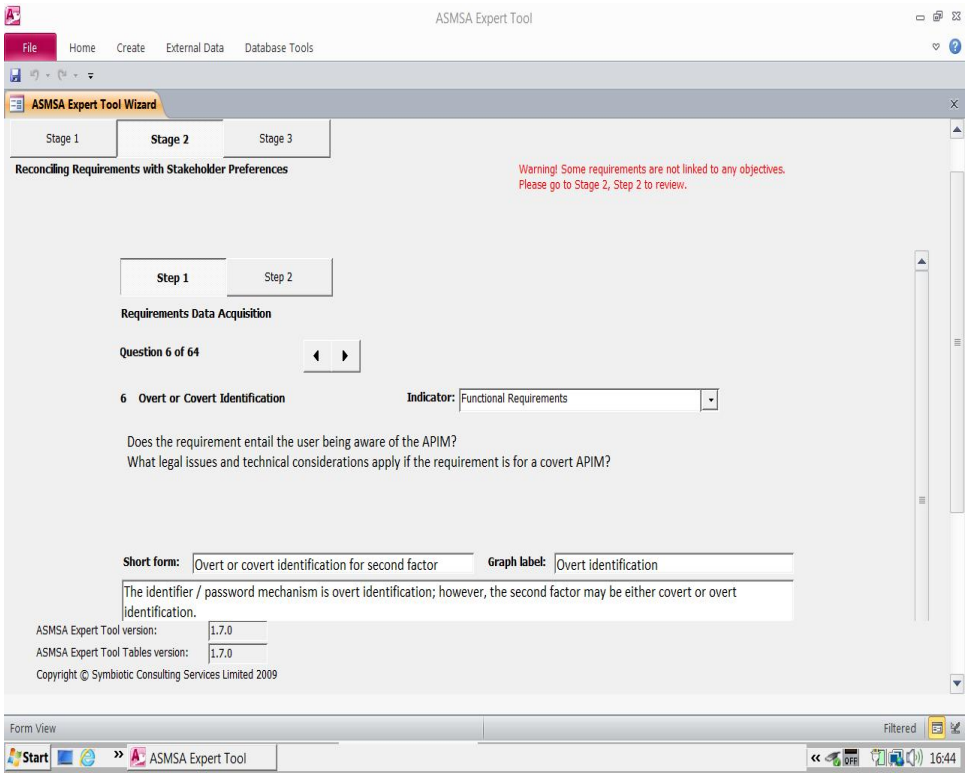

Figure 5.4: Entering Acquired Data into the ASMSA-DSS Prototype

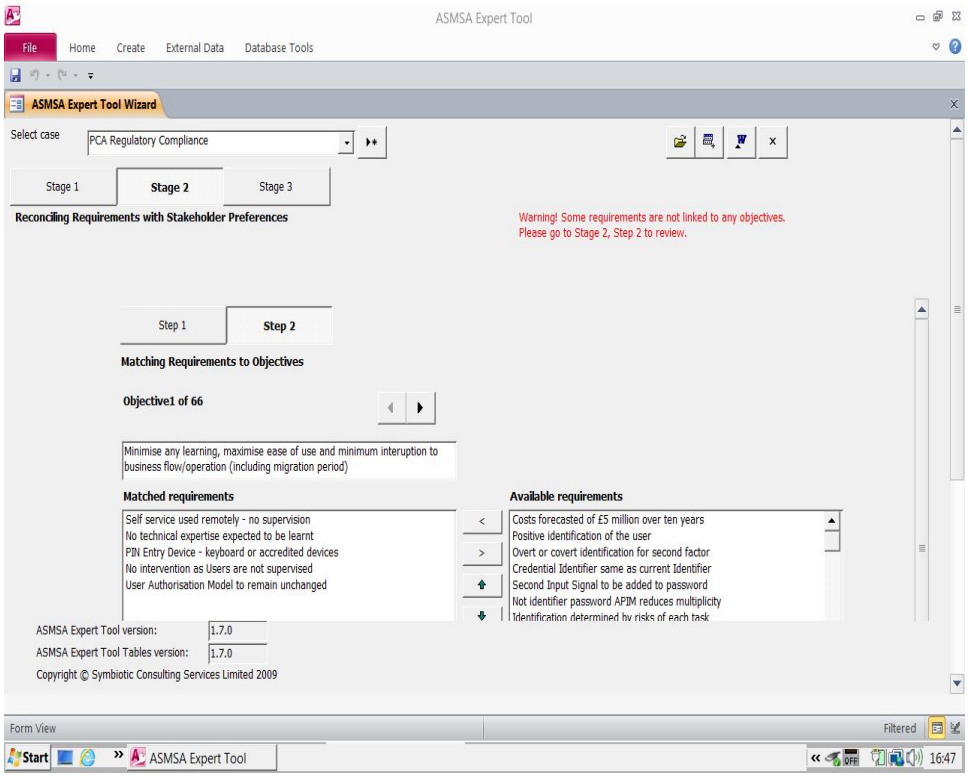

Figure 5.5: Manipulating Acquired Data in the ASMSA-DSS Prototype

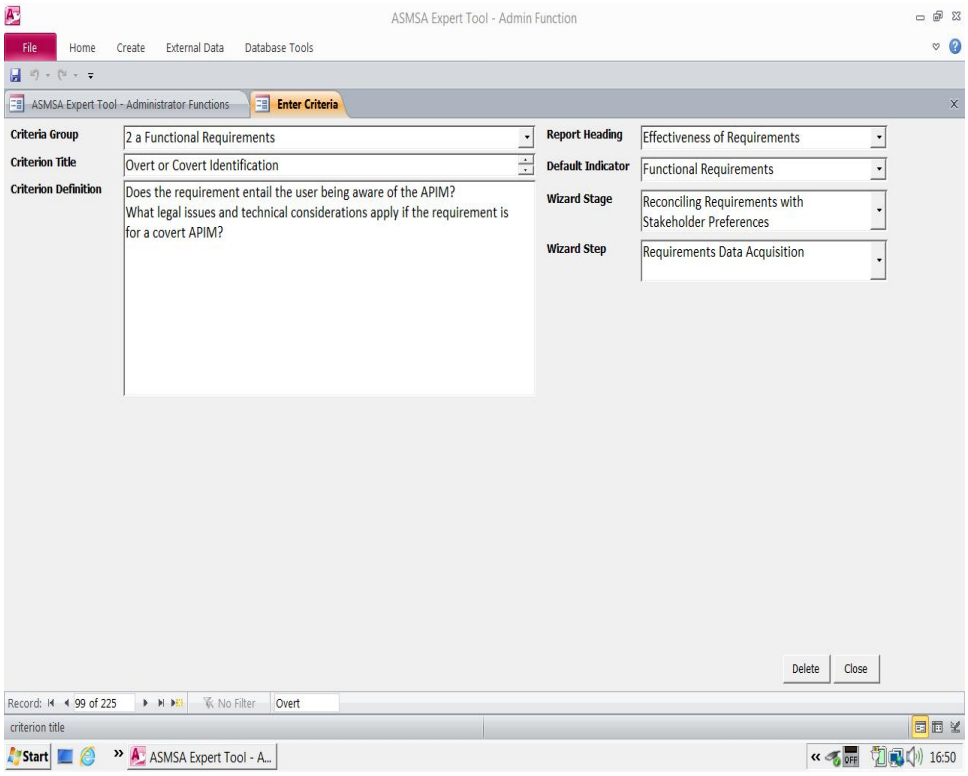

Figure 5.6: Managing Factors in the ASMSA-DSS Prototype

The ASMSA-DSS prototype is also designed to be utilised by an administrator user with the functionality to add, amend and delete a factor or to move a factor between evaluation themes. We used the administrator user account to add the initial factors identified in our review of the literature. We also used this account to add the steps within each stage of the ASMSA Selection Method. The administrator user account also contains functions to rename a factor title or to revise the criterion question related to a factor.

Figure 5.6 shows as an illustration of the ASMSA-DSS prototype's user interface for an administrator user's task to amend a criterion question relating to a factor. In the example the criterion question text alongside the 'Criterion Definition', shown in Figure 5.6, may be amended by the administrator user. We used this functionality to revise our criteria questions as a result of our factor evaluation efforts.

The administrator user's amendment of the criteria questions are then reflected in the ASMSA-DSS prototype's user interface when an evaluator user attempts to enter acquired data, in this case a requirement for covert or overt identification, in the respective dialogue,

box as shown in Figure 5.4.

We used this administrator account extensively to update the prototype as a result of our factor validation efforts. We used the evaluator user account to enter the subject data acquired from each case study against the respective factors and also to subsequently manipulate that acquired data. The evaluator user account was used by the Director of Risks during Corporation X's utilisation of the ASMSA Methodology to determine the optimal two factor authentication solution for their employees and agents.

5.7.2 Development of the ASMSA-DSS Prototype

Our method to develop the ASMSA-DSS prototype commenced with producing a functional specification for a decision support system based upon the initial ASMSA Methodology. We then tested the core functionality of the prototype against our functional specification, for example adding textual information acquired to a factor data field. We updated the factor labels, the criteria questions and the factor explanation notes iteratively as the result of our efforts to validate our identified factors.

We based our implementation of the ASMSA-DSS around the Microsoft Access 2007 database product because this application was readily available to us and amendments to the visual basic application code could be achieved relatively easily. We took the decision to use commercially available software to implement the ASMSA-DSS prototype in order to allow us to focus our efforts on pursuing our case study research activities. For our prototype, we did not wish to spend significant effort on assessing and learning to use an artificial intelligence software programming language, such as LISP (LISt Processing).

Our ASMSA-DSS prototype implementation contains a series of front-end data entry forms and back-end databases. The prototype's application code, compiled using visual basic in the .net environment, provides the functionality for the front-end data entry forms and also the facilities to search for textual strings in acquired data, and to generate reports from the data, stored in its back-end databases.

5.8 Summary of Chapter

This chapter provided descriptions of our efforts to identify factors to evaluate an APIM and also to develop a systematic methodology for selecting APIMs for an application context, in order to address our first two research questions.

We described the characteristics of the selection problem and explained our rationale for developing a systematic methodology and how a systematic methodology could be used to select an APIM. We described the ASMSA Methodology and how it could be used as a means to acquire data pertaining to an application context and to evaluate that data in a systematic fashion in order to support decision-making.

In order to address our first research question, we detailed our method to identify factors for evaluating APIMs for an application context. We then described our method to classify the factors we identified in the literature. These factors are presented in tables in Appendix A.

Based upon our classification of our factors and their classification into evaluation themes, we then describe our method for developing an evaluation framework and a selection method for our systematic methodology. We provided a description of the underlying principles upon which the ASMSA Methodology is designed. We also provided a detailed description of the ASMSA Methodology and its components.

We described the ASMSA-DSS prototype. This implementation is a decision support system based upon the components of the ASMSA Methodology. We briefly described our software development approach and have given examples of how the prototype may be used to support our research aims and to manage large volumes of qualitative and quantitative data.

In the next two chapters, we describe our efforts to validate our identified factors and their associated criteria questions using data from our two retrospective case studies. We validate the design and assess the efficacy of the ASMSA Methodology in our third case study.

CHAPTER 6

Case Study of an EU State's eID Card Programme

Contents

This chapter describes our case study of an EU state's eID Card Programme. We begin by describing the background details of our case study and the data acquired. We then discuss the results of our efforts to validate our identified factors using data from this case study. We then focus on our main unit of analysis by examining the approach pursued by the EU state's eID Card Programme. We also examine interviewees' retrospective insights on the

expert-led approach pursued by the programme, using our analytical framework, in order to identify methodological learnings. Finally, we draw our initial conclusions on our two units of analysis.

6.1 Background on the EU State's eID Card Programme

This section describes the background of this programme without revealing details about the state, organisations or individuals involved in the research. This section builds upon the information provided in Section 4.3.1. We anonymise the identity of our interviewees and their organisations in accordance with the agreed consent arrangements. Therefore, we provide general descriptions about subjects and objects rather than divulging specific names.

Our case study relates to a member state of the European Union (EU) which was one of the earliest states in the world to introduce an Electronic Identity (eID) card for the purposes of providing on-line authentication for its citizens. It was possibly one of the most mature eID card deployments, at the time of our research, judging by the extent and quality of educational material made available to its citizens by the state's Information and Communications Technology (ICT) Agency. There are several scientific papers on the ID card's implementation and deployment, particularly the identification of security and privacy vulnerabilities relating to the eID card's usage on the Internet, produced by members of the indigenous academic community. Our case study period concentrates from the inception of the eID Card Programme in 1999 until 31st December 2010.

The aim of this EU state's eID Card Programme was primarily to replace paper based national identity cards with a contact smart card, containing an Integrated Circuit Card (ICC). The eID Card would be designed to provide face-to-face identification and also on-line authentication of the state's citizens to government and commercial relying parties. The introduction of the eID card was considered by the EU state's Ministry of the Interior (MOI) to be an enabling technology to support this state's strategic objective to increase on-line transactions, as part of the state's drive to modernise its society's use of technologies.

The EU state's eID Card Programme had three main objectives:

- to migrate from a paper based identity card to an eID smart card in order to reduce counterfeiting;

- to introduce on-line authentication capabilities for its citizens on approved Internet applications; and
- to enable its citizens to generate digital signatures in compliance with national legislation, representing that EU state's adoption of the EU Directive on Electronic Signatures.[1]

This state's citizens had used identity cards since the Second World War. The state's National Identity Registry (NIR) maintained the central repository containing information on citizens which mainly consisted of a citizen's national identifier reference, their biographical data, and a facial image. The NIR had developed information systems for managing citizen's personal data and the local municipality governments possessed systems to perform the registration of citizens and eID card administrative duties.

The MOI, through its system integrator partnerships, was the sole issuing authority for producing the eID cards to the state's citizens. There were many organisations, including government departments and commercial businesses, which relied on the eID card for citizen identification and authentication, for both face-to-face identity verification purposes, e.g. by the police authorities, and also for on-line transactions over the Internet, e.g. government websites.

Relying party organisations, e.g. the police, used the facial image embossed on to the surface of the plastic eID Card for the face-to-face identity verification functionality. The cryptographic capabilities of the eID card are used by relying parties for authenticating citizens' transactions over the Internet. The citizen was required to enter their Personal Identification Number (PIN) to activate the cryptographic capabilities of their private keys embedded in the eID card. The citizen typically transacted remotely with federal government websites in order to submit their income tax returns; with local municipal government in order to request rubbish disposal facilities; and with commercial organisations in order to purchase goods and to use on-line services.

The state's MOI concluded that a plastic smart card with a contact ICC and specific logical properties, together with other physical controls, would offer the appropriate counterfeit protection. It transpired that the programme concentrated the majority of its efforts on the development and deployment of the functional capabilities of the eID card and the associated middleware to enable the on-line identification and authentication of its citizens, by relying

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML

parties, for eGovernment and eCommerce services.

6.2 Data Gathered

This section describes the data gathered using our stated data collection techniques, described in Section 4.4, in terms of documentary objects acquired; subjects interviewed; and the recording of our own observations.

6.2.1 Documentary Evidence

Our case study documentary evidence comes mainly from three main sources; namely, official government sources in the EU state, the state's indigenous academic community and study reports produced by internationally recognised organisations, e.g. OECD and independent research bodies supported by EU funding.

Much documentary evidence was acquired from the EU state's federal government websites and from the official publications issued by the federal and local governments of that state. Our interviewees obtained the necessary authority from their respective organisations to release some programme documentation to us, e.g. tender documentation, which were no longer in the public domain.

6.2.1.1 EU State's Publications

We found 22 publications which were produced either by the state's MOI, its Information and Communications Technology (ICT) Agency, or by departments in its regional governments. We refrain from producing a list of these publications because their titles would enable the identification of the programme in this case study.

The most pertinent documents to our case study research were those produced, by a professional services company, for the EU state's MOI; the ICT Agency; and the NIR. These documents included the Request for Proposal (RFPl) for the manufacturing, personalisation and distribution of digital identities and the provision of certification services. The ICT Agency and the eID Card Programme were formally established shortly after the production of these documents.

The confidential eID card chip (ICC) specifications and the requirements for certification practice statements for the eID card documents contained sufficient detail to enable us to obtain a technical understanding of the eID card's functionalities. Our interviewees, who assisted in the production of these documents at the professional services agency assigned to the programme, released these confidential documents to us.

The ICT Agency published strategy reports on the usage of eID cards in order to promote eGovernment and eCommerce transactions. The ICT Agency's annual activity reports provided an historical account of the type of activity that occurred during the programme's development and deployment phases. The ICT Agency also published a series of system architecture documents and specifications for web application developers in relying party organisations which could use the eID card's capabilities for authenticating citizens' on-line transactions. The ICT Agency also maintained a website that described the capabilities of the eID card, a link for citizens to download the middleware for the eID card application, installation guidelines for that middleware, and authorised suppliers of eID card readers. The on-line resources that describe the eID card itself, the smart card reader specifications and the associated middleware component were particularly useful in clarifying the functional aspects of the eID card.

Our analysis of this documentary evidence showed that the programme concentrated upon developing and circulating the eID card itself in the first instance before developing the smart card reader middleware technologies and designing the application architectures to enable the issued eID cards to be used for on-line applications. The state's federal government had also established two privacy laws about six years prior to the inception of the programme. Most of the relying party websites related to eGovernment services and there were very few commercial eCommerce services available on-line.

We were unable to gain access to the three feasibility reports for the eID card produced by different sources between 1999 and 2001; however, one of our interviewees outlined the recommendations contained in each report during our interview session.

6.2.1.2 Scientific Papers from Indigenous Academic Community

We found 15 in-depth analytical research papers, from the indigenous academic community, which identified flaws in the eID card's design.

These publications highlighted the security vulnerabilities and privacy protection deficiencies in the eID card during its usage for on-line transactions. These papers often contained recommendations on how to modify the eID card's logical design in order to reduce the risks associated with the identified design flaws. Many of these papers argued that the removal of the design flaws would lead to the increased utilisation of the eID card by citizens. Some of these papers also suggested alternative applications for the eID card to those applications approved officially by the ICT Agency.

Citizen under-utilisation of the eID card's capabilities for on-line authentication of citizens' transactions was a common theme amongst these publications. Citizen under-utilisation of the eID card had occurred for many reasons as we explain in Section 6.4.4.

6.2.1.3 Independent Reports on eID Cards

We found 14 study reports and surveys of national electronic identity cards and eGovernment authentication services.

These pan-European publications provided both qualitative and quantitative data which was useful for comparing social attitudes on similar eID card deployments in other EU states. We also found a security alert issued by a Computer Emergency Readiness Team (CERT) relating to the eID card's middleware.

The breadth and depth of documentary evidence enabled us to not only validate our identified factors but also gain an understanding of the development and deployment approach pursued by the programme.

6.2.2 Interview Transcripts

We now describe the protocols and data acquired from two semi-structured interviews conducted with two InfoSec practitioners (Interviewee F and Interviewee S) from the professional services company which were assigned to the programme team.

We were introduced to Interviewee F through a professional colleague, who had worked with this person in the same professional services company on a social security identity card contract in the EU state. We were introduced to Interviewee S by a fellow Royal Holloway Ph. D. student who had worked briefly with this person on a Public Key Infrastructure (PKI)

contract in the EU state.

Interviewee F acted as the lead expert consultant within the programme and his team was tasked to produce the RFPl tender notice for the MOI and also the eID card's specifications. The objective of his assignment was to help modernise the systems that managed the ID card for the ICT Agency and also for the NIR, which were operated by separate government entities. The assignment was also to explore the possibility of incorporating the functionality of other existing identity documents, e.g. social security identity card, into the new eID card.

Interviewee S was also employed by the same professional services company and acted as the eID card lead architect. His main responsibilities were the development of the eID card's architecture and the PKI's design. His activities also included writing the test specifications, producing system integration documentation, specifying the middleware and software drivers, and overall project coordination for the deployment of the eID card for on-line transactions.

Our interviewees from the professional services company had gained recent experience on assignments relating to the issuance of electronic bank payment cards, under the EMV Global Payment Card Scheme, which are used by bank customers in ATMs and retail card payment devices. These bank payment cards used a PIN to authenticate the card holder.

Interviewee F described the background of his company's involvement and the nature of their professional services engagement as follows:

> "*There had been two feasibility studies that were not conclusive and the MOI called upon an external consultancy to finalise the requirements for the eID Card. One study, produced by academics at an indigenous university, provided evidence for significant cryptographic controls, mainly from a cryptographic threat perspective; however, the MOI wanted the team [which he represented] to stipulate requirements from practical considerations.*"

As far as we were aware these interviewees did not advise or collude with each other regarding their involvement in our research. These individuals provided their consent on the basis that identity remained confidential. Interview S acknowledged, however, that that aim may be difficult to achieve due to his *"renowned and significant contributions to the programme"*. At the end of the interviews both interviewees offered to answer further questions by email exchange. They both provided further clarification of their answers to our questions following their review of the interview transcripts. There were two further email

exchanges with Interviewee S to clarify our understanding of the deployment.

We designed our interview questions, shown in Appendix B, to ensure that the interviewees had indeed been involved with the programme by ascertaining their role, activities and their contributions to some of the programme's deliverables. Our questions were also posed to enable us to obtain an understanding of the issues encountered during the programme and, most important to our inquiry, to acquire our interviewee's personal insights on the approach pursued by the programme.

We made the purpose of the interviews clear to the interviewees at the outset, as shown by our briefing and questions in Appendix B, that our intention was not to criticise the programme's approach or comment on the deployment itself. We explicitly acknowledged that decisions by the programme were based on the data available and the circumstances prevailing at the time. The two interviewees could have acted defensively; however, our data shows they were prepared to discuss openly the strategy pursued by the programme, the events that occurred, the eventual outcomes and their thoughts on the merits and drawbacks on their programme's approach. We provide extracts from these transcripts in Section 6.4.5.

We undertook semi-structured telephone interviews with our interviewees. Interviewee F did not want our conversation to be recorded. Therefore, we generated an interview transcript note to represent our understanding of the conversations in the interview. Interviewee F then revised our transcript note of that conversation. Interviewee S agreed for the interview to be recorded. We transcribed that recording and Interviewee S corrected the transcript document directly.

These interviewees were given the opportunity to make revisions to the transcript draft to ensure their utterances reflected their intentions and also the facts recorded were accurate, e.g. the correct sequence of the events in the programme. Their recollections of the events needed validation because our interviews were conducted more than five years after their activities in the programme. Both interviewees provided other documentation, e.g. the RFPl, which was no longer in the public domain, and some confidential material, e.g. the ICC's logical specifications.

We also exchanged email correspondence with two other individuals; one individual from the EU state's ICT Agency that managed the eID card and the other individual being a researcher in information security from an indigenous university.

We attempted to obtain an interview with a representative from the ICT Agency responsible for managing the eID card deployment; however, executive approval was not forthcoming. This individual, being a public spokesperson for the ICT Agency responsible for promoting the eID card, however, agreed to provide us links to four sets of his publicly available conference presentation slides and to answer our questions via email.

We also attempted to interview an academic researcher who had published several papers on the eID Card Programme. He also managed a dedicated website on government eID cards. He declined our request to be interviewed, however, he directed us to many useful publications which detailed the history of this state's eID card programme and also revealed some of the eID card's vulnerabilities and deployment issues.

6.2.3 Our Observation Memos and Reflection Notes

We produced an observation memo immediately after each interview and also after the changes requested by the interviewees following their reviews of the transcripts. We stored these memos in a diary format in a Microsoft Word document.

We also produced 26 reflection notes during our qualitative analysis of our data using the Atlas.ti CAQDAS tool. Our analysis included the comparison of the key statements contained in different data sources, in the interviewee transcripts and in the documentary evidence. These reflection notes also describe our observations of each source's perspective, patterns identified in our data regarding preconditions and eventual outcomes, and our identification of patterns in the approach pursued by the programme.

6.3 Validation of Our Identified Factors

This section describes our efforts and results, at Stage 6 of our research implementation plan, to validate our factors for evaluating APIMs and our criteria questions for acquiring the relevant data, both of which were based upon our review of the literature.

In order to validate these identified factors we first define our criteria which we used in our validation assessment efforts. We then provide the results of our validation assessment efforts using these definitions and the data acquired from this case study.

6.3.1 Our Factor Validation Criteria

We define the criteria which we used in our efforts to validate our factors for evaluating APIMs using data acquired from our three case studies. We then describe our methods and the tools which we used to validate our factors in our acquired data.

Silverman argues [265] that textual analysis of qualitative data consists of two main activities:

- Firstly, counting the number of **mentions** of specific textual strings in source data (quantitative); and
- Secondly, what these mentions are about (thematic or sometimes referred to as discourse analysis).

We were seeking to confirm that a factor exists within our data by locating at least one **mention** of that factor in the textual data in order to **ground** that factor. We use the term **grounded** from the qualitative data analysis technique, as defined in grounded theory research [253, 274, 47], in order to conduct our validation assessment.

Our focus was identifying the thematic relevancy and breadth of factors for evaluating the application context in order to enable the optimal APIM to be identified. The number of em mentions of a factor in our data helped us to confirm its thematic relevancy. We were also seeking to identify new factors in our empirical data to supplement the factors identified from our review of the literature. We also needed to determine which of our identified factors cannot be grounded empirically and were, therefore, irrelevant to real-world evaluations.

For our assessment each factor was appraised in terms of its label's description, the proficiency of the criterion question to acquire data relating to that factor and the relevancy of the acquired data on decisions to select an APIM. The data would enable the evaluation of an application context and the requirements for an APIM together with the attributes of candidate APIMs. We also assessed the factor's consistency with other factors, e.g. contradictory, and whether the breadth of factors may be considered as complete.

We define our criteria for validating factors relating to the evaluation and selection of APIMs as follows:

Factor Identifier Label is defined as the identifier of a factor in an evaluation theme and

whether the properties, e.g. distinctiveness, of the factor's identification label is sufficient in order to understand that factor and its properties for evaluation.

Factor Relevancy is defined as the appropriateness of a factor and its associated criterion question which requires evaluation in order to select an APIM.

Factor Consistency is defined as the congruency of a factor with respect to other factors in an evaluation theme and whether the factor's associated criterion question is suitably constructed to elicit the relevant data from the application context data.

Completeness is defined as the comprehensiveness of the set of identified factors in order to evaluate the application context and candidate APIMs. In short, have all the factors for an evaluation been identified and are there any replications to be removed?

We considered that provided that the factor is mentioned verbatim as textual content, i.e. directly, in our data or is alluded to, i.e. can be deduced indirectly, then for the purposes of our validation efforts we interpreted that factor to be *grounded*. We do, however, differentiate between direct and deduced grounded factors in the report of our validation results.

We used the qualitative data coding method, at a descriptive level, as described in Section 4.5.2, to identify the textual strings relating to our factors for evaluating APIMs in our acquired data. The Atlas.ti CAQDAS tool was used to annotate all the textual strings relating to our factors which we identified in our data. The textual strings relating to an existing factor was allocated to the pertinent field in our ASMSA-DSS tool to indicate that that factor had been grounded. Textual strings relating to a new factor, which we had not previously identified, meant that we had discovered a new factor for evaluating APIMs.

We added the new factor into our ASMSA-DSS tool and then allocated the respective textual strings from our data set to that new factor. We then generated reports from our ASMSA-DSS tool showing those of our original factors (and also new factors) which had been grounded in our data, with relevant supporting textual data, as validation evidence. These reports then enabled us to concentrate on those of our original factors which were Not-grounded in our data.

We analysed our data set again in an attempt to find textual strings which would enable us to deduce the validation of those factors which were Not-grounded. This deduction was necessary where our data, in textual form, did not contain the textual strings sought in order for that factor to be grounded. We exercised a degree of interpretation in our validation of

factor *mentions* in our textual data because of the differing terminologies and expressions found in our data. Some of our deductions relied upon plausible assumptions. For example, we deduced that a budget was set to meet the supplier's costs to manufacture and personalise the eID card in accordance with the specifications for the eID card contained in the ICT Agency's RFPl.

The use of the Atlas.ti CAQDAS tool was used to search for alternative textual strings in our data set. Where we located the pertinent data, the relevant textual strings, upon which our deductions were based, were added to the respective factors in our ASMSA-DSS tool. We used the qualitative data coding method, at a conceptual level, as described in Section 4.5.2, to identify the evaluation themes in our validated factors.

A final summary report was produced from our ASMSA-DSS tool which enabled us to identify those factors that were grounded, new factors, deduced factors and factors that were Not-grounded in our data.

6.3.2 Results from Our Factor Validation Efforts

This section presents the results of our efforts to validate the factors at Stage 6 of our research implementation plan, as shown in Figure 4.3 on page 124, using the criteria definitions in Section 6.3.1 and the data gathered in this case study.

We provide results showing those of our initial factors which were grounded in our data, new factors identified in our data set, those of our initial factors were deduced and those of our initial factors which we were unable to ground in our data, for each evaluation perspective. We explain the reasons as to why in several instances that a factor identifier label or a criterion question required enhancement.

The rows in Table 6.1 represent the results of our factor validation assessment as follows:

1. The *Grounded Factor* row shows those instances where our factors are present or mentioned in our data.
2. The *Deduced Factor* row denotes those instances where the data acquired required minor degrees of interpretation and also plausible assumptions to be made in order to ground that factor.
3. The *Not-grounded Factor* row shows, and is defined as, those instances where factors

were not found or mentioned in our acquired data. The reasons why we were unable to ground these factors in our data are discussed in the following sub-section.

4. The *Relabelled Factor* row depicts those instances where the factor label required enhancement, due to the inadequacy of its descriptive label, irrespective of whether the factor could be grounded or deduced or was found to be Not-grounded.

5. The *Revised Criterion Question* row represents those instances where the criterion question to acquire data relating to the factors required significant revision. Grammatical errors and rephrasing of questions for clarity purposes are excluded here. The scope covers those cases where the factors were such that the current structure of the criterion question may have inadvertently excluded certain APIM configurations or failed to acquire the appropriate data relating to that factor.

6. The *Deleted Factor* row represents redundant factors which were subsequently removed from the respective evaluation theme.

7. The *New Factor* row represents those new factors identified in our case study data.

8. The *Reclassified Factor* row represents those instances where a factor was moved, i.e. reclassified, from one evaluation theme to another evaluation theme in a different perspective.

9. The *New Evaluation Theme* row represents the addition of a new evaluation theme to an evaluation perspective.

10. The *Evaluation Theme Name Change* row shows the number of evaluation theme name changes within a perspective. For example, we changed *Task Environment* to *Task Dialogue* because we considered that the latter better describes its classification and its purpose of capturing data relating to the user's task interaction and not the ergonomic environment in which the automated personal identification task is undertaken. Task environment factors are evaluated by several factors in the Usage Environment Evaluation Theme in the Understanding Perspective.

Table 6.1 shows the number of factors before this case study, at the top of the table, and the number of factors following our effort to validate the factors at the foot of the table. The number of evaluation themes is shown for each evaluation perspective. Table 6.1 contains three columns to correspond to the Understanding Perspective, Effectiveness Perspective, and Efficiency Perspective of the ASMSA Evaluation Framework and also a summary column.

Factors For Evaluating APIMs	**Understanding Perspective**	**Effectiveness Perspective**	**Efficiency Perspective**	**Row Totals**
Pre-Case Study Stage 3 Conceptual Groups	**34 factors 5 factor groups**	**74 factors 6 factor groups**	**99 factors 7 factor groups**	**207 factors 18 factor groups**
Grounded Factors	47 (77%)	45 (74%)	46 (46%)	**138 (62%)**
Deduced Factors	8 (13%)	10 (16%)	17 (17%)	**35 (16%)**
Not-grounded Factors	6 (10%)	6 (10%)	37 (37%)	**49 (22%)**
Relabelled Factors	19	9	10	**38**
Revised Criteria Questions	16	7	13	**36**
Deleted Factors	3	1	1	**5**
New Factors Identified	14	3	3	**20**
Reclassified Factors (Between Perspectives)	+16 net	–15 net	–1 net	**0**
New Evaluation Themes	+2	+4 –1	+2	**+7**
Evaluation Theme Name Change	4	3	4	**11**
Post Case Study Stage 6 Evaluation Themes	**61 factors 7 factor themes**	**61 factors 9 factor themes**	**100 factors 9 factor themes**	**222 factors 25 factor themes**

Table 6.1: Factor Validation Results using the EU State's eID Card Programme Case Study Data

We directly grounded the majority, i.e. 62% of our original factors in our data out of the new total of 222 factors identified, the latter figure includes 20 new factors identified. If those factors which were deduced, i.e. 16%, are also included, then the result of our validation effort improves to 78%, with 22% being Not-grounded out of the total number of 222 factors now identified. We disassemble these high-level results in the next sub-section.

The 25 evaluation theme tables in Appendix C show which of our original factors were grounded, deduced and Not-grounded in our case study data. We detail the 20 new factors which we identified in our data and also show which factors were deleted due to replication in Appendix C. We also indicate those factors which required their factor identifier label to be changed or their criteria question to be amended. We assign an identifier to each factor, e.g. A.1.1. (denoting stage created, evaluation theme and factor reference number) to a specific factor in these tables so that its validation may be tracked, e.g. label revised or reclassified, through each stage of our research implementation plan.

6.3.3 Discussion of Our Validation Results

This sub-section disassembles and discusses the results from our efforts to validate our factors, which originate from our review of the literature. We also highlight some of the limitations on our validation efforts due to the lack of available data relating to the reliability and usability aspects of the eID card.

We acknowledge that the main issues which influenced our validation results may emanate from our interpretive bias, or our inability to identify the necessary text in our data to ground that factor, or our failure to acquire the relevant data. It is also possible that we were unable to ground some factors because of the absence of the relevant data in that the programme may have overlooked some factors, e.g. usability of the eID card for on-line transactions.

The deduction of some factors relied critically on our interpretation of the data evidence. We were cognisant that our deductions needed to be logical and that our assumptions required plausibility. For example, we deduced, and we believe that it is highly probable, that the MOI set a budget for the programme although we were unable to establish the exact budget amount. We reiterate that our objective of our validation was to determine whether the factor had been considered by the programme as evidenced by the case study data gathered. Knowledge that a budget existed, in all plausibility, sufficed for our factor deduction validation.

Additionally, our inability to locate the pertinent text in our data for some factors may have influenced our validation assessment results. In order to improve our efforts here an alternative researcher could have also performed this validation task; however, such resources were not available to us. Therefore, a degree of caution needs to be exercised in the interpretation of these factor validation results based upon our inaugural validation effort using data from this case study.

Our results are next examined in more detail using our factor validation criteria defined in Section 6.3.1.

6.3.3.1 Factor Identifier Labels

Our results show that 38 of our initial set of 207 factors, about 18%, required their factor labels to be improved. Similarly, 36 of our criteria questions, about 17%, required enhancement to ensure that the correct data for that factor are acquired from the application context. In some respects our criteria questions were too specific and required generalisation in order to allow for greater flexibility in the acquisition of relevant data. Some criteria questions required enhancement because our phrasing was overly complex.

In order to reduce these ambiguities so as to improve clarity, we considered that each factor would benefit from having explanatory note describing why the factor needed to be evaluated. Essentially, this explanation clarifies the factor's purpose. We considered that the precise explanation of a factor would then make it easier to assign an appropriate factor identifier label and also to construct a concise criterion question. We show these factor explanations in the tables of Appendix E, which were produced during our efforts to validate our factors at Stage 9 of our research implementation plan, using data from the EU state's eGates Programme Case Study.

Therefore, we amended our ASMSA-DSS tool to allow for the inclusion of a factor explanation note for each factor in preparation of our efforts to validate these factors using the data from succeeding case studies.

6.3.3.2 Relevancy of Our Factors

Relevancy is indicated by the number of instances where factors can be grounded directly or can be grounded indirectly through interpretation. Those factors that cannot be grounded

may be considered to be irrelevant.

The results of our validation efforts, shown in Table 6.1, warrant further explanation and also careful scrutiny in order to obtain an understanding of their implications to answer our first research question. The intention here is not to describe variations of each factor but to explain our results generally.

As 86% of our 202 original factors (five were deleted) were grounded, directly or deduced, we regard that these factors are relevant for the evaluation of this type of APIM. A new factor identified in the data is considered to be validated. Therefore, the remaining 49 factors, representing 22% of our new total of 222 identified factors, require explanation as to why these factors were Not-grounded in our data.

Our Not-grounded factor validation results can be interpreted in one of three main ways:

1. the factor is not relevant, or
2. either the programme team did not actually consider these factors (they may have overlooked the factor or thought the factor to be irrelevant or thought the factor could be ignored), or
3. alternatively the programme team did consider the factor, but chose to keep such data confidential or did not produce any data relating to that factor.

Our data suggests that the factors which were Not-grounded in the Usability Results Evaluation Theme, shown in Table C.20, corresponds to the second interpretation where the usability issues associated with the eID card's usage for conducting on-line transactions was ignored by the programme. Our data also suggests that the factors in which were Not-grounded in the Reliability Results Evaluation Theme, shown in Table C.19, corresponds to the third interpretation that reliability testing was performed but the result data were not publicly disclosed.

Most of the 37 Not-grounded instances, in the Efficiency Perspective, as shown in Table 6.1, relate to these two aforementioned evaluation themes. The results and our interpretations require elucidation concerning their implications in order to answer our first research question.

While reliability test results are often classified as confidential it does not necessarily follow

that reliability test specifications and the corresponding results data were not generated by the programme. We believe that it is reasonable to assume that an eID card test specification was produced, based upon the eID card specifications in our acquired documentary evidence, and that the tests were performed by the eID Card Programme. We, therefore, consider that our reliability factors are relevant but remain Not-grounded due to the unavailability of the data. We recognise that the organisational need for information confidentiality, by controlling access to reliability test data, may prove problematical for us to achieve our research aim by grounding these factors through further empirical research.

Our failure to ground some of the usability factors has three plausible explanations. Firstly, usability factors do not have to be evaluated; however, any such argument contradicts much of the evidence found in the literature [27, 38]. A second explanation is that we failed to identify these factors in our acquired data.

A third explanation is that the relevant data were not produced. We believe that it is plausible that usability issues were deliberately or inadvertently ignored by the programme and usability test data were not generated. We would have expected to have found usability design guidelines, produced by the programme, on behalf of the ICT Agency, for organisations developing applications for the eID card. They produced, however, extensive technical documentation to integrate the technical components associated with performing the authentication of citizens' transactions using the eID card. The programme may have also considered that the usability of the eID card to be beyond the scope of their responsibilities and left such issues to relying parties, e.g. government departments, local municipality administrations and commercial organisations, and their website designers to resolve.

Alternatively, the programme may have considered that usability issues encountered by their citizens would be recoverable as and when the usability design flaws occurred or they may have considered such usability design flaws to be a low priority issue. The familiarity of bank payment cards to the citizens, using similar artefacts frequently in cash machines appeared to have influenced the programme team's strategy on evaluating usability issues for the eID card. Interviewee S claimed that *"as there were similarities of the bank payment card and the eID card in size and physical appearance, it was assumed, by the programme team, that citizens would be familiar with using eID cards"*. The eID card was designed to be used by citizens in their own home with their own computer and smart card reader devices or used in kiosks located in public places, e.g. shopping malls.

We found that the programme ran into usability issues with citizens experiencing problems

in downloading the eID card middleware from the ICT Agency's website and installing it on their home computers. We recognise, in hindsight, that we could have been more persistent in our attempts to interview citizens who had had experience of using the eID card with an on-line service. We were, however, unable to recruit citizens who had experience of using the eID card for on-line transactions and also willing to participate in our research. We conclude, therefore, that in all probability the programme team deliberately ignored usability issues associated with using the eID card.

We understand that our data for each case study is unlikely to be complete and there is always a need to gather a comprehensive data set. Nevertheless, we recognised that some of our identified factors may not be relevant to all cases. Equally, we acknowledge that some factors may be more relevant than other factors for some cases. Therefore, we retained those original factors that we were unable to ground in the data of this case study as we anticipated that we may be able to ground them in further case study research. We also recognised that the absence of a complete data set to ground our factors may hamper our future validation efforts.

Our assessment results suggested that data from further case studies were required to improve the relevancy of our identified factors and their associated criteria questions.

6.3.3.3 Consistency of Our Factors

We found very few of our factors were self-contradictory and we did not find incompatibilities between our factors.

This result can be explained partly in that we classified our original factors into evaluation themes, within each perspective, making it easier to assess the congruency of those factors in that group. Each factor is, therefore, a characteristic of a main conceptual evaluation theme. For example, the Aesthetic Minimalist Design Factor (A.15.5.) is an integral element of the Usability Results Evaluation Theme, shown in Table C.20 in Appendix C, to determine the usability of an APIM.

We restructured our evaluation themes which resulted in a net increase of seven evaluation themes to the original 18 evaluation themes. We also renamed 11 of our evaluation themes to improve the alignment with the factor concepts which we found in our data. We also identified 20 new factors in our case study data during our validation assessment. Most of

these new factors related to the newly created evaluation theme entitled *Envisaged Issues Evaluation Theme*. This evaluation theme is explained in Section 6.3.3.4 and is represented by the factors shown in Table C.14 of Appendix C. We also recognised the need to rename 11 evaluation theme titles to represent these conceptual themes in a more descriptive manner.

As only 16 factors needed to be reclassified, our results lead us to believe that there is a reasonably high degree of consistency in our factors, in that they are placed within the appropriate evaluation perspectives.

6.3.3.4 Completeness of Our Factors

As there are only five factors that were deleted, due to replication, our results here suggest that factor redundancy is low. It can also be interpreted as meaning that the identification of all the relevant factors was far from complete at this juncture of our research. This interpretation is supported by our results in that we identified 20 new factors in our case study data.

One important pattern recognised in our data led us to create three new conceptual themes; namely, Envisaged Issues Evaluation Theme (Table C.14), Envisaged Vulnerabilities Evaluation Themes (Table C.15) and Forecasted Costs Evaluation Theme (Table C.16). The eID Card Programme appeared to have made many compromises between the requirements, as reflected by the architectural designs and eID card specifications, and the eventual deployment.

We consider that such compromises, whether inconsistencies between stakeholders' objectives, the requirements for an APIM or the deployed APIM actually deployed need to be recorded so as to identify disparities between these perspectives using our evaluation framework. For example, while there may have been a consensus amongst the state's agencies concerning the eID Card Programme's objectives there were discrepancies between the eID card's specifications and the deployed eID card. Our interviewees acknowledged the need for compromises on deliverables during the programme. Our creation of new factors was aimed at recoding these underlying disparities.

Interviewee S also described a specific issue encountered after the deployment commenced and the technological compromises that resulted because he believed that the technical issue was not considered adequately during the programme. "*I think that the major surprise from*

the government point of view and most of the citizens' point of view was to discover that identity was not enough. To authenticate the person, name or an identifier, was not enough in a lot of cases. You, especially for business applications, also needed some other attributes. Basically, this problem did not come in the physical environment and people would just sign manually and nobody verifies the signature. But now everybody wants to automate the process because of the chip and the digital identity they need to put the processes in place obviously. Then they realised they do not have the information [in the deployed APIM]."

Therefore, factors and criteria questions relating to design compromises identified in our data formed the basis of our new Envisaged Issues Evaluation Theme. This conceptual theme acknowledges the often varying tensions in an APIM programme, from the different perspectives held, on the objectives of the APIM, the stated requirements for the APIM and the APIM eventually deployed. Equally important, as we found in our validation, is the need to state here that the same factor may be included in each of ASMSA's three perspectives; for example, budgeted costs, estimated costs, and actual costs. We apply different factor identity labels to distinguish between the respective factors.

From our factor validation efforts using this case study data, we have identified 222 factors, as shown at the foot of Table 6.1, which have been classified into 25 evaluation themes within our three evaluation perspectives.

6.3.4 Patterns in Our Validation Results

This initial case study research reveals that there are some early indicative trends that can be extracted from our validation efforts. These indicative trends help to partly answer our first research question to identify and validate those factors which should be evaluated in order to select the optimal APIM for a given application context.

As the majority of our initial factors in the Understanding and the Effectiveness Perspectives were grounded or deduced, using the data from this case study, we identified that 122 factors require evaluation for the introduction or revision of an APIM. These factors represent the objectives and the requirements *for an APIM* in an application context. Conversely, we identified 100 factors which describe the *attributes of an APIM and its capabilities*; however, 37 factors out of the original 98 factors (1 deleted), i.e. 38%, were Not-grounded.

We consider that it is too early to claim that we have formulated a complete list of validated

factors. Many of our original factors were not validated directly, i.e. 17% were deduced, and some of these factors and the Not-grounded factors may not be relevant for evaluating APIMs. Equally, we recognise that our list of factors may not (ever) be complete.

In the absence of data to validate the factors in the Usability Testing Evaluation Theme and the factors in the Reliability Testing Evaluation Theme, we believe that it is too early to draw any conclusions about the validity of the factors in the Efficiency Perspective. Significant gaps in our case study data and the reliance on our own interpretations mean that we are cautious about making any claims based on these early indicative results. Additional case studies are required to validate our original set of factors and to identify further factors and evaluation themes.

The patterns in our validation results indicate that the majority of our criteria questions, i.e. 186 out of 222 factors (84%), were reasonably well constructed in order to acquire the relevant data in this application context. We recognised that some of the factors' identifier labels still required descriptive refinement, although the majority, i.e. 184 factors out of 222 factors, served their purpose during our factor validation efforts.

We conclude from these initial validation results that our factors are some way off from reaching their saturation point in terms of comprehensiveness and maturity in terms of their relevancy and conciseness to provide a full answer in order to our first research question.

6.4 Methodological Observations on the Programme's Approach

This section describes the eID Card Programme's approach for selecting the APIM for their application context. Our case study commences by describing the prevailing circumstances at the time of the eID card's conceptualisation through to its deployment, which includes a period covering three years' live operation. We also describe the major events that occurred during the programme and strategies pursued by the programme together with the eventual outcomes. We also provide the retrospective comments, on programme's methodological efficacy, from our two interviewees who worked on the programme.

Our aim here was to also identify, through qualitative analysis of our data, patterns in our data which indicated that underlying mechanism's influenced the programme's deliverables. We also provide an historical account of the decisions made by the eID Card Programme

during the different phases to deploy the eID card.

6.4.1 The eID Card Programme's Approach

This EU eID Card Programme Case Study proved to be a compelling case study in that the breadth and quality of our data enabled us to build a detailed historical account of the eID Card Programme over our ten year study period. Our two interviewees provided their incisive methodological insights on the approach pursued by the programme and also provided detailed explanations of the key issues encountered during their assignments to deploy national eID cards. Figure 6.1 represents the programme's approach pursued during our case study period, which was produced from the Atlas.ti CAQDAS tool following our descriptive coding of the data gathered. Figure 6.1 is based upon Miles and Huberman's causal network diagram [203] for representing a narrative flow of events in a programme commencing with antecedent variables, intervening variables, and outcome variables.

Figure 6.1 shows the sequential progression of the programme from its inception through to the outcomes as at the end of our case study period. Figure 6.1 should not be construed as a causal network as our data are insufficient to identify direct causal effects throughout the programme. The conditions prevailing at the time of the programme's inception, depicting the antecedent variables, are shown in the boxes in the left column and the eventual outcomes, i.e. outcome variables, are shown in the boxes in the right column of Figure 6.1. The boxes in between the preconditions column and the outcomes column represent the strategies pursued and the significant events that occurred during the programme, i.e. the intervening variables.

Our main finding was that the eID Card Programme did not follow a systematic methodology containing step-by-step method. Interviewee F stated that *"we used the skills of the practitioners and took a pragmatic approach using our skills from years of experience"*. Interviewee S commented that *"the decision was fairly straightforward to select a plastic card for the eID card, similar in size to a bank payment card, with citizens using a PIN to authenticate themselves remotely"*.

We found that the professional services company was required to deliver a feasibility report for eID cards to the MOI in four months. Their feasibility study, upon which the MOI's major decisions were based, was completed under much pressure and contained many assumptions about relying parties' and citizens' requirements. We did not, however, establish the exact motive behind the MOI's drive to progress the programme at such pace. The MOI's

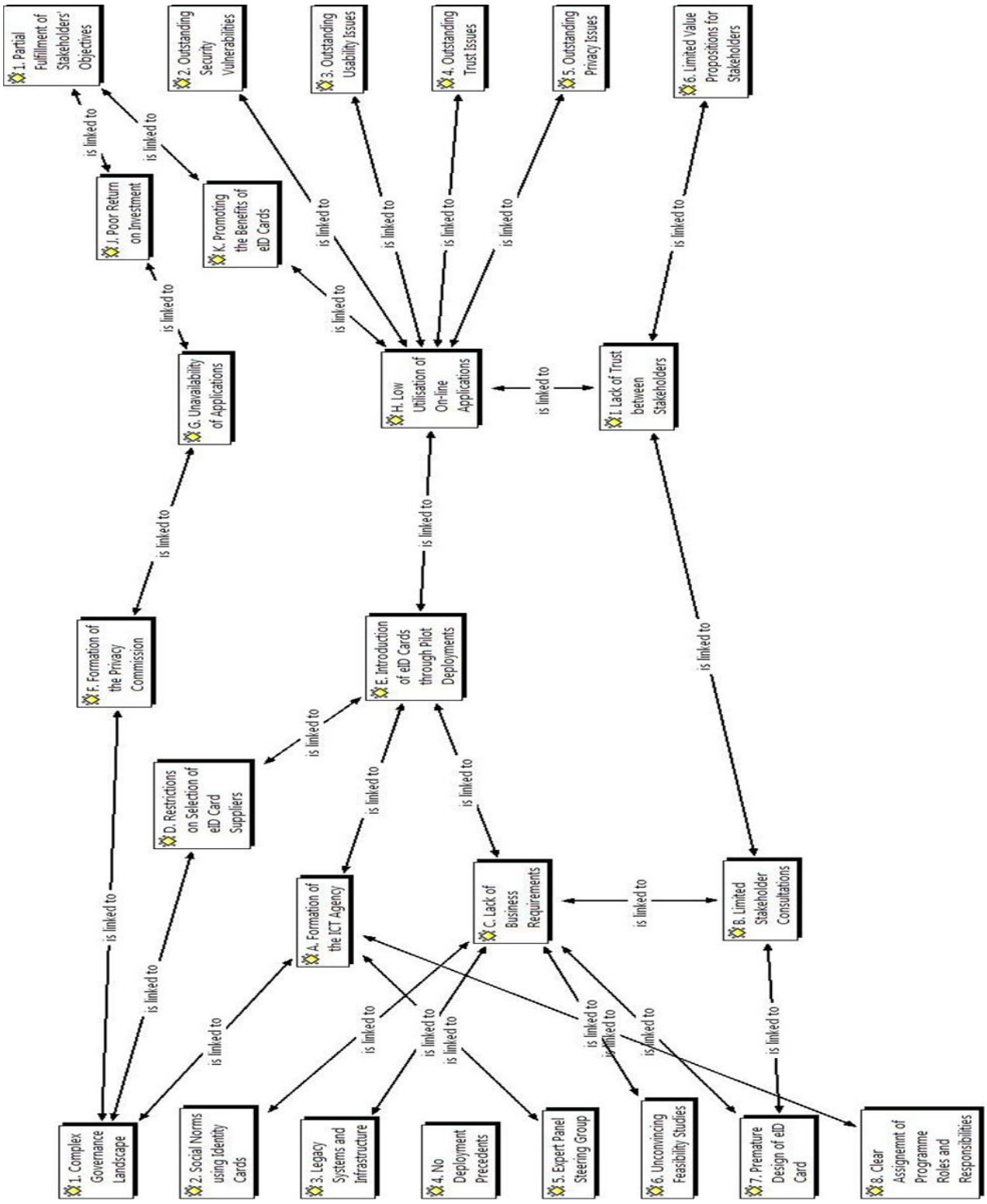

Figure 6.1: Approach Pursued by the EU State's eID Card Programme

underlying political agenda appears to have influenced the programme's early activities to concentrate on replacing the paper based identity cards as a matter of priority.

We found that the programme concentrated on the production and distribution of the eID cards to citizens for the first five years and postponed their programme activities to establish requirements for on-line transactions. Our findings show that the programme focused on establishing eID card specifications for card personalisation and technical specifications for a certification authority service provider to issue the eID card. The programme curtailed its efforts to establish specifications to use the eID card's functionality for on-line transactions.

The programme conducted consultations with federal and local government departments in respect of the objectives and business requirements for the eID card. Little attention appears to have been afforded to the gathering of the objectives and the business requirements of commercial relying party organisations, notably the indigenous banking sector, for conducting on-line transactions. Additionally, the programme did not conduct consultations with the state's citizens.

In the absence of consultations with the commercial stakeholders, as relying parties, and its citizens, as users, the programme had to make many assumptions, particularly on the type of business on-line applications which would use the proposed authentication capabilities of the eID card. The programme, based on their assumptions of the nature of the relying parties' business transactions, pursued a standards based approach for the implementation of the eID card. The eID card contained the citizen's private keys, associated X.509.3 compliant digital certificates and the citizen's facial image. The eID cards were distributed to citizens, usually, upon the expiry of their paper based identity card.

In early 2006 the programme then turned its attention to developing middleware technologies to facilitate the usage of the eID card's potential capabilities for authenticating citizens' on-line transactions at relying parties' websites. The programme concentrated on developing middleware for browser applications running on Microsoft Windows operating systems. The programme team took over three years to resolve the technical problems relating to integrating their middleware utility with the Microsoft Windows operating systems together with various browser applications in order to enable a citizen to use their eID card in a compliant smart card reader to complete an on-line transaction. This middleware utility for citizens and the specifications for relying parties to build compliant website interfaces were not made public until 2007.

The main outcome of the eID Card Programme was that commercial relying party organisations remained reluctant to build retail business applications for citizens on their websites which would use the eID cards' authentication capabilities. Also citizens tended to avoid using their eID card for authenticating on-line transactions with federal and regional government entities. As at the end of our case study period after a decade into the programme there were very few relying party applications which used the eID card's functionality to authenticate citizens for on-line transactions.

The EU state's main objective for the programme was fulfilled by replacing a paper based identity card with an eID card which was more resistant to counterfeit or falsification. The on-line authentication capabilities of the eID card, regarded by the programme as a long-term objective or supplementary objective, remained under-utilised by the relying party organisations and also by the state's citizens, as at the end of our case study period.

Our data suggests that the underlying mechanism, in that the MOI controlled the programme's activities by instructing them to avoid conducting consultation with external non-government stakeholders including its citizens, influenced the adoption strategy and the usage of the eID card for on-line transactions. Our data suggests that the MOI preferences were to issue eID cards, as replacements, as quickly as possible at the expense of conducting meaningful consultations with external stakeholders.

The MOI and the programme appeared to be concerned that allocating resources to resolve citizen acceptability and privacy issues could have become protracted by engaging with political activist groups. We found that the lack of relying party on-line applications, providing significant benefit to citizens, was the main cause for the under-utilisation of the eID cards' on-line capabilities.

The next three sub-sections provide a detailed historical account of the eID Card Programme by describing the conditions prevailing at the time the programme was established, describing the significant events that occurred and strategy pursued by the programme, and describing the eventual outcomes as at the end of our case study period.

6.4.2 Prevailing Conditions

We provide a list of the conditions prevailing at the time the eID Card Programme was established, informally around 1999, with supporting descriptions.

1. **Complex Governance Landscape** The EU state had passed federal laws relating to the national identification card and privacy laws and had also established the NIR's systems and infrastructure to support the paper based identity card. There was a complexity of roles and responsibilities between the federal state's agencies, the regional state government agencies, and the municipalities for managing identity cards and for managing citizen's personal data.

2. **Social Norms of Possessing Identity Cards** In this EU state identity cards for citizens had been obligatory since the Second World War. Citizens had become accustomed to carrying identity cards and showing these security documents to the police and other authorities upon demand. There appeared to have been a general perception, according to our interviewees, that fingerprint authentication functionality, on an eID card, would not be socially acceptable. A facial image printed on the plastic eID card which was also stored as a JPEG file in the ICC were deemed to be socially acceptable.

3. **Legacy Systems and Infrastructure** The paper based identity cards were supported by a national register of citizens through a national registration system operated by the NIR. Electronic identity cards for social security benefits and driving licences had recently been introduced into the public domain. An early objective was to merge the functionalities of the different eID cards into one national eID card with multiple purposes. The federal government had gained experience in operating identity management systems for the paper based national identity card and the existing eID cards. Local municipalities had established procedures for undertaking registration processes for all these different card types. There were, however, many system legacies, in terms of separate information systems and procedures for managing the registration processes for these different identity cards. The registration of citizens and their entitlement to possess an identity card relied on the experience of the civil servant staff in the municipalities.

4. **No Deployment Precedents** Our interviewees claimed that there were no precedent national eID card deployments offering on-line authentication capabilities operating in Europe or worldwide from which the programme could learn or use as the basis for their development and deployment. There were, at that time, two other EU states introducing eID cards, which were at the same conceptualisation stage in their programmes, as our case study. Our interviewees acknowledged that the pioneering nature of these eID card programmes, venturing into deploying innovative solutions, attracted high risks not only in terms of delivery, but also acceptance by citizens.

6. Expert Panel Steering Group The EU state's MOI had appointed a panel of five experts to act as a technical steering committee. There appeared to have been a general perception in the panel then, that the migration to a plastic eID card from the paper based identity card, similar to a bank debit or credit payment card, using PIN authentication, would be acceptable to citizens. The panel believed that a plastic card, carrying a visible chip (ICC), similar in appearance to bank payment cards in circulation, could be used by citizens in both face-to-face identification scenarios and also for on-line transactions. The panel of experts recommended to the MOI and to the programme that the use of biometrics would be infeasible because the technology was perceived, by them at that time, to be too immature and too expensive for purpose.

6. Unconvincing Feasibility Studies In late 2000 the Council of Ministers in the EU state approved the eID card concept study. Following three feasibility studies the state's Council of Ministers decided upon the basic concepts of the eID card with X.509.3 standard certificates for authenticating citizens remotely. Also, the new eID card would not be integrated with existing chipped cards. These feasibility studies for the MOI contained recommendations that citizens would readily adopt an eID card with a chip; however, smart card readers for eID cards were not available at that time. The third and final feasibility study was completed in just four months. The urgency placed on the professional services company to deliver their feasibility report in such a short space of time meant that many assumptions were made regarding citizens' attitudes to performing transactions on-line. There was also a lack of consultation with commercial organisations as to what type of on-line services they would consider making available to citizens to use the authentication functionality of the proposed eID card. Additionally, the regional governments' and municipalities' objectives and business requirements for the eID card appear to have been evolving at that time.

7. Premature Design of eID Card The eID cards' design was formulated from the recommendations contained in the third feasibility study. In 2001 the Council of Ministers approved the basic concepts for the eID card and decided to incorporate certificates into the smart card. Citizen access to their private keys stored on the smart card, for on-line authentication and for digital signatures, was to be protected by a four digit PIN. A citizen's national identification number was to be included in their X.509.3 subscriber certificates, embedded in the ICC, in order to link the eID card to the citizen for the related on-line transactions. The eID card would also display the citizen's name and their national identity number and their facial image. The ICC would contain the

citizen's autobiographical data, private keys and certificates and the citizen's facial image in JPEG file format. Essentially at that conceptualisation stage, the decision on the eID card specifications and the programme's responsibilities and deliverables had already been made by the MOI before consultation with stakeholder relying parties and citizens had taken place.

8. **Clear Assignment of Programme Roles and Responsibilities** The MOI assigned the roles and responsibilities for the governmental entities involved with the programme and also the programme's objectives and deliverables. The MOI was responsible for the overall infrastructure and for managing the legal framework to ensure eID card aligned with privacy regulations. The municipalities were to continue to perform registration and enrolment processes with citizens; however, for the new eID card this administrative task also involved the delivery of the eID card's PIN, contained in sealed PIN mailer envelope, to the citizen. The MOI was also responsible for selecting the eID card production supplier, the personalisation supplier, and the certification authority services supplier. The MOI delegated the responsibilities to the programme to produce the specifications for the eID card and the X.509.3 certificates together with the certification practices statement requirements document.

In the first five years of the development of the eID card the programme concentrated on producing the eID card and delivering these artefacts to its citizens. The specifications describing the interfaces between the eID card, smart card readers, operating systems and client's browser together with relying party's web based applications were not produced until 2007.

6.4.3 Strategies Pursued and Significant Events

We now describe the strategies pursued by the programme during the development and the deployment phases of the eID card programme, together with significant events that took place during that period up until 2011. The programme commenced developing the eID card around summer 2001.

According to Interviewee F *"the eID Card Programme team took a 'business driven approach' to deal with the complex processes that can be broken down into two discrete functions; namely, the processes to make the card and the processes to use the card"*. The programme, according to our interviewees, did not follow a system development methodology or a

programme management methodology.

We provide a list of the intervening variables, which include the strategies pursued by the programme and the significant events that occurred.

A. Formation of the ICT Agency The ICT Agency was formally established by the MOI in 2001 to run the eID Card Programme from 2002. Its main role was to represent the MOI and fulfil the objectives of the federal government for the eID card's deployment. The programme was also required to communicate information on the eID card and the progress of the programme to the public, through a dedicated website and also through annual activity reports. It also had the responsibility for undertaking the marketing activities relating to the usage of the eID card for on-line transactions on behalf of the MOI.

B. Limited Stakeholder Consultations There appears to have been very little consultation between the programme and the commercial sector during the early development phase of the programme to elicit external stakeholders' objectives. Limited consultation took place between the programme and public sector organisations, mainly with federal civil servants and local government representatives from regional governments and municipalities. According to Interviewee S *"many commercial stakeholders adopted a wait-and-see approach that made the limited consultation processes that were conducted difficult to progress to any agreed conclusions"*. Interviewee S believed that it was a critical mistake by the MOI to specifically exclude banks from the very few consultations that did take place, as he regarded that *"the banking industry had the potential to deliver the so-called 'killer applications' to citizens"*. There also appears to have been no consultation during the development stage of the programme with citizens or citizens groups regarding their use of eID cards. The consequences of limited stakeholder consultation were that the programme had to make many assumptions concerning requirements on the utilisation of the eID card for on-line transactions.

C. Lack of Business Requirements In the absence of business requirements the programme adopted an *" open standards approach"*, as described by Interviewee F, for the design of the eID cards and the production of specifications. The available ISO Standards, e.g. ISO 7816, were used to define the interactions between the operating system, the card reader and the eID card's chip. The use of smart cards and smart card readers for authenticating users remotely was a major technical challenge in the latter part

of the programme. The programme team did not have business requirements from stakeholder organisations which might introduce on-line applications due to the lack of consultations. Equally, the programme did not have any requirements from citizens or citizen groups as to how they might use the applications with a smart card and smart card reader.

D. Restrictions on Selection of eID Card Suppliers Following formal tender processes, the MOI selected the eID card manufacturer, the eID card personalisation supplier and the certification authority services provider in 2002. These suppliers were required to integrate their proposed systems with the existing national identity systems at the NIR and the registration information systems used by registration officers in the municipalities. All of these suppliers had to have operations located in that EU state.

E. Introduction of eID Cards through Pilot Deployments The first eID cards were delivered to a small group of selected civil servants in the first quarter of 2003. The first pilot to issue eID cards through a municipality took place in the second quarter of 2003. Following a number of further pilot deployments during late 2003 and early 2004, the nationwide roll-out commenced in the third quarter of 2004. From the third quarter of 2006, all issued national identity cards were to be the new eID cards and the paper based identity cards were no longer to be issued. By 2009, all citizens in that EU state possessed an eID card.

F. Formation of the Privacy Commission In 2004, the EU state set up its Privacy Commission (PC) to act as an independent supervisory body for data protection of citizen's private data. The PC was mandate to authorise relying party's applications which used citizens' national identity numbers for on-line eID card authentication purposes.

G. Unavailability of Applications Pilot on-line applications did not appear until around 2007. The facility for citizens to check or amend their personal details at the NIR appeared to have been the initial application. There were a number of technical problems and usability issues encountered by the programme with these initial applications. The programme required revisions in the Microsoft Windows operating systems in order to enable the eID card, in the smart card reader, to function with the middleware utility and the browser applications to authenticate the citizen. According to Interviewee S *" the eID card middleware utility that was made available to the public originally was, for the average computer user, technically challenging to install"*. Many early adopters failed to install the middleware and drivers for the eID card to function as

intended by the programme. These problems remained until 2009, when a middleware installation and configuration wizard application was developed by the programme and made available on the ICT Agency's website for citizens to download. These problems appeared to have contributed to the low utilisation of on-line applications by citizens which required authentication using the eID card. At the end of our study period there were over four hundred on-line applications available.

H. Low Utilisation of On-line Applications In 2007, as very few smart card readers had been purchased by citizens, the MOI, with the ICT Agency, formulated a strategy to increase the on-line utilisation of the eID card by distributing 100,000 smart card readers free of charge. The MOI targeted the delivery of these devices to specific citizen groups, e.g. teenagers, based on the assumption that these identified groups would readily use the eID card for applications that were available at that time. Additionally, the MOI, through the ICT Agency website, made citizens aware of the eID card programme and the benefits of using the eID card for on-line transactions. The MOI also pursued a strategy to coerce manufacturers to reduce their prices on smart card readers. Most of the early applications which relied on the eID card's on-line authentication capabilities came mainly from the public sector, departments in the federal government and regional governments, rather than the commercial sector. For example, there was a pilot application introduced in 2007 for citizens to report crime to the police on-line.

I. Lack of Trust between Stakeholders The formation of the Privacy Commission was a federal government response to the claimed potential abuse of citizens' privacy, by organisations, from citizens' usage of their eID card for authenticating on-line transactions. There was a perception, according to one of our interviewees, that government authorities would be more trustworthy than commercial enterprises in handling citizens' national identity number and other personal information. Both interviewees also claimed that the Privacy Commission and many citizens regarded the risks associated with the commercial organisations' management of citizens' private data, including their national identification number, to be very high. Both our interviewees claimed that there was a general perception amongst citizens that commercial organisations would use citizens' private data for direct marketing purposes. Interviewee S also claimed *"that there was also a certain degree of mistrust, by many indigenous commercial enterprises, in the technical capabilities of the eID card, as several vulnerabilities had been exposed by the indigenous academic community"*. Interviewee F also claimed

that *"the lack of trust openly displayed between these organisational stakeholders was a contributory factor to explain citizens' low utilisation of eID cards for authenticating on-line transactions"*.

J. Poor Return on Investment Our interviewees also claimed that commercial enterprises regarded the business risks associated with developing and operating on-line services to be too high. Such deployments would incur excessive costs with the potential to generate only moderate financial rewards. Both our interviewees claimed that the Privacy Commission's strict interpretations of the EU state's privacy laws made it very difficult for commercial entities to develop profitable applications because of the effort and costs involved to comply with the Privacy Commission's security requirements. According to Interviewee F *"the main driver for the federal government was not based on a return on investment consideration"*. The investment by the EU state's federal government, through its MOI and the ICT Agency, was primarily to issue identity cards that were more resistant to counterfeiting. Increasing its functionality for authenticating on-line transactions, through the use of a *common* identification and authentication mechanism was only a secondary objective.

K. Promoting the Benefits of eID Cards The marketing of the eID card in both the public and private sector appears to have lacked coordination. Citizens often received conflicting advice from various government sources and commercial sources over several years. According to Interviewee S: *"citizens are not always aware of the on-line services that are available or where to obtain information on them or the benefits of these services"*. Interviewee F commented that *"the deficient marketing strategy proved to be one of the main stumbling blocks to utilisation"*.

We next describe the outcomes of the eID Card Programme as at the end of our case study period.

6.4.4 Programme Outcomes

The main outcome of the programme, according to our interviewees, is the under-utilisation of the eID card for authenticating on-line retail business transactions.

We found that most of the issues encountered by the programme during the development and deployment phases, as described in the previous sub-section, remained outstanding as

at the end of our case study period. We list the outcome variables from the programme outcomes together with supporting descriptions together with explanations proffered by our interviewees.

1. **Partial Fulfilment of Stakeholders' Objectives** The MOI's main objective was achieved; however, the utilisation of the eID card for on-line transactions, in both the public and commercial sector, remained low. Our data suggests that the second objective had not been achieved by the end of our case study period. By 2011 all citizens in the EU state possessed an eID card and also there were similar national identity eID cards issued for non-citizens and minors in that state. Citizens' on-line usage of the eID card remained low despite the promotional strategies pursued by the MOI and the ICT Agency. Our interviewees and some of our documentary evidence showed that the low utilisation was caused by the lack of applications that were of sufficient benefit to citizens. Interviewee S concluded that *"once these beneficial applications become available citizens may then be persuaded to purchase smart card readers and install the middleware application"*.

2. **Outstanding Security Vulnerabilities** The indigenous academic community published many articles which revealed several security vulnerabilities associated with the eID card. Interviewee F acknowledged that *"in hindsight the inclusion of citizens' national identity number in the subject's X.509.3 certificates was unnecessary"*. Similarly, Interviewee S admitted another technical oversight, by the programme team, which related to the passing of attribute values between the eID card's middleware and the relying parties' on-line applications for the associated authorisation processes. A small number of security vulnerability alerts had been issued by independent security analysts that related to program coding flaws in the middleware utility.

3. **Outstanding Usability Issues** There were some outstanding usability issues associated with the installation of the middleware utility and its configuration. There was also usability issues associated with the eID card's digital signature functionality. Interviewee S stated that *"the inclusion of latter functionality to perform digital signatures prolongs and complicates the installation of the middleware utility"*. We were unable to establish whether there are usability problems associated with citizen's usage of the eID card for authenticating their on-line transactions. We deduced that the programme did not produce usability guidelines for relying parties' developers because there was an assumption that the citizen interaction dialogue to enter a PIN value was already

familiar to citizens.

4. **Outstanding Trust Issues** According to Interviewee S, that *"the apparent mistrust between the commercial sector and the EU state's Privacy Commission regarding the approval to use of citizens' national identification numbers led to very few commercial organisations that were willing to develop on-line applications that exploited the capabilities of the eID card"*. Interviewee F concluded that *"the lack of consultation by the programme with the commercial organisations, notably the banking sector, was the prime reason why these stakeholders, as relying parties, remained reluctant to develop on-line applications"*.

5. **Outstanding Privacy Issues** There appeared to remain, amongst the EU state's population generally, a concern over commercial enterprises' use of citizens' national identification numbers and citizens' private information. Public concern over the protection of their private data in conducting on-line transactions is another plausible reason for low utilisation, despite the Privacy Commission's supervision of those enterprises that have complied with the privacy regulations. The eID card was configured so that its on-line capabilities could be deactivated. A citizen could request their local municipality, acting as the registration authority, to deactivate their eID card by revoking (as the subject) their certificates. We were unable to find data on citizen deactivation requests to the municipalities.

6. **Limited Value Propositions for Stakeholders** According to our data, the lack of beneficial on-line applications meant that there were insufficient benefits to citizens to encourage them to invest money, time and effort to purchase a compliant smart card reader and to install the middleware utility on their desktop or laptop. According to Interviewee S: *"it is difficult to ascertain exactly how many card readers are in operation; however, the commercial sector indicates that the number remains far too low for them to consider investing in developing on-line services"*.

Interviewee F summarised the EU state's eID card initiative: *"the objectives of an eID card must fulfil long-term goals and some would need a ten year period to see the benefits"*. We believe that it is plausible that the MOI adopted a long-term strategy to fulfil their main aim initially and to address their secondary aim, of rectifying security vulnerabilities and issues relating to the eID card deployment, over several years as the technologies matured.

6.4.5 Methodological Insights

We now provide retrospective comments from our two interviewees on whether the approach pursued by the programme was efficacious for the eID card deployment. Essentially, we asked them two questions:

1. What should the programme have done in hindsight; and
2. Is there any methodological learning from your experience?

The purpose of our questions were designed acquire data in order to identify methodological proficiencies and deficiencies and also learnings from the approach pursued by the programme.

6.4.5.1 Efficacy of the Programme's Approach

Both our interviewees confirmed that they would not change their *"expert-led"* approach to developing the eID card. Both our interviewees acknowledged, however, that the deployment and marketing strategy of the eID card programme required a different approach to the one pursued. Importantly, both our interviewees considered the eID card deployment to be the optimal solution which met both the MOI's primary and secondary objectives.

Despite these claims, our data suggests that the eID card possesses known security vulnerabilities and there are privacy design flaws. We found no data linking under-utilisation of the eID card with citizens' negative attitudes towards levels of identity assurance for on-line transactions. Interviewee S acknowledged that *"some aspects of the eID card's functionality relating to authorisation attributes were overlooked by the programme"*.

Interviewee F commented that *"the marketing strategy proved to be one of the main stumbling blocks to deployment and the lack of consultation with professional bodies who expressed their reluctance to issuing the ID cards"*. Our data shows that these professional bodies, e.g. notaries, offered commercial products and services to citizens at that time and the state's introduction of a common eID card could have jeopardised their future business incomes.

We have categorised our interviewee's insights into methodological learnings relating to consulting stakeholders, investigating assumptions, anticipating evolving stakeholder attitudes, validating identification technologies in context and tracking the programme's progress.

6.4.5.2 Consult Stakeholders

Both our interviewees commented that the stakeholder consultations were very badly managed by the programme. The programme had not instigated the task to identify the direct and indirect stakeholders which could have potentially used the eID card for authenticating citizens for on-line transaction purposes.

Interviewee F concluded that *"proper consultation with stakeholders and the resolution of citizen's requirements and privacy issues play an important role in respect of the acceptance of on-line services, whether provided by government or by the commercial sector"*. Interviewee stated *"that exclusion of representatives from the banking industry was a misguided strategy"* because he regarded *"the banking industry as being the most likely sector to provide the services that would be beneficial to citizens"*.

Both our interviewees commented that they encountered many objections raised by stakeholders, some of which they considered were valid issues. They also encountered, however, many obstacles which they considered were aimed at protecting specific organisation's interests. Interviewee S commented on a specific pressure group's criticism of the eID Card Programme's activities: *"they even sometimes tried to kill the project saying that it [eID card solution] should do this and this but well nothing really. We should do something and you should hire us to make studies and do things that way. They are a bit dangerous in fact"*. The programme team suspected that some of these issues were designed to prevent or hinder the deployment of the eID card.

Interviewee F stated that *"a government centred consultation approach, with legislative backing, could inform citizens on their rights; however, any consultation would have to have an expiry date to prevent the consultation period becoming protracted"*. This type of facility was available to the eID card programme, through municipalities, but was not used extensively. He also suggested that *"the eID card programme could have exploited the use of local groups to build dialogue with citizens as end users of the eID card"*.

Interviewee F considered that *"state's eID card programmes need to facilitate long-term goals and acknowledge that benefits are not immediately demonstrable"*. He concluded by stating that *"this problem is best addressed by stakeholder participation to stand a better chance of achieving these long-term goals"*. Interviewee S reiterated that *"in the private sector the business drivers would only come once the benefits can be realised by both commercial organisations and also the citizens, as consumers"*.

Our interviewees' opinions on the merits stakeholder of consultation and participation demonstrates that stakeholder consultation processes need to be managed proficiently in order to achieve effective dialogue on stakeholders' objectives for an APIM.

6.4.5.3 Investigating Assumptions

The pressure on the programme to deliver the feasibility study, produce the eID card specifications and select suppliers in such a short timescale, to the exclusion of consulting commercial stakeholders, appeared to be a deliberate strategy pursued by the MOI. According to Interviewee F *"these consultations would have delayed the delivery of the eID cards considerably"*.

Conversely, Interviewee S stated that *"making so many assumptions about the possible applications increased the risks to the programme"*. He continued by commenting that *"we should have made more challenges on the assumptions that were made early in the programme. Such challenges would have then helped us to reduce the risks associated with these assumptions and to get a clearer picture on stakeholders' objectives"*.

Our interviewees' comments suggest that an approach that investigates assumptions relating to the application context and clarifies stakeholders' objectives for the APIM could reduce programme delivery risks. The investigation processes should according to our data be proportional to the complexities and uncertainties of the application context.

6.4.5.4 Anticipating Evolving Stakeholder Attitudes

Our data suggests that programmes need to accommodate evolving attitudes towards citizen usage of new identification technologies.

Interviewee F stated that *"there had been a landscape change in citizens' attitudes towards the management of electronic data and privacy concerns in the last decade"*. He suggested that *"there is a now a strong requirement to recognise the rights of the citizen and that EU states providing electronic identity cards need to be careful about privacy issues and the aggregation of information in various government departments and also by the commercial sector"*. He commented that *"some EU states instruct their various governmental departments to have a separate identifier in order to prevent identification though data aggregation"*.

Interviewee S considered that *"regular consultation with citizen groups may have helped to reduce some of the privacy issues in the eID card deployment, e.g. the removal of the subject's national identity number from the certificates in the eID card"*.

Both our interviewees considered that citizen's perception of using an eID card for authenticating on-line transactions had changed over the decade. They both concluded that the marketing tactic to distribute free smart card readers to target younger citizens was correct in that they believed that this social group would be more likely to use the new identification technology.

These comments demonstrate that there is a need for state eID card programmes to not only consider evolving attitudes towards privacy issues but also changes in citizens' perceptions about using eID cards for the authentication of on-line transactions.

6.4.5.5 Validating the Technology in Context

We found that the programme was unsure as to whether the eID card was capable of functioning and performing as required in the intended operating environments.

Interviewee S suggested that *"there should be more experiments on the functional aspects of the eID card and better estimations on longevity and usability of such systems at the outset"*. Additionally, he commented that *"there is always the danger that some software technology is simply not available or scalable that can handle millions of users"*. The programme could not test a prototype of the eID card because the Microsoft Windows operating system needed to be enhanced specifically to meet the requirements of this eID card programme.

Interviewee S claimed that he would have preferred *"to have removed some of the technological assumptions, using a prototype, by demonstrating the on-line transactions operating in the municipality with the individuals involved in order to improve the visualisation of the equipment required and their interactions"*. This increased visibility, he suggested, *"would have helped many stakeholders understand how these elements work together"*. This understanding, he continued, *"would have helped develop the specifications for the certification authority services that were required to issue over 8 million subscriber certificates"*. He commented that *"the certification authority provider's estimation of the subscriber certificates got the scaling badly wrong and their pricing of these certificates was miscalculated seriously"*.

An approach that exploits opportunities to validate an APIM prototype in an operational application context could assist a programme gain understandings on potential functionality and performance capabilities of different identification technologies and their configuration options.

6.4.5.6 Tracking the Programme's Progress

Both our interviewees recognised the need for some methodological support tools to help a programme track its progress to fulfil stakeholders' objectives.

Interviewee F suggested *"that a tool indicating the progress of a programme might be a useful tool to programme managers"*. He also suggested that *"a tool that could validate or invalidate stakeholders' objectives with stakeholders would be useful to the industry and other stakeholders alike. It would also benefit the users of the identity management system"*. He continued: *"as a minimum it could help identify possible delays, or as a maximum, such an evaluation could supply evidence to cancel the programme"*. He quoted the Australian eID card programme as an example stating that *"it was terminated when the proposed solution gained better visibility and understanding on its implications to stakeholders' interests"*.

Our case study findings suggest that a tool for reconciling stakeholders' objectives could assist stakeholders and IS programme in their efforts to design, develop and deploy APIM, in some application contexts. Our data suggests that such tools could be most efficacious during the conceptualisation and design phases of national electronic identity programmes.

6.5 Methodological Learnings

This section describes the methodological learnings from the patterns recognised in our case study data relating to the expert-led approach pursued by the eID Card Programme. We also reflect on the efficacy of the programme's approach to select the optimal APIM.

Interviewee F commented that *"there is always a constant political agenda associated with [national] eID card programmes"*. His statement supports our supposition that underlying political interests influence the design of an APIM. In this case study the 'stakeholders underlying political agendas' influenced the eID card's design, the timings and priority of the programme's deliverables and also helped to explain the programme's inadequate efforts

to consult with commercial stakeholder organisations and with citizens.

Notwithstanding the political influences the selection of an eID card and its configuration, an expert-led approach appears to be an efficacious methodology to select an APIM when the stakeholders' decision is straightforward.

6.5.1 Approach Led by Experts

We provide explanations from our case study data to support our aforementioned statement on methodological efficacy, by classifying the patterns in our data on the methodological proficiencies and deficiencies of an expert-led approach.

6.5.1.1 Methodological Proficiencies

From our analysis of our case study data we found that an expert-led approach was efficacious because the decision for the eID card solution was reasonably straightforward for its intended application contexts. Our data suggests that the selection of the eID card and its configuration was not one single decision but a series of design choices in respect of developing, configuring and promoting the eID card to match the application context and to address a variety of constraints, including technological legacies and social norms.

Our data suggests that the selection of a plastic card with an ICC, containing a citizen's subscriber certificates and protected by a PIN, was a straightforward configuration choice for the eID Card Programme. Our documentary evidence, however, reveals that there were several acknowledge flaws in the design of the eID card. While there were claims of technical expertise by our interviewee practitioners, gained from their previous experience in identity card deployments using face-to-face citizen identification, there were, however, *no precedent national eID card deployments* from which the programme team could formulate their specifications for on-line transactions.

We found that the programme placed heavy reliance on expert practitioner knowledge and skills and did not appear to use an established project management methodology, e.g. Prince2, to manage the programme. The possibility of using an established IS development methodology had not occurred to our interviewees.

The design configuration of the eID card appears to have been based on the technical

recommendations of expert practitioners in the programme team. In turn, these practitioners were partly influenced by an external panel of five prominent experts in the steering group. As biometrics were considered by the steering group to be too technically immature and disproportionately expensive at that time, the expert practitioners' recommendations to the programme for a knowledge based mechanism, e.g. a PIN, to activate the eID card's logical functionality appears, therefore, to have been a straightforward choice.

We found that this expert-led approach enabled the programme to respond quickly to requests for deliverables made by the MOI sponsor. The use of a systematic methodology may have reduced the programme's flexibility to allocate resources to produce a deliverable in the time scales set by the MOI. Both our interviewees, however, acknowledged that there were methodological learnings to be elicited from their experiences in this programme, which we have described in Section 6.4.5.

6.5.1.2 Methodological Deficiencies

This expert-led approach appears, however, to have encountered difficulties in the design phase due to diversity and significance of many assumptions which were made by the programme team. The main assumptions related to relying party organisations' and citizens' objectives and requirements for authenticating on-line transaction. Both our interviewees conceded that there should, in hindsight, have been more challenges on the assumptions made by the programme team. Our data suggests that there was an over reliance on our two interviewees, as security practitioners' assigned to this programme, to produce eID card specifications in the absence of the objectives and requirements for an APIM.

The design errors identified relate to security vulnerabilities and the protection of citizen's private data. Interviewee S, as an expert practitioner, also concede that the programme also overlooked the capturing of vital attribute data for the authorisation process which are generated during the on-line authentication session of a citizen. Our data also reveals that there were usability problems with installing the middleware utility because there was insufficient expertise in the programme team to assist with the interaction designs.

The main causes for the design errors appear to emanate from a lack of consultation with external stakeholders, an inability to build a functional prototype because the technologies were not available at the time, and failure to demonstrate the eID card system, or a simulation, in operation to stakeholders. The programme did not appear to have given external

independent discipline experts the opportunity to evaluate the eID card specifications and implementations despite the concerns raised by the indigenous academic community.

The testing of the eID cards with the middleware utility appears to have overlooked the security and privacy vulnerabilities which were later found during examinations by external entities, e.g. the academic community. The security vulnerabilities uncovered by external examination may have been known by the programme or it may be that their testing of the eID card was deficient. Our data suggests that there were gaps in the knowledge and skills within the programme team in specific disciplines, e.g. a usability specialist.

Our data also suggests that the lack of consultation with commercial organisations resulted in organisations, as relying parties, being reluctant to develop on-line commercial applications for citizens. Similarly, the lack of consultation with citizens to ascertain their value proposition, i.e. benefits of using the eID card, resulted in low utilisation of the eID card. Our data suggests that the lack of consultation was a deliberate strategy pursued by the MOI and was not an outcome from using an expert-led programme approach.

Our data suggests that a multi-disciplinary approach, engaging a range of discipline expert practitioners, with alternative perspectives, may have assisted the programme team to reduce some of the eID card's design errors. Our data also suggests that such an approach in a programme of this nature needs proficient engagement with potential replying parties and the intended user community in the application context in order to reduce assumptions relating to the objectives and requirements for an APIM.

6.5.2 Our Reflections on Methodological Efficacy

Our reflections on methodological efficacy concentrate on the time taken by the programme to execute their expert-led approach and the accuracy of the selected APIM.

We did not locate an objective in our data which indicated the programme delivery timescales for the eID cards to be made available to citizens. Similarly, we did not locate data which established the proposed delivery timescales for the architecture and functionality to enable citizen's to conduct on-line transactions using the eID card. We found that the programme's approach took about three years to achieve the MOI's primary objective and approximately seven years to fulfil the MOI's secondary objective. The MOI's third objective for electronic signature capability appeared to have taken a low profile; however, the ID card incorporated

a digital signature functionality.

The delay on the second objective was caused mainly by the technical restrictions of the Microsoft Windows operating systems which were beyond the programme's control. Our data suggests that an approach which excludes the validation of technologies in the conceptualisation phase is a high risk strategy. Suppliers may not always be willing or technically able to enhance their technologies. Our data shows that the supplier did enhance their technology; however, those enhancements delayed the programme's secondary deliverable severely.

We found that the MOI opted to progress the eID card implementation quickly in the initial stages rather than to instruct the programme to consult with potential stakeholder organisations and citizens. Our data suggests that the MOI considered that such consultations would have become protracted due to the programme's attempts to reconcile these stakeholders' risks and issues. We believe that it is plausible that the MOI, through the programme, opted to pursue their primary goal in their desired (unpublished) timescales, which were not known within the programme team, at the expense and risk of not accomplishing their secondary objective until much later.

In the absence of objectives set by the programme our reflections on accuracy are based upon the programme outcomes and the claims made by our two interviewees. Our data suggests that the programme's approach resulted in the selection of the optimal eID card solution. There were, however, design errors relating to eID card's on-line authentication functionality caused mainly by the programme having to make many design assumptions and also the over reliance on some of its discipline experts.

According to both of our interviewees the programme selected the optimal APIM, despite its low usage, exposed security vulnerabilities, outstanding privacy issues, and minor usability design flaws. Our documentary evidence suggests that these adverse outcomes could have been avoided. The programme could had devoted more effort during the conceptualisation and design phases of the eID card to evaluate its potential effects on citizens' on-line experiences and its impact upon relying parties' web application systems.

We believe that is difficult to substantiate any claims of selection accuracy because the external stakeholders' objectives, including citizen's viewpoints, were not acquired by the programme team. Also, it appears that the programme did not set metrics to measure the effectiveness of the solution. A post programme review in order to assess the efficacy of approach pursued by programme was not undertaken.

Our data suggests that an expert-led approach appears to be efficacious when the choice of APIM is reasonably straightforward to the stakeholders in the application context and the discipline experts involved with the programme possess the relevant range of skills and knowledge to deploy that APIM. Both our interviewees, however, acknowledged, based on their experiences, and our other acquired data suggests that an expert-led approach could be enhanced.

6.6 Our Conclusions from this Case Study

In this section we describe our conclusions on our efforts to validate our identified factors using data acquired from this case study. We also summarise our conclusions on the methodological efficacy of an expert-led approach to select an APIM.

6.6.1 Efforts to Validate Our Factors

Our conclusions, based upon the data acquired in this case study, are that the majority of our identified factors are relevant for evaluating APIMs.

From our validation assessment, we have ascertained that our factor list for evaluating APIMs is not complete. Moreover new factors need to be identified and redundant factors should be removed from our list. Many of our validated factors, at this stage in our research, lack terminological consistency. We ascertained that there is a need to develop explanatory text for each factor in order to reduce ambiguity in our factor identifiers, i.e. their descriptive labels.

Further empirical research is required to extend the range of factors for evaluating APIMs.

6.6.2 Methodological Efficacy

We conclude that an expert-led approach is efficacious for programmes to select the optimal APIM when the choice is straightforward and the programme is prepared to rely on expert practitioner knowledge and capabilities to deploy that selected APIM.

Our evidence suggests, however, that a programme might benefit from using tools to reconcile the APIM's proposed design against stakeholders' objectives in the conceptualisation and

design phases of a programme. We found that the *underlying mechanisms* that controlled the programmes' activities influenced its ability to challenge the significant assumptions, relating to stakeholders' objectives and requirements, upon which the eID card design was based.

The methodological insights from the two interviewees, as expert insiders, proved most valuable in gaining understanding about the dynamics of an APIM programme and the efficacy of an expert-led approach.

Further empirical research is needed to ascertain the impacts on the selection of an APIM when that choice is not so straightforward to the programme. Further research should also encompass circumstances when a programme does not have access to wide range of expert practitioner knowledge and skills.

In the next chapter, we describe our efforts to further validate our identified factors and their associated criteria questions and also elucidate on methodological learnings from data acquired from our second case study.

CHAPTER 7

Case Study of an EU State's Border Control eGates Programme

Contents

This chapter describes our case study of an EU state's Border Control eGates Programme. We begin by describing the background details of this case study and the data acquired. We continue by discussing the results of our efforts to validate our identified factors using data from this case study and describe the patterns that we recognised in our assessment results. Next, we examine the iterative deployment approach pursued by the eGates Programme for

our main unit of analysis. We also examine interviewees' retrospective insights on the approach pursued by the eGates Programme in order to identify methodological learnings. Next, we compare the methodological patterns identified in our data relating to the approaches pursued by the eID Card Programme and the eGates Programme. Finally, we draw our conclusions on our analysis of the data from these two retrospective case studies for our two units of analysis.

7.1 Background on the EU State's Border Control eGates Programme

This section describes the background to this programme without revealing details about the state, organisations or individuals involved in our research. This section builds upon the information provided in Section 4.3.2.

As with all our case studies, we anonymise the subjects and their organisations in order to protect their interests, in accordance with the agreed consent arrangements; therefore, we give general descriptions about subjects and objects rather than provide specific names. Our case study concentrates on the period from the inception of the EU state's eGates Programme in November 2007 until December 2012.

This case study focuses on an EU member state that commenced deploying Electronic Gates (eGates) for automated border control crossing inspections, using Electronic Passports (ePassports), of passengers around 2008. States commenced issuing ePassports which complied with the International Civil Aviation Organization (ICAO) Doc 9303 Specification on Electronic Machine Readable Travel Documents (eMRTDs) [146, 41] in 2004. An ePassport was a type of eMRTD. Other forms of eMRTDs included biometric residence permits and national identity cards.

In October 2012 the ICAO's Technical Advisory Group (TAG) reported [147] that 23 countries had deployed Automated Border Control (ABC) systems, which used ICAO compliant eMRTDs, to automatically verify passengers. The earliest ABC deployments were at airports in Australia and Portugal. We use the term eGates to imply a form of ABC system, which uses an ICAO compliant eMRTD, to verify its holder.

The types of ABC systems being piloted in airports were either *biometric identification* deployments or *biometric authentication* deployments. Biometric identification systems

used an enrolled biometric feature, e.g. iris or fingerprint modalities, to identify a person and did not, therefore, require a security document. Biometric authentication systems used a security document, e.g. an ePassport, which was authenticated electronically using X.509.3 digital certificates. Following the successful authentication of the eMRTD by the eGates' inspection system the holder's biometric feature, i.e. facial image, was then captured and compared against the extracted image from the eMRTD, in order to verify its holder. All state's ePassport's issuing authorities distributed their certificates and Certificate Revocation Lists (CRLs) to their indigenous border control police authorities and to other states' border control police authorities, through a centralised digital certificate distribution hub, in order to support the eMRTD authentication process.

The self-service eGates were designed to inspect EU citizen's ePassports at border control crossings in airport terminals. Passengers arriving at airports had the option to use the eGates, in order to pass through immigration control, rather than queuing at the manned border control police channels. The eGates' inspection systems validated the authenticity of the ePassport and also captured the holder's facial image in order to verify that representation to the facial image extracted from the holder's ePassport.

Typically, a set of eGates comprised several parallel enclosures or physical channels each with an eMRTD Radio Frequency Identification (RFID) scanner, an initial physical barrier, which opened once the passenger's eMRTD was authenticated by the inspection system. The eGates also comprised a camera to capture an image of the passenger's face and a second physical barrier, which opened for the successfully verified passenger to walk though and exit the border control environment. At the time of the programme's inception there were several eGates pilot deployments, with different configurations, in Australia, Asia and Europe between 2005 and 2007, which verified passengers' identity automatically at border control crossing points in airports.

The eGates, in our case study, were normally supervised by two border control police officers. Typically, one border control police officer acted as the eGates' system operator, watched a monitor screen that displayed the progress of each passenger as they navigated their way through the eGates' enclosures. The other border control officer, who acted as an usher in front of the eGates, encouraged passengers to use the eGates and to assist those passengers who were experiencing difficulties with using the eGates. Also, where appropriate, the usher would redirect ineligible passengers to the queues for the manually operated border control channels. Certain passengers were ineligible to use the eGates because their ePassport

was not chipped, or because the passenger's nationality was outside the EU or because the ePassport presented by the passenger to the eGates failed to authenticate correctly, i.e. was potentially a counterfeit. There were two different eGate configurations deployed by the programme at the state's airports which were provided by the different eGates manufacturers in two separate supplier consortia.

Typically, the passenger placed their ePassport on to an ePassport RFID reader. If the ePassport was not authenticated successfully, the usher referred that passenger to join the manual border control checks performed by border control police officers. If the ePassport authenticated correctly, then the ePassport holder was prompted, by the first eGate barrier raising, to walk into the eGate enclosure to a fixed position for the facial capture process. A camera then scanned the passenger's face and this captured data was compared to the facial image extracted from the ePassport. If the captured facial image data matched the facial image data extracted from the ePassport, to a predetermined verification threshold, the second barrier in the eGate enclosure lifted and the passenger was allowed to pass through the border control crossing. Essentially, eGate passenger inspections were self-service processes which was supervised by two border control officers.

The particular state in our case study pursued a strategy to pilot both types of ABC system, with a *biometric identification* deployment at one major airport and *biometric authentication eGates*, with various configurations, also at this major airport and also at terminals in several regional airports. The biometric identification pilot deployments involved capturing passenger's iris image data for identifying passengers whereas the eGates pilot deployments involved the use of the passenger's authenticated ePassport to perform facial verification. We will later reflect on the state's border control police decision to continue to operate the eGates deployments for verifying passengers and to gradually withdraw the biometric identification deployments.

7.2 Data Gathered

This section describes the data gathered using our stated data collection techniques, described in Section 4.4, in terms of documentary objects acquired, subjects interviewed, and our own observations and reflections.

The eGates Programme pursued an iterative deployment approach that produced some design

specifications from evaluating several deployment configurations. We discuss the status of these deployments, i.e. proof of concept, trial and pilot, in Section 7.4. Stakeholder objectives and business requirements documentation were not created by the programme at the outset.

7.2.1 Documentary Evidence

We concentrated on gathering data from a variety of reliable sources because we were unable to gain formal consent to access documentation produced by the programme itself.

Through our interviews with members of the programme team we discovered that the programme's focus was on producing test plans and test result reports rather than documentation, such as a feasibility study, business requirements document, risks assessment, privacy impact assessments. We were unable to find documents which described the business rationale or objectives for introducing the eGates. Indeed, as we discuss later in Section 7.4, our data suggests that these documents were not actually produced at all due to the approach pursued by the programme.

The main source of our documentary data came from ICAO, particularly the Technical Advisory Group (TAG), which produced the specifications for eMRTDs and the specifications for testing the eMRTDs with inspection systems.

The list of publications acquired from ICAO include:

- Biometric Deployment of MRTDs Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using MRTDs [140];
- MRTDs Development of a Logical Data Structure (LDS) for Optional Capacity Expansion Technologies v 1.7 [141];
- Guide to Interfacing eMRTDs and Inspection Systems [142];
- Doc 9303 MRTDs Part 1 Machine Readable Official Travel Document Volume 2 Specifications for electronic Enabled MRTDs with Biometric Identification Capability [146];
- MRTDs: History, Interoperability and Implementation v1.4 [154];

- MRTDs RF Protocol and Application Test Standard for ePassports - Part 2 Tests for Air Interface, Initialisation and Anti-Collision and Transport Protocol [143];
- MRTDs RF Protocol and Application Test Standard for ePassports – Part 3 Tests Application Protocol and Logical Data Structure [144];
- MRTDs RF Protocol and Application Test Standard for ePassports – Part 4 Reader Tests for Air Interface Initialisation and Anti-Collision and Transport Protocol [145];
- Guidelines on eMRTDs and Passenger Facilitation [148];
- Technical Advisory Group Report on Machine Readable Travel Documents Twenty-First TAG Meeting Dec 2012 [147]; and
- ICAO MRTD Report Global Standardization Volume 7 Number 2 [150].

Another major source of case study documentary data, specifically on eGates deployments in Europe, came from the Frontex Organisation. Frontex was the European Commission agency responsible for the management of operational cooperation at the external borders of the EU Member States.

The list of publications acquired from Frontex include:

- BIOPASS Study on Automated Biometric Border Crossing Systems for Registered Passenger at Four European Airports [106];
- SeBoCom Pre-Study: A Preliminary Study on Secure Border Communications [75];
- BIOPASS II Automated Biometric Border Crossing Systems Based on ePassports and Facial Recognition: RAPID and Smartgate [107];
- Beyond the Frontiers - Frontex: The First Five Years [111];
- Frontex Annual Risk Analysis 2011 [109];
- Ethics of Border Security produced by University of Birmingham for Frontex [301];
- Futures of Borders - A Forward Study of European Border Checks [114];
- Best Practice Guidelines in the Design, Deployment and Operation of Automated Border Control Crossing Systems [110];

- Frontex Risks Analysis Network Quarterly Issue 3 July-Sept 2011[112];
- Operational and Technical Security of Electronic Passports [108]; and
- Situational Overview on Trafficking Human Beings [113]

We also located reports from non-EU organisations, such as the World Bank, which described the problems faced by border control police to balance security, e.g. detection of illegal immigrants and the illegal trafficking of human beings, while improving passenger facilitation, e.g. reducing passenger queues at border control crossings. We also found publications relating to cross-border control systems, e.g. Schengen Information System (SIRENE), used by states' border control police to identify persons wanted for extradition. We also found video footage on the Internet demonstrating the use of the eGates at airports in Australia.

The list of publications acquired from other recognised organisations include:

- EU Schengen Catalogue–Schengen Information System (SIRENE): Recommendations and Best Practices [66];
- European Commission–Biometrics at the Frontier: Assessing the Impact on Society [90];
- UK Home Office–Physical data: voluntary provision Iris Recognition Immigration System (IRIS) Scheme Definition Document [296];
- International Air Transport Association (IATA)–Simplifying Passenger Travel: Ideal Process Flow V2.0 [149];
- British Airports Authority MiSense Summary Report V 2.00 [37];
- UK House of Lords European Union Committee 9th Report of Session 2007-08 Frontex: the EU External Borders Agency Report with Evidence [297];
- European Commission–Communication COM(2008) 359 final A Common Immigration Policy for Europe: Principles, Actions and Tools [62];
- German Federal Office for Information Security (BSI)–Technical Guideline TR-03110-1 Advanced Security Mechanisms for MRTDs [41];
- European Commission–Guidelines Integrated Border Management in EC External Cooperation [89];

- The World Bank–Collaborative Border Management: A New Approach to an Old Problem [115]; and
- Centre for European Policy Studies–Border Security, Technology and the Stockholm Programme [74]

We found very few scientific publications relating to automated passenger identification or border control eGates. Nevertheless, we found MacLeod and McLindin's contribution [191] on a Methodology for the Evaluation of an International Airport Automated Border Control Processing System particularly valuable to this case study. We found that there were many similarities in the approach pursued by the eGates Programme to MacLeod and McLindin's recommended methodology.

We found the main difference between their theoretical methodology and the eGates Programme's approach was mainly that the programme did not define the problem space in order to capture the raw qualitative and quantitative data for analysis. We discuss this absence of data which defined the identification problem in this case study in greater detail in Section 7.5.

For our specific case study we located publications from the relevant state's national press, specialist industry publications, presentation slides from pertinent industry conferences, and discussion threads in a professional network community, e.g. LinkedIn eGates Professionals Group. Some of our documentary data came from the state's border control police authority's website. We also discovered a government department report relating to the border control police authority's performance and the impact of deploying eGates for automatic border control inspections.

7.2.2 Interview Transcripts

We also acquired data from conducting eight face-to-face semi-structured interviews which were recorded, transcribed and subsequently reviewed by the respective interviewee. The questions posed in our interviews are shown in Appendix D.

We designed our interview questions to ascertain the interviewee's role in the programme, their activities and their contributions to some of the programme's deliverables. Our questions were also designed to acquire their insights on the approach pursued by the programme and

the issues encountered during the programme in order to ascertain the proficiencies and deficiencies of the programme's approach.

We did not, however, use these questions for our interviews with passengers because we wanted to them to concentrate on their most recent experiences of using an eGate, as subjects, in order to acquire data on usability factors. We requested our two passenger interviewees to recall each experience and, where relevant, asked them to explain any difficulty encountered.

Our interviewee set comprised three members of the border control authority's eGates Programme (Interviewees A, B and C), three eGates supplier employees (Interviewees X, Y and Z), and two passengers who had used the eGates on a regular basis (Interviewees M and N). We had, therefore, established the means to gather data from the organisation which owned and operated systems supporting the eGates, organisations which supplied the eGates technologies and passengers who used the eGates. We were, however, unable to interview police officers, as users of the eGates, in order to complete our interviewee set. We failed to obtain the necessary authorisation from the border control police authority to interview border control police officers or their union representatives. A police officer's role, as a user of the eGates, was to monitor the displays which showed the status of each passenger verification transaction.

Interviewees A, B and C were seconded, at the request of the senior management in the border control police authority, to the programme team. Interviewee A's role, seconded from the border control police's research and development department, was to act as the immigration and customs expert advisor to the programme. Interviewee B's role, seconded from the travel document inspection department, was to act as a security expert on ABC inspection systems. Interviewee C was seconded from one of the airport authorities and had acted as their leading representative on the International Air Transport Association (IATA) Simplifying Passenger Travel Interest Group. Interviewee C's role was to act as a programme manager in the eGates Programme.

We were introduced to Interviewee A by a professional colleague who had worked with this person on a previous project relating to the issuance of ePassports for the EU state's Ministry of the Interior (MOI). Interviewee A assisted us in recruiting Interviewees B and C who were all close colleagues in the programme. Interviewee B introduced us to three eGates supplier employees.

Interviewee X represented a global technology manufacturer that supplied ICAO compliant

RFID scanning devices to electronically read data from an eMRTD. Interviewee X's role was to ensure that his RFID scanning devices were compatible with the border control systems and managed the related technical issues that arose during the deployments. Interviewee Y represented one of the two companies that manufactured the eGates which were deployed by the programme. As a pre-sales engineer his duties were to ensure that his company's eGates were technically compatible with the border control systems and he also dealt with performance issues, which centred mainly on the usability of the deployed eGates. Interviewee Z was a pre-sales engineer who represented a company that installed and configured the eGate deployments. This company was a systems integrator and did not actually manufacture the eGates. Interviewee Z's role focused on the integration of eGates systems and the border control systems and dealt mainly with technical compatibility and performance issues.

We made it clear to all the aforementioned interviewees, at the outset, that the purpose of our interview, as reflected in our briefing emails and questions posed in Appendix D, was to ascertain their views on the approach pursued by the programme. All interviewees were provided with an explanation of the aims of our research.

Interviewee M and Interviewee N were our long-term friends from the European banking industry. During a social gathering both interviewees expressed an interest in our research on eGates. Both our friends were citizens from our case study state and were frequent air travellers who had had experience from using biometric identification systems and also eGates. Their experiences were not confined to our case study state as they had used other ABC systems in other EU member states on several occasions. Interviewee M was the leader of a municipality who often went on his holidays to his apartment in Portugal. Interviewee N was a sales representative in the food production industry who often travelled to see her clients in Europe.

We refrain from including data from our own personal experiences of using eGates. We were conscious of the need to pose open and unbiased questions to our two interviewees in order to avoid influencing their descriptions of their experiences. We reiterated to them that we were interested in gathering data from their recent personal experiences of using eGates at airports in our case study state.

All interviewees provided their approval as to the accuracy of the transcripts produced from the interview recordings. Some parts of the transcripts were amended or removed, at the request of interviewees, due to the sensitive nature of their statements. We provide extracts

from our final interview transcripts in Section 7.4.

7.2.3 Our Observation Memos and Reflective Notes

We produced an observation memo immediately after each interview and also after the changes requested by the interviewee following their review of the respective transcript. These memos helped us to gain an understanding of the interviewees' perspectives and their attitudes towards the programme's approach and the utility of the eGates deployments.

We also produced 20 reflective notes during our qualitative analysis of our acquired data. Our analysis included the comparison of the key statements made by different stakeholders both in the interviewee transcript data and in the documentary data. These reflective notes were created and stored within the Atlas.ti CAQDAS tool. Our notes also describe the patterns that we identified in our data regarding the outcomes from the iterative approach pursued by the programme.

7.3 Validation of Our Factors

This section presents the results of our efforts to validate the factors as at Stage 9 of our research implementation plan, as shown in Figure 4.3 on page 124, using the criteria definitions in Section 6.3.1 and the data gathered in this case study.

We then provide a discussion on our results and a description of the patterns that we recognised in our assessment. We also compare the results of this assessment against our assessment results using data from the EU state's eID Card Programme Case Study.

7.3.1 Results from Our Factor Validation Effort

Despite the absence of documentary evidence, generated by the programme itself, we were able to validate more factors using the data in this case study, than using the data from the EU state's eID Card Programme Case Study. We discuss this improvement in our assessment results in the next sub-section.

Table.7.1 shows the total of 222 factors as at Stage 6 of our research implementation plan, at the top of the table, and the status of the 234 identified factors for evaluating APIMs as at

Factors For Evaluating APIMs	**Understanding Perspective**	**Effectiveness Perspective**	**Efficiency Perspective**	**Row Totals**
Pre-Case Study Stage 6 Evaluation Themes	**61 factors 7 factor themes**	**61 factors 9 factor themes**	**100 factors 9 factor themes**	**222 factors 25 factor themes**
Grounded Factors	38 (63%)	55 (79%)	68 (65%)	**161 (68%)**
Deduced Factors	14 (24%)	10 (14%)	29 (28%)	**53 (23%)**
Not-grounded Factors	8 (13%)	5 (7%)	7 (7%)	**20 (9%)**
Relabelled Factors	28	21	28	**77**
Revised Criteria Questions	36	33	43	**112**
Deleted Factors	1	0	2	**3**
New Factors Identified	0	9	6	**15**
Factor Explanations	60	70	104	**234**
Factor Theme Name Change	1	1	3	**5**
Post Case Study Stage 9 Evaluation Themes	**60 factors 7 factor themes**	**70 factors 9 factor themes**	**104 factors 9 factor themes**	**234 factors 25 factor themes**

Table 7.1: Factor Validation Results using the EU State's eGates Programme Case Study Data

Stage 9, at the foot of the table, following our validation efforts.

Table.7.1 shows that the total number of factors had increased overall by 12 and the majority of our identified factors, i.e. 68%, were now grounded. The results also show, however, that over one third of the factors required their label to be more descriptive and that over half of the criteria questions required enhancement to elicit the required information from the application context.

Next, our results are examined in more detail.

7.3.2 Discussion of Validation Assessment Results

The unavailability of documentation from the programme influenced how we used our acquired case study data to validate our factors.

As described earlier, the programme adopted an iterative deployment approach, which involved eGates pilot deployments from various manufacturers, with different configurations, at several airport terminals in the state. Interviewee A stated that *"this approach meant that the programme produced very little documentation in terms of agreed stakeholders' objectives and business requirements"*. The programme concentrated upon producing documentation covering design specifications and operational performance constraints which were incorporated into the Request For Product (RFP) procurement document.

Interviewee B claimed that *"these documents were rushed and were not fully completed because of the Minister of the Interior's unexpected public announcement and instruction to the programme to install eight further sets of eGates within ten weeks"*. We describe the eGates Programme's development and deployment approach later in Section 7.4; however, for our factor validation assessment, we acquired data from other creditable sources. We used the ICAO Doc 9303 specifications on MRTDs, e.g. an ePassport, and the video footage on eGates together with data collected from our interviews with our supplier employees in order to ground our identified factors in the Effectiveness and Efficiency Perspectives of our evaluation framework.

In the absence of documentary data describing stakeholders' objectives to introduce the eGates, we relied on interviewee comments and had to make deductions, based upon our plausible assumptions, in order to ground the factors in the Understanding Perspective. The lack of documentary data generated by the programme, however, restricted our ability to identify new factors in the Understanding Perspective.

7.3.2.1 Factor Identifier Labels

We found that 77 of our 222 factors, i.e. 35%, required their factor label to be more descriptive. Our results also show that at least 50% of our criteria questions required enhancement. This first result is broken down into 45%, 34%, and 28% for the Understanding, Effectiveness and Efficiency Perspectives respectively. The second result is broken down into 59%, 54% and 43% respectively.

Our first result suggests that the factor descriptions were more accurate according to the type of perspective and the degree of granularity of the data relating to that factor, e.g. a false acceptance rate. Factors in the Understanding Perspective are primarily concerned with evaluating knowledge about the application context and the stakeholders' objectives for the APIM. This information tended to be broad and conceptual in nature. Factors in the Effectiveness Perspective were descriptive in terms of APIM's functionality and performance requirements. Factors in the Efficiency Perspective related to specific configuration detail, e.g. the identifier data assigned to identify a subject, and, by nature, concerned required factual information.

Our second result suggests that it is more difficult to construct criteria questions to acquire factual data than questions to acquire data that are conceptual in nature. Our difficulty to construct concise criteria questions to acquire factual data may be explained by Homburg's hierarchical multi-objective decision-making model [134] where objectives are characterised by broad implicit declarations and the subordinate sub-objectives are concise explicit statements. The results of our validation efforts showed that the higher the level of granularity of the data related to a factor the more likely that that factor label and its associated criteria question needed revision.

We also found that many of our criteria questions were too narrow and were only relevant to specific types of APIM. Therefore, we identified the need to generalise the phrasing of these criteria questions so as to accommodate all types of APIM.

We concluded that our strategy to introduce factor explanations for our identified factors, in this case study was justified as these explanations enabled us to locate inadequacies of our factor description labels and their associated criteria questions. Our factor explanations also helped to identify that around 10% of our factors needed reclassification within each perspective. The tables in Appendix E reflect those factors which were reclassified between evaluation themes. There were no factors or evaluation themes which required reclassification between perspectives.

7.3.2.2 Relevancy of Our Factors

The comprehensiveness of the data that we were able to collect enabled us to directly ground the majority of our identified factors. The data also enabled us to make plausible deductions to ground most of our remaining factors.

Our assessment shows that 79% of the factors in the Effectiveness Perspective, excluding nine new factors, out of 70 factors were grounded and 14% were deduced leaving only 7% Not-grounded. This result was mainly due to the availability and granularity of detail in the ICAO specifications on issuing eMRTDs and electronically inspecting eMRTDs. These specifications were designed primarily to ensure technical interoperability between issued ePassports and the *reading* of the ePassports with a border control police officer manually passing the RFID chip in the ePassport across an ePassport RFID scanner. The same specifications were also applied for passengers performing the same task as part of a *self-service automated inspection* process, using eGates.

We were only able to ground 65% of the factors in the Efficiency Perspective, excluding new and deleted factors, out of 104 identified factors and needed to deduce 28% of our factors in this perspective. This meant that 7% of our factors were Not-grounded. While the aforementioned ICAO specifications helped to ground many of the factors relating to the configuration of the eGates we had to make many assumptions on factors relating to the reliability and usability of the eGates.

Our data shows that the programme generated much test data on the reliability and usability of the eGates using observation techniques, video recordings of passengers using eGates, and from conducting interviews with passengers after they had used the eGates. As these test data were not available to us we used our documentary evidence and interview transcripts from our two passenger interviewees to validate the factors in the Usability Results Evaluation Theme, shown in Table E.20. Many of the factors in the Reliability Results Evaluation Theme, shown in Table E.19, however, were Not-grounded or required deduction due to the restrictions on releasing sensitive data to us.

We also identified the need to amend five evaluation theme titles slightly in order to improve clarity of the classification of our evaluation themes. We found that 9% of our original factors, located in the literature, were Not-grounded. We discuss the patterns of our assessment results, including cross-case analysis using data from both of our retrospective case studies, in Section 7.3.3.

7.3.2.3 Consistency of Our Factors

The introduction of an explanation note for each factor highlighted the need to reclassify approximately 10% of our factors. The reclassification of our factors across perspectives are

reflected in the tables in Appendix E.

From our assessment efforts, we recognised the need to differentiate between the operator or user of the APIM and the subject to be automatically identified. We found 15 factors and their associated criteria questions needed to be revised to reflect this distinction. Our results here suggest that either the factors were reasonably consistent or our method for assessing the consistency of factors was deficient, or possibly that our factor classifications need further refinement.

We believe that further empirical research will assist in the reducing the remaining inconsistencies between our factors and also improve our efforts to define the scope of each factor in the relevant evaluation theme.

7.3.2.4 Completeness of Our Factors

From our assessment, we identified 15 new factors which were classified into the evaluation themes of the Effectiveness and Efficiency Perspectives.

The lack of documentary data from the programme was the main reason behind our inability to identify new factors for the Understanding Perspective. We found that only three of our identified factors needed to be deleted due to redundancy. The identification of 15 new factors suggested that, after validating our factors using data from two case studies, we had not reached the saturation point where we could claim that the factors for evaluating APIMs were in any way complete.

In order to reduce the reliance on our deductions and assumptions, we concluded that further empirical research, generating data from the use of the ASMSA Methodology, would improve our factor validation efforts.

7.3.3 Patterns Recognised in our Assessment Data

We now describe patterns recognised in our factor validation assessment in order to answer our first research question. We also provide a cross-case analysis of our validation efforts in this case study and the results of our validation efforts using the data from the EU state's eID Card Programme Case Study.

We consider that our first research question has not, after using data from two case studies, been answered completely. Our case study data, however, has enabled us to reach a point where we consider that most of our evaluation themes in our evaluation theme have been validated, although all factors in our evaluation themes may not be entirely complete. We believe that the research effort needed to establish a comprehensive list of factors may need to investigate many different types of application contexts. Indeed, we believe that it would be inappropriate to claim that such a list is (ever) complete because of the impracticalities of empirical verification.

The comparison of the factor validation results in this case study to those results from the previous case study reveals general trends. The cross-case comparison reveals that the total directly grounded factors in this case study increased to 68% from 62% of the directly grounded factors in our assessment of the data acquired from the EU state's eID Card Programme Case Study. Additionally, the percentage of Not-grounded factors has reduced to 9% for this case study from 22% as in our initial case study. Conversely, the percentage of deduced factors increased to 23% in this case study from 16% as in our initial case study.

This pattern suggests that either our acquired data was more comprehensive for this second retrospective case study than our initial retrospective case study, or that our identified factors for evaluating APIMs are becoming more descriptive, through enhancement, or that some of our assumptions for this case study may not be entirely plausible.

From our cross-case comparison of validation results, we found that 157 out of 207 76% our identified factors, originally located in the literature, were grounded directly, at least once, in the data of our two retrospective case studies. Factors identified in our case study data sets are, by definition, grounded. Therefore, excluding the eight factors which were originally identified, 42 20% out of our original 207 factors have been either deduced or Not-grounded.

From further analysis of these remaining factors we found that following five factors were Not-grounded in either of our two retrospective case study data sets:

1. Duress Policy in the Policies Evaluation Theme (Identifier A.17.8.) –see Table E.7. in Appendix E);
2. Template Update Notification Factor in the Reliability Results Evaluation Theme (Identifier A.16.19.) –see Table E.19. in Appendix E);
3. Signal Retrieval Strategy Factor in the Usability Results Evaluation Theme (Identifier

A.15.9.) –see Table E.20. in Appendix E);

4. Signal Meaningfulness Factor in the Usability Results Evaluation Theme (Identifier A.15.10.) –see Table E.20. in Appendix E); and

5. Backup Methods Factor in the Technology Management Theme (Identifier A.16.8.) –see Table E.21. in Appendix E).

The relevancy of these five factors requires scrutiny during further factor validation assessments. Also, these assessments should aim to eliminate the need for validating our identified factors using our deductions and our plausible assumptions. We recognise, however, that some factors may only be relevant for certain types of application contexts or particular types of APIMs.

The significant increase from 38 relabelled factors in our initial assessment to 77 relabelled factors in our second assessment suggests that our factor identifier's descriptions still needed improvement to make them more illustrative of our identified factors. Similarly, the revised criteria questions from 36 in our first assessment up to 112 instances in our second assessment suggests that our criteria questions also needed enhancement. Nevertheless, we consider that our strategy to include an explanation note for each factor had a positive impact upon our validation results in the second assessment. The explanations assisted us to identify the descriptive deficiencies of our factor identifiers and also to identify the improvements required for our criteria questions.

We concluded that further assessments were needed to validate our factors which had not been directly grounded in the data of our two retrospective case studies. The acquisition of relevant data is key to validating these remaining factors. We consider that using our identified factors in our methodology to evaluate an APIM for a real-world application context, using a participative research approach, e.g. action research, as described in Section 4.1.9.3, may offer greater potential to further validate our factors than using data from another retrospective case study. We describe our efforts to validate our factors (and to identify new factors), by gathering data from employing the ASMSA Methodology in the Corporation X 2FA Case Study.

7.4 Methodological Observations on the Programme's Approach

For our main unit of analysis on methodological efficacy, we now describe our interviewees' observations on the programme's approach to deploy eGates at terminals in several airport locations. We commence by providing an historical account of the eGates Programme.

7.4.1 The eGates Programme's Approach

We begin by describing the prevailing conditions at the time of the eGates Programme's inception. We then describe the strategies pursued by the programme and the significant events that occurred during the programme, and the eventual outcomes as at the end of our case study period.

The programme pursued an *iterative deployment* approach to introduce the eGates into border control crossings. This approach involved several deployment, test and review cycles. There was confusion, however, amongst our interviewees as to the actual approach pursued by the programme. During the programme there were several eGates introduced, either as *proof of concept* or *pilot* deployments, in various airport terminals operating with different configurations simultaneously. Interviewee B used the term *"experimental approach"* while Interviewee C claimed that the programme followed *"robust methodological development processes"*.

Interviewee A claimed that *"the eGates were installed as an experiment, to ascertain whether eGates would be "useful" to border crossing controls"*. The main undocumented objective, according to Interviewee B was *"for the eGates to increase the throughput rate of border control passenger inspections without compromising security"*. At that time there were long passenger queues in airports at manually operated border control crossings.

The iterative deployment approach required the programme team to gather data, during passengers' usage of the eGates, from several deployment iterations. Acquired data were then analysed and the eGates' configurations were subsequently revised and retested with passengers. The main outcomes from the approach pursued appears to be the sporadic availability of the eGates at some airport terminals, passenger confusion as to whether they are eligible to use the eGates, and usability problems, particularly for infrequent travellers.

We found that the programme did **not** follow a formal systematic methodology. One of our supplier interviewees interpreted the two initial deployments as *"proof of concept"* installations; however, the programme did not produce a feasibility study document or criteria evaluate those deployments. The programme produced designs and specifications for the eGates based upon these initial deployments. We found that there were no documents outlining stakeholders' objectives or business requirements for an ABC; however, the business problem appeared to be understood by our interviewees. The programme's task was to integrate new eGates technology into existing infrastructures and systems rather than to introduce a complete solution to address their recognised business problem.

None of our interviewees claimed that the eGates deployments had been a success or a failure; although, most interviewees thought that benefits of the stakeholders' investments in the eGates would be reaped over a long period. Much of the programme effort went into iterative performance testing with suppliers enhancing and reconfiguring their systems in order to improve automated passenger inspection throughput rates. We found that there were increases in passenger inspection throughput rates only at major airport terminals. The eGates deployed at smaller terminals were under-utilised. We also found that the eGates were not always available at the major terminals because there were outstanding contractual issues. Also these eGates and the supporting systems did not possess sufficient processing capacity to serve passengers, on occasions, at peak demand.

We found that the deployed eGates had not been evaluated by the programme team to ascertain whether the programme's main objective *to increase the throughput rate of border control passenger inspections without compromising security* had been met. The programme team did not even attempt to gather the biometric authentication decision accuracy data required in order to assess their main objective.

Interviewees A claimed that *"the performance objective that had been set could not be easily assessed in practice"*. There appeared to be a difficulty in gathering the relevant data sets on manual border control inspections and also the eGates inspections in order to assess whether the main objective was achieved. Both data sets were required to establish *ground truth knowledge* [1] the genuineness of the verified passengers and their ePassports. This genuineness would then allow the programme to identify verification false acceptances and verification false rejections. Additionally, as Interviewee A commented, that *"a border control police*

[1] Dunstone and Yager describe [86] ground truth knowledge as a correct data match because the biometric verification comparison, between data samples acquired, originate from the same genuine user.

officer may have behaved differently if they became aware that their identification decisions were being monitored in order to test their performance accuracy".

Figure 7.1 is a representation of the programme's approach which has been generated from the Atlas.ti CAQDAS tool following our descriptive coding of the data gathered. Figure 7.1 is designed to show the progression of the programme from its inception through to the programme's outcomes as at the end of our case study period. Figure 7.1 should not be construed as a causal network as our data were insufficient to identify direct causal effects throughout the programme.

The conditions prevailing at the time of the programme's inception, represented by antecedent variables, are shown in the boxes in the left column and the programme's outcomes, represented by outcome variables, are shown in the boxes in the right column of Figure 7.1. The boxes in between the preconditions column and eventual outcomes column represent the strategies pursued and the significant events that occurred during the programme, i.e. the intervening variables.

In order to protect the identity of our case study, we refrain from providing dates in Figure 7.1; however, we provide elapsed months in our descriptions to reflect the impact that the MOI's imposed delivery timescales had on the programme's outcomes.

7.4.2 Prevailing Conditions

This sub-section describes the prevailing circumstances prior to the programme's inception. There were notable variations in our interviewees' accounts regarding the prevailing conditions to commence the eGates Programme. Our aim, from a critical realist standpoint, was to analyse each interviewee's perspective and not to establish the irrefutable truth.

According to Interviewee A *"the programme commenced when the head of the state's border control police authority watched a manufacturer's eGates in operation, at a technology exhibition, and then decided to experiment with the eGates to ascertain whether they would be beneficial to the border control authority's operations"*. The eGates Programme Team was setup shortly afterwards with a mandate to determine the automated passenger inspection capabilities of eGates deployments at the state's airports and seaports.

Interviewee C stated, however, *"the introduction of eGates was the next step onwards from the passenger identification experiments that had been performed in other states"*. This

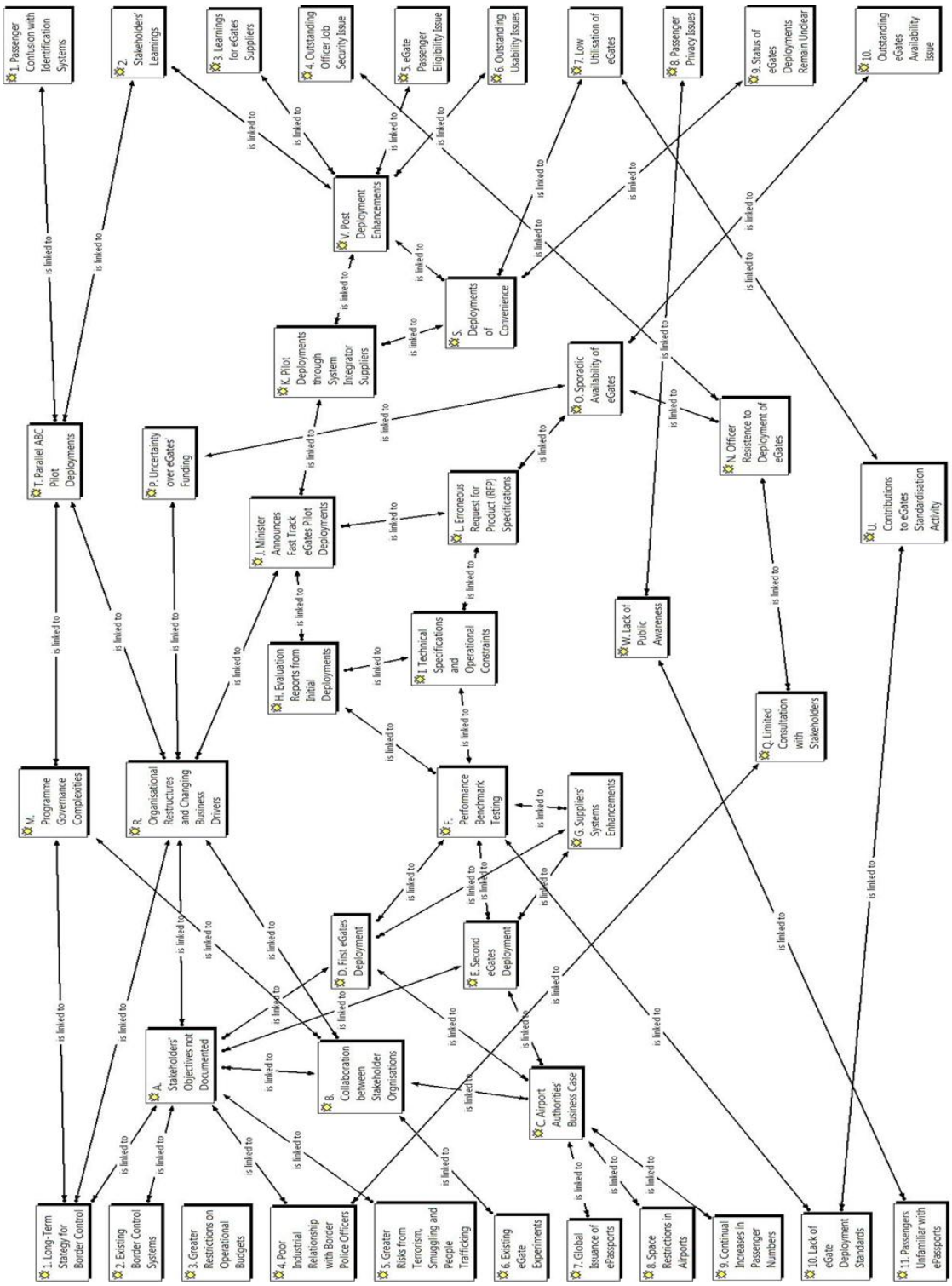

Figure 7.1: Approach Pursued by the EU State's eGates Programme

interviewee, as a member of the International Air Transport Association (IATA) Simplifying Passenger Travel Interest Group, had conducted research into how a passenger journey through an airport could be improved through the use of technology, particularly by reducing the passenger queues at border control passenger inspections.

We provide a list of the conditions prevailing at the time of the programme's inception with supporting descriptions.

1. **Long-Term Strategy for Border Control** The MOI had published a five year strategy to encourage the introduction of innovative technologies into border control crossing locations as a response to the projected increases in passenger numbers and the threats emerging from terrorist attacks, illegal immigration and people trafficking.

2. **Existing Border Control Systems** There were border control systems, with high security classifications, which assisted the border control police officers to detect stolen passports and also to identify individuals that appeared on a blacklist. These officers were trained to detect fraudulent and counterfeit passports and other forms of travel document, e.g. identity cards. They also received psychological behaviour training in order to pose incisive questions to passengers about the legitimacy of their visit to the state.

3. **Greater Restrictions on Operational Budgets** The border control police authority management, in response to government operational budget restrictions, had pressure placed upon it to reduce its operational costs.

4. **Poor Industrial Relations with Border Police Officers** The industrial relations between the border control police officers, represented by their unions, and the border control police authority's management team had deteriorated over several years.

5. **Greater Risks from Terrorism, Smuggling and People Trafficking** The risks of these illegal activities, together with illegal immigration, were constantly increasing and the threats posed to the state's citizens were reported regularly in the media.

6. **Existing eGate Experiments** Deployments of eGates in other states either complemented a biometric identification ABC or were run as standalone biometric verification ABC experiments. Several of these ABC experiments were supplier-funded.

7. **Global Issuance of ePassports** The introduction of ePassports meant that an increasing number of passengers carried an ICAO compliant ePassport, with an ICC, containing

their biographical and biometric data to enable automated passenger inspections at border control crossings. All ePassports contained, in accordance with the ICAO DOC 9303 Specification [146], the holder's facial image and there were many EU states' ePassports that contained the holder's fingerprint images.

8. Space Restrictions in Airports Airport authorities sought to improve the utilisation of the restricted space in airport terminals in order to realise further commercial opportunities.

9. Continual Increases in Passenger Numbers Long passenger queues at airport border control inspection points were regularly reported in the media, not only in the case study state, but in many other states worldwide.

10. Lack of eGate Deployment Standards There were no interoperability or security standards that the programme could use to assist with the configuration of the eGates.

11. Passengers Unfamiliar with ePassports Passengers were unfamiliar with ePassports, in that they were not aware that they possessed an ePassport or that it had an ICC which could be used in an eGate or similar ABC.

Interviewee A conceded that *"there were very few instances of this technology around the world and therefore we had no preconceptions and no standards against which to judge them. So we thought what we would do was to run restricted trials, put them in and see what happens to establish a kind of baseline, if you like. We would measure them in terms of transaction times, performance accuracy, ease of use, that kind of thing to try to establish a baseline"*.

7.4.3 Strategies Pursued and Significant Events

This sub-section describes the strategies pursued by the programme and the significant events that took place during the programme.

The terms *experiment*, *proof of concept*, *trial*, *pilot* and *prototype* were used interchangeably by our interviewees and the exact status of the deployment appeared to have caused much confusion, not only amongst our interviewees involved directly in the programme, but also those interviewees involved externally, such as the eGates manufacturers. Irrespective of their declared deployment status, the eGates deployments were actually operating in a live

production environment in that they were integrated into the existing systems' infrastructure and being used by passengers. The eGates were authenticating real ePassports and were capturing passengers' biometric features.

The strategies pursued and the significant events that occurred during the programme are as follows:

A. Stakeholders' Objectives Not Documented We found that the programme did not document the stakeholders' objectives for the eGates. Benchmark performance objectives, however, were set during the two initial *proof of concept* deployments.

B. Collaboration between Stakeholder Organisations A collaboration agreement was established between the border control police authority and the two airport authorities around month three to explore the use of eGates for automatic passenger inspections.

C. Airport Authorities' Business Case The two airport authorities established a joint business case to fund the two initial eGates' *proof of concept* deployments for the border control police authority. The programme reached an agreement with a technology consortia, including an eGates manufacturer, to deploy the eGates at two airport terminals.

D. First eGates Deployment The first eGate deployment commenced around month 8. The objectives of the initial eGates proof of concept deployment differed between our interviewees. Interviewee C claimed that *"the purpose of the trial was to look at the viability of technology to replace immigration officers to offer an alternative route across the border for passengers"*. Interviewee B claimed that *"the proof of concept focused on consistency of security and passenger throughput rates"*.

E. Second eGates Deployment We found that the second deployment in month 10 was not planned by the programme team. A second technology consortium offered to install their eGates solution at an alternative airport terminal. Whether a fortuitous coincidence or an engineered opportunity, it allowed the programme to run two 'proof of concept' deployments in parallel with two different eGates configurations.

F. Performance Benchmark Testing The programme created a variety of metrics in order to establish an understanding of the baseline performance of the eGates in an operating environment. From the iterative evaluations, the eGates were reconfigured on several occasions in order to improve the passenger throughput rates. The programme

employed usability specialists, security specialists and operational management consultants in order to establish a set of baseline performance benchmarks.

H. Evaluation Report from Initial Deployments An evaluation report was produced by the programme, mainly covering the technical performance of the eGates. It recommended the deployment of eGates with specific caveats on the eligibility of suitable passengers. We found that this evaluation report was produced hurriedly and we explain the reasons shortly in Point J.

I. Technical Specifications and Operational Constraints During the production of the evaluation report, the programme was also engaged in producing technical specifications and operational constraints documentation for the various components. A list of over 200 specifications was produced, some of which were classified as mandatory features and the remaining as desirable features. Our data suggests that these documents were completed hurriedly by the programme team because the MOI announced, unexpectedly to the programme team, that further eGates were to be installed at other airport terminals within ten weeks by the end of month 21. These hurriedly completed specifications formed the basis of the RFPs issued, for several of the eGates systems' sub-components, which were published in procurement journals.

J. MOI Announces Fast Track eGates Pilot Deployments We found that the programme team members were under the impression that the two initial deployments were to last for at least another six months followed by a period of evaluation in order to produce the evaluation report and also technical specifications. The justification for the fast track pilot deployments was never explained by the MOI to the members of the programme team.

K. Pilot Deployments through System Integrators The fast track deployment plan to install a further eight eGates in other airport terminals, commenced in month 19 to meet the month 21 deadline set by the MOI. The programme used the existing supplier framework contracts with system integrators because this strategy was considered to be the most expedient way to procure the eGates systems' sub-components.

L. Erroneous RFP Specifications The programme produced the RFP specification documentation hurriedly in response to the minister's deployment deadline. According to Interviewee Y *"those RFP documents contained many errors and omissions in comparison to the two pilot eGates deployments [that were in operation]"*.

M. Programme Governance Complexities The governance structure and responsibilities for deploying the eGates at specific ports appears to have been complex and subject to different managerial influences and personal opinions. The programme used Prince2 qualified project managers who controlled the programme using risk registers, issue logs and project plans in line with the Prince2 Programme Methodology. Interviewee B stated, however, *" that border control management changed and altered deliverables without those amendments being discussed or recorded [with the programme team]"*.

N. Officer Resistance to Deployment of eGates The border control police officers, as operators, were opposed the introduction of eGates. Interviewee A confirmed that *"the officers' concerns over job security as the main reason behind the border control police officers' opposition to supervise the eGates"*.

O. Sporadic Availability of the eGates There were many occasions when the eGates were not available to passengers. We found there were two main causes: firstly, border control police officer resistance to operating and supervising the eGates; and secondly, the eGates' subsystems failed frequently as there was a lack of operational support resources to monitor the operation of the eGates' systems. The investment required to support these deployments was due to outstanding contractual issues between the border control police authority and the airports authorities to support the eGates.

P. Uncertainty over eGates' Funding The uncertainty surrounding the future funding of the eGates hampered the programme to establish support arrangements for the two initial proof of concept deployments and the eight additional fast track eGates deployments. This uncertainty resulted in programme delays and difficulties in respect of decisions relating to purchasing equipment and resolving system failures.

Q. Limited Consultation with Stakeholders Our data suggests that consultation took place on a regular basis between the programme and its main stakeholders, i.e. the border control police management and the two airport authorities. Also the two initial deployments provided the programme team with the opportunity to consult with passengers, as subjects, about their experiences of using eGates. The consultation between the programme and the border control police officers and their two unions, however, appeared to have been inadequate to resolve the police officers' concerns about job security.

R. Organisational Restructures and Changing Business Drivers We found that the border control police authority's organisation was restructured on several occasions during the programme. These organisational restructures resulted in the business drivers for

eGates being revised regularly due to personnel changes in the senior management positions of the border control police authority.

S. Deployments of Convenience We found that the eGates were not deployed at airport terminals that would derive most business benefit. The eGates were installed at those airports which agreed to accommodate the eGates within the imposed deployment deadlines.

T. Parallel ABC Pilot Deployments The biometric identification system pilot deployments and the eGates deployments continued to be available to passengers at different terminals and airports. We found that the parallel operation of both types of automated border control crossing systems caused confusion amongst the passengers using these systems.

U. Contributions to Standardisation Activities Several individuals in the programme team contributed towards the standardisation efforts to establish usability and digital certificate management interoperability guidelines for eGates.

V. Post Deployment Enhancements Following the deployment of the eight fast track eGates the border control police authority then made several requests, through the programme team, to the eGates' suppliers to improve the passenger inspection throughput rates.

W. Lack of Public Awareness We found that the border control police authority's strategy to minimise the publicity and educational material on the deployment of eGates impacted the passenger usage of the eGates.

7.4.4 Programme Outcomes

This sub-section describes the outcomes of the eGates Programme, as provided by our interviewees, and our analysis of the documentary data. We include plausible causal explanations, where appropriate, in the following list of programme outcomes.

1. Passenger Confusion with Identification Systems We found that passengers were confused as to which type of ABC system they were using at an airport terminal and how to operate each system.

2. Stakeholders' Learnings We found that the border control police authority and the airport authorities gained much technical and operational know-how about deploying

biometrics solutions. They also gained understanding on the commercial feasibility and performance capabilities of operating eGates at airport terminals.

3. Learnings for eGates Manufacturers The eGates' manufacturers to the programme gained the opportunity to validate and refine their products, using passengers with authentic ePassports, in production environments.

4. Outstanding Officer Job Security Issue We found that the border control police authority's management had not resolved the job security issue with the unions for border control police officers. As a result the eGates were often unavailable to passengers. We discuss the consequences of the programme's lack of consultation with the border control police officers, as eGates stakeholder users, later in Section 7.5.

5. Passenger Eligibility Issue We found that passengers were unaware that they were eligible to use the eGates. Passenger misunderstandings were caused by the lack of public awareness of ePassports and their capabilities. A contributory factor was the complexity of the passenger eligibility criteria to use eGates which were specified in the eGates evaluation report.

6. Outstanding Usability Issues Interviewee B conceded that there were outstanding usability issues with the eGates. We found three main explanations relating to the outstanding usability issues despite usability experts being engaged in the programme. Firstly, infrequent usage appeared to be an important factor because many passengers used the eGates only once or twice a year and forgot how to use the eGates. Secondly, the eGates' passenger interactions were not uniform across the deployments which caused passenger confusion. We found that the eGates' Human Computer Interface (HCI) not only differed between the various manufacturers of eGates but also both eGates' manufacturers had deployed slightly different configurations of their eGates as they continued to refine their products. Thirdly, the system feedback to passengers was either non-uniform, in part was non-existent or was not integrated so as to provide a coherent experience for passengers.

7. Low Utilisation of eGates We found that passenger utilisation of the eGates was generally low despite the programme having introduced several measures to encourage passengers' to use the eGates. We also found that some eGate deployments were operating below capacity at several locations whereas at other locations the eGates struggled on some occasions to respond to peak demand.

8. Passenger Privacy Issues Interviewee N expressed concerns relating to *"the border control police authority storing and forwarding biographical and biometric data to other government departments"*. None of the programme interviewees or the supplier's interviewees commented on issues surrounding the subsequent usage of passengers' data gathered from eGates passenger inspections or the need to protect the acquired biometric data.

9. Status of eGate Deployments Remained Unclear We found that the interviewee members of the programme team and also the suppliers were unclear as to the status of the eGate deployments throughout the programme and as at the end of our case study.

10. Outstanding eGates Availability Issue We found that the sporadic availability of the eGates remained an outstanding issue. This issue was due to unresolved technical problems because of the absence of a support contract. Additionally, the manning of the eGates remained unresolved between the border control police authority and with police officers because of the latter's concerns over job security.

7.4.5 Methodological Insights

We now provide retrospective insights from our interviewees, excluding the passenger interviewees, on whether the approach pursued by the programme was efficacious for the eGates deployments.

The purpose of our questions were designed acquire data in order to identify methodological proficiencies and deficiencies and also learnings from the approach pursued by the programme. We then compare their responses with documentary evidence acquired on methodological efficacy.

7.4.5.1 Iterative Deployment Approach

We found that our interviewees had mixed views on the merits of the programme's iterative deployment approach and there was general agreement that some activities could have been improved.

Interviewee B summed up the programme's approach: *"I don't think the way that we did it was a good way. I think the lessons learned review exercise highlighted the various problems"*.

7.4.5.2 Inability to Determine the Utility of Deployed eGates

We found that the programme team were unable to determine whether their performance objective for the eGates deployments had been fulfilled. The performance objective established appears to have been flawed due to impracticalities of measuring the accuracy decisions on passenger identity verification processes.

The programme established a passenger throughput rate objective which stated that one eGate inspection should equate to five police officer inspections, in the same time frame, without diminishing the existing security controls. Our data shows that the programme did not, and, perhaps, could not gather all the relevant performance data to determine the actual utility of the eGates against the manual inspections. We found that while throughput timings were gathered by the programme team the data relating to the accuracy of the passenger verification decisions, whether executed by the eGates or performed by police officers, were not acquired.

Interviewee A described the theoretical basis upon which the prime objective was originally set: *"Humans [border control police officers] you know do make mistakes - they can look at a photograph and fail to match it against the real live face and then machines are great. But it also depends on the quality of the technology and now if we can get these accuracy percentages up then, I think, probably you could say that they [eGates] are slightly better than people [border control police officer] at that kind of thing. Where it comes to such things as making qualitative judgments about people [passengers] then that is more difficult. A more complex logical operation is when you are looking at somebody that says this person is this gender, of this age, from this country, they have travelled by this route - what does that suggest to the border control police officer? So, yes, I think, on balance I'd say it probably made us [border control police authority] better at things because the donkey work has been taken away from the officers and left them with the more complex assessments"*.

These insights suggest that a methodology for selecting an APIM should incorporate processes for validating performance objectives set by stakeholders. Moreover, these processes should include considerations as to how the data are to be collected in order to enable the utility of an APIM to be evaluated objectively.

7.4.5.3 Multi-Disciplinary Programme Team

We found that the programme adopted collaborative working arrangements with a variety of discipline experts from each stakeholder organisation.

The range of experts covered disciplines such as legal and compliance, health and safety regulations, ergonomics, operational research, physical security, information security, usability, functional and system performance testing, security accreditation, biometrics and procurement. The multi-disciplinary team enabled the programme to evaluate the deployments from several disciplinary perspectives and identified operational constraints, e.g. health and safety regulations, which resulted in the refinement of the eGates' specifications.

From these findings, it would appear that a methodology to select an APIM would benefit by adopting a multi-disciplinary approach to assist decisions on APIM deployments.

7.4.5.4 Articulation of Stakeholders' Objectives and Business Requirements

We found that the programme team focused their attention on producing documentation that described the eGates solution rather than documenting stakeholders' objectives or business requirements for the eGates. The specifications for the eGates included operational passenger throughput rates, identification threshold rates and descriptions of operational constraints; however, there were very few statements in terms of business objectives and requirements.

Interviewee Y described the impact of the programme's focus to produce technical specifications for eGates rather than articulating their business requirements on the deployments: *"From my experience working on other bids in other countries focusing on technical specifications rather than business requirements restricts supplier ingenuity and increases the cost of proposals. Border authorities still seem to be listing extensive technical specifications which makes each tender distinct from each other, meaning that an 'off the shelf' product offering impossible. By putting a larger emphasis on business objectives and requirements rather than technical specifications, you allow suppliers to propose different technologies and some freedom to design the solution. Suppliers, generally, have greater expertise on the technology and being restrictive with the technical specifications serves to increase the cost of proposals"*.

These insights suggest that a methodology for selecting an APIM should include processes

for documenting stakeholders' objectives and their business requirements, as recommended by Hull et al. [138] for all information systems.

7.4.5.5 Methods for Establishing Business Requirements

We found that there were benefits in using a *proof of concept* eGates deployment in a production environment because it assisted the programme to assess the capabilities of identification technologies of fulfilling stakeholders' objectives.

The two *proof of concept* eGate deployments in different production environments served as valuable tools which enabled the programme to set achievable performance objectives. The deployments also helped to identify the capital and operational cost elements associated with the eGates, which would have formed part of the input into the financial feasibility of introducing and maintaining the eGates. Those deployments were not, however, used by the programme to establish the business requirements for the eGates.

The method of establishing technical specifications adopted by the programme relied upon the border control police authority's ability to control the eGates' deployments in the airport terminals. There may, however, be some application contexts where stakeholders may not have the same degree of control over the environment to pursue this approach in order to gather their requirements for an APIM.

These insights suggest that a methodology should determine the methods for gathering the business requirements for the APIM at the outset. A proof of concept deployment, if the application context permits, appears to be an efficacious method for identifying and setting performance objectives for an APIM.

7.4.5.6 Specifying Performance Tests and Testing Methods

We found that the programme had to specify the performance tests and invent their own testing methods to evaluate the eGate deployments.

While there are standards, such as ISO/IEC 19795-1:2006 [161], for the evaluation of biometric systems, which principally cover testing for error rates, setting thresholds together with identification and verification acceptance rates. Interviewee A claimed that *"the programme had to devise their own tests and methods for testing eGates"*. As Wayman et

al. conclude [312] most performance testing methods generate *technology* test metrics and do not incorporate operational environment factors or human behaviour factors. Our data suggests that the programme spent considerable effort in devising tests that were appropriate to their key throughput performance objective.

These insights suggest that a methodology to select an APIM should include processes to define the performance tests in order to determine whether performance objectives for the APIM can be and have been achieved. A methodology should also include processes for establishing the appropriate data acquisition methods, relevant to the application context, to enable the objective evaluation of an APIM's performance.

7.4.5.7 Consultation with the Users

We found that the cooperation of border control police officers, as the eGates' users, were vital to the operation of the eGates.

The programme's inadequate management of the consultation processes with the police officers to address their concerns over job security was a plausible explanation to the police officers' reluctance to supervise the eGates. Conversely, we found that the consultations and collaborations between the two main stakeholders, the supplier consortia, and the consultation with passengers, as subjects, appears to have worked satisfactorily.

Well-structured consultation processes, as recommended by Hemmati [128], had the potential to help the programme to address and possibly resolve police officers' concerns, which could have avoided or reduced the impacts relating to the police officers' reluctance to operate the eGates. Even if the programme's consultation processes had been proficient, there was another plausible reason regarding the police officers' reluctance to supervise the eGates. There had been a series of industrial disputes, relating to enforced redundancies, between the border control police authority and the police officers. The introduction of eGates was seen by the police officers and their unions to be another threat to their job security.

Our data suggests that the programme did not handle this sensitive issue proficiently, despite the potential consequences of police officers jeopardising the operation of the eGates. There may be some circumstances where stakeholders are unable to resolve their conflicting objectives. We conclude from these insights that investments for an APIM would, in such cases, appear to be unwise until major conflicts are reconciled or the impacts of conflicting

stakeholders' objectives are minimised sufficiently.

These insights suggest that a methodology to select an APIM should seek to reconcile conflicts in stakeholders' objectives, particularly users of the APIM, in the early stages of a programme.

7.4.5.8 Purpose of Deployment Stages

We found that the programme team and also the supplier consortia were not only unclear as to the status of each eGate deployment, but also there was confusion regarding each deployment's purpose.

Interviewee Y described the approach pursued by the programme team and compared it to his experiences of deploying eGates in other states: *"Overseas we are seeing a lot of implementations now who follow a similar deployment model [as our case study], which is to have a proof of concept, then a pilot and then a roll-out. What they [our case study] did in some ways was to have the proof of concept which was more like pilot and the pilot which was more like a roll-out"*.

These insights suggest that a methodology to select and configure an APIM should define the purpose and status of each deployment.

7.4.5.9 Evaluation Factor Check List

Three of the programme interviewees stated that they would have benefited from having worked with a *a factor check list* to help them to identify and consider the various aspects relating to the deployment of eGates.

Each interviewee explained their insights behind the need for a factor check list in the following comments:

- Interviewee A stated *"At the time there was very little in the way of standards for implementing biometric systems and there was very, very little experience within border control authorities on how these things work"*.
- Interviewee B stated *"It would have been useful because at least we would have had something else external to fall back on to say 'yes, that this is the accepted process'*

and 'we haven't done that'. So in that way it's a bit of reassurance".

- Interviewee C stated *"We would then have been able to have produced a document saying 'yes that we've done these ones [considered these factors] but we haven't done these ones and this is why' and that document doesn't exist"*.

These insights suggest that a methodology containing a factor check list could be beneficial to programmes to enable the evaluation of a range of factors prior to the selection of an APIM for their application context.

7.4.5.10 Clarity of Stakeholders' Objectives and Commitments

Interviewees A and B made similar statements in that the programme lacked direction because the border control police authority did not make clear its objectives or confirm its commitment for deploying the eGates to members of the programme team and also to other stakeholders, including the supplier consortia.

Our interviewees also claimed that there was insufficient transparency as to the border control police management's primary objective for introducing the eGates into airport terminals. The political motives for the fast track eGates deployments were not made clear to the programme team. The suspected MOI's underlying motives, as intimated by our interviewees, inhibited the programme's decisions as to where to install the eGates and also the eGates deployment configurations.

These insights suggest that a methodology for selecting and configuring an APIM should encourage stakeholders to clarify their objectives and their commitment to a programme at the outset.

7.5 Methodological Learnings

This section describes the methodological learnings from the patterns that we recognised in our case study data relating to the iterative deployment approach adopted by the programme. We also reflect on the efficacy of the programme's approach to select the optimal APIM.

While we were unable to ascertain the underlying political motives behind the MOI's insistence on the fast track eGates deployments the programme's approach was sufficiently

flexible and agile to deliver the additional eGates in the required timescales. The rapid eGates deployments, however, attracted a variety of issues. The deployed eGates possessed usability design flaws which impacted the passenger throughput rates. The eGates were under-utilised in some airport terminals and some eGates deployments had restricted capacity.

Notwithstanding the political influences on the eGate deployment timescales, an iterative deployment appears to be an efficacious methodology to select an APIM when there is a need to be flexible and responsive to the demands of an evolving application context.

7.5.1 Iterative Deployment Approach

We provide explanations from our case study data to support our aforementioned statement on methodological efficacy, by classifying the patterns in our data on the methodological proficiencies and deficiencies of an iterative deployment approach for the selection and deployment of eGates at border control crossings.

7.5.1.1 Methodological Proficiencies

From our analysis of our case study data we found that the iterative deployment approach was efficacious because the programme needed to deploy the eGates rapidly into an ever changing border control crossing environment which needed to increase the number of passenger inspections and also respond to the threats posed by terrorists and human traffickers.

The approach pursued by the programme was based on the opportunity to test the eGates in a controlled production environment with passengers. The iterative deployment approach appeared to have been beneficial to the programme team in helping them to refine their specifications after gaining knowledge and experience from operating the eGates. Manufacturers of the eGates were able to validate and refine their eGate products in response to the passenger utilisation data acquired during live operation.

We found that the use of a range of discipline experts assisted the programme significantly in producing and refining the technical specifications for the eGates. The iterative deployment approach had the potential flexibility to develop a business requirements document. The planned activities for producing the latter document were unexpectedly truncated.

An iterative deployment approach appears efficacious when there is an opportunity to validate

the proposed identification technologies in a production environment. The approach also appears efficacious when the circumstances dictate that the introduction or enhancement of identification technologies is required to be deployed rapidly.

7.5.1.2 Methodological Deficiencies

We found the main deficiency of this iterative approach related to the programme's inability to determine whether the eGates achieved the stakeholders' business objectives. The programme did not attempt to acquire the relevant data in order to determine whether the deployed eGates actually fulfilled the stakeholders' primary objective to increase passenger border control inspections within specific decision accuracy constraints. Our data also shows that this primary objective appeared to have been diluted during the programme.

The lack of documented stakeholders' objectives and business requirements in this approach meant that the programme team had no foundations upon which to develop tests for the eGates, i.e. acceptance tests. Also, there appeared to have been no effort to gather the relevant data in order to demonstrate that the MOI investments in the eGates had been worthwhile.

The programme's focus was primarily on increasing passenger throughput rates which meant that significant effort was afforded on improving the usability of the eGates. We found, however, there remained outstanding usability design flaws in the passenger interactions with the eGates' various components. The existence of usability design flaws is explained by the approach pursued by the programme as follows:

- The passenger eGates interactions differed between the eGates deployed in terminals of other airports in the EU state and also in other states. The programme did not appear to attempt to standardise these interactions in the EU state.
- Some of the components, such as the ePassport RFID readers, were intended to be used by border control police on a regular basis and were not designed to be used by passengers sporadically. The programme did not request manufactures to design components which were compatible for passenger self-service interactions.
- The absence of guidance on the capabilities of ePassports and the operation of eGates for the travelling public not only had an impact on passengers' willingness to use the eGates, but also influenced those passengers who attempted to use the eGates.

We found that willing passengers' mental model of how the eGates actually operated differed considerably to the actual interaction model. Interviewees M and N encountered difficulties in using the eGates initially and both stated that the eGates' design *"was not intuitive"*.

The border control police authority's strategy to rely on passengers to familiarise themselves with the eGates through frequent usage to overcome these usability design flaws appeared to have failed. Also the authority's strategy to limit educational material in the public domain did not appear to have been an appropriate marketing approach because passenger utilisation of the eGates remained low as at the end of our case study period. The authority's eGates awareness strategy, however, should not be construed as a deficiency of the programme's iterative approach.

While the programme team was comprised of many discipline experts, we found that issues relating to the protection of passengers' private data were overlooked by the programme. Our passenger interviewees expressed their concerns regarding the EU state's use of their private data, used for eGates inspections, which could be used for other unknown purposes. Our data suggests that a list of factors for evaluation APIMs and other methodological tools could have eased the reliance on the discipline experts in the programme.

Our data also suggests that tools which assist with the articulation of business requirements and techniques which aid the consultation processes, particularly where stakeholders possess conflicting objectives, could be valuable during the conceptualisation and requirements gathering phases of a programme.

7.5.2 Our Reflections on Methodological Efficacy

Our reflections on methodological efficacy concentrate on the accuracy of the decision for the eGates and the lapsed time taken by the programme to execute their iterative deployment approach.

Our discussions on accuracy should be based upon the eGates deployments' ability to fulfil the main stakeholders' primary objectives; however, these objectives were not documented and were diluted during the programme. The programme was also unable to acquire the relevant data to substantiate whether the selected APIM solution was optimal, in terms of meeting the stated performance objectives. Consequently, our reflections on the methodological accuracy of an iterative deployment approach are founded upon the outcome of the

programme.

We found that the programme's iterative deployment approach resulted in the optimal ABC system being selected; however, the configuration of the technologies resulted in usability design flaws. Our data suggests that these design flaws were an indirect consequence of deploying pilot eGates before the programme team and the usability specialists had completed their task on the configuration of the passenger dialogue with the eGates' components.

The programmes's approach enabled the eGates to be deployed expeditiously, possibly, to counter rising public concern regarding the effectiveness of the state's manual border control operations. Efforts to eradicate some of the identified usability design flaws were curtailed by the programme because there was insufficient funding and time remaining within the minister's imposed deployment deadline.

Additionally, as Interviewee Y stated, *"if the programme team had spent more effort on articulating their business requirements rather than producing technical specifications for the eGates then the suppliers would have had the opportunity to use their expertise to configure the eGates to meet those stated objectives and business requirements"*.

We found that the selection of eGates, using an internationally issued and recognised secure document, i.e. an ePassport, operating in biometric verification mode was preferred by the border control police authority to the biometric identification system operating in biometric identification mode. We found that there were several key considerations which influenced the authority's decision.

The key decision related to the size of the subject population in that there were more passengers with ePassports than passengers who had registered or with the state's biometric identification system. A secondary deciding factor was that the state had invested considerably in issuing ePassports and most of the infrastructure had already been put in place for the border control police authority to electronically inspect passengers' ePassports. The introduction of eGates to allow passengers to carry out self-inspections was an extension to these existing capabilities.

As with many iterative development approaches, it is a problem to decide when the iterations should cease and the implementation deployed into the production environment [34]. Our data suggests that the programme team were close to completing the eGates passenger interaction designs in order to reduce the usability design issues encountered. At that point,

in month 19, there could have been a reasonable argument made by the programme to delay the pilot installation until the usability experts and the manufacturers had completed their interactive design work. Our interviewees confirmed that their work was truncated abruptly because of impending budgetary constraints and the decision was made to install the eGates on a more aggressive timescale.

We conclude that an iterative deployment approach appears to be efficacious when there is a need for the programme to be flexible and responsive to the demands of an evolving application context. Our data suggests that stakeholders, however, need to be able to control the application environment in order to allow different APIMs and their configurations to be evaluated in a live production environment.

7.6 Cross-Case Analysis of Programmes' Approaches

This section compares the methodological learnings from our two retrospective case studies in order to develop our initial theories on methodological efficacy for selecting APIMs.

Our most important finding in our two case study data sets is that neither programme assessed whether the APIM that had been deployed actually fulfilled the respective stakeholders' objectives. Our data sets also suggest that an APIM needs to be evaluated in terms of its ability to fulfil stakeholders' objectives in order to demonstrate that the investments in the programme and the APIM deployed have been worthwhile.

We also found that neither programme used a systematic methodology, and relied on discipline experts to select and configure the APIM. Nevertheless, our interviewees, some of whom were discipline experts, conceded that there is a need for methodological tools to assist in the complex processes of selecting and configuring an APIM. The need for methodological tools, such as a DSS, concurs with the IdM experts' views reported in Royer's research [257].

We also found that both programmes spent more effort on articulating technological specifications of solutions rather than establishing stakeholders' objectives and business requirements for an APIM. An iterative deployment approach appears to be methodologically advantageous when the programme needs flexibility and agility to respond to an evolving application context.

The eGates Programme was able to control the eGates operating environment to examine the technologies; however, some programmes may not be afforded such opportunities to repeatedly test their APIM designs. The eID Card Programme's approach, which concentrated initially on the distribution of eID cards to its citizens, had to develop new technologies and enhance existing technologies to enable the eID card to function in the intended application context.

While the two programmes' approaches differed significantly, we found that both programmes encountered difficulties in encouraging their intended subject communities to use the respective APIM. The data from both our case studies revealed that there was low utilisation of the respective APIMs. A plausible explanation for these low utilisations could lie in the inability of the programmes to convey the benefits of their respective APIMs, and the advantages of the underling services, to their user communities.

An alternative plausible explanation for the low utilisations is that both programmes failed to adequately consult with the respective user communities on their requirements for the APIM. Designs and specifications for the respective APIMs were produced or the APIM was deployed without the programmes engaging with the respective user communities. We found that usability design flaws also have a significant influence on users' willingness to use new APIMs.

The methodological learnings identified in the data from our two case studies are summarised in the following list:

- Proactively manage stakeholder consultation processes;
- Determine the benefits of an APIM to stakeholders, including the user community;
- Reconcile stakeholders' objectives and commitments;
- Improve the production of business requirements;
- Track the programme's progress;
- Use a factor check list for evaluating APIMs;
- Investigate programme assumptions;
- Anticipate evolving subject attitudes;
- Define tests and testing methods during the conceptualisation phase of a programme;

- Validate proposed technologies in the application context, where opportunities permit;
- Define the purposes of each deployment phase; and
- Engage a multi-disciplinary team.

These methodological learnings, based on current practices, suggests our supposition that a systematic methodology may be efficacious in selecting the optimal APIM in circumstances which differ to those conditions surrounding the programmes in our two retrospective case studies.

7.7 Conclusions from the Case Study

In this section we describe our conclusions of our efforts to validate our factors for evaluating APIMs. From our qualitative analysis of our case study data sets we have identified several methodological learnings which may be incorporated into a systematic methodology to select an APIM for a given application context.

7.7.1 Efforts to Validate Our Factors

Our conclusions from this case study are that our identified factors have been validated with a few exceptions. Further validations of these factors, however, are dependent upon gaining access to the relevant data and the generation of the relevant data.

We have validated our factors using data from case studies which we have classified as being of heterogeneous and federated identification types. We believe that the use of our factors, embedded in our systematic methodology, applied to a real-world application context, provides a better opportunity to support our efforts to further validate our factors.

7.7.2 Methodological Efficacy

We conclude that an iterative deployment approach is efficacious for programmes to select the optimal APIM when there are demands to introduce the APIM rapidly and the objectives and requirements for an APIM have not be articulated.

The absence of documented stakeholders' objectives and business requirements, however, hampers assessments to determine an APIM's *fitness* for its intended purpose in the application context. Importantly, we discovered that stakeholders' political and commercial motives, not expressed in the form of objectives, impact the decisions relating to the configuration of an APIM's deployment.

From our cross-case analysis of our findings, we consider that sufficient methodological learnings have been identified in our two data sets to support our exploration into the efficacy of a systematic methodology as an alternative approach to select APIMs. In the next chapter, we describe our efforts to validate our methodology and our assessment of its efficacy by gathering data from its use to select the optimal APIM in a real-world application context.

CHAPTER 8

Assessing the Efficacy of the ASMSA Methodology

Contents

This chapter describes our efforts to assess the efficacy of the ASMSA Methodology. We begin by developing criteria to assess the efficacy of a methodology to select an APIM. We then describe the Corporation X's Two Factor Authentication (2FA) Project in which we used the ASMSA Methodology and also the data acquired in this case study. We describe and discuss the results of our efforts to validate the ASMSA Methodology's components, including its factors, using data from this case study. For our main unit of analysis, we then assess the efficacy of the ASMSA Methodology, as a systematic methodology, using our proposed efficacy criteria and the data acquired in this case study. We identify patterns of methodological efficacy from our cross-case analysis of our three case study data sets. From the patterns identified, we develop our initial theory on the efficacy of methodologies to select an APIM. Finally, we draw conclusions on our two units of analysis from this case study.

8.1 Criteria to Assess the Efficacy of a Methodology

This section describes the development of assessment criteria in order to assess the efficacy of methodologies to select the optimal APIM for a given application context. The criteria established in this section address our third research question relating to how the efficacy of a methodology to select an APIM itself be assessed. We describe the criteria at this juncture

so that our assessment of ASMSA's efficacy from its inaugural use in Corporation X's 2FA Project and the results of our assessment, described Section 8.6, may be understood.

Given the alternative ways to select an APIM for an application context, there is a need to establish criteria in order to assess the efficacy of different methodologies or approaches to select APIMs. In particular, while we have established the ASMSA Methodology as a systematic way to select an APIM for an application context, we need to validate the methodology and, importantly, assess the extent of its efficacy to select the optimal APIM. We believe that an assessment of a methodology's efficacy to select an APIM is not valid unless there are criteria established upon which to conduct such assessments. Equally, the relevant data needs to be gathered in order to assess the methodology's efficacy against such established criteria.

The results from these efficacy assessments may then indicate as to when a particular type of methodology could be more efficacious than other approaches based upon the circumstances surrounding the application context. Decision authorities and their programmes may then benefit by possessing knowledge on the proficiencies and limitations of different methodologies to enable them to pursue a particular approach for their application context.

From our review of the literature on decision-making methods [173, 294, 77, 316], we considered that Lai and Hwang's criteria [179], designed for assessing fuzzy decision-making methods, provided a suitable foundation upon which to develop our criteria to address our third research question. Their criteria involve the following considerations:

- the method's execution time;
- the size of the considered problem;
- the accuracy of the selected solution with respect to optimal decision variables and/or objective function and constraints;
- the method's simplicity of use;
- the simplicity of computer program to execute the method's algorithm; and
- the method's applicability to real-world (large-scale) problems.

Lai and Hwang's six criteria for assessing the efficacy of decision methods formed the basis of our efforts to develop criteria for assessing methodologies for selecting an APIM, in order

to address our third research question. We believe that the nature of the selection problem to select an APIM is complex, particularly as it involves many factors and stakeholders with differing perspectives. We adapt Lai and Hwang's criteria [179] for assessing the efficacy of our methodology in an assessment model founded on Jayaratna's Normative Information Model-based Systems Analysis and Design (NIMSAD) Framework [165]. We describe and explain our reasons for using Jayaratna's (NIMSAD) Framework [165] later in Section 8.1.7.

We now develop our criteria for assessing a methodology's efficacy to select the optimal APIM based upon Lai and Hwang's criteria [179].

8.1.1 Methodology's Execution Effort

We interpret execution time not as the elapsed time for using the method for the selecting the APIM but the actual endeavour expended in using the methodology.

Data relating to effort expended by individuals in a programme, in carrying out the methodology's tasks, needs to be gathered during the life time of the programme and possibly post-deployment of the APIM. Historical data contained in project plans and contractor's time-sheets and other similar sources may provide the means to quantify effort expended. It may be difficult on occasions, however, to differentiate between employees' effort involved in using a methodology and their core activities of their job functions, e.g. performing risk assessments.

In summary, we propose that a methodology's execution effort is assessed by measuring the man-day resources in a programme or project to introduce or revise an APIM using that methodology.

8.1.2 Size of Application Context's Problem

We interpret this criterion to assess the application context's problem in terms of its size, both dimensionality and proportionality.

We define proportionality for our purposes as the extent to which the selection of the APIM impacts the stakeholders' assets and resources, either favourably or deleteriously. Dimensionality is defined as relating to the number of different types of stakeholders and the complexity of their relationships involved in the application context.

We propose a classification, based upon calibrated estimations as defined by Hubbard [136], in order to assess the size, in terms of dimensionality and proportionality, of the methodology in relation to application context's problem. We use qualitative indicators because of the complexities of measuring intangible impacts upon organisations with precision.

In summary, the proportionality of the application context's problem is assessed in terms of whether the impact is 'minimal', 'moderate ' or 'significant' to the direct or indirect stakeholders. The dimensionality of the application context's problem is assessed in terms of whether the relationships between the stakeholders are 'simple', 'average' or 'complicated'.

8.1.3 Accuracy of Methodology's Selection

Our criterion to assess the accuracy of a methodology to select the APIM differs depending upon whether the assessment is for theoretical purposes or alternatively for practical reasons to assist decision-makers in choosing the appropriate selection methodology.

Avison and Fitzgerald contend [18] that the practical problems of creating exactly the same environment in an organisation to compare information systems developed by different methodologies are insurmountable. They argue that, in practice, there is a lack of ability to demonstrate methodological repeatability and also highlight the difficulty in the reproducibility of results. They argue that the tighter, more specific the methodology, the more reproducible are the results, particularly if the methodology specifies the exact techniques and tools to be employed under each circumstance.

We consider that their arguments apply equally to employing two methodologies in parallel for selecting the optimal APIM for a given application context. Therefore, for assessing methodological accuracy, we propose the use of key decision variables for theoretical comparison tests of methodological accuracy. For conducting real-world comparisons, we propose that the efficacy of the methodology is determined by assessing the uncertainties surrounding an application context and also the characteristics of a methodology.

Theoretical Accuracy For the purposes of comparing the theoretical accuracy of methodologies we propose that an assessment should use key decision variables relating to annual loss expectancy, financial impact on productivity, financial impact on regulatory compliance, and financial impact of changes in utilisation.

The assessment is conducted by comparing the financial implications to stakeholders of each methodology using a test scenario case where a current state is to be transformed to a desired state. We consider, however, that comparing the degree of closeness of measurements of a quantitative result to an object's actual true value is not apposite for our purposes.

Mont et al.'s analysis [207] of organisation decision-makers' concerns identified the following core strategic outcomes of relevance in the identification and authentication space:

- security risks with metrics from data breaches and incidents;
- productivity impacts with metrics from correctly granting access rights;
- compliance to regulations with metrics from audit failures; and
- costs incurred with metrics from fixed and operational budgets.

The introduction of an APIM or the revision of a deployed APIM may impact stakeholders' security risks, productivity, and ability to comply with regulation. All of our proposed variables are measured quantitatively in financial terms using calibrated estimations [136].

The impact of a subject's privacy being compromised and the possible emotional stress, however, cannot be measured in pure financial terms [35]. Some subjects may avoid or refuse to use an APIM in a particular application context. The costs associated with users opting to use other services, e.g. loss of customers' business, may be calculated in financial terms. Conversely, users may be attracted to use a service because the APIM's level of assurance has been enhanced. We propose, therefore, to include utilisation with Mont et al.'s key outcomes for measuring Theoretical Accuracy (TA) of a selection methodology.

Based upon the assumption that each methodology selects a different APIM for the test scenario case we calculate the theoretical accuracy of a selection methodology using the following formula:

TA = STATEwithoutINVESTMENTinAPIM –

(STATEwithINVESTMENTinAPIM + CostsOfINVESTMENTinAPIM)

Where STATE includes the addition of key decision variables consisting of:

1. Annual Loss Expectancy (ALE);

2. Financial Impact on Productivity (FIP);
3. Financial Impact on Regulatory Compliance (FIRC); and
4. Financial Impact on Changes in Utilisation (FICU).

We define the variable utilisation as the financial impact of a subject's change of usage of the related information system. This utilisation variable, however, may not always be relevant to all test case scenarios because the test may include an assumption that users do not have the freedom to avoid the use of the APIM.

We propose that theoretical accuracy is measured by comparing different methodologies' values, using our proposed formula, based on extrapolating the financial estimations in the key decision variables. The methodology with the highest value is deemed to be the most accurate, theoretically, for selecting the APIM. The investment in an APIM selected by a methodology may bring positive or negative impacts to these key decision variables. Theoretically, it is possible that different methodologies select the same APIM; however, the comparison of the key decision variables should help to identify inconsistencies and also help to validate the hypothetical calibrated estimations.

Real-world Accuracy According to Jaquith [164] security return on investment calculations, based upon the inaccuracies and assumptions of ALEs, are inadequate for practical usage.

While there may be many strategic decision-makers in an organisation, possibly with different priorities, decisions within an organisation are often made by empowered committees or decision authorities, on behalf of the organisation's executive or board of directors. Similarly, where there are several stakeholders involved in a programme, a steering committee, consisting of empowered representatives, is often mandated to make decisions in respect of the appropriate development methodology for the application context. We assume, therefore, that decision-makers seek appropriate methodologies which provide the required accuracy by assessing the circumstances surrounding the application context.

Jayaratna and Holt advocate [166] that selection criteria for methodologies should include the consideration of the methodology user, the available time, the client, the human resources, the financial resources, and the culture of an organisation together with the characteristics of the methodology as a problem solving process.

Property	Criteria to Assess an Application Context's Situation
1. Programme's Objectives	Are the programme's objectives vague, not agreed, considered unrealistic and have not been formulated or set?
2. Problem Definition	Are the problems in the application context well understood and are the causes well appreciated?
3. Attitudes	Are the stakeholders' attitudes uncooperative and non-flexible?
4. Boundary Conditions	Are the boundary conditions for the application context vague, which includes the description of the application context and the subject community?
5. Communications	How reliable and effective are the communications between the stakeholders?
6. Relationships	How complex and political are the relationships between the stakeholders?

Table 8.1: Criteria to Assess an Application Context's Situation [165]

Property	Criteria to Assess the Characteristics of a Methodology
1. Repeatability	Is the methodology documented so that its processes are repeatable by evaluators?
2. Granularity	Are the stages and tasks in the methodology well-defined and specific so that it is capable of reproducible results or are the descriptions of the methodology's tasks vague?
3. Outputs	What are the outputs of the methodology during its decision processes?
4. Control and Productivity	To what extent does the use of the methodology improve programme control and productivity in producing decision process outputs?
5. Tools	Does the methodology include tools and tool sets with educational material for the evaluator?

Table 8.2: Criteria to Assess the Characteristics of a Methodology based on Avison and Fitzgerald's Recommendations [18]

We adopt Jayaratna's selection criteria [165] on ill-structured situations, as shown in Table 8.1, to assess the circumstances surrounding an application context. We also used criteria based on Avison and Fitzgerald's methodological recommendations [18], as shown in Table 8.2, to assess the characteristics of a methodology to select an APIM.

8.1.4 Methodological Simplicity

We interpret the simplicity of using a methodology to select an APIM for a given application context in terms of the knowledge and the skills necessary for the competent use of the methodology.

We define *methodological simplicity* for our efficacy assessment as the ease of learning a new methodology by a competent practitioner or group of practitioners. We assume that discipline practitioners would be involved in using such a methodology rather than non-experts who may possess knowledge about the application context. This learning criterion includes the processes to develop a practitioner's competency to use the methodology through training and the provision of educational materials.

We propose to assess methodological simplicity by eliciting practitioner's views in respect of effort involved to learn and use the methodology. Practitioner feedback containing various data types that is unstructured suggests a qualitative indicator is more relevant for this efficacy criterion.

Therefore, we propose to elicit feedback from practitioners using the classification of 'intuitive', 'tolerable', and 'arduous' to gauge a methodology's simplicity.

8.1.5 Executable as a Computer Program

We interpret this criterion to mean whether a methodology to select an APIM can be implemented as a computer program, to execute its processes and algorithms, and the effort required to learn to use the computer program. We assume that methodological processes which are expressed in the form of a computer program offer more structure and methodological rigour than a paper oriented approach. A paper oriented approach relies upon human involvement to ensure that the methodological processes contained in a document are executed.

Some methodologies and some of their processes may not translate easily into a computer program, particularly the processes for acquiring the data from the application context. Similarly, processes used by discipline experts may not translate easily into an application program.

Turban and Watson advise [294] that expert systems are designed to mimic human experts and are used to:

- give advice on complicated, specialised issues;
- teach or train the non-expert;
- provide timely consultation or offer second opinion; and
- explain how a conclusion is reached or why additional information is needed.

While the difficulty and the effort to build a computer application program which mirrors a methodology may be significant, we propose that this criterion is based upon the degree to which the methodology's computations and processes can be automated in a program.

We exclude data input processes because we assume that the entry of subject data into the program would involve some form of human intervention.

In summary, we propose two forms of measurement for this assessment criterion. The number of executable processes in a computer program representing a methodology is expressed as a percentage of the methodology's total processes. Also, we propose the classification of 'negligible', 'moderate', and 'significant' to indicate the effort required to learn and use the methodology's computer application program.

8.1.6 Capability of Methodology to Address Real-World Problems

We interpret this criterion to assess the extent to which a methodology to select an APIM is capable of being applied to real-world automated personal identification problems.

We define *capability* as the ability to use the methodology, with its actions and processes, in order to achieve certain actions or outcomes through a set of controllable and measurable faculties, features, functions, processes, or services applied within the limits of the application context. The question of application to real-world problems also highlights the issue of accountability of evidence-based decision-making versus the reliance, possibly full dependency, of expert practitioners' recommendations.

The breadth and depth of analysis in theoretical research may not always provide sufficient evidence concerning a methodology's practical use in a real-world application context. Empirical validation, however, helps to give an indication of the *credibility* of research behind the methodology and its capability of being applied to real-world problems.

We believe that the capability of a methodology for use in the real-world should be based upon practitioners' feedback from using the methodology. The inaugural use of the ASMSA Methodology in the Corporation X Case Study enabled us to generate relevant empirical data in respect of its applicability to address a large-scale, real-world problem.

For this criterion, we propose that the degree of a methodology's capability of being applied to a real-world automated personal identification problem, is to be based on the methodology's proficiency classification of 'ineffective', 'acceptable', and 'effective' to produce an APIM selection outcome.

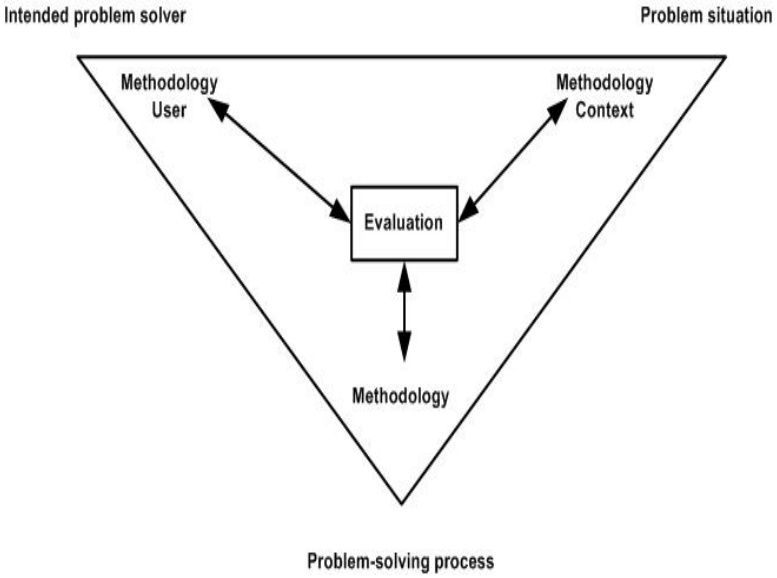

Figure 8.1: Jayaratna's NIMSAD Methodology Evaluation Framework [165]

8.1.7 A Framework for Assessing the Efficacy of a Methodology

We propose to use our six criteria to assess the efficacy of a methodology, to select the optimal APIM for a given context, within Jayaratna's NIMSAD Framework.

Jayaratna explains [165] that the role of methodologies is to offer different ways, through their philosophy, structure, steps, and ways of performing the steps, of undertaking processes in order to achieve an aim. We use Jayaratna's NIMSAD Framework, shown in Figure 8.1, representing the *problem situation*, the *intended problem solver*, and the *problem solving process* elements as our framework to assess the efficacy of a methodology to select the optimal APIM using our proposed efficacy criteria. We use Jayaratna's NIMSAD Framework to concentrate our efforts to assess the efficacy of our methodology, as a problem solving process, in various application contexts rather than assessing the capabilities of the problem solver. We assume that problem solvers are expert practitioners in this discipline with varying knowledge and competencies; however, the impact of the problem solver, as a variable, needs to be accommodated, as Fléchais et al. acknowledge [102], in a methodological assessment.

We justify our adoption of Jayaratna's NIMSAD Framework as our model to assess the efficacy of our methodology because we were unable to locate models in the literature which evaluated the utility of different classes of methodologies on a generic basis. We believe

that Jayaratna's seminal work [165], which focuses on the assessment of information system development methodologies, is sufficiently generic to be used as a model to assess the efficacy of our methodology. His work on assessing methodologies is highly cited and the principles of NIMSAD appear in a variety of text books on the evaluation of information system development methodologies, e.g. Avison and Fitzgerald [18].

Data for conducting efficacy assessment, based on our proposed criteria, need to be acquired during the use of the methodology. Efficacy assessments, using these acquired data may then be assessed by applying the efficacy criteria after the use of the methodology (and possibly the deployment of the APIM). A post-deployment methodological efficacy assessment may present little practical value to stakeholders' decision authorities because it may not be possible for stakeholders to reverse decisions made on an APIM deployment easily. In practice the assessment of a candidate methodology or approach may be more beneficial to decision-makers **before** the programme commences or possibly **during** a programme. A post-deployment methodological efficacy assessment may help to researchers to identify methodological learnings.

We used the ASMSA Methodology in the Corporation X Case Study in order to generate empirical data to assess its validity and to assess the extent of its efficacy for selecting an APIM in a real-world enterprise application context. We also aimed to identify those circumstances as to when a systematic methodology may be efficacious. We describe the results of our case study research and our assessment of the ASMSA Methodology's efficacy in the succeeding sections of this chapter.

8.2 Background on the Corporation X 2FA Project

This section describes the background of this project without revealing details about Corporation X, supplier organisations or individuals involved in the research. This section builds upon the information provided in Section 4.3.3.

We anonymise the subjects and the organisation in order to protect their interests, in accordance with a non-disclosure agreement established between Corporation X and us dated 1st October 2010. Therefore, we provide a general description about subjects and objects rather than specific names. We are also unable to provide output reports containing information about Corporation X and its operations which were generated while using the ASMSA

Methodology. Our case study period commences at the inception of the project in September 2010 until April 2013.

8.2.1 Objectives of Corporation X's 2FA Project

The main business objective for Corporation X to commence this project was to seek options to deploy a 2FA APIM originated from the need to comply with the financial regulatory authorities' security requirements on the protection of on-line financial transactions.

Corporation X's Group Head Office (GHO) had formulated a policy to deploy smart cards across all Corporation X's worldwide businesses in order to meet financial regulatory authorities' security requirements for 2FA. The DoR for the Asia Region was of the opinion that this policy and the smart card 2FA solution was not suitable for many of Corporation X's business entities in Asia.

A secondary objective for the project was that the additional authentication factor should not dilute the effectiveness of the current user factor authentication mechanism. The DoR's aim was not necessarily to improve identity assurance because Corporation X had no evidence to suggest that such risk mitigation improvements were necessary.

8.2.2 Corporation X's Application Context

The 2FA capability was needed to supplement Corporation X's user identifier and password user authentication systems for peripatetic executives, employees and over 400,000 insurance agents. The necessity to introduce 2FA was driven by the financial regulatory authorities in Asia, primarily the Monetary Authority of Singapore (MAS). The regulators had issued (or were imminent) security specifications which mandated the use of two factors for authenticating users' on-line financial transactions.

Corporation X's peripatetic executives, irrespective of their location, required access to commercially sensitive corporate information. Employees, mainly based in local Corporation X office premises, required access to information systems containing details about clients and their policies, insurance products and other corporate resources.

Peripatetic insurance agents required to access Corporation X's information systems in order to submit their insurance policy sales transactions which included their clients' personal

data. Agents also required access to Corporation X's sales work-flow tracking system, which included details about commissions allocated to their sales. These insurance agents were not Corporation X employees but were agents (either independent or employed by brokerage firms) operating in different regions and countries of Asia. Most of these insurance agents were individuals operating as independent sole traders. Some of the agents used Corporation X's sales source automation tool, which incorporated user authentication functionality, using identifiers and passwords.

Corporation X employees attended induction training sessions which included guidance on their responsibilities to comply with the company's security policies. The roles and responsibilities of employees were incorporated into the corporation's standard employment contract. Corporation X's security policies specified how employees were to use and protect their passwords to enable them to access company systems. Employees received regular communications regarding security awareness and reminders about managing their passwords securely. Similar reminders to executives regarding their responsibilities were intermittent.

Agents signed agency agreements with Corporation X which detailed their responsibilities for managing identifiers and passwords to access Corporation X's information systems. Agents, typically, used their own devices, e.g. laptops and mobile phones, to conduct their business service interactions with existing and potential clients and the Corporation X did not wish to change that operating model.

8.2.3 Research Collaboration Protocol

We agreed a project plan with the DoR that used the processes in the ASMSA Selection Method to drive the project's activities. The DoR performed the Multiple Stakeholder Processes (MSPs) technique by managing all the interactions with the three user groups, Corporation X's internal departments in Asia and with London GHO. All our communications with Corporation X were conducted via the DoR in accordance with the terms of the consent agreement.

Our criteria questions, represented in the ASMSA-DSS, were used to acquire data relating to Corporation X's application context and the data describing the requirements for introducing 2FA for its users. The acquired data stored in the ASMSA-DSS were used to generate a Request for Information (RFI) which was sent to five short-listed 2FA supplier companies.

Corporation X opted for a One-time Authentication Code (OTAC) as the second user authentication credential. The code was delivered to the user's mobile device using the SMS. For brevity, we label this 2FA solution as (OTAC-SMS). The user was required to enter their user identifier, their password and the additional OTAC during the interaction sessions with Corporation X's information systems.

We were unable to utilise the ASMSA Methodology in the third stage of our method (to evaluate candidate options) due to unforeseen events, which we explain in Section 8.5.3. We describe the prevailing conditions surrounding the project, the events that occurred during the use of the ASMSA Methodology, the outcomes of Corporation X's 2FA Project, and the DoR's methodological efficacy insights in Section 8.5.4. Next we describe the data that we acquired during the use of the ASMSA Methodology in this case study.

8.3 Data Gathered

The majority of data acquired were gathered using structured and semi-structured interviews with Corporation X's DoR. These data included email exchanges of correspondence with Corporation X's DoR. All interviews were recorded, transcribed by us, and the transcriptions subsequently reviewed by the DoR. Thus the availability of the DoR to participate in these activities was essential to our research in this case study.

We also depended upon his experience as a senior information security practitioner for our research. The DoR had worked in information security, mainly in the finance industry, for nearly 25 years, at various levels from technical systems operation to his then current DoR position, which involved managing information risk across a large Asian organisation with 26 business entities in 13 countries. He outlined his experience: "*So the security work I have done in that time - I've managed technology; I've reviewed technology and implemented technology; I've implemented, written, directed and implemented policy; directed implemented in managed procedures and processes; and managed teams*".

The DoR explained his rationale for using the ASMSA Methodology and engaging with us in our research for his 2FA Project: *" The objective I have is to be able to go back to Group Head Office, who are dictating policy, and say that we have looked at this [problem] and this [our preference] is the position. What I want to have is the ability to be able to demonstrate, in a qualitative and quantitative fashion, that we have taken account of their desires, for two*

factor authentication and we have a defence, that is a document that describes the reasons why in one country you might do it and in another country you might not. That's why I am doing the exercise [using the ASMSA Methodology] with you, to understand objectively rather than subjectively, to provide the evidence behind our decision".

The DoR assumed the responsibility, as part of his job description, to create and to manage Corporation X's2FA Project and also to perform its tasks, with support from some of the staff in his unit.

8.3.1 Interviews

The interviews were either structured interviews conducted face-to-face or semi-structured conducted remotely using the Skype conferencing system.

The first two structured interviews were used in conjunction with the ASMSA-DSS to gather data relating to the application context. We conducted a semi-structured interview that focused upon clarifying the requirements statements for the generation of the RFI document.

In the final part of the case study period, as our prime research objective, we also conducted three semi-structured interviews with the DoR to gather data on his insights on ASMSA's methodological efficacy and its impact upon Corporation X's efforts to select the optimal 2FA mechanism.

We used the ASMSA-DSS to structure and drive the interview dialogue to acquire data relating to the first two stages of the ASMSA Selection Method. We posed the criteria questions to the DoR and the DoR's replies were recorded and transcribed. The transcribed text replies were then assigned to the corresponding factors in the ASMSA-DSS. Reports were generated from the ASMSA-DSS and sent to the DoR for his review. Any amendments or additional information requested by the DoR were added to the data contained in the ASMSA-DSS. The DoR also ensured accuracy, completeness and consistency of the data maintained in the ASMSA-DSS relating to the application context.

The semi-structured interviews also focused on the clarification of utterances made by the DoR in previous interviews or to clarify points contained in email exchanges. Additionally, we used these semi-structured interviews to confirm our progress through the steps of the ASMSA Selection Method and also to agree the interview arrangements to proceed with the next steps of our method. We used semi-structured interviews with the DoR to validate the

factors and the associated criteria questions in Stage 3 of the ASMSA Selection Method.

The DoR, in one of the latter semi-structured interviews, announced that his responsibilities on Corporation X's 2FA Project had changed and the decision to select the 2FA solution would now be managed by the Head of IT Operations (HoITP). This unforeseen event meant that it was necessary to terminate the use of the ASMSA Methodology because the HoITP requested a technology supplier to provide their recommendations on a 2FA selection. Our research, however, did not end at this point because we were able to conduct interviews regarding methodological efficacy after the OTAC-SMS solution had been deployed in an Asian state.

The DoR's activities were curtailed during the latter stages of Corporation X's 2FA Project, after the RFI responses had been gathered from the short-listed 2FA solution suppliers but before the selection of the OTAC-SMS solution. The HoITP, who was now responsible for the 2FA Project, used the RFI produced by the ASMSA-DSS, to engage with discussions with a preferred supplier. This supplier was also in consultation with the HoITP to provide network monitoring capabilities to Corporation X in Asia. The HoITP selected the OTAC-SMS from this supplier and not the original short-listed 2FA suppliers that responded to the RFI.

Despite these unforeseen events, and most important to our research aims, the DoR participated in further interviews to furnish us with his insights on the efficacy of the ASMSA Methodology and the eventual outcomes of Corporation X's 2FA Project.

8.3.2 Documentary Evidence

The security requirements specification from the MAS was the only external item of documentary evidence acquired. We were not given access to Corporation X's information systems or corporate documentation with the exception of their standard RFI template.

Data acquired and reviewed in the first two stages of the ASMSA Selection Method was used to produce Corporation X's RFI document. We extracted data from the ASMSA-DSS which was then inserted into Corporation X's standard RFI template. We are unable to use the information contained in the supplier responses to Corporation X's RFI for our research purposes, although the DoR made all the specialist 2FA supplier responses available to us. These data were excluded from our analysis because we had not gained consent from these suppliers to use their data for our research. As we explain in Section 8.4.1.3, Corporation X

chose not to seek their consent in the covering letter that accompanied the RFI document that was sent to the short-listed 2FA suppliers.

Also, we were not given access, for commercial reasons, to the RFI response documentation from the supplier that was awarded the contract to provide the technologies for OTAC-SMS to Corporation X. The DoR confirmed, however, that all the short-listed 2FA suppliers had provided details of their OTAC-SMS solution in their RFI response as well as other alternatives which included the use of smart cards. The DoR considered that from his evaluation of the short-listed supplier RFI responses he believed that the OTAC-SMS was the optimal 2FA solution for their application context.

8.3.3 Our Observation Memos and Reflective Notes

We produced 20 observation memos from our interview sessions with the DoR. We also generated 15 reflective notes, during our analysis of the data acquired during the interview sessions.

We produced our observation memos immediately after each interview with the DoR and also after changes requested by him following his review of the interview transcripts. These memos helped us to gain an understanding of the DoR's perspective of the tasks involved in selecting a 2FA mechanism. It also enabled us to gain an understanding of his attitude towards using a systematic methodology for assisting with the decision processes.

We also produced 15 reflective notes during the quantitative analysis of our data. Our analysis included comparisons of the key statements made by the DoR in the interview transcripts and the documentary data contained in his email exchanges. These reflective notes were created and stored within the Atlas.ti application program.

8.3.4 Reports Generated

We generated several reports, using the acquired data contained in the ASMSA-DSS, for the DoR during the case study. The RFI document was sent to several potential technology suppliers with identity management product offerings.

From the data acquired we generated a report from the ASMSA-DSS which described Corporation X's objectives and requirements for a second factor authentication mechanism.

A second report was generated that showed the reconciliation of Corporation X's objectives with their stated requirements. All these reports were reviewed by the DoR in terms of their completeness, accuracy and consistency. Commercially sensitive information, e.g. Corporation X's budget, was removed from the RFI by the DoR.

8.4 Validation of the ASMSA Methodology and its Components

This section describes the results, at Stage 12 of the research implementation plan, as represented in Figure 4.3 on page 124, of our efforts to validate the ASMSA Methodology consisting of its selection method and its factors for evaluating APIMs, associated criteria questions and factor explanations.

Stage 12 represents the final step in our research implementation plan to validate the ASMSA Methodology and to assess its efficacy by using data acquired from using it in a real-world case study. Our efforts to assess the efficacy of the ASMSA Methodology using the data acquired from the Corporation X 2FA Project Case Study and our efficacy criteria established in Section 8.1 are described in Section 8.6.

8.4.1 Validation of the ASMSA Selection Method

We followed the systematic processes in the ASMSA Selection Method, as described in Section 5.6, to acquire data from the application context for all three perspectives in the ASMSA Evaluation Framework. We used the criteria questions in our structured interviews with the DoR to acquire subject data for each factor.

From the agreed interview transcripts, the data acquired using the criteria questions were inserted against the respective factors into the ASMSA-DSS's database. At the end of each stage of the method, we produced a summary report for the DoR to review which showed his verbal responses to the respective criteria questions. Following his review of the report the data in the ASMSA-DSS were amended accordingly.

We used this cyclical data acquisition and validation processes with the DoR in all three stages of our method.

8.4.1.1 ASMSA Selection Method Stage 1

The first structured interview session concentrated acquiring subject data for the factors relating to the Understanding Perspective.

We then conducted a second interview with the DoR to ascertain the objectives for the revision to Corporation X's user authentication mechanism. Data on the objectives were inserted into the ASMSA-DSS's database.

8.4.1.2 ASMSA Selection Method Stage 2

In the next interview session we used the criteria questions to ascertain Corporation X's requirements for the second factor authentication mechanism.

A report showing the DoR responses to the criteria questions in the Effectiveness Perspective was reviewed by the DoR to review and the ASMSA-DSS's database was subsequently updated.

The next interview with the DoR concentrated on reconciling the stipulated requirements to the articulated objectives for the APIM. Again we used the ASMSA-DSS to assist us with this task involving the DoR. At this juncture we had now completed the first two stages of the ASMSA Selection Method. The DoR requested us to extract data from the ASMSA-DSS's database and insert that data into Corporation X's standard RFI template in order to produce a RFI document. This document sought 2FA product information and indicative pricing from several specialist suppliers in Asia.

8.4.1.3 Suppliers' Responses to Corporation X's RFI

The covering letter that accompanied the RFI document did not seek to gain consent from these suppliers in respect of using their responses for our research purposes. This omission was not erroneous. Corporation X considered that it would be unsuitable to put such a request into their covering letter because the DoR was of the opinion that the suppliers would not respond in a meaningful manner or at all.

The DoR furnished us with four supplier RFI responses. The absence of a supplier's consent, however, meant that the data contained in the RFI response correspondence could not be

used by us to validate the factors in ASMSA's Efficiency Perspective. We describe how we overcame this problem in Section 8.4.1.5.

8.4.1.4 Corporation X's HoITP's Initiative

During the period while Corporation X was waiting for the suppliers' responses Corporation X's HoITP in Asia also handed the RFI to another supplier. This supplier was in discussions with Corporation X to supply network infrastructure monitoring services to its Asian businesses.

Corporation X's HoITP decided to select a one-time authentication code, delivered by short messaging service, (OTAC-SMS) 2FA solution from this network infrastructure supplier rather than the solutions proposed by the short-listed suppliers. It should be noted that three of the short-listed suppliers had OTAC-SMS solution offerings described in their RFI responses.

That supplier's OTAC-SMS solution was piloted by Corporation X in Singapore for around 6 to 9 months and there were no significant issues encountered with this deployment, according to the DoR.

8.4.1.5 ASMSA Selection Method Stage 3

The DoR agreed to take part in a further structured interview to validate the factors in the Efficiency Perspective based on his knowledge of Corporation X's OTAC-SMS deployment.

In this interview he agreed to confirm the relevance of the criteria questions in ASMSA's Efficiency Perspective to the 2FA solution that was deployed in Singapore. He was only able to provide brief statements as he was restricted, claiming commercial sensitivities, from providing much of the detail relating to the 2FA deployment. The main omissions related to specific details surrounding security testing and identity assurance results and also the precise costs of selected solution.

We then produced a final report detailing the DoR's responses for all of ASMSA's perspectives for the DoR to review. Following final amendments, we used these data to conduct our validation of our factors for evaluating APIMs.

In conclusion, we had utilised the ASMSA Methodology with the DoR in order to select the optimal 2FA solution for Corporation X's application context. Despite the fact that we were unable to use data provided by the suppliers in order to compare the attributes of different solutions to the stipulated requirements, we nevertheless were able to validate our method's systematic processes.

We acknowledge that the ASMSA Selection Method needs to be further validated with different application contexts, possibly using alternative research methodologies. We consider that the ASMSA Selection Method does not require enhancement at this stage of our research because its usage was incomplete in our case study. We believe that it would be unwise to enhance the ASMSA Selection Method based upon our validation from its incomplete inaugural use in a real-world application context. Therefore, we refrain from amending any of ASMSA Selection Method's processes until we have acquired additional relevant empirical data from using our methodology in other application contexts.

8.4.2 Discussion on Factors Validation Assessment Results

Despite the absence of documentary evidence, we were able to validate nearly all our identified factors, i.e. 99%, using the interview data acquired in this case study. Table 8.3 shows the number of factors for evaluation as at Stage 9 of our research implementation plan, at the top of the table, and the status of the factors and criteria questions post case study as at Stage 12, at the foot of the table.

We also identified 21 new factors in this case study data. Some factors were merged resulting in an overall reduction of nine factors. Our results also show that 33 factors, about 14%, required their label to be more descriptive, which is a significant reduction from 35% as we found in the results of our factor validation effort using the data from the eGates Case Study. Also, there was a significant decrease in the need to revise the criteria questions.

The results of our efforts to validate our identified factors are detailed in the next three sub-sections.

8.4.2.1 Factor Identifier Labels

We found that 33 out of our 234 factors, i.e. 14%, required their factor label to be more descriptive. Our results also show that at least 26% of our criteria questions still required

Factors For Evaluating APIMs	**Understanding Perspective**	**Effectiveness Perspective**	**Efficiency Perspective**	**Row Totals**
Pre-Case Study Stage 9 Evaluation Themes	**60 factors 7 factor themes**	**70 factors 9 factor themes**	**104 factors 9 factor themes**	**234 factors 25 factor themes**
Grounded Factors	66 (98%)	76 (99%)	101 (99%)	**243 (99%)**
Deduced Factors	0 (0%)	0 (0%)	0 (0%)	**0 (0%)**
Not-grounded Factors	1 (2%)	1(1%)	1 (1%)	**3 (1%)**
Relabelled Factors	17	10	6	**33**
Revised Criteria Questions	22	15	25	**62**
Deleted Factors	4	0	5	**9**
New Factors Identified	11	7	3	**21**
Factor Explanations Revisions	26	14	24	**64**
Factor Theme Name Change	0	0	1	**1**
Post Case Study Status of Factors Evaluation Themes	**67 factors 7 factor themes**	**77 factors 9 factor themes**	**102 factors 9 factor themes**	**246 factors 25 factor themes**

Table 8.3: Factor Validation Results using the Corporation X's 2FA Project Case Study Data

further enhancement. Our first result is broken down into 7%, 4%, and 3% for the Understanding, Effectiveness and Efficiency Perspectives respectively. The second result is broken down into 10%, 6%, and 10% respectively.

The first result shows that the factors description labels are more accurate according to the depth of granularity of the data related to the factor. This trend falls in line with the results of our eGates validation efforts. We describe other patterns in our results from our cross-case analysis of our evaluation efforts in Section 8.4.3.

Our second result shows a significant reduction in the number of criteria questions that needed refinement. The results from our validation efforts show that the number of criteria questions requiring revisions were similar across our evaluation framework's perspectives. We were unable to recognise patterns in the factor explanation revisions across our framework's perspectives.

The reduction of factor labels and criteria questions revisions can be explained by the fact that we have only included those factor labels, criteria questions and factor explanations where there is a material change required rather than cosmetic or grammatical improvement as in our previous validation efforts. Also these reductions in revisions may be explained by our efforts to refine factors and criteria question during each validation iteration.

The DoR encountered difficulties in acquiring data for some of the criteria questions because the criteria questions, as phrased, did not appear to be relevant to the application context. The DoR suggested that the criteria questions could be better structured by using a concise leading question which is then supplemented with subordinate criteria questions rather than posing long and complex questions. He suggested that *"this structuring could assist in overcoming the narrowness of some of the criteria questions and it would also help to improve the alignment to the factor label and also the factor explanation"*.

Additionally, the DoR commented that the terminology of some factor labels still needed improvement to aid clarity, which should then improve the understanding of their relevancy to the application context.

8.4.2.2 Relevancy of Our Factors

The high availability of relevant data in this case study enabled us to directly ground 99% of our identified factors. All factors were grounded in the data as relevant except three factors,

one in each perspective. The DoR's direct response to each criterion question also enabled us to avoid the need for us to use our own interpretations and deductions to validate a factor's existence in our data.

The factors identified in the literature which were Not-grounded in this case study data are:

1. Subject Duress Policy factor (A.17.8.) in the Policies Evaluation Theme (see Table F.7 in Appendix F);
2. Privacy Controls Erosion factor (A.8.10.) in the Privacy Compliance Evaluation Theme (see Table F.9 in Appendix F); and
3. Device Calibration factor (A.16.14.) in the Manageability Evaluation Theme (see Table F.21 in Appendix F).

We comment on these three remaining factors and the impact of the data gathering method on our results in Section 8.4.3.

These results show that the increased availability of the relevant data improved our validation efforts to ground the factors. Conducting our research using an individual who was directly involved in a project enabled us to acquire a richer set of relevant data for the validation of our factors.

8.4.2.3 Consistency of Our Factors

We found that the introduction of factor explanations assisted in the identification of inconsistencies amongst our factor labels, and criteria questions and also between the factors themselves.

Our results indicate that the factor explanations themselves also required refinement so as to better align with the descriptive label of the factor and the associated criteria questions. Generally, we found that we needed to improve the factor explanations on the same criteria questions because the criteria question was often not adequately posed to acquire the relevant data relating to its corresponding factor.

We also found during our validation effort that some of our factors needed to be merged. This meant that the merged factors then required new generalised factor labels, criteria questions

and factor explanations to be created. For example, the merging of whether the data upon which a user may be authenticated may use knowledge data, biometric data, data generated by an artefact, or a combination of these elements. For the purposes of evaluation, these data can be represented by a single factor entitled 'Subject Signal Data' (A.12.8.) which is located in the Security Architecture Evaluation Theme, as shown in Table F.17 of Appendix F.

The need to revise the title of only one evaluation theme from 'Technology' to 'Manageability' suggests that our evaluation themes are consistent in relation to the ASMSA Evaluation Framework and also align with the data acquired from our case studies.

8.4.2.4 Completeness of Our Factors

From our validation assessment we identified 21 new factors, which were mainly in the Understanding Perspective.

Our results suggest that the improvement gaining access to the relevant data in this case study to data acquired in the eID Card Case Study played an important part in our efforts to identify new evaluation criteria. We consider, however, that we have not reached the saturation point where we could claim that the factors for evaluation are in any way complete. Indeed, our results suggest that further factors for evaluation may be found using a participative research methodology, such as the action research methodology, in other application contexts. Additionally, a range of application contexts with different types of automated identification problems may also reveal further factors for evaluation.

The deletions that are shown in Table 8.3 were due to the merging of factors rather than the deletion of the factor for relevancy reasons. The DoR suggested that the ASMSA Methodology, and the ASMSA-DSS, should allow for supplemental factors to be added to the evaluation in order to provide flexibility in the evaluation of the application context to accommodate different types of organisations and cultures.

We conclude that it may be difficult to determine whether the factors for evaluating APIMs could ever be complete. We believe, however, that through our efforts to validate the factors using data from our case studies we have established an adequate set of factors, classified into evaluation themes, in an evaluation framework to enable the inaugural use of the ASMSA Methodology for evaluating an APIM to be applied in a real-world application context.

8.4.3 Patterns Recognised in Our Factor Validation Efforts

Our cross-case analysis of our efforts to validate our identified factors shows that there has been a progressive improvement in our results.

As can be seen in Table 8.3 there was a significant improvement in the number of factors validated using the data from this case study. There was, however, only slight improvement in validation between the initial validation using the eID Card Case Study data and the second validation using the eGates Case Study data.

The Duress Policy factor was the only factor identified in our review of the literature which was Not-grounded in the data in any of the three case studies. We acknowledge that a duress policy for an application context may rarely be necessary for an APIM. These results also suggest that the data gathering method was a key factor in acquiring a comprehensive data set upon which to validate the factors. The eID Card Case Study and the eGates Case Study used data that were acquired and used retrospectively. In this case study the factors contained in the ASMSA-DSS were used as a check list by the DoR. He conceded that *"I've evaluated many more factors than I would have done without such a list*".

The use of the ASMSA Methodology in this case study helped the DoR to focus on articulating the objectives for the APIM and also setting the measurements for assessing the effectiveness and efficiency of proposed candidate APIMs. These elements formed the majority of the new 21 factors identified in this case study.

Our results demonstrate that the use of the ASMSA-DSS as a tool, in a participative approach, to gather the relevant data to validate the factors has been far more productive than our attempts to validate the factors using data from retrospective case studies. We consider that the improvements in our validation efforts were probably a combined effect of the improved method to acquire the necessary data and also the employment of the ASMSA Methodology in this case study.

We conclude that further factors for evaluation may be identified by using our methodology in other application contexts.

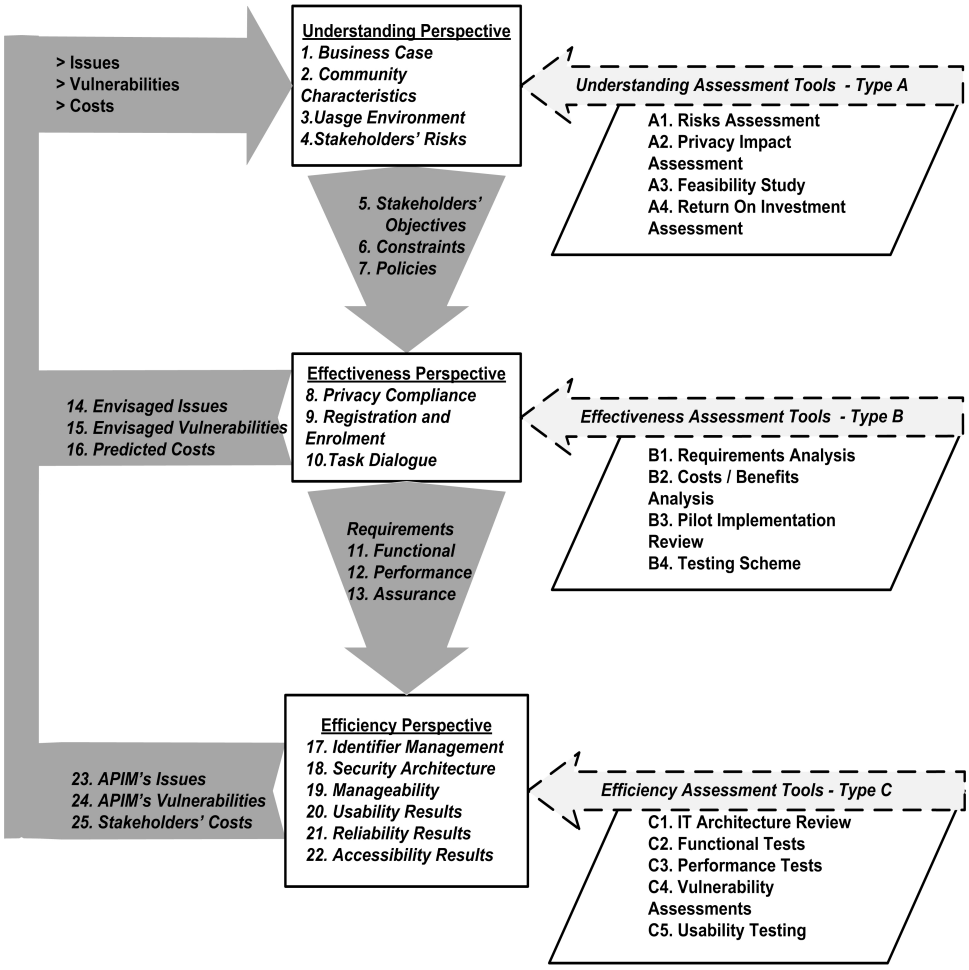

Figure 8.2: Our Revised ASMSA Evaluation Framework

8.4.4 Validation of the ASMSA Evaluation Framework

The ASMSA Evaluation Framework has been further developed from our analysis of the factors in the three case study data sets acquired which resulted in the introduction and amendment of evaluation themes.

Our revisions are represented in Figure 8.2, which now reflects how a particular evaluation theme impacts upon succeeding perspectives. The changes in evaluation themes and the repositioning of the evaluation themes represent the main amendments to our original evaluation framework, as shown in Figure 5.1 on page 188.

The other amendments to the ASMSA Evaluation Framework relate to the changes made to

our factor identifier labels, our criteria questions and our factor explanations following our analysis of our three case study data sets.

The ASMSA-DSS tool was updated to reflect the revisions in our evaluation themes, our factors and our criteria questions which are integral elements of the ASMSA Methodology. We believe that enhancements may be necessary to ASMSA's Methodology by further validating its usage, in a range of application contexts. Similarly, feedback on its usage by a range of discipline experts may assist in identifying methodological enhancements.

8.5 Methodological Observations from Using ASMSA

This section describes the prevailing conditions at the inception of the 2FA Project, the use of the ASMSA Methodology during the project, the outcomes of the project, and the DoR's methodological insights.

Figure 8.3 is a representation of the 2FA Project which has been generated from the Atlas.ti CAQDAS tool following our qualitative coding of the data gathered. Figure 8.3 is designed to show the sequential progression of the project from its inception, the use of the ASMSA Methodology through to the outcomes as at the end of our case study period. Figure 8.3 should not be construed as a causal network as our data are insufficient to identify direct causal effects throughout the project.

The antecedent variables representing the conditions prevailing at the time of the project's inception are shown in the boxes in the left column and the outcome variables are shown in the boxes in the right column of Figure 8.3. The boxes in between the antecedent variables and the project outcomes columns, i.e. the intervening variables, represent the stages and steps of the ASMSA Selection Method and the significant events that occurred during the project.

8.5.1 Prevailing Conditions

We provide a list of the conditions prevailing at the time of Corporation X's 2FA Project's inception with supporting descriptions.

1. Regulatory Compliance The MAS was the only financial regulator in Asia, at that time,

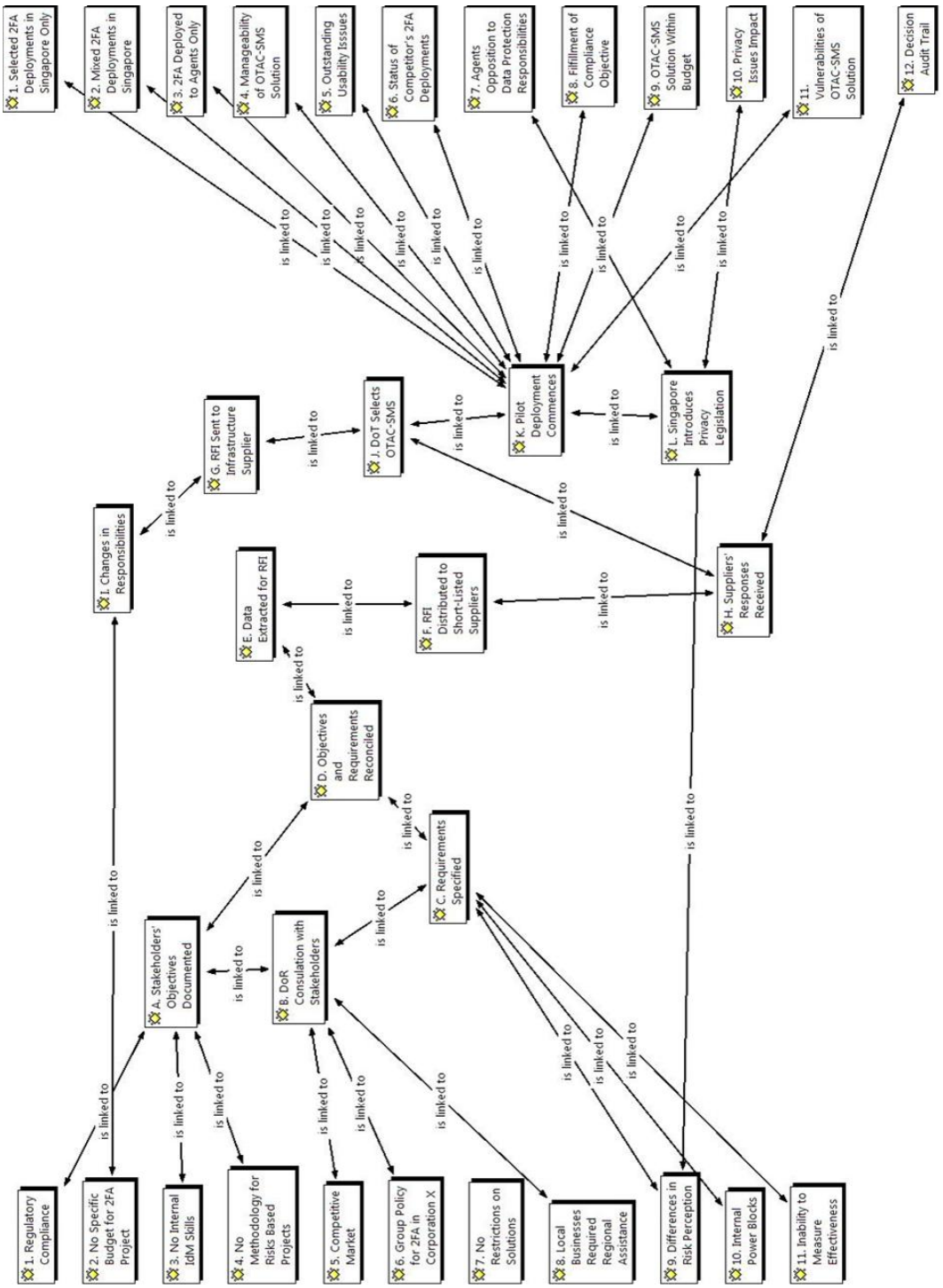

Figure 8.3: Approach Pursued by Corporation X's 2FA Project

to have issued a requirement for financial institutions to introduce 2FA solutions for their employees and insurance agents.

2. No specific budget for 2FA Project The responsibility for the 2FA Project fell to the DoR as part of his role and responsibilities for information risk for Corporation X's Asia Region. There was no specific budget allocated to engage external discipline experts and the project tasks would be undertaken by the DoR and his InfoSec team. The DoR acted as the sponsor and the 2FA Project Coordinator.

3. No Internal Identity Management Skills Corporation X had no internal identity management specialists employed at that time; however, there were information security specialists that reported to the DoR. The DoR managed the region's security governance framework comprising of risk accountabilities, security policies and security operations that were maintained by his team. The DoR was also the architect of Corporation X's security governance framework. His role meant that he consulted with Corporation X's Asian business executives to manage business risks on a regular basis.

4. No Methodology for Risks Based Projects Corporation X did not have a methodology for selecting an APIM and they did not use a methodology for selecting other security related technologies. His InfoSec team members, however, often used a risk assessment methodology to assist Corporation X's business operations to identify risks and to determine the concomitant security controls.

5. Competitive Insurance Market Corporation X's main income was expected to come from its Asian business operations and the introduction of 2FA was viewed as a potential obstacle on their agents' productivity to achieve their sales targets. Corporation X's insurance business competitors, however, would also need to introduce a 2FA solution for their respective employees and insurance agents or brokers. The DoR explained that *"Singapore was a mature market and insurance agents, typically, did not like having anything interfering with their liaison with their customer or potential customer. The competition to recruit insurance agents in Asia was incredibly intense between insurance companies"*.

6. Group Policy for 2FA in Corporation X Corporation X's GHO in London mandated the use of smart card tokens to achieve 2FA regulatory compliance. The Regional Head Office (RHO) in Hong Kong had some degree of autonomy in that it could challenge the GHO policy decisions provided that evidence could be gathered to demonstrate an

adverse impact on local business operations or that such policy decisions contradicted local regulations or social norms of the indigenous cultures.

7. No Restrictions on 2FA Solutions Corporation X was leading the way for the insurance industry in Asia to comply with the regulatory authorities' security requirements to introduce a 2FA APIM for user access control. The main focus of the 2FA Project was to explore alternative 2FA candidate solutions, including the use of biometrics, and select the 2FA solution that would best match Corporation X's operating business model. The solution, however, needed to incorporate Corporation X's current identifier and password authentication method.

8. Local Businesses Required Regional Assistance The compliance to 2FA regulation was regarded by Corporation X's local business entities as a regional issue rather than a single company business issue. Many of the local businesses sought guidance from regional office to investigate complex issues surrounding technology. Corporation X's local businesses relied on the regional office to operate their systems and infrastructure because the technical expertise was not available locally.

9. Differences in Risk Perception Corporation X's perception was that there were no increased risks associated with conducting on-line insurance transactions which differed to the financial regulatory authorities' risks perceptions.

10. Internal Power Blocks The conditions within the regional offices were not always conducive for collaborative working as some senior executives were keen to exploit the fuzzy responsibility boundaries relating to information risk management, security operations, and technology and infrastructure operations to build their personal influence.

11. Inability to Measure Authentication Effectiveness Corporation X was unable to determine the effectiveness of its current user identifier and password authentication mechanism. The metrics for establishing such effectiveness had not been defined. The audit logs, generated by the different computer systems, the security incidents reported, and the statistics on password reset requests together with other relevant data were not amalgamated in order to provide an indicative measurement of effectiveness of the current authentication system.

The DoR stated that the 2FA Project was not one of Corporation X's highest priority projects at that time. Nevertheless, an early start to investigate the possibility for ascertaining the

optimal 2FA solution was regarded as advantageous as it would enable Corporation X to work at a reasonable pace in order to select and deploy the selected 2FA solution to each business in Asia at the appropriate juncture.

8.5.2 Significant Events in Corporation X's 2FA Project

This sub-section describes the significant events that took place during Corporation X's use of the ASMSA Methodology to steer the 2FA Project. The DoR and his team followed the ASMSA Selection Method's processes during Stage 1 and Stage 2; however, the planned use of Stage 3 of the method was superseded by an unexpected event.

We provide a list of the significant events which occurred during the 2FA Project.

A. Stakeholders' Objectives Documented The stakeholders' objectives for introducing 2FA were established during Stage 1 of the selection method within the constraints imposed by the regulatory authorities' security requirements.

B. DoR Consultation with Stakeholders During Stage 1 the DoR liaised with business units and also with the three user communities to ascertain their objectives for 2FA.

C. Requirements Specified The processes in Stage 2 enabled the DoR to establish a baseline set of requirements for the 2FA.

D. Objectives and Requirements Reconciled The DoR used the ASMSA-DSS to match the requirements to the stated objectives, which identified some irregularities and inconsistencies. Following his review, some of the objectives and requirements were revised; however, there were no redundant requirements identified. Some objectives were merged and generalised by the DoR.

E. Data Extracted for RFI Data in the ASMSA-DSS was extracted and imported into Corporation X's standard RFI template. Some data were removed, e.g. total budget allocated to project and its deployment for commercial reasons.

F. RFI Distributed to Short-Listed Suppliers We carried out investigations on behalf of the DoR to identify specialist providers of identity management products based upon criteria provided by the DoR. The supplier had to demonstrate significant presence and experience of operating in Asia. The DoR wanted to ensure that the 2FA systems were capable of being maintained by a financially stable supplier with a track record for

supporting their products over a protracted period. A short-list of suppliers was agreed with the DoR and the RFI was emailed to these chosen suppliers requesting them to respond within six weeks. Despite the covering letter that accompanied the RFI stating that the suppliers could seek further clarification on Corporation X's requirements none of them chose to do so.

G. RFI Handed to a Network Infrastructure Supplier Corporation X's HoITP handed the RFI to the network infrastructure supplier during negotiations relating to the provision of network monitoring services.

H. Suppliers' RFI Responses Received Five RFI supplier responses were received by Corporation X within the stated deadline. The DoR conducted an evaluation of these RFI responses and concluded that he had sufficient evidence to demonstrate that an OTAC-SMS solution was preferable to the smart card solution recommended by GHO. His evaluation report to the GHO which was endorsed by the regional executive board was not made available to us.

I. Changes in Responsibilities The HoITP assumed responsibility for the 2FA Project from the DoR.

J. HoITP Selects OTAC-SMS Solution The HoITP selected the OTAC-SMS solution from the network infrastructure supplier rather than from one of the short-listed suppliers. The regional board of directors confirmed their agreement to the HoITP's selection recommendation.

K. Pilot Deployment Commences A pilot deployment of the selected OTAC-SMS 2FA solution commenced in Singapore with a limited number of insurance agents.

L. Singapore Government Introduces Privacy Legislation During Corporation X's pilot deployment of the OTAC-SMS solution, with its Singaporean insurance agents, the Singapore Government introduced the Personal Data Protection Act 2012. This law required businesses to protect citizens' private information. For Corporation X the scope of the legislation included their insurance agents' biographical details, particularly their mobile telephone number, and also Corporation X's customers' private data.

The outcomes of the 2FA Project are described in the next sub-section.

8.5.3 Outcomes from Corporation X's 2FA Project

The DoR considered Corporation X's 2FA Project to be successful during an interview at the end of our period of study.

We found that Corporation X's 2FA Project was perceived as successful because the deployment of the OTAC-SMS solution allowed Corporation X to claim compliance to the Singapore Authorities' security requirements without adversely impacting its business operations. The DoR expressed the view that '*the use of the ASMSA Methodology has been beneficial to achieving Corporation X's main objective of rejecting Group Head Office's recommended smart card 2FA solution*'.

We found the following project outcomes in our data:

1. **Selected 2FA Deployment Only in Singapore** The selected OTAC-SMS solution had been deployed in Corporation X's businesses in Singapore; however, it had not been introduced across to any of their businesses in different countries in the region. Singapore was the only country that had published a regulatory requirement for 2FA. The number of insurance agents currently using the 2FA solution at that time was less than five percent because the local Corporation X's businesses had been reluctant to deploy the solution due to local market sensitivities and competitive forces.

2. **Mixed 2FA Deployments in Singapore** Some insurance agents were still using the original smart card 2FA solution. The local businesses in Singapore, however, were considering migrating from the smart card solution to the OTAC-SMS solution. The local business units were reluctant to migrate because they had invested and had committed to furnishing their agents with the smart card solution. The local business units had gone ahead with the GHO mandated smart card solution without considering the regional head office's recommended 2FA solution. The local business units had received feedback from agents complaining how difficult and how unusable they found using a smartcard and to have to carry the reader equipment with them as well as their mobile phones and laptop devices.

3. **2FA Deployed to Agents Only** Insurance agents in Singapore were the only users of the OTAC-SMS solution. A number of initiatives which affected the agents use of Corporation X's systems had commenced in the other countries, such as Hong Kong. GHO was also looking at authentication mechanisms on mobile devices for its

executives rather than smart cards.

4. **Manageability of 2FA Solution** The OTAC-SMS solution was found to be easier for Corporation X's internal technology resources to manage than the smart card solution. Corporation X wanted to avoid the management of software code executing on their insurance agents' devices. The DoR stated that agents had a range of ageing hardware and software: *"So I've seen agents that are using Windows 95 still on battered old laptops. If we started introducing software into the agents' devices we will almost certainly have run into problems with compatibility across different platforms, capabilities of different machines etc."*.

5. **Outstanding Usability Issues** Corporation X's insurance agents in Singapore had complained that both of Corporation X's 2FA solutions were complicated to operate. The DoR stated that *"there was a feeling, expressed by them, that particularly the smart card solution, but also even the OTAC-SMS solution, was interfering with their customer interaction"*.

6. **Status of Competitor's 2FA Deployments** Some insurance companies had deployed a smart card solution and some had opted to deploy a similar OTAC-SMS solution. Only one insurance company deployed a biometric solution where the agent's fingerprint was captured by the laptop which was supplied by that competitor. According to the DoR, the deployed solutions appeared to reflect the way that each competitor managed their agents. Where companies supplied equipment to their agents then these competitors opted for a more intrusive 2FA solution with software managed on supplied devices. Smaller competitive companies had selected OTAC-SMS solutions.

7. **Agents' Opposition to Data Protection Responsibilities** Corporation X's businesses in Malaysia, scheduled as the next country to deploy the 2FA solution, encountered resistance from their agents. Their agents were opposed to fulfilling their data protection responsibilities in order to comply with the Malaysian Privacy Laws. The DoR commented that *"some of them [agents] were, at various times, demonstrating outside of Corporation X's branches stating they didn't accept their new contract because it contained additional clauses specifying their new responsibilities to keep customers' information confidential"*.

8. **Fulfilment of Corporation X's Compliance Objective** The MAS had not yet confirmed that Corporation X's OTAC-SMS solution complied with their security requirements. While the regulator had not given any guidance on the expected solution's capabilities

they retained the right to inspect the deployed 2FA solution. The regulators in Singapore would, according to the DoR, normally suggest that improvements in the controls were needed to a deployed solution. The DoR considered, however, it unlikely that the regulators would request companies to invest in a totally new solution.

9. OTAC-SMS Solution Within Budget The costs of deploying the OTAC-SMS solution in Singapore did not exceed the original budget. According to the DoR, the budget was set originally for a smart card solution and that amount was deliberately over-budgeted.

10. Privacy Issues Impact The 2FA Project had also highlighted the need to undertake further work to ensure that Corporation X's processes align with the privacy laws in which its companies operate. The Singapore Data Protection Law contained a requirement in respect of companies' mandatory use of a 'Do Not Call Register' indicator. The law prohibits companies from sending SMS messages to persons unless they have obtained their prior consent. Corporation X's legal team in Singapore was testing that statutory requirement for use of SMS messages with their agents and the OTAC-SMS solution.

11. Vulnerabilities of OTAC-SMS Solution Corporation X had identified a number of vulnerabilities associated with the OTAC-SMS solution. Corporation X planned to introduce other counter measures to improve the availability of the access codes to the agents and also introduce further controls relating to the protection of agents' data, e.g. agents' mobile telephone numbers. Corporation X found it difficult to conduct an assessment of the effectiveness of their 2FA solution. Since the introduction of the 2FA Project the DoR had embarked on a separate work stream to improve the reporting of security breaches. His team had reviewed security incidents over the last five years and found that the information relating to the reported security incidents to be of insufficient depth to assign breaches to specific authentication failures.

12. Decision Audit Trail Corporation X had produced a decision audit trail by using the ASMSA Methodology to investigate the options for a 2FA solution. The DoR stated that *"there are benefits in having such a trail because it could be used, having arrived at their selection, that Corporation X could demonstrate, from the output from the methodology, that we followed a structured process"*. He also stated that *"regulators are quite often more interested in the process of how the control is determined rather than in the actual practical implementation of the solution. The audit trail acts as evidence to show a regulator that we evaluated several different 2FA solutions from*

alternative suppliers and our reasons for the eventual OTAC-SMS selection".

We now provide methodological insights from the DoR following his use of the ASMSA Methodology in Corporation X's 2FA Project and a description of current decision-making processes on security issues in Corporation X.

8.5.4 Methodological Insights

Generally, the DoR thought that the ASMSA Methodology, aided by the ASMSA-DSS tool, was of reasonable assistance to Corporation X's 2FA Project. He said that it helped him to produce evidence, in the form of a decision audit trail, to demonstrate the reasons behind the selection of the OTAC-SMS solution rather than the recommended smart card solution. The DoR claimed that he had never used a methodology or a structured approach such as ASMSA.

He stated that *"the key thing for me was the structured approach. So it did make us, make me, consider all the different aspects - you know things that you might not have thought about were driven out by going through those structured questions and answers approach. So, I think, that was quite important as it did highlight some things that hadn't occurred to us. I think then again, as we said before, that having that output available [from the ASMSA-DSS tool] helped us to create a fairly comprehensive RFI"*.

He continued by stating that *"it was useful to be able to present back to some of the regional [executives] and particular regional information technology risk committee, bear in mind that some of these people are not a technology people, they are not security people, but they understand operational risk. It allowed us to present that sort of audience and say look here guys these are the things that we thought about. Audit in particular, obviously, will audit an implementation. So having had that background from the methodology it does help when they do an audit because they have that background there, they know why we ended up with that solution. That makes it easy for them. And then finally, obviously, you have the audit trail available to demonstrate to regulators, or anybody else that comes in and asks, of the processes that we went through, and our thoughts and the way we developed them is also very useful"*.

The DoR considered that our methodology was suitable for projects which had to evaluate long-term solutions with significant investments. He explained that *"where you're consid-*

ering putting in something that essentially is the foundation of how you manage to control access to systems and data or devices, so anything that can identify the individual accurately would benefit from that level of rigour". He thought that our methodology was inappropriate for situations where a decision needed to be made quickly; he quoted *"in two days"*.

The DoR explained Corporation X's current approach for decision-making, which included the use of weightings against the particular factors: *"We would normally form a number of perspectives on a solution, from a technology, an information security and a business view point. A working group in a specific meeting would evaluate all the options and assess them based on the different perspectives of those different audiences. Once the decision is made we then move to essentially a financial approval process that also includes within it assessments of non-financial benefits that could be meeting of regulatory requirements or satisfying a particular business requirement which isn't financial or a financially based requirement"*.

He explained how our methodology and the ASMSA-DSS tool could assist Corporation X's current decision processes: *"The initial assessment would be to get the facts together so the output from the tool gives us essential information and then it would be an examination that would look at both the quantitative and qualitative factors. The quantitative evaluation would be typically around the cost issue but then we would factor in more subjective views like on the qualitative aspects of usability and manageability that are particularly important"*.

He confirmed that *"we might do a weighting against those factors and if we found say that one solution was affected significantly by the higher cost, but had higher level of satisfaction with some of the less more qualitative aspects then we might look at that solution and choose it over cheaper solution that scored a better score, just because of the low cost. So we try to factor in the different perspectives to make sure that were not just choosing the cheapest option but choosing the right option regardless of cost, accepting that there might be a higher price"*.

He concluded that Corporation X's decision processes are seeking optimal solutions; however, there are occasions where the decision, even with the weightings, is not clear-cut. He explained that on such occasions *"there is a discussion process and ensuring that there is an understanding within the working group (and the working group composition will vary depending upon what the solution is) that ensures as to why a decision has been made, which factors have been more influential in making a decision and the reasons behind that particular factor, whatever it might be, outweighing any other factor"*.

His comments suggest that the ASMSA Methodology is reasonably efficacious when the APIM is of significant importance to the stakeholders. The structure of the methodology and the production of a decision audit trail appear to complement Corporation X's current decision-making processes.

8.6 Assessment of the ASMSA Methodology's Efficacy

We describe the results of our assessment of the ASMSA Methodology's efficacy using our criteria, described in Section 8.1, and the data acquired from this case study. In this section, we also briefly describe the results of our cross-case assessment of methodological efficacy using the data sets from our three case studies.

8.6.1 Effort to Use the ASMSA Methodology

Our assessment involves the comparison of the effort expended by the DoR to use the ASMSA Methodology during Corporation X's 2FA Project against his normal project activities. The DoR continued his normal daily responsibilities while undertaking the tasks in the project.

The DoR claimed that he had spent about 40 man hours on using our methodology, representing roughly 10% of his total daily effort during the first two stages of the 2FA Project. He claimed that the effort increased to around 30% to 40% of his daily effort during his involvement with production of the RFI and his evaluation of the RFI responses, from the identity management technology suppliers, which took place over a ten week period. As the DoR did not use Stage 3 of our method our estimate of his execution effort was approximated at 225 man hours in total, assuming a 10 hour working day. We acknowledge that our estimate may be understated.

In respect of his effort on using the ASMSA Methodology the DoR commented that *"having an overhead of 30% to 40%, if you call it an overhead, is not a bad thing. It gives us, by using a methodology that has structure behind it and a visible audit trail behind it, more confidence in our decisions as opposed to a more ad hoc type review where people would come up with ratings and import these and do it on a spreadsheet. Yes, it's [the methodology] probably added some time to it [the decision process] but I think its added more confidence to the end decision and, to me, that is probably worth the extra effort"*.

In summary, the use of the ASMSA Methodology requires supplementary effort of approximately 30% to 40% to those activities in a project to select an APIM. The use of a systematic methodology, however, appears to bring the benefit of additional confidence into the decision-making processes.

8.6.2 Size of Application Context's Problem

This section describes the results of our assessment of ASMSA Methodology's efficacy in terms of its proportionality and dimensionality to the application context's problem.

We assess the impact of the business problem on Corporation X to be of 'moderate' proportion because the potential loss of insurance agents to competitors, through an inappropriate 2FA solution, could reduce Corporation X's new income streams.

The DoR provided an affirmative response that use of the methodology was proportionate to the size of their business problem. He explained the reasons behind his affirmative response: *"This is something that is all about managing what is potentially a significant risk for us. And if we don't get that right then we end up exposing ourselves to a greater level of risk or even regulatory sanction or failures in the solution that could cost significantly more"*.

He also provided further explanation on the proportionality aspects of using a systematic methodology from a general perspective: *"If we were looking at a short-term fix to a solution then probably not. But if you are looking at something in our case which is going to be a long-term solution with the significant costs involved and then making the investment. You need to make sure you have the right solution because in the end having the right solution is probably going to save you significant sums of money. I've seen a number of instances where less rigorous processes are being followed and after a couple years, or even less, then, if you find your solution doesn't meet your requirements you're back to square one. You can then incur costs to take out the old solution, find a new one and then re-implement. So, yes, it is proportionate on something like this"*.

We assess the dimensionality of the problem in respect of the relationships between the stakeholders involved in the 2FA Project as 'complex'.

The DoR explained his assessment regarding complexity of the relationships relating to the Corporation X's business problem in Asia: *"We have a very complex environment. We've got 26 operations in 13 countries, multiple different types of user from employees at lower*

levels, to senior management, to the agents, who are not our employees, and will be using their own technologies. So having the tool and the methodology there to work through that process systematically was useful certainly and gave me the chance to think more about those different aspects of use then I would have done probably otherwise".

In summary, our assessment of the acquired data suggests that the use of the ASMSA Methodology is *reasonably* efficacious when the size of problem has a *moderate* impact upon the stakeholders' business operations and the relationships of the entities in the application context are *complex*.

8.6.3 Accuracy of APIM Selection

We assess the accuracy of the ASMSA Methodology using our criteria to evaluate the application context's situation and the characteristics of the methodology.

The project's objectives were clear to the DoR; however, the objectives and requirements for the 2FA deployment were not known at the project's inception. The problems associated with improving user authentication were not fully appreciated by the DoR, particularly the strength of opposition from the insurance agents in respect of adding further demands on their time. The DoR, however, had a sound appreciation for some of the causes of those parts of the problem that he did understand, particularly in respect of managing security controls. The stakeholders in Corporation X appeared to cooperate and communicate frequently; however, we identified tensions between the regional office and the local business units. There appears to have been some friction between the DoR and the HoITP in terms of the responsibility for selecting a 2FA solution. The DoR claimed that the relationships in the application context were complex, particularly Corporation X's relationships with their insurance broker companies and their agents, as employees or independent contractors.

We assess the ASMSA Methodology to be repeatable in that its processes are documented to a reasonable granularity and, therefore, we consider the methodology is usable by other evaluators to produce similar results. The outputs from using the ASMSA Methodology are a categorisation of the data acquired to aid the evaluator in considering many interrelated factors and the production of due diligence evidence in a decision audit trail. According to the DoR, the methodology's systematic processes gave structure and control to the 2FA Project so as to improve its productivity, particularly for the generation of the RFI document.

From these data we consider that the methodology was *reasonably accurate* in its use to select the optimal 2FA for this application context. Our assessment here is supported by the evidence that similar insurance companies in Asia selected an OTAC-SMS solution, although these companies, as far as the DoR was aware, did not use a systematic methodology.

In our final interview the DoR admitted that he was unsure as to the effectiveness of the deployed 2FA solution: *"Okay, there isn't an easy answer to that. A lot of what we are trying to build at the moment is a picture using log data and questionnaires. We have a six year of history of incidents in a database. So what we are doing with that, in particular, at the moment, is that we are trying to build a view that says what's the most frequent cause of incidents, what is the trend on each of those incidents, and where do they come from? So that the type of thing we're trying to work on and its not yet fully there but that's where this [Methodology] could come in if we could then demonstrate that by using the two factor authentication we have less losses of data through failures in identification and authentication"*.

We have incorporated criteria questions into the relevant evaluation themes of the ASMSA Evaluation Framework so that organisations are encouraged to define, at the outset, metrics upon which to evaluate the utility of their APIM and also to define the methods for gathering the relevant data in order to conduct utility appraisals.

In the absence of attempts by Corporation X to assess the effectiveness and efficiency of its current and the deployed 2FA solution we are unable to make further claims on methodological accuracy and whether the solution chosen was indeed optimal for this application context. Corporation X had not defined metrics to measure the effectiveness and efficiency of their authentication systems. We consider that the defining of such metrics should be based upon the objectives and requirements for deploying the APIM in the application context. The DoR recognised that the collation of appropriate data are essential to determine the effectiveness of their security controls.

We conclude that the accuracy of an approach to select the optimal APIM cannot be assessed realistically unless pertinent metrics are defined and the relevant data are acquired from that application context. Our case study results confirm Jaquith's argument [164] of the need for organisations to quantify their security goals.

8.6.4 Methodological Simplicity

This section describes the results of our assessment of ASMSA Methodology's efficacy, in terms of its methodological simplicity, as defined by our criterion in Section 8.1.

We assess the methodology's simplicity of use as 'tolerable' based upon the DoR's following comments: *"Relatively simple - but I think the tool [ASMSA-DSS] is very wide-ranging and very broad and, therefore, while of itself its not difficult, I think the scope that it tries to cover makes it difficult, on occasions, to complete all the required requests [Answer all the criteria questions]. In a way it has a sort of benefit in as much that it makes you think through everything - the drawback is that it makes you think through everything!"*.

He also added that *"one things that was quite good was having a more structured way of thinking [stressed] about what it is you are trying to do'*. We also questioned the DoR as to whether our methodology, including our DSS tool, should be used by a generalist aided by a discipline specialist or a mixture of discipline experts. He considered that *'it would need a specialist of some description to lead. I don't think you could have a generalist doing it other than facilitating and project management possibly. There has to be a specialist in there who has an understanding of information security, information risk, not necessarily a deep understanding of technology, but at least a familiarity with the terms. Somebody needs to understand the meaning of false positives and all these things. That would tend to say the generalist would not be able to it without a significant amount of [learning] work on their part"*.

In summary, our assessment suggests that the methodology's efficacy, in respect of its simplicity of use, is *tolerable* for an identity management discipline expert.

8.6.5 Executable as a Program

This section describes the results of our assessment of ASMSA Methodology's efficacy in terms of whether it can be represented by an executable program.

From our assessment, we consider that about 85% of ASMSA Methodology's processes are represented as an executable program in the ASMSA's DSS. This assessment includes the functionality for data input, data transformation and data reconciliation activities by an evaluator.

The MSP technique is not incorporated into the ASMSA-DSS implementation because we consider that many of its processes require human to human interaction. Human involvement is also needed to transform and reconcile the data in the ASMSA-DSS. Our DSS is not designed to select the optimal APIM automatically but to manage the large volume of data to support the selection processes. Human intervention is also required to score the attributes of candidate APIMs against the stipulated requirements.

Based upon the DoR's comments we assess the effort required to learn and use ASMSA's DSS, as designed, is 'moderate'. The DoR concluded that *"the structure and the method and the approach [ASMSA-DSS] seems to fit logically what you would do in establishing what your objectives are, you map and develop your requirements, and map the two together. Its like a standard type of business analysis type of approach. So the logic is not an issue at all. It works fine"*.

In summary, our assessment suggests that the majority, around 85%, of the methodology's processes are executable as a program within a DSS, which requires user intervention to carry out data input and manipulation tasks. We assess the effort required to learn and use ASMSA's DSS is *moderate*; however, we acknowledge that the ASMSA-DSS might benefit from some functional and usability enhancements to make it easier to learn and use.

8.6.6 Capability of the ASMSA Methodology to Address Real-world Problems

This section describes our assessment regarding ASMSA Methodology's capability to address real-world problems.

Although our methodology was not used entirely in the 2FA Project, we assess the ASMSA Methodology as having an *acceptable* capability of being applied to address real-world problems.

We base our assessment on the DoR's retrospective insights: *"Okay, I think where we are now is, given the amount of time that has gone into this, we started off with a sort of nebulous statement from our Group Head Office that said, you have to put in two factor authentication. The chosen solution in Group Head Office (GHO) was a smart card [vendor's product named], which works for GHO, which is about 600 people in one location. They might travel a lot but they are based in one single office. The difficulty that we face in Asia is that we have in excess of, well around 400,000 to 500,000 people, in a variety of locations and not all of*

them are in our offices. So, for us, the GHO recommended solution was going to be a very difficult implementation problem and ongoing management problem. So, from my perspective having some structure and some sort of logic behind the way we approached this meant that I could get myself in a position where I can go back to the GHO people and say we have looked at this [recommendation] and smart card [vendor product] and it isn't practical for us in Asia. I know it isn't but I haven't got any evidence behind it [his unsubstantiated conclusions]. What this [methodology] gives me a demonstrable and repeatable processes with evidence of what has been looked at, why have we looked at it, and what we are trying to achieve with it".

He explained the benefit of using the ASMSA Methodology for his real-world problem: *"So for me the big benefit is having that record of the considerations that go into that. The evidence behind that and the ability to say, if someone comes along and says why did you make that decision? You can go back into the output of the tool and say this is where that came from [audit for justification]. A lot of the work that I do, with other areas of information risk, is around building up the evidence to support that fact that we need to make an investment in either people, process or technology. This is another tool, a powerful tool, what is for probably, arguably, one of the more significant information security or risk investments that we would have to make*".

In our final interview with the DoR, in response to our question on the methodologies' applicability in the real-world, he commented: *"I see no reason why not from what I have seen"*. In response to our question as to whether he would use the methodology again he replied that *"we probably would. One of things we have to be conscious of is that, and I use Singapore and Cambodia as two contrasting examples. Singapore is a mature market for us. Its got access to skills and knowledge that allow it to manage its infrastructure quite tightly. Cambodia, on the other hand, is a very immature market for us. The skills in Cambodia, not just Cambodia but also in other countries to manage a complex technology like this, do not exist. So, it is entirely possible that if we were looking to do a roll-out in Cambodia, for instance, we might well run through the process again using the previous inputs just to validate that they fit for that particular country. The issue is complex and we do not have internal expertise to support us in making investment decisions on the technology and solutions or to consider fully the management and support options involved in the long-term. Use of the tool helped guide those decisions"*.

In summary, our data suggests that the ASMSA Methodology's has an 'acceptable' capability

of being applied to select APIM in order to address personal automated identification problems in real-world application contexts. Our methodology has been used in a single application context and we acknowledge that further empirical research is needed to assess its efficacy in other types of application contexts.

8.6.7 Cross-Case Assessment of Methodological Efficacy

While we recognise that there are benefits, both theoretical and for practical purposes, in performing cross-case comparisons of methodological efficacy, using the data from our three case studies, we refrain from conducting a full assessment because our data from our two retrospective case studies are incomplete.

We were unable to acquire the relevant data relating to the effort expended by discipline experts in these programmes, although we believe the effort was considerable taking into account the range of experts engaged in the programmes and the programmes' duration over several years. We were also unable to acquire data in order to assess methodological accuracy because the data was not produced, as far as we could ascertain.

Crucially, we found in all of our case studies that the APIM organisations, as system owner stakeholders, did not define metrics in order to measure the utility of the deployed APIM for their application context. Therefore, it is difficult to determine whether the deployed APIMs were optimal solutions for their application contexts and, in turn, the extent of the methodology's efficacy used to select the respective solutions.

We found in all three case studies that APIM system owners had little understanding of the utility of the deployed APIM because in each case the programmes experienced difficulty in establishing 'ground truth' as to whether the claimed digital identity related to a transaction was invoked by the genuine person. An assessment on the accuracy of the methodologies to select the optimal APIM in real-world application contexts, therefore, relies upon improvements in acquiring the relevant data so that the utility of the deployment may be ascertained. Once the utility of APIM deployment and data related to other key factors are acquired an assessment on the methodological accuracy may be conducted objectively.

These three data sets suggest that the problems relating to the selection of APIMs are of significant or moderate importance to the stakeholders involved in the application context. It may also suggest that our selection of case studies is biased towards application contexts

where the impacts upon stakeholders are moderate or significant. Our data from all of our three case studies, however, highlights the complexities of the relationships between the stakeholders and the intricacies of selecting, configuring and operating APIMs.

We found that expert-led approaches for selecting APIMs relied upon practitioners' capabilities and intuition. The programmes' processes in the two retrospective case studies were not documented; therefore, another evaluator may find the respective approaches difficult to repeat. Conversely, the ASMSA Methodology, with its systematic processes and rigour is assessed as being *capable* of reproducing similar results. From the DoR comments in our third case study, we assess that the methodology was 'reasonably efficacious' based on the circumstances surrounding the particular 2FA Project.

The circumstances of some application contexts may be more conducive to a flexible expert-led approach and there may be occasions when the rigour of a systematic approach may be more efficacious. In the next section, we describe the extent of the ASMSA Methodology's efficacy by assessing the circumstances surrounding the application contexts of our three case studies so as to explain when a systematic methodology might be efficacious.

8.7 Circumstances when Using a Systematic Methodology may be Efficacious

This section answers our fourth research question on the extent to which a systematic methodology is efficacious for selecting an APIM and if so, under which circumstances, with explanatory reasons.

8.7.1 Clear-cut Decision Versus Comprehensive Evaluation

A systematic methodology appears to be efficacious when a programme is required to evaluate the application context thoroughly and consider a range of candidate APIMs in order to fulfil articulated stakeholders' objectives and requirements.

The circumstances surrounding Corporation X's 2FA Project fulfilled the majority of Jayaratna's criteria [165] to be considered as an ill-structured situation. We found that there were no defined objectives or requirements for introducing 2FA. A feasibility and cost estimations for introducing 2FA had not been researched. Similarly, the problems involved

with remote user authentication were not fully understood and the insurance agents' strong opposition to introduce 2FA had been underestimated by Corporation X.

The communication dialogues between the 2FA Project with Corporation X's business units appeared to be well-developed. We found, however, that the DoR and the HoITP's vaguely defined responsibilities in respect of dealing with the problem seemed to cause friction and their working relationship appeared strained. Also, the processes for decision-making amongst executives were complex and appeared to be influenced by both political and personal motives. The DoR needed compelling evidence, based on a comprehensive approach, to counter the smart card solution mandated by GHO in London.

The DoR in recognition of his uncertainty of the suitability of the mandated smart card solution persuaded Corporation X's executives in their Hong Kong RHO to establish the 2FA Project in order to:

- ascertain firm objectives for introducing a 2FA mechanism in order to validate GHO's vaguely defined aims;
- gain an understanding of the problems to introduce a 2FA solution from different stakeholder perspectives; and
- produce detailed arguments based upon local conditions to challenge GHO mandate to utilise smart cards as a 2FA mechanism for Corporation X's operations in Asia.

Conversely, from our review of our data in the two retrospective case studies, an expert-led approach and an iterative deployment approach appear to be efficacious when there an obvious solution is apparent. We found that such decisions on solution designs were made early within a programme. We found in the data of our retrospective case studies, however, that in neither case did the programmes establish stakeholders' objectives or specify the requirements for the APIM.

The programmes' objectives and the application contexts' problems appeared to be well understood and the underlying causes of the problems were sufficiently appreciated so that these two programme's concentrated on designing the solution rather than producing requirements documentation, based upon an evaluation of the application context.

From the initial use of the ASMSA Methodology a systematic methodology appears to be more efficacious than an expert-led approach when there is little understanding of the

application context's problem, there is doubt about the suitability of the recommended APIM, and there is a desire to establish stakeholders' objectives and requirements in order to evaluate various candidate APIMs.

8.7.2 Experts' Capabilities Versus Systematic Processes

A systematic methodology appears to be more efficacious than an expert-led approach when a decision-maker places more reliance upon repeatable systematic processes than on the capabilities of their discipline experts to select an APIM.

We found that the approaches in the retrospective case studies relied heavily upon the capabilities of discipline experts when evaluating the selection and configuration of an APIM. We also found that both programmes in these retrospective case studies did not follow a systematic plan of activities. We also identified that some processes were overlooked by the programme or insufficient time was afforded to discipline experts to complete their tasks satisfactorily.

The data in the retrospective case studies suggests that there were gaps in the knowledge and skills within the programme team in specific disciplines, for example the eID Card Programme lacked a usability specialist. We found that discipline experts' advice was often ignored or discarded by the programmes' senior management. The consequences of these actions by the programmes' senior managers, or by the decision authorities, may explain the unavoidable vulnerabilities and issues, particularly usability deficiencies, in the deployed APIMs.

In Corporation X's 2FA Project, the DoR, who was not a discipline expert, used our factors as a check list and followed the systematic processes in the ASMSA Selection Method to evaluate a range of factors that influenced Corporation X's eventual selection. The outcome of Corporation X's 2FA Project was the rejection of the original mandated 2FA solution. The systematic methodology provided supporting evidence, from the evaluations of several candidate solutions against objectives and requirements, so that the project was able to recommend and justify an alternative solution.

Our data also suggests that the selection of an APIM requires the engagement of identity management discipline experts in addition to other specialists in a programme. The importance and the complexity of some application contexts in some ill-structured situations may

demand the use of a systematic methodology and the engagement of a range of discipline experts.

8.7.3 The Need for a Decision Audit Trail

A systematic methodology appears to be more efficacious than an expert-led approach when a decision audit trail is required to provide comprehensive evidence of the systematic processes performed in the programme and that the data acquired may be used to justify the APIM selected.

Our data in Corporation X's 2FA Project suggests that there were benefits in producing a decision audit trail which could be used to demonstrate to internal decision authorities and to external parties, e.g. regulatory authorities, the systematic processes that were performed in order to justify Corporation X's selection. Our data shows, however, that additional effort is required to use a systematic methodology.

The main benefit of using a systematic methodology appears to be that it engenders confidence in the final decision because of the structure and the rigour enforced by the approach. The methodology ensured that assumptions were challenged by the DoR and that a comprehensive range of factors were evaluated, even if the impact of some of those factors on the final decision was negligible.

We did not identify the presence of a decision audit trail in our data sets from our two retrospective case studies. Additionally, we found in the data of both retrospective case studies that many assumptions were unresolved despite the acknowledged risks to deliverables in the respective programmes.

8.7.4 Stakeholder Consultation Impact

The ASMSA Methodology, incorporating the MSP technique, appeared in the Corporation X 2FA Case Study to have had little impact upon resolving users' concerns relating to the selection of the APIM. Despite the DoR consulting with insurance agents' representatives, through several interviews, the 2FA solution chosen was not acceptable to these users because it added additional tasks to Corporation X's sales processes.

Our data does not fully support the supposition that proficient stakeholder consultation

processes necessarily result in the optimal APIM being selected by a programme. We assumed that an MSP technique would enable Corporation X to select a 2FA solution which would resolve of users' objectives. We identified data in the Corporation X 2FA Project Case Study that issues surrounding usability deficiencies and data privacy protection issues were not addressed adequately by the project. Our data suggests that users were seeking transparent authentication utilising techniques, as described in Clarke's survey [54], and the project did not appreciate this factor adequately. Corporation X dismissed the supplier's proposal for a keystroke dynamics 2FA solution on the grounds that the technology was immature and that Corporation X would be dependent upon the product specialists for its maintenance.

We found in our eID Card Case Study that insufficient effort was afforded to consultation by the programme with citizens and commercial organisations that could potentially use the eID card for authenticating citizens in respect of their on-line services. While some stakeholder groups erected technical or privacy obstacles, as perceived by our interviewees, the exclusion of stakeholder representatives from specific industries was, according to Interviewee S, *"a misguided strategy"* because that industry sector had the potential to supply services that would be beneficial to citizens. Interviewee F concluded that *"proper consultation with stakeholders and the resolution of citizens' requirements and privacy issues play an important role in respect of the acceptance of on-line services, whether provided by government or by the commercial sector"*.

We found similar consultation deficiencies in the eGates Case Study where the programme did not consult with the border control police officers or their union representatives. The outcome of that strategy was that border control police officers did not always supervise the eGates during their operation, which, as a consequence, meant that the eGates were often closed to passengers.

Our data suggests that the inadequate consultation processes in both programmes were contributory factors only to the configuration deficiencies of the respective APIMs, which led to the under-utilisation of the respective APIMs. We were unable to locate data that directly correlated the cause of the under-utilisation to the lack of consultation with intended user communities or the acceptability of the proposed APIMs in the respective case studies.

We found in our Corporation X 2FA Project that despite the DoR using the MSP technique to consult with the various user communities, primarily with the insurance agents, the proposed 2FA deployment was not entirely acceptable to a large majority of the insurance agents.

From the insurance agents' perspective the OTAC-SMS solution burdened them with an additional task, which impacted their sales productivity.

Participative design has the potential to explore mutually convenient solutions; however, our data in this case study shows that an optimal solution, as far as its acceptability to the insurance agents was concerned, eluded Corporation X. The MSP consultation processes in the ASMSA Methodology, however, enabled Corporation X to identify a more suitable 2FA solution than the original smart card solution mandated by their Group Head Office.

In view of our inconclusive findings, we consider that further research is necessary to establish the causal effects of using MSPs or similar techniques to engage in consultations with stakeholders, particularly subjects, and the acceptability of the deployed APIM to the subject community.

8.8 Our Initial Theory on Methodological Efficacy

From the patterns recognised in our three data sets, as described in the previous section, we now develop our arguments to support our initial theory on methodological efficacy for selecting an APIM. Our data sets suggest that a systematic methodology is *reasonably* efficacious for selecting the optimal APIM when there is a need for a comprehensive evaluation; particularly for application contexts where the surrounding circumstances are ill-structured.

Methodological efficacy assessments can only provide indicative accuracy results on optimality because such assessments are restricted, in practice, due to incomplete data sets. Organisations appear to be reluctant to divulge sensitive data on the reliability and performance of APIMs. Additionally, until organisations define their specific metrics, to measure the utility of the deployed APIM, and actually gather the relevant data in order to assess its optimality for the application context, we believe that research on methodological efficacy is limited to presenting indicative results and tentative theories.

Therefore, there are limitations on our efforts to develop an initial theory on methodological efficacy due to:

- the restrictions placed on accessing sensitive data; and
- the absence of relevant data.

Nevertheless, we identified sufficient patterns in our data sets to enable us to provide some general trends in respect of methodological efficacy. The limitations of conducting empirical research, using a systematic methodology, together with the restrictions on the release of sensitive authentication data by organisations mean that we adopt a cautious stance on developing theories about methodological efficacy for selecting APIMs.

We conclude from our research, but we do not prove irrefutably, that a systematic methodology is *reasonably* efficacious when the range of circumstances surrounding the application context dictates that a programme requires to conduct a comprehensive evaluation in order to select the optimal APIM. The extent of that efficacy, for such comprehensive evaluation, includes ill-structured circumstances when a programme requires to:

- consider a range of candidate APIMs in order to fulfil stakeholders' objectives and requirements;
- place dependence on repeatable systematic processes in order to reduce reliance on the capabilities of discipline experts; and
- produce a decision audit trail as comprehensive evidence of the processes executed in the programme in order to justify the APIM selected.

These circumstance exemplars, however, are not exhaustive and additional circumstances and supplementary explanations may be revealed from further empirical research.

8.9 Summary of Chapter

In this section we describe our conclusions on our efforts to validate our identified factors using data from this case study which involved the use of the ASMSA Methodology in Corporation X's 2FA Project. We also summarise our conclusions on the methodological efficacy of using our systematic methodology to select the optimal APIM for an application context.

8.9.1 Efforts to Validate the ASMSA Methodology

We conclude that our factors are relevant to evaluate a real-world application context in order to select the optimal APIM. We have also initially validated the ASMSA Selection Method

and ASMSA Evaluation Framework, using data acquired from a real-world application context. We acknowledge, however, that further empirical research is necessary to refine our methodology's components, particularly the terminology of our criteria questions and to enhance our factor explanations.

We have validated that our factors for evaluation are consistent within the ASMSA Evaluation Framework and that our criteria questions are sufficiently general, to acquire data from the application context. We recognise that our identified factors, their descriptive labels, the criteria questions and the factor explanations would benefit from further refinement using alternative empirical research methodologies and also in a diversity of application contexts. Based upon our data acquired and our validation assessments, we consider that our 25 evaluation themes provide a solid foundation upon which to conduct further evaluations in other real-world application contexts.

Our cross-case analysis of our factor validation assessment results revealed that the availability of data played a key role in our efforts to validate our factors and to enhance our criteria questions and factor explanations. We also conclude that we have not reached a saturation point for identifying all the relevant factors for evaluating APIMs for every type of application context. We consider, however, that claims that factors for evaluating all application contexts are complete could be difficult to substantiate.

We regard our efforts in this case study to have initially validated the ASMSA Methodology and to have corroborated the coherence of its constituent components. Nevertheless, we acknowledge that the ASMSA Methodology requires further validation through usage in other application contexts. Further use of the ASMSA Methodology may also assist in identifying enhancements to augment its methodological efficacy.

8.9.2 Methodological Efficacy

We have ascertained that the extent of the ASMSA Methodology, as a systematic methodology, is reasonably efficacious in certain circumstances which surround the application context.

Data from our three case studies confirmed our supposition that the selection of the optimal APIM is more than a technological problem. We found that decision-making is problematical because of stakeholders' difficulties in articulating the nature of the problem which exist

in ill-structured situations, the diversity of varying stakeholder views of that problem and their objectives for the APIM together with the absence of a method to evaluate proposed solutions objectively. The difficulties in articulating the objectives and requirements for an APIM in these situations, in turn, impact the decisions on selecting the optimal APIM. The selection processes need to consider a wide range of factors; however, such decisions are based upon incomplete data, many assumptions, conflicting stakeholder objectives, poorly articulated requirements and evolving attitudes towards business processes and users' views on identification technologies.

The methodological insights from our initial use of the ASMSA Methodology and the data acquired enabled us to identify three circumstances for conducting a comprehensive evaluation. We found that these circumstances had a significant influence on the extent of our systematic methodology's efficacy to select the optimal APIM.

We conclude, but we do not prove irrefutably, that an organisation should conduct a comprehensive evaluation when the circumstances surrounding the application context necessitates that its programme needs to:

- establish objectives and requirements for an APIM in order to evaluate a range of candidate APIMs;
- employ repeatable systematic processes in order to reduce their reliance on the capabilities of discipline experts; and/or
- produce an audit trail of the programme's method which may be used as evidence to justify the APIM selected.

Our initial theory is that systematic methodologies, for selecting the optimal APIM, are *reasonably* efficacious when the circumstances surrounding the application context are such that an organisation needs to conduct a comprehensive evaluation.

In the final chapter we summarise our achievements from conducting our empirical inquiries, describe the limitations of our research and provide our recommendations for future research.

CHAPTER 9

Summary and Conclusions

Contents

This final chapter presents a summary of our research achievements, including our justified contributions to the body of knowledge, and the limitations of our research efforts. We conclude by recommending avenues for further research.

9.1 Summary of our Research Achievements

We provide a summary of our research achievements resulting from our efforts to address our research problem and our four research questions. We compare our achievements to the knowledge in the literature in order to justify the originality of our contributions.

We designed four research questions in order to address our research problem. Our first research question was designed to identify and validate a range of factors which need to be evaluated in order for decision-makers to select the optimal APIM. Our second research question was designed to establish a means of representing the systematic processes necessary to acquire data about the application context so that the optimal candidate APIM may be identified. Our third research question was designed to identify criteria upon which to assess the efficacy of a methodology to select the optimal APIM for a given application context. The fourth research question was designed to assess the extent to which a systematic methodology is efficacious for selecting the optimal APIM, and if so, under which circumstances with validated reasons, and if not, with corroborated explanations.

From our research efforts to address these four research questions our achievements and contributions to knowledge are:

- the identification and validation of factors which require evaluation in order to select the optimal Automated Personal Identification Mechanism (APIM) for a given application context;
- the development of a systematic methodology, entitled Approach for Selecting the Most Suitable APIM, designed to select the optimal APIM for a given application context. We developed the ASMSA Decision Support System (ASMSA-DSS) as a tool to support the usage of the ASMSA Methodology;
- the identification of criteria to assess the efficacy of a methodology to select the optimal APIM for a given application context; and, most important to our research problem,
- that a systematic methodology is *reasonably* efficacious when the range of circumstances surrounding the application context dictates that a programme requires to conduct a comprehensive evaluation in order to select the optimal APIM

In the next four sub-sections, we justify our claim of each achievement against the respective research question.

9.1.1 Identification and Validation of Factors to Evaluate APIMs

We summarise our efforts to identify and validate factors which should be evaluated in order to select the optimal APIM for a given application context.

From our review of the literature we identified that there are many diverse factors which should be evaluated in order to select the optimal APIM. The factors appear in a diversity of literature sources with varying perspectives; however, there is an absence of a consolidated list which incorporates factors from all perspectives.

Through our empirical research, we consolidated and validated 91 percent of the 201 factors which we found scattered across the literature. Our empirical research also enabled us to identify a further 26 factors, 15 factors and 21 factors in the data from our eID Card Programme Case Study, our eGates Programme Case Study and our Corporation X 2FA Project Case Study, respectively.

We have validated 243 out of 246 identified factors which should be evaluated in order to select the optimal APIM for a given application context. We have also classified these identified factors into 25 evaluation themes, as shown in the tables of Appendix F. In turn, these evaluation themes are incorporated into the ASMSA Evaluation Framework, as described in Section 5.5, to model the APIM selection problem from the Understanding, Effectiveness and Efficiency Perspectives.

We found, through the use of ASMSA Methodology in the Corporation X 2FA Project Case Study, that we were able to validate 99 percent of our identified factors. We acknowledge, however, in Section 8.4.2.4, that it may be difficult to substantiate claims that the list of factors for evaluation could ever be complete.

There are several publications [157, 38, 295] which discuss the issues surrounding some of these factors and their impact upon the selection of APIMs. These publications do not place these factors within an evaluation framework or model; however, Royer's contribution [257] is an exception. Royer lists [257] six high-level factors for quantitative analysis without providing specific definitions of these factors, how the related concepts are to be interpreted in the application context, or how the data acquired is analysed by his Decision Support System (DSS). Our efforts differs from Royer's contribution [257] because our factors are supplemented with explanations, contain criteria questions to acquire the relevant subject data and are classified into 25 evaluation themes, which are integrated into a qualitative evaluation framework.

A strict interpretation of our research efforts to address our first research question limits our contribution to the body of knowledge to the identification and validation of 62 new factors for evaluation. Our efforts, however, also concentrated on the collation of factors in

the literature and those identified in our empirical inquiry into a consolidated list. In turn we classified our validated factors into evaluation themes which are placed in an evaluation framework. Our list of factors may be used by a programme as an *aide-mémoire* to serve a reminder that all our factors require evaluation in order to select the optimal APIM.

We justify our claim of making an original contribution to the body of knowledge because a consolidated list of factors from different perspectives in an evaluation framework did not previously exist in the body of knowledge.

9.1.2 Development a Systematic Methodology to Select an APIM

We summarise our efforts to ascertain how information pertaining to an application context can be acquired and evaluated by developing a systematic methodology so as to determine the optimal APIM.

From our review of the methodological tools in the body of knowledge we identified that there is a scarcity of systematic methodologies to conduct evaluations in order to select the optimal APIM. We ascertained that most tools focus on the quantitative evaluation of the different types of solutions, e.g. biometric identification systems, without giving sufficient consideration to the characteristics of the typical application contexts in which they are designed to be deployed.

Ashbourn's approach [15], with its associated Pentakis software tool, is limited to evaluating biometric solutions. Royer developed [257] the Enterprise IdM Decision Support System to focus on the evaluation of identity management systems in enterprises. The main aim of Royer's research [257] was to develop a DSS, using mathematical modelling, rather than creating a methodology. The heuristic approaches in the literature do not include any methods containing discrete steps and are limited in their scope to evaluating solution types, e.g. biometrics, or certain application context types, e.g. an enterprise context.

The absence of detailed methods in heuristic approaches in the literature [101, 228, 303] do not enable the approaches' processes to be repeated by different evaluators. These approaches rely on the capabilities of discipline experts and their interpretation to select optimal security controls for the application context. In contrast, our inquiry involved the development of a systematic methodology, with a detailed method, capable of repetition, so that the optimal APIM may be identified, with consistency, for a given application context.

We designed our second research question so that a systematic methodology could be considered as a potential approach to acquire information pertaining to a given application context in order to support the selection of the optimal APIM for that context. Expert-led and iterative deployment approaches, as we described in our two retrospective case studies in Chapters 6 and 7 respectively, represent alternative selection methodologies.

In contrast, we specifically designed the ASMSA Selection Method with its discrete steps, incorporated into three stages, in order for an evaluator to use its processes to acquire data, in a systematic fashion, for all types of application contexts. Equally, the ASMSA Methodology is designed to acquire data about all types of solutions so that candidate APIMs may be evaluated against the stipulated requirements for the APIM. Our methodology pursues a 'fitness for purpose' philosophy by encouraging an IS development programme to describe the requirements for an APIM related to its intended application context. This strategy then enables an evaluator to assess candidate APIMs' capabilities to fulfil the stipulated requirements.

Our criteria questions, as defined in Section 5.2.4 and represented in the tables of Appendix F, are designed to acquire subject data systematically, using the ASMSA Selection Method, from primary data sources. These data sources may be assessments in respect of the application context, e.g. risks assessment, conducted by an IS development programme or documents produced by external parties, e.g. suppliers' technical product specifications.

While there may be commercial methodologies in existence, we justify our claim of making an original contribution to the body of knowledge because these methodologies have not been published, as far as we can ascertain, to enable scientific review. We specifically developed the ASMSA Methodology to address the absence in the body of knowledge of a systematic methodology to select an APIM.

We developed the ASMSA-DSS as a by-product of our research efforts to meet our need to represent the ASMSA Methodology's processes and to manage the large volumes of data acquired from our empirical research. We did not, however, originally set out to develop a Decision Support System tool.

9.1.3 Creation of Criteria to Assess a Methodology's Efficacy

We summarise our efforts to establish how the efficacy of a methodology to select an APIM can itself be assessed. We identified and developed criteria in order to assess the efficacy of methodologies to select the optimal APIM for a given context.

We attempted to assess the efficacy of the approaches which were used in each of our two retrospective case studies using our efficacy criteria. We identified proficiencies and deficiencies of each approach; however, we encountered unexpected problems surrounding the absence of relevant data in order to perform an assessment of the approaches' selection accuracy.

In our efforts to assess the accuracy of the methodologies used in all of our case studies, we found that none of the organisations defined metrics in order to evaluate the utility of a deployed APIM. Additionally, we found that organisations have difficulty in determining 'ground truth' relating to accuracy of APIMs' decisions to identify or authenticate genuine subjects. Therefore, we were not able to assess these methodologies' accuracy in their selection of the optimal APIM in any of our three case studies due to the absence of relevant data.

In our Corporation X 2FA Project Case Study we found that organisations utilised readily available data from system logs and also conducted specific tests, e.g. password quality checks. The Director of Risks (DoR) acknowledged, however, that the measurement of the utility of security controls in Corporation X needed to be improved generally. The data (and absence of data) from our empirical inquiry provides further evidence to support Jaquith's claims [164] that organisations are relying upon incomplete data in order to determine the utility of their security controls.

Therefore, the accuracy of a methodology to select the optimal APIM for a given application context is difficult to assess, in practice, until such times as organisations define their utility metrics and the data needed to conduct an accuracy assessment are acquired from the application context. We have created, however, an accuracy criterion for conducting methodological comparisons, which is defined in Section 8.1.3.

From our research efforts, we conclude that an assessment of a methodology's efficacy should be based upon the following six criteria, which are defined in Section 8.1:

1. the methodology's execution effort;
2. the size (dimensionality and proportionality) of the application context's problem;
3. the accuracy of methodology's selection;
4. the methodology's simplicity;
5. the extent to which the methodology is executable as a computer program; and
6. the capability of the methodology to address real-world problems.

Our third research question was framed so as to address the identified gap in the body of knowledge to determine the efficacy of a methodology or approach to select the optimal APIM. We justify our claim of making an original contribution to the body of knowledge in that we have identified and developed criteria, to be employed within an assessment framework as detailed in Section 8.1.7, to assess the efficacy of a methodology to select the optimal APIM for a given application context.

9.1.4 When to Use a Systematic Methodology for Selecting an APIM

We summarise our efforts to determine when a systematic methodology may be efficacious for selecting an APIM.

We framed our research problem so as to determine the extent to which a systematic methodology, as a tool, may be efficacious for selecting an APIM rather than simply determining its viability alone. Our research strategy was based upon our supposition that such a systematic methodology would be efficacious for selecting the optimal APIM for some application contexts but not conducive for every application context.

Our inquiry into the extent of the systematic methodology's efficacy aimed at identifying those circumstances surrounding an application context which favour the use of such an approach. From the identification of these circumstances we would then be able to explain the extent of its efficacy and develop initial theories regarding the usage of systematic methodologies in different types of application context.

We conclude that *a systematic methodology may be reasonably efficacious when the characteristics of the application context are such that an organisation needs to conduct a comprehensive evaluation in order to select the optimal APIM*.

Our conclusion is based upon our assessment using our efficacy criteria and the data acquired from the initial use of the ASMSA Methodology and also data acquired from two retrospective case studies.

Our initial theory on methodological efficacy is founded upon three explanations as a result of our data analysis. We found that an organisation should conduct a comprehensive evaluation when the circumstances surrounding the application context necessitates that its IS programme needs to:

- establish objectives and requirements for an APIM in order to evaluate a range of candidate APIMs;
- employ repeatable systematic processes in order to reduce reliance on the capabilities of discipline experts; and/or
- produce an audit trail of the programme's activities which may be used as evidence to justify the APIM selected.

We believe, however, that further research will reveal additional explanations. We also established in our Corporation X 2FA Project Case Study that the use of our systematic methodology appears to engender confidence in the final decision because of the structure and the rigour enforced by a systematic methodology with its well-defined processes.

In contrast, from our cross-case analysis of our data sets from our two retrospective case studies, we ascertained that an expert-led approach is efficacious when the characteristics of the situation, classified as a federated governance framework type, are such that:

- a programme determines that there is an obvious optimal APIM for the application context and there is no need to establish stakeholders' objectives and requirements for the APIM or consider alternative solutions; and
- a programme's decision-making on deploying an APIM relies solely on the capabilities of discipline experts and their recommendations.

Additionally, we ascertained that an iterative development approach is efficacious when the characteristics of the situation, classified as an heterogeneous framework type, are such that:

- there are demands on a programme to introduce an APIM rapidly; and

- the objectives and requirements for an APIM have not been articulated by the programme.

We conclude that a systematic methodology may not be efficacious when the characteristics of the situation, irrespective of governance framework type, are such that an organisation does not need to carry out a comprehensive evaluation because there is an apparent obvious optimal APIM. Therefore, there appears to be no valid reason for organisations to establish stakeholders' objectives and requirements in order to evaluate a range of candidate APIMs. Additionally, our data suggests that a programme which requires a flexible and rapid approach to decision-making on an APIM, relying on the capabilities of discipline experts rather than repeatable methodological processes, should not utilise a systematic methodology.

We found, however, that the methodological deficiencies identified in the data of our two retrospective case studies do not support Siponen's argument [266] that InfoSec tools for selecting APIMs should be rigorously developed in alignment with practices. Our retrospective case study data suggests that while expert-led and iterative deployment approaches offer flexibility to a programme, the practices and processes pursued by discipline experts were not documented and, thus, would be difficult to repeat. The methodological deficiencies identified in our two retrospective case studies also suggest that a systematic methodology may enhance the efficacy of current approaches by introducing structure into the approaches' processes.

We conclude, however, that a comprehensive evaluation, utilising a systematic methodology, which produces documented stakeholders' objectives and requirements for an APIM assists efforts to ascertain whether an APIM is *optimal* for its application context. Conversely, the absence of stakeholders' objectives and requirements for an APIM hampers such assessments because there is an absence of defined utility metrics upon which to conduct an evaluation of a deployed APIM.

We regard our claim of making an original contribution to the body of knowledge with a fair degree of scepticism. Nevertheless, we believe that while our contributions in regard to this specific research question are modest, they do represent an initial venture towards the understanding of a complex phenomenon. We adopt a cautious stance in respect of creating an initial theory on the extent of a systematic methodology's efficacy to select the optimal APIM for an application context due to the boundaries on our research efforts. Moreover, the limitations of our results from the single use of the ASMSA Methodology and our incomplete

efficacy assessment places constraints on the creation of our initial theory.

Therefore, our conclusions and our tentative theory are formulated cognisant of the limitations of our empirical research, the efficacy of the ASMSA Methodology, and the data acquired from our three case studies.

9.2 Limitations of our Research Efforts

While we have addressed our research problem by investigating the extent of a systematic methodology's efficacy to select the optimal APIM for a given application context, there are limitations of our research efforts which impact our results and conclusions. The limitations identified relate to the access to sensitive data, the absence of relevant data, the incomplete usage of the ASMSA Methodology in the Corporation X 2FA Project Case Study, our case study sampling strategy, the influence of the problem-solver variable, and the restrictions of the case study research methodology.

Although we have established an initial theory on the efficacy of a systematic methodology, we conclude that it would be unwise to make any claims of generalisability due to the limitations of our research efforts.

9.2.1 Access to Sensitive Data

Organisational control on the release of sensitive data was a major consideration in the selection of our three case studies. These control restrictions became ever more apparent during the progress of our research, particularly the importance on acquiring data regarding the reliability and usability of deployed APIMs.

The availability of data from the three case studies played a significant part in our efforts to validate our identified factors for evaluating APIMs and also to assess the optimality of the deployed APIM. We recognised that it was necessary to gain an understanding of the application context, which would not only influence data gathered from using the systematic methodology but, most importantly, affect the observed outcomes.

The data acquired from the two retrospective case studies were used to validate factors located in the literature and, most importantly, to identify the proficiencies and deficiencies of current approaches. These two cases did not provide an opportunity to use our systematic

methodology as an *intervention mechanism*, mainly because the selection of the respective APIMs had already been made by stakeholders. These case studies were beneficial in acquiring data on approaches pursued by programmes and the identification of methodological proficiencies and deficiencies by discipline expert practitioners.

Our strategy to ascertain that a factor was evaluated, e.g. budget, without the need to obtain the exact amount assisted our efforts to validate our factors. There may be other strategies which may acquire adequate data for research purposes; however, organisations may be reluctant to reveal sensitive information about the severity and costs associated with security breaches caused by a malfunctioning or compromised APIM.

Overcoming the barriers relating to organisations' sensitivity in releasing data in respect of the vulnerabilities and issues surrounding a deployed APIMs is crucial to ascertain whether the selected APIM is indeed optimal for a given application context.

9.2.2 Absence of Relevant Data

Crucially, we found that organisations do not use metrics upon which to conduct an assessment of the utility of a deployed APIM. Equally, in the absence of defined utility metrics organisations do not generate relevant data for assessment purposes.

Organisations in our case studies appeared to analyse data that is readily available rather than collect the relevant data in order to assess it against predefined utility assessment criteria. Consequently, our methodological efficacy assessment was incomplete because we were unable to gather the relevant data for these application contexts in order to determine the accuracy of the respective approaches to determine the optimal APIM.

In the absence of the relevant data in the Corporation X 2FA Project Case Study, as discussed in Section 8.6.3, our assessment of our systematic methodology's efficacy, in terms of its accuracy to select the optimal APIM, was incomplete. Similarly, we were unable to complete an assessment of the approaches pursued by the programmes in our two retrospective case studies due to the absence of stipulated utility metrics and also the absence of relevant data. We acknowledge, therefore, that further research is necessary to assess the efficacy, particularly the accuracy, of a systematic methodology (and of other approaches) on the basis that the relevant data on the deployed APIM can be acquired from the application context.

Irrespective of the methodology pursued, our research highlights the need for organisations to

introduce policies to define their utility metrics for deployed APIMs and to acquire relevant data in order to ascertain whether the deployed APIM is optimal. Current practices are limited in the extent to which organisations can conduct such evaluations due to incomplete data sets.

We have incorporated effectiveness and efficiency factors, together with relevant criteria questions into the ASMSA Methodology to assist stakeholders to define pertinent utility metrics for their application context. We have also produced a criterion to measure a methodology's accuracy in determining the optimal APIM.

We conclude that the absence of defined utility metrics and the relevant data generated from the use of APIMs in practice makes empirical research to understand the efficacy of different methodologies problematic.

9.2.3 Incomplete Usage of the ASMSA Methodology

The initial use of the ASMSA Methodology with the Corporation X 2FA Project Case Study enabled us to identify some of the circumstances in which a systematic methodology appears to be efficacious.

Our conclusions regarding methodological efficacy can only be cautious because the Corporation X 2FA Project did not use the ASMSA Methodology in its entirety. We did not foresee the changes of project responsibility in Corporation X, which had an impact on the use of the ASMSA Methodology in this case study. We were, however, ever conscious of the risks of conducting such empirical research, cognisant of Silverman's warnings [265] of employing a participative research methodology.

We believe that the complete use of our ASMSA Methodology in a real-world situation should provide further understandings on the efficacy of systematic methodologies to select the optimal APIM for a given application context.

9.2.4 Case Study Theoretical Sampling Strategy

We conclude from our research, but we do not prove irrefutably, that a systematic methodology is reasonably efficacious for selecting the optimal APIM, when applied to the *APIM enterprise governance framework type*, as defined in Section 2.4.4. Our conclusions on

methodological efficacy and initial theory may, however, not apply to all types of application contexts.

We designated the Corporation X 2FA Project Case Study as an APIM enterprise governance framework type. While we selected other case studies which were classified as federated and heterogeneous governance framework types in line with our case study sampling strategy stated in Section 4.1.9.1, our results show that our case study theoretical sampling strategy was defective.

Our theoretical case study sampling strategy, based upon governance framework types, appeared to have had a negligible impact on our methodological efficacy findings. From our research efforts we consider that a future case study theoretical sampling strategy should be based upon the characteristics surrounding the application context.

We conclude that further research is required using our ASMSA Methodology to establish the extent of its efficacy when the characteristics of the application context are considered to be well-structured or ill-structured situations. We believe that this sampling strategy may yield the relevant data to further develop the generalisation of our initial theory on methodological efficacy.

From using our systematic methodology, in these differing situations, the inquiry should aim not only to identify the circumstances when the methodology is efficacious but also explanations to support claims of efficacy.

9.2.5 Impact of the Problem-Solver Variable

While we have begun to address our methodological efficacy research problem we concede that discipline experts' skills and knowledge and their practices may influence the use of a methodology.

Jayaratna's NIMSAD framework, shown in Figure 8.1 on page 319, identifies the problem situation, the problem solving process and the intended problem-solver as the three main variables for assessing a methodology. Our research concentrated upon the efficacy of the systematic methodology as our main unit of analysis; however, we acknowledge that the effects of the problem-solver variable should not be ignored.

The knowledge, skills and competencies of the discipline experts and the extent to which

their assessments influenced the selection of the APIM, irrespective of approach pursued, was a recurring issue encountered throughout our research. Fléchais et al. recognises [102] the importance of the facilitator's knowledge when utilising AEGIS approach and the training required to use that methodological tool. As we recognised in Section 8.7.2, there may be advantages in amalgamating the skills and knowledge of identity management specialists and channelling those capabilities into formalised systematic processes.

We ascertained in our Corporation X 2FA Project Case Study that a discipline expert practitioner is required to use the ASMSA Methodology because it relies upon the skills and capabilities of discipline experts to interpret the criteria questions against the acquired subject data from the application context. The results from our single use of the ASMSA Methodology, in the Corporation X 2FA Project Case Study, provides preliminary evidence on the nature of problem-solver's skills and capabilities required to use our systematic methodology.

We found from our analysis of data from our two retrospective case studies that discipline expert-led approaches possess methodological deficiencies. Our retrospective case study data, however, suggests that discipline experts may benefit from improving their practices by using tools to manage the large volumes of acquired data during a programme. These tools would assist them in evaluating complex interrelated factors in order to select the optimal APIM.

We conclude that further research is needed to understand discipline experts' skills and their practices and how, as a problem-solver, they may influence the efficacy of a systematic methodology.

9.2.6 Boundaries of the Case Study Research Methodology

This section discusses the issues encountered during our use of the case study research methodology and identifies the restrictions imposed on our efforts to address our research problem.

We defend our choice of the case study research methodology despite the difficulties encountered in obtaining formal consent from organisations and commitment from individuals in the first instance to participate in our research. Introducing the criterion that the cases were to be of similar mechanism type, e.g. facial biometric system, would have restricted our case study options and would have contradicted our theoretical sampling strategy of researching

cases from each of the governance framework types, as defined in Section 2.4.4.

Investigating the same type of problem, in different case studies, may enhance cross-case analysis by removing the variables associated with the application context type. Conversely, investigating different automated identification problems may ensure the acquisition of a rich data set because of the diversity offered by each case study.

From our research efforts we discovered that it is imperative to gain consent to access sensitive data otherwise partial data sets may impede research efforts to understand the efficacy of different approaches to select an APIM. Equally, the relevant data needs to be generated by organisations in order to assess the utility of a deployed APIM.

We recommend that further empirical research involving the use of our ASMSA Methodology should not use the case study research methodology. We believe that the action research methodology is appropriate to acquire relevant data relating to methodological efficacy. The risks of using action research methodology, however, warrants the formulation of contingency arrangements to minimise deleterious impacts upon the research implementation plan should unexpected events occur or the objectives of the research become blurred to the researcher or organisation.

We also recommend, from our research experiences, that it is vital to consider the issues surrounding empirical inquiry thoroughly and design the research protocols meticulously, given the importance of gaining access to sensitive data.

9.3 Recommendations for Further Research

Following our conclusions and identified limitations, we now provide three main recommendations on further research avenues to improve the understanding of the efficacy of methodologies to select the optimal APIM for a given application context.

9.3.1 Recommended Minimum List of Factors

From our efforts to identify and validate the factors for evaluating an APIM we believe that future research should focus on establishing a recommended minimum list of factors for evaluating APIMs.

Our results from using the ASMSA Methodology in a single application context suggests that there is a need for further empirical research to identify other pertinent factors in order to establish such a recommended minimum list. Also, as we proposed in Section 7.3.3 and Section 8.4.2.4, that future inquiry should use the action research methodology so that the researcher, from their direct participation, may gain insights into the complexity of an IS programme with its underlying stakeholder's motivations, its discipline experts' practices and its methods used to select the optimal APIM.

We believe that research effort to establish a recommended minimum list of factors for evaluating APIMs would be a reasonable and worthy theoretical aim which could also be beneficial to organisations by informing practice and policy.

9.3.2 Enhancement of ASMSA Methodology

We conclude, based the results of the inaugural use of the ASMSA Methodology, that our methodology needs to be enhanced and that the ASMSA Decision Support System (ASMSA-DSS) requires refinement.

We acknowledge that some of our criteria questions, factor labels and factor explanations need enhancement based upon the results of their use in the Corporation X Case Study. Firstly, we need to generalise the phrasing of several criteria questions so as to make them relevant to all types of application context. Secondly, we need to improve the clarity of each criterion question to enable the methodology user to acquire the relevant data. Thirdly, although we did not originally plan to create an explanation for each factor, we consider that many factors' explanations should be more precise. The aim of this last improvement is to clarify why the factor should be evaluated in order to acquire the relevant subject data, from the application context's primary data, in order to answer the associated criterion question.

We believe that the ASMSA Methodology provides a reasonable methodological foundation upon which to conduct evaluations in the real-world which could generate relevant data to assist with the refinement of our methodology. Similarly, we believe that use of the ASMSA-DSS, as a tool, could assist organisations with the selection of an APIM for an application context in the real-world. We also believe that the use of the ASMSA-DSS by other discipline expert practitioners in ill-structured situations may generate relevant data to enable us to refine the functionality, and the usability, of our decision support tool.

9.3.3 Efficacy of Alternative Methodologies

We believe that in the future some of the commercial methodologies to select APIMs may become publicly available and other methodologies on selecting APIM may be published enabling them to be scientifically reviewed.

We believe that further research should concentrate on the development of other APIM selection methodologies so that theoretical comparisons on methodological efficacy may be conducted. We recognise the need to use the ASMSA Methodology in alternative application contexts in order to develop our initial theory on a systematic methodology's efficacy. We believe, however, that the use of another approach used in parallel in the same investigation is unlikely to be acceptable to an organisation and such a research strategy may be impractical.

As we assumed in Section 1.6, that there are impracticalities of comparing two methodologies simultaneously in the real-world. Alternative empirical research designs need to be considered sagaciously in order to gain further understandings regarding methodological efficacy. The opportunities, however, to investigate methodological efficacy in the real-world may be limited. We conclude, therefore, that theoretical comparisons of methodological efficacy have the potential to contribute further understanding to the body of knowledge.

Innovations in identification technologies continue unabated, ever widening the diversity of identification systems and authentication systems and their configurations. In the meantime, we anticipate that the scrutiny of current approaches will intensify as governments, businesses and societies increasingly depend on effective and efficient systems for the automated identification of persons.

We have established a systematic methodology and we believe that comparable methodologies will be developed in order to assist organisations' discipline experts with the complexities of evaluating and selecting APIMs. We believe that it is essential to further understanding of the extent of these methodologies' efficacy and the circumstances which favour their usage.

Appendix A – Evaluation Themes and Factors Identified (Stage A)

This appendix contains 18 evaluation theme tables relating to the factors for evaluating an APIM, which we identified from our review of the literature, as at Stage A of our factor evaluation effort, representing Step 3 of our Research Implementation Plan.

We assign an identifier to a factor, e.g. A.1.1. (denoting stage created, evaluation theme and factor reference number) to enable each factor and its criterion question to be tracked through each subsequent validation.

The tables in this appendix contain the following evaluation themes: The tables in this appendix contain the following evaluation themes:

Table A.1 Strategic Issues Evaluation Theme;

Table A.2 Risks Assessment Evaluation Theme;

Table A.3 Social Acceptability Evaluation Theme;

Table A.4 Risks Controls Evaluation Theme;

Table A.5 Business Case Evaluation Theme;

Table A.6 Functionality Evaluation Theme;

Table A.7 Community and Usability Evaluation Theme;

Table A.8 Privacy Compliance Evaluation Theme;

Table A.9 Credential Registration Evaluation Theme;

Table A.10 Controls' Performance Evaluation Theme;

Table A.11 Assurance Requirements Evaluation Theme;

Table A.12 Security Architecture Evaluation Theme;

Table A.13 Identifier Credential Evaluation Theme;

Table A.14 Reliability Testing Evaluation Theme;

Table A.15 Usability Testing Evaluation Theme;

Table A.16 Technology Evaluation Theme;

Table A.17 User Accessibility Evaluation Theme; and

Table A.18 Owners' Costs Evaluation Theme Evaluation Theme.

Factors	**Criteria Questions**	**Source/Identifier**
Security Rationale	What are the business objectives of the system owner entity in respect of the considered need to protect assets or instigate a change in protection? Is this aim to review the security of assets the result of a risk assessment or the impact from a major security incident leading to the formation of a change programme for the APIM?	[252] (A.1.1.)
Security Benefits	Will the APIM be used to protect data and/or assets belonging to one or many entities? What are the types of entities, e.g. corporate or government, involved with the application context? Has consultation with entities been made with reference to a state or corporate policy for the appropriate security assurance?	[118] (A.1.2.)
Costs Forecasted	What are the system owner's estimated programme costs for the APIM? Have these forecasts been based upon similar protection needs over a specified period? Do estimated costs draw on information from similar implementations, from initial system designs, from vendors' estimates or from suppliers' tender submissions?	[238] (A.1.3.)
Political Considerations	What political or economic matters may hinder or support organisational change? How does this impact upon the APIM selection?	[252] (A.1.4.)
Corporate Dynamics	What commercial or competitive or organisational issues could hinder or support the entity's change programme (fraud, industry regulation alignment, staff privacy, data access etc.)? How do these issues affect entities, e.g. profitability?	[118] (A.1.5.)
Regulatory Constraints	What legislation will affect the data that the entity may store for the intended user population, e.g. Data Protection Acts, Privacy Laws?	[56] (A.1.6.)
Legal Imperatives	What legal issues could hinder or support a change programme (privacy, data access etc.) to deploy an APIM?	[56] (A.1.7)
Expert Opinion	Has the entity's application been discussed with knowledgeable and independent members of respected information security professional groups?	[295] (A.1.8.)

Table A.1: Strategic Issues Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Attack and Compromise Probability	What is the likelihood of a compromise event occurring? Does this projection incorporate an analysis of historical attacks and changes in threat intelligence?	[171] (A.2.1.)
Impact Value Rating	What is the estimated impact value or severity score on the assets being protected if stolen or destroyed or modified? Does this estimate include losses, administrative costs as a result of a compromise and the indirect financial consequences of the entity's reputation being adversely affected?	[171] (A.2.2.)
Vulnerabilities	What are the known exploitable weaknesses in existing (or potentially in new) operations or APIMs that protect assets including technology, people and process controls and their integration?	[247] (A.2.3.)
Assurance Effectiveness	What evidence is required to demonstrate the APIM's ability to meet the security assurance requirements set?	[247] (A.2.4.)
Environment Characteristics	Where will the APIM operate? Will it be in public spaces, physically controlled environments, restricted networks or open networks? What are the physical conditions, devices, artefacts or other intelligent processing resources available? Does this description also include physical and social measures or conditions that limit or restrict access to information resources?	[295] (A.2.5.)
Operational Context	What are the operational circumstances where the user is engaged with the APIM to perform tasks to access an asset and/or service? Who are the parties involved and what role do they perform with respect to the transactions or access to the asset? For the APIM's owner will the parties involved be employees (private), business partners/customers (commercially confidential), state citizens (private) or a combination of these entities in a heterogeneous application?	[95] (A.2.6.)
Threat Motivation	What are the underlying stimuli or goals that may lead to attacks to compromise the APIM? Do these motives include financial fraud, corporate espionage, intellectual challenge, error, state espionage or terrorism?	[95] (A.2.7.)
Risks Mitigation	How does the organisation want to address the risks identified to provide access or entitlement to the intended user population? Do the options for risk mitigation include risk alleviation, e.g. by introducing or revising controls; risk transference, e.g. by taking out insurance against potential losses; risk avoidance, e.g. by terminating, user access or limiting some of the functionality; risk assumption, e.g. by performing due diligence in formally accepting the risks and monitoring the exposure or impact levels? Do the organisation's operating rules mandate an agreed approach to Risk Management within a cyclical framework to evaluate assets and their protection periodically?	[171] (A.2.8.)

Table A.2: Risks Assessment Evaluation Theme

Factors	Criteria Questions	Source/Identifier
User Population Relationship	What is the relationship of the user to the APIM's owner, e.g. service provider, employer etc and any intermediaries e.g. infrastructure provider?	[1] (A.3.1.)
User Obligations	Will potential users be required to provide their consent or acceptance to responsibilities or liabilities? To what extent do these obligations negate the benefits of the customer proposition for potential users?	[1] (A.3.2.)
Social Attitudes	What is the attitude of the intended user communities towards APIMs that address similar business or social problems? What are the social problems with these existing APIMs? To what degree does the existing method or intended way of identifying users cause difficulties? Do these issues include user perceptions which may restrict the use of an APIM to capturing biometric data that may be private and believed to be intrusive? Would an APIM be, or be perceived as, endangering health, safety or welfare (including Inclusivity) of the user? Has consideration been given to the following issues which may influence the options for an APIM: user privacy concerns; user/public perception of intrusiveness; target population characteristics including physiological, cognitive and behavioural traits; and user difficulties, e.g. disabilities in capturing specific types of biometric data or use of devices or artefacts?	[295] (A.3.3.)
Community Membership	Will the system and APIM be openly available to all parties? Are there membership restrictions or conditions for the intended user community?	[295] (A.3.4.)
Users' Trust	To what extent will the user community firmly believe in the competency of the APIM's system owner to act dependably, securely and reliably within the specified operational context?	[250] (A.3.5.)
Users' Costs	What are the potential costs and/or effort for each party involved in their use of the APIM that includes hardware and software, its compatibility with the user's processes and the need for supporting infrastructure?	[250] (A.3.6.)

Table A.3: Social Acceptability Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Policy Implementation	What is the method chosen to achieve the entity's change programme's objectives? Does the policy include the minimising of risks by introducing or revising controls given the operation context and strategic considerations?	[300] (A.4.1.)
Risks	What are the entity's (and possibly user) risks that are to be controlled (potentially minimised) by the APIM?	[171] (A.4.2.)
Budget	What funds have been allocated by the organisation to minimise unacceptable risks? Do the aims include countermeasures to reduce direct financial losses and associated administrative costs as a result of a personal identification mechanism compromise, if sole or main control mechanism?	[300] (A.4.3.)
Security Policy	What are the aims of the intended courses of action to protect information assets and resources ? Does this protection or change in protection fulfil a stated business target or goal?	[300] (A.4.4.)
Privacy Policy	What are the aims of the intended courses of action to protect user's private data? Does the protection or change in protection of a user's personal information fulfil a stated goal?	[300] (A.4.5.)

Table A.4: Risks Controls Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Business Problem	Is the personal identification problem fully understood and defined in terms of requirements and not solutions? To what degree are the existing mechanisms actually effective?	[295] (A.5.1.)
Business Case Sponsorship	Is the requirements analysis supported with a business case and justification for expenditure?	[295] (A.5.2.)
Requirements Gathering Methodology	How will the requirements for the APIM be established? Will this process involve prototyping or will they be established through formal requirements capturing procedures? Is the choice governed by the organisation's preferred system development methodology or restricted by tendering processes? How will the users be involved in stating their requirements (if at all)?	[103] (A.5.3.)
Constraints	What external or internal organisational issues (employee rights, privacy, etc.) could hinder a change programme or project's efforts to introduce or revise an APIM?	[295] (A.5.4.)
Standards	What standards impact the choice of an APIM, its use and or processes? Which information Security controls for user authentication, the use of cryptography or biometrics are required to be complied with?	[238] (A.5.5.)
Signal Data Exchange	Will there be a need to exchange user signal data between other organisations with similar mechanisms utilising the same user signal data or human characteristic? Do interoperability specifications exist?	[98] (A.5.6.)
External Performance Benchmarks	Have there been any performance or security tests or evaluations of biometric or authentication mechanisms similar to the intended application context and business problem? What are the learning outcomes?	[295] (A.5.7.)

Table A.5: Business Case Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Positive or Negative Identification	Will the APIM be used for positive identification (proving a person is already enrolled) or negative identification (proving a person is not enrolled) or a consolidation of both to meet one or more requirements?	[295] (A.6.1.)
Overt or Covert Identification	Does the requirement entail the user being aware of the APIM? What legal issues and technical consideration apply if the requirement is for a covert APIM?	[295] (A.6.2.)
Credential Identifier	How will the enrolled user be uniquely recognised? Will the user require anonymity? Is there a need for pseudonymity, where the identifier masks the user's true identity?	[247] (A.6.3.)
Alternatives Investigated	Has there been an investigation into the alternatives to the biometric or user authentication mechanisms to address the identification problem? Fundamentally, are biometrics really needed or desirable?	[295] (A.6.4.)
Multiple User Input Signals	If both positive and negative identification are required, is there a requirement to use same authentication or identification data, or is there potential for the combining of two or more separate user input signals, e.g. fingerprint and voice, face and voice, personal identification number, digital certificates and passwords etc?	[247] (A.6.5.)
Task Dynamics	Is the APIM to operate as a sub-process for the user as part of an overall task, e.g. cash machine transaction, or does it constitute the entire task, e.g. inspecting an ePassport? Where is the position of the identification process within the interaction to fulfil a user's task?	[103] (A.6.6.)
User Supervision	Is the user's interaction with the biometric device or other input device watched by authorised personnel or is it self-service and unobserved?	[295] (A.6.7.)
Environmental Control	To what degree does the operating environments, including remote sites, enable the APIM's owners (and user population) to control the technology processes and, where relevant, to monitor user behaviour?	[65] (A.6.8.)
Compromise Scenarios	What types of deceptive user scenarios can be foreseen?	[63] (A.6.9.)

Table A.6: Functionality Evaluation Theme

Factors	Criteria Questions	Source/Identifier
User Attitude	What is known about the user population and the entities that operate the APIM? Has the user population been surveyed to determine their attitude towards using a biometric or authentication mechanism? Does a strong negative response indicate a need to reformulate plans or possibly the instigation of a proactive education programme?	[295] (A.7.1.)
User Population Education	Is the user population likely to resist educational material supplied to assist in the introduction of a new or revised APIM? Has consideration been given to educating the users to allay their doubts/fears about utilizing a specific authentication or biometric mechanism?	[295] (A.7.2.)
Multiplicity Impact	What are the number and similarity in operation to other APIMs used by the intended user population, i.e. multiple credentials (e.g. User Accounts and passwords)? Does the APIM require differentiation from other similar APIMs to avoid possible user confusion?	[8] (A.7.3.)
Population Traits	Does the majority of the target user population have characteristics that could pose disadvantages or advantages for the possible APIM design options being considered? What is the particular mix of users with respect to impact upon the success of any APIM, in terms of: population demographics–age, ethnic origin, gender, occupation; user physiology–facial hair, disabilities, height, iris colour, skin tone; user behaviour–dialect accent, expression, intonation, facial expressions, written language, movement pose, prior activity, stress, tension or mood; and user appearance–bandages, clothing, contact lenses, cosmetics, glasses, hairstyle, hair-colour, rings and tattoos?	[295] (A.7.4.)
Task Sequence	What is the position of the APIM function within the user's task to achieve the desired goal? What impact could the potential APIM have upon the user in achieving the overall task including speed and accuracy? What outcomes need to be avoided from poor HCI design?	[329] (A.7.5.)
User Technical Expertise	To what extent would the user population have the capacity to acquire specific skills, if required?	[327] (A.7.6.)
Frequency of Use	Will the expected usage frequency or patterns of APIM usage lead to users becoming habituated or remaining non-habituated?	[295] (A.7.7.)
Trust Between Subjects	Does trust between the APIM's owner or organisation and the various supporting parties exist and could that lead (potentially) to a degree of reliance for users to operate the APIM as intended?	[1] (A.7.8.)
Impact Upon Users	What are the likely consequences to the user if the APIM failed to detect unauthorised access relating to a specific user or if failed to verify or identify an authorised user?	[1] (A.7.9.)
Security Motivation of Authorised Users	What incentives could be employed to encourage appropriate use of the APIM? What are the possible disadvantages or liabilities that would apply if authorised users were found or proven to be negligent?	[250] (A.7.10.)
User Cooperation	Is it correct to assume that authorised users will cooperate fully?	[295] (A.7.11.)

Table A.7: Community and Usability Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Privacy Laws and Privacy Policies	What directives, international conventions, international and local laws and regulations are applicable to the private data that could impact the requirements for an APIM? Is the credential to indicate the users name? Are there guidelines on what is considered to be private data and how it is to be protected?	[247] (A.8.1.)
Privacy Laws Compliance	Has an individual within the organisation, possibly in its corporate governance function, been assigned responsibility to ensure privacy compliance?	[295] (A.8.2.)
Privacy Impact Assessment	Has an impact assessment been made and documented in respect of the privacy issues that may impinge upon the requirements for the APIM?	[283] (A.8.3.)
Privacy Asset Register	What processes need to be put into place to write, publish, and maintain a clear and comprehensive document listing the types of information that may be collected, e.g. transactional information, personal data in an identifiable form? Does the document state the purpose of data collection, the data that may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency? Are applicants to be provided full disclosure of the intended uses of the credential and the related privacy implications?	[98] (A.8.4.)
Privacy Asset Appeals Procedure	What appeals procedures are to be maintained for those applicants who are denied a credential or for those authorised users whose credentials are revoked without explanation?	[98] (A.8.5.)
Privacy Asset Access Control	What processes are to be in place to ensure that only personnel with a legitimate need to access the privacy information, used within the APIM, are authorised? Does this safeguard include handling disputes relating to personal data stored and data maintained for purposes of applicant registration and credential issuance?	[247] (A.8.6.)
Privacy Asset Compromise	What processes are required to be in place to coordinate with approved entity, authority or agency officials to define consequences for the APIM or other systems violating privacy policies?	[247] (A.8.7.)
Privacy Assurance	What assurance is required to show that the technologies used in the implementation of the APIM allow for continuous auditing of compliance within stated privacy policies and practices governing the collection, use, and distribution of private information?	[98] (A.8.8.)
Privacy Security Controls	What are the security controls to be applied to accomplish privacy goals, where applicable? Is the management of the private data under the immediate control of the APIM owner or the individual? What are the technologies and infrastructures available to support these requirements?	[98] (A.8.9.)
Privacy Security Controls Erosion	What assurance is required to show that the technologies and controls used to implement the APIM does not erode privacy protections relating to the use, collection, and disclosure of private data in an identifiable form? Does this requirement include the protection against unauthorised access to users' private data or credential data stored on artefacts?	[247] (A.8.10.)

Table A.8: Privacy Compliance Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Identity Approval/ Authorisation	What organisations have been approved to supply an identifier or credential or provide authorisation against identity evidence submitted by the potential user, i.e. applicant seeking to obtain a user account and a credential?	[98] (A.9.1.)
Identity Clearance	How will the identity knowledge or documentary evidence presented by the user be verified?	[98] (A.9.2.)
Unacceptable Identity Evidence	What are the unacceptable identity source documents as determined by policy and visual/electronic identity inspection procedures?	[98] (A.9.3.)
Unacceptable Users	What does the policy stipulate in determining acceptable applicants as potential users?	[98] (A.9.4.)
Identity Proofing Rules	What are the identity registration processes and will interpretation guidance be made available for operatives?	[98] (A.9.5.)
Approved Authorities	Which entities are to receive delegated powers to approve the issuance of an identifier and a credential to an applicant?	[98] (A.9.6.)
Identity Proofing and Registration	What is the process to examine source identity evidence furnished by the applicant before issuing or using the APIM's credential?	[98] (A.9.7.)
Remote or Local Application	Is the applicant to appear in-person as part of the registration process or is this process to be undertaken remotely with other controls?	[98] (A.9.8.)
Acceptable Identity Evidence Sources	What are the acceptable identity source documents as determined by policy? During identity proving, what evidence is the applicant required to provide in terms of forms of identity evidence in original form? Will operatives and applicants be provided with a list of acceptable issuing bodies identity source documents and the means to recognise or verify the authenticity of identity documents presented or identity data gathered?	[98] (A.9.9.)
Identity Proofing Compromise	Do risks dictate that the identity proving, registration and issuance process need to adhere to the principle of separation of duties to ensure that no single administrator has the capability to issue an APIM identifier or credential without the authorised cooperation of another authorised administrator?	[98] (A.9.10.)
Identity Proofing and Registration Accreditation	Does the identity proofing and registration processes used to verify the claimed identity of the applicant require accreditation?	[98] (A.9.11.)
Accreditation Processes Applicability	Which entities do the identity proofing and registration processes accreditation rules apply to?	[98] (A.9.12.)
Approved Processes Adoption	What authorisation is required before the adoption and use of approved identity proofing and registration processes?	[98] (A.9.13.)

Table A.9: Identifier Credential Management Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Operational Ergonomics	Will the APIM operate in consistent conditions or various environments? What are the non-standard conditions which reveal APIM constraints?	[95] (A.10.1.)
User Signal Enrolment	What are the constraints that would determine how the APIM captures the user's initial input signal? Is there an existing user enrolment policy? Is the user required to be present? What other user data, e.g. autobiographical, are required?	[295] (A.10.2.)
Input Signal Tolerations	During operational use, will the APIM be required to automatically flag poor quality signal input data? How much of the input can be reasonably tolerated to be flagged as poor quality data?	[295] (A.10.3.)
Throughput Rates	What are the throughput rate requirements, i.e. timing maximums?	[95] (A.10.4.)
Impostor Pass/ False Alarm	What is the acceptable decision threshold determined by the risks in the application context? How are these rates to be determined?	[177] (A.10.5.)
Impostor Probability	What is the acceptable probability to the entities that an impostor user input signal being accepted at least once in a given number of attempts?	[295] (A.10.6.)
User False Non-match Toleration	How many false non-match errors would the organisation accept and the user population tolerate as acceptable rates for user input signal false acceptance and false rejection?	[57] (A.10.7.)
Multiple Attempts Limit	In the case of a user input signal false non-match how many additional attempts for identification should the user be permitted?	[177] (A.10.8.)
Intervention Rate	What is the tolerable rate for false user input signal non-matches which require intervention by trained staff, if applicable?	[295] (A.10.9.)
Impostor Detection	What is the acceptable probability that a false user input signal match setting being sufficiently low enough to deter deliberate compromise?	[177] (A.10.10.)
Combining Mechanisms	Would the acceptability of user input signal false matches or false acceptances become more palatable to the owner (or possibly the user) by combining two or more user input signals for the operational context?	[177] (A.10.11.)
User Equipment	What are the operational constraints that would determine how an APIM capture the user's input signal during enrolment and live usage?	[15] (A.10.12.)
Enrolment Supervision	Do security policies dictate that the enrolment process needs to be supervised in order to achieve the required user input signal quality?	[295] (A.10.13.)
Maximum Enrolment Time	What is the longest time permitted for successful user input signal enrolment?	[295] (A.10.14.)
Maximum Enrolment Attempts	How many attempts at signal enrolment should the user be allowed?	[295] (A.10.15.)
Alternative Arrangements	Are work-around measures required should a user be unable to provide a valid input signal for enrolment, either temporarily or permanently?	[295] (A.10.16.)
Vendor Support	What type of quality control and statistical evidence are vendors required to offer on the performance of the enrolment and identification processes?	[295] (A.10.17.)
Environment Variance	What are the environmental factors that may affect user input signal enrolment and signal processing during live operation?	[295] (A.10.18.)
Template Protection	Are security controls required to protect the APIM's input signal data, e.g. authentication data, biometric images or template data?	[295] (A.10.19.)
Backwards Compatibility	Is backward compatibility required to separate APIMs in different authorisation domains?	[125] (A.10.20.)
Flexibility	What are the potential factors which may influence stating suitability measurements for the APIM?	[238] (A.10.21.)
Scalability	What scalability is desired for the APIM? Is the user population forecasted to grow significantly during the APIM's projected life?	[125] (A.10.22.)
Upgrade Impact	What are the acceptable disruption, for the APIM owner and its users, if upgrades were to be possible to the APIM?	[295] (A.10.23.)

Table A.10: Controls' Performance Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Attack Protection	What are the likely technology resources and/or social skills that will be used to compromise the APIM (either its entirety or at user level)? Is the APIM required to resist and detect attacks in order to protect information assets? What are experiences of past attacks and does this intelligence suggest changes in potential attacker's motivation? How closely does this assessment align with stated user signal performance to detect or deter an impostor being falsely accepted at least once in a number of attempts?	[313] (A.11.1.)
Operational Quality Assurance	What test data are essential, as evidence, to assure the APIM's design will operate reliably, in line with the performance requirements?	[313] (A.11.2.)
Documentation and Test Data Availability	What information will be made available to evaluators and users, including external or internal designs, to test assurance performance? Does the APIM design documentation need to be kept confidential?	[202] (A.11.3.)
Functional Testing	What is the desired reliability to ensure the APIM implementation functions correctly? Is the implementation to be exposed only to documented attacks and which it is designed to counter? Is the implementation to be tested by external expertise? What are behavioural expectations in response to each attack test on the APIM?	[177] (A.11.4.)
Audit	What audit information is required to fulfil legal obligations and risk management functions? Does the audit information need to include any or all of the following: the number of new biometric records accepted or new credentials issued, amended or revoked; the number of records verified, the number of users the APIM was unable to enrol; the quality measurements for the captured user signal data; the amount of APIM down time; the APIM errors by type; and the average enrolment processing time on a daily, weekly, and monthly basis?	[295] (A.11.5.)
Performance Assessment Methodology	What is the evaluation approach, e.g. Common Criteria Evaluation Methodology, to test and evaluate candidate APIMs' performance in order to make an objective assessment (and repeatable results) based on the test data sets and substantiated results produced?	[63] (A.11.6.)
Assurance Test Regime	What are the tests required to prove the effectiveness of the APIM (holistic and within each component)? What is the test environment in which the evaluation will take place?	[238] (A.11.7.)
Resources Allocated	What funds, personnel and tools will be committed to the change project or programme to design, implement, test, deploy and operate the APIM?	[63] (A.11.8.)

Table A.11: Assurance Requirements Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Identification/ Authentication Model	To what extent does the solution design or vendor proposals meet the requirements for the APIM and have specifications with validated test data been provided? Does the model align with policies and relevant standards? How does it align with the infrastructure that is used to implement the security policy in an organisation? Does it address physical, procedural and IT security controls in a holistic way?	[171] (A.12.1.)
Credential Storage	Does the APIM require the user to possess and use an artefact, e.g. a token, to store or to generate and protect users' signal data?	[125] (A.12.2.)
User Input Signal Storage	Is the user's input signal data stored centrally or stored on an artefact or a combination of both?	[295] (A.12.3.)
Mechanism Processing Location	Will there be a centralised database or distributed storage medium, where a user will be required to carry his/her biometric or authentication data on a portable artefact to allow the APIM to operate universally?	[295] (A.12.4.)
Mechanism Processing Infrastructure	What are the network, systems, devices, software and processes required to support the APIM design? To what degree will the APIM owner have operational control over the components, e.g. the Internet, browser, or public key infrastructure, devices, to support the processing locations?	[295] (A.12.5.)
Processing Protection	How will the user input signal captured be protected during acquisition for either local processing or extracted and communicated for remote processing? How will the result be communicated to users and what preventative measures protect against compromising the result notified?	[295] (A.12.6.)
Alternative Identifier Types	Will a biometric feature or a name or code act as a unique identifier? Is that feature compatible, in terms of degradation, with the expected lifetime of the authorised access or recognition requirement?	[247] (A.12.7.)
Biometric Modality Selection	Where user input signals are based upon biometric features are all the elements, e.g. biometric modality template file size and storage medium elucidated in the detailed design?	[295] (A.12.8.)
Knowledge Data Selection	Where user input signals are knowledge based are all the elements, e.g. data composition and user's cognitive actions, elucidated in the detailed design?	[250] (A.12.9.)
Mechanism User Maintenance	Does the detailed design describe the tasks to support the APIM? How are users added or deleted from the APIM? How are user's data maintained? How is a user's claimed identity verified?	[295] (A.12.10.)
Maintenance Effort	How easy and often is it necessary to change or reissue authentication data, keys, tokens, and software or recapture of biometric samples?	[295] (A.12.11.)
Associated User Data	What associated user data are required to be stored, e.g. autobiographical data, with the identifier and identification data?	[250] (A.12.12.)
Signal Processing	Does the detailed design describe the APIM's functions, e.g. capturing the user's input signal, and how data are protected during all processes?	[95] (A.12.13.)
Combined User Input Signals	Does the design use multiple input signals or templates or data types related to each identifier? Will the user generate data from an artefact or token generation device or remote system?	[95] (A.12.14.)
Costs Influences	What factors in the security architecture are most likely to increase or decrease costs of the APIM?	[95] (A.12.15.)
Database Contingency	Is database backed-up and restore required if the identifiers and user template or data for the APIM are lost, amended or destroyed?	[171] (A.12.16.)
User Training Need	Is user interaction with the APIM intuitive or based on familiar designs? Will users require training on how to use the APIM, as designed?	[9] (A.12.17.)
Performance Tests	Have there been any performance or evaluations of the APIM or similar mechanisms in a comparable application context?	[194] (A.12.18.)
Practical Experience	What are the experiences from owners/users/administrators from using this APIM in environment similar to the context application?	[295] (A.12.19.)
Vendor Assessment	What is known about the potential vendors/integrators experience and capabilities for delivering the APIM to the proposed design?	[295] (A.12.20.)

Table A.12: Security Architecture Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Credential Lifetime	What is the intended life of the APIM's identifier, credential and artefacts to provide continued access or entitlement to the information asset?	[98] (A.13.1.)
Credential Authenticity	What are the rules for officials or administrators to undertake credential issuance? Are these tasks automated? Is the verification of identity evidence a separate task undertaken independently during the applicant registration process?	[98] (A.13.2.)
Credential Integrity	What are the rules for officials or administrators to undertake other credential management processes, e.g. issuing replacements or revoking credentials? Are these tasks automated?	[98] (A.13.3.)
Credential Maintenance Process Adoption	What authorisation is required for entities and their officials to adopt and operate credential maintenance processes?	[98] (A.13.4.)
Credential Maintenance Requirements	What are the processes for issuing and maintaining identification credentials, including the processes for revocation and providing justification for credential withdrawal reasons to former users, if necessary?	[98] (A.13.5.)
Credential Delivery Verification	At the time of credential issuance, what are the processes to verify that the person to whom the credential is to be issued (and on whom the background verification was completed) is the same person as the intended applicant/recipient as approved by the authorised organisation during the person's registration?	[98] (A.13.6.)
Credential Use Location	Where will the processing of the initial user input signal to the related credential take place? What are the conditions for normal operational use of the Identifier Credential?	[98] (A.13.7.)
Credential Accreditation	What processes are to be established to issue a credential and/or other related devices to users from approved suppliers whose reliability has been vetted by the APIM owner or agency and so approved or authorised in writing, i.e. accredited?	[98] (A.13.8.)

Table A.13: Identifier Credential Evaluation Theme

Factor	Criteria Questions	Source/Identifier
Sampling Normalisation	Will the APIM use more than one instance of captured user signal or biometric input data to create the enrolment template?	[177] (A.14.1.)
Signal Entropy	Is there sufficient inherent variation or randomness in the user's input signal to avoid candidate identification collisions?	[95] (A.14.2.)
Threshold Performance	Does the accuracy of the APIM comparison results meet the required Impostor Pass/False Alarm decision threshold? What is the impact upon performance from the adjustment of the threshold setting?	[238] (A.14.3.)
Deceit Resistance	What is the difficulty, in terms of knowledge and resources, to synthesise an unauthorised entity of generating valid/correct user input signals?	[177] (A.14.4.)
Artefact Counterfeiting	What is the difficulty, in terms of knowledge and resources, to deceive an APIM by producing a counterfeit copy of an artefact?	[177] (A.14.5.)
Circumvention Susceptibility	What is the difficulty, in terms of knowledge and resources, to circumvent the APIM, without the need to deceive the processing logic?	[177] (A.14.6.)
Identification Time	What is the time to: activate the sensing device; capture user input signals; extract signal parameters; retrieve files and other ancillary processing; compare the input signals against those stored; communicate between the various APIM components; and effect notification of acceptance or rejection or other results? What are the possibilities to shorten the overall processing timescales?	[238] (A.14.7.)
Device Maintainability	What is the probability that an APIM related device will perform its intended function over a specified interval of operation?	[177] (A.14.8.)
Device Interfacing	Are supporting devices and artefacts functioning correctly for their intended purposes in a way that meets the APIM's requirements which prevents them being disabled or the APIM being circumvented? Is the installation to be tamper-evident with physical integrity and use sensors to detect attempts at circumvention or possess similar controls?	[177] (A.14.9.)
Signal Predictability	Is the APIM's signal authentication data sufficiently disguised to prevent strangers, friends and family etc. from determining it?	[250] (A.14.10.)
Signal Abundance	What is the APIM's number of possible user input signal or signal extraction permutations or total key space?	[250] (A.14.11.)
Signal Disclosure	Is the APIM's authentication or key or verification data easy to record or transfer, easily observed at entry or almost impossible to disclose?	[250] (A.14.12.)
Signal Robustness	Does the APIM's signal data capture device withstand various known attacks, e.g. keyboard loggers, brute force attacks, theoretical attacks?	[250] (A.14.13.)
Signal Privacy	Does the APIM's signal data contain the user's private details, e.g. iris? Does the user approve the use of this private data and its protection?	[250] (A.14.14.)
Signal Confidentiality	Is the signal data revealed during entry or transmission, in full, partially or not at all?	[250] (A.14.15.)
Technical Vulnerabilities	What are the known exploitable weaknesses in existing operations (processes, technology and people together with their integration) to protect assets?	[271] (A.14.16.)
Failure to Enrol Rate	Average number of users in the test case that are unable to provide an input signal of sufficient quality for identification or authentication?	[288] (A.14.17.)
Assurance Evidence	What evidence demonstrates the APIM's ability to meet the assurance requirements set?	[57] (A.14.18.)
Average Time of Impostor Try	Time to detect impostor attempts, including repeated tries averaged, regardless of successful verification over all impostor attempts?	[288] (A.14.19.)
Average Time of Verification Try	Time to achieve correct user verification including repeat attempts averaged over all attempts and tests?	[288] (A.14.20.)
Average Number of Impostor Capture Failures	Number of failures in capturing user signal data averaged over all impostors' attempts?	[288] (A.14.21.)
Average Number of Genuine Capture Failures	Number of failures in capturing signal data from genuine subjects averaged over all genuine subjects' attempts?	[288] (A.14.22.)

Table A.14: Reliability Testing Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Interface Use	What data have been generated from the APIM's usability tests? Do the results provide evidence that both the authorised users and the APIM's administrators usage of the APIM's Human Computer Interface, artefacts, tokens or devices' interactions are as intended? Are there identified usability issues which introduce adverse or undesirable user behaviour that may compromise the effectiveness of the APIM?	[288] (A.15.1.)
Convey Security Features	Does the APIM's human computer interface convey the available security features to the user?	[167] (A.15.2.)
Visibility of Mechanism Security Status	Does the APIM's human computer interface have the ability for the user to observe the security status of internal operations?	[167] (A.15.3.)
Intuitive Interface	To what extent is the APIM's human computer interface comforting and naturally easy to learn?	[167] (A.15.4.)
Aesthetic and Minimalist Design	Does the APIM's human computer interface convey or display only relevant security information?	[167] (A.15.5.)
Error Reporting and Assistance	Does the APIM's human computer interface show error messages that are detailed and state, if necessary, where to obtain help?	[167] (A.15.6.)
User Satisfaction	Does the APIM's human computer interface aid the user in having a satisfactory experience with the APIM and other related components?	[288] (A.15.7.)
Depth of Cognitive Processing at Enrolment	Does the user require cursory rehearsal, visual co-ordination, cognitive activity or no effort in order to provide user signal data?	[250] (A.15.8.)
Signal Retrieval Strategy	Is recall of the signal (authentication data) from the user's memory to use the APIM with or without cues or recognition focused? Does the APIM support or prompt the user to recall their input signal data supplied upon enrolment and the procedures for using the APIM's interactive design?	[250] (A.15.9.)
Signal Meaningfulness	Is the user signal used by the APIM system assigned, self-assigned by the user, meaningful to the user or deducible only by the user?	[250] (A.15.10.)
Task Convenience	Is the APIM likely to be operationally acceptable aligning with the user's task or duties? Is the APIM easy to learn within that task? Do the APIM's interaction processes and signal data need to be memorised? Are allowances made for human error or limitations?	[57] (A.15.11.)
User Signal Preference	What is the users' preference for signal type? Is the biometric modality chosen likely to be accepted against other modalities which may be more familiar or less intrusive?	[288] (A.15.12.)
Privacy Impact	Does the use of the APIM affect user's feelings or beliefs?	[57] (A.15.13.)

Table A.15: Usability Testing Evaluation Theme

Factors	Criteria Questions	Source/Identifier
System Resources	What are the computer system and network resources envisioned to support the overall APIM?	[295] (A.16.1.)
Mechanism Anticipated Life	What is the APIM's predicted life expectancy? Will it be designed to allow upgrade or migration or replacement of the APIM? How do these aspects impact upon the choice of using different user input signals or vendor's proposals?	[295] (A.16.2.)
System Functionality	Has full consideration been given to all functions and components to support the APIM? Does this description include: user data collection; user input signal data capture and parameter extraction; data transmission; data translation; signal processing; template or image storage; and user security management features and training information?	[295] (A.16.3.)
Technology Impact	What is the impact of the proposed APIM in terms of hardware, software, personnel and training upon existing infrastructure?	[295] (A.16.4.)
Existing Technologies	Is there a list of the available hardware and software to support the APIM?	[295] (A.16.5.)
Interoperability	Will interoperability of the APIM with other existing, possibly alternative APIMs, in the intended application context be an issue?	[160] (A.16.6.)
Processing Capacity	What is the processing power and media storage needed to support the APIM locally and/or a server at a central location?	[295] (A.16.7.)
Back-up Methods	What are the back-up procedures should the APIM fail totally or partially in resulting in the total or temporary unavailability of all users' signal data?	[295] (A.16.8.)
Criticality of Contingency Plan	Is there an appropriate contingency plan and disaster recovery policy to ensure continued operations in the event of an APIM failure, partially or totally?	[295] (A.16.9.)
Repair Response Times	What are the proposed repair response times and the planned delivery of replacement parts? Is this acceptable to the system owner and the user community?	[295] (A.16.10.)
Roles Assignment	What are the roles and responsibilities for the various parties involved with the APIM? Has an operational role been assigned for a security officer, security operator, an auditor, an administrator, an APIM manager, a standard user, and privileged users?	[295] (A.16.11.)
Personnel Support	Are technical support personnel, or substitutes, critical to the operation of the APIM available?	[15] (A.16.12.)
Continual Training	What are the training requirements for users and the administrators, of the APIM for the initial usage also for ongoing operations?	[15] (A.16.13.)
Device Calibration	Are the user input signal capture devices capable of performing automatic self-diagnostic and calibration tasks continually?	[15] (A.16.14.)
Lockout/ Thresholds Maintenance	How does the APIM support a lockout or threshold for excessive invalid access attempts by authorised users? How are these lockouts and thresholds changed securely?	[295] (A.16.15.)
Subject Supervision	What competencies and involvement are acceptable for administrators to supervise subject enrolment?	[295] (A.16.16.)
Enrolment Process Support	Is it required that a supervisor has the ability to intervene in the enrolment process to improve the quality of the user's signals?	[295] (A.16.17.)
Tamper Protection	Are there tamper deterrent and tamper indicative technologies available to notify errors in the APIM?	[295] (A.16.18.)
Template Update Notifications	Will the audit trail flag changes to data relating to an enrolled template; or the template itself; or any changes in user access rights as safeguards to detect unauthorised tampering?	[295] (A.16.19.)
Data Protection	What technological safeguards have been implemented to safeguard the integrity and confidentiality of the user signal and privacy data the APIM captures, stores, processes and transmits?	[295] (A.16.20.)

Table A.16: Technology Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Operational Enablers	Does the user require any special technical expertise, particular artefacts or devices, special software or hardware devices to use or access the APIM?	[250] (A.17.1.)
Inclusivity – Disabilities	Are there any sensory, physical, cognitive skills that would prohibit or restrict impaired users from using the APIM as designed?	[250] (A.17.2.)
Device Usage Effort	What is the time and effort spent in fulfilling these following tasks: –application and enrolment processes –authentication processes –replacement of authentication data or keys –securing of authentication data or keys –other administrative functions?	[177] (A.17.3.)
Use Maintenance Effort	What are the likely users effort involved with managing: –APIM and associated devices or artefacts; –back-ups and expiration or retraction of authentication access; or –loss of authentication data or keys?	[177] (A.17.4.)
Use Convenience Comparison	Is the user's time consumed at replacement, enrolment and operational access together with maintenance functions convenient in relation to the importance or responsibilities or liabilities in performing their task?	[250] (A.17.5.)
Device Provisioning	Does the APIM operate using commonly available technology or are the components specialised dedicated to that APIM or underlying service? Is processing performed centrally and shared with ubiquitous devices? Does device provisioning, and contributions made by the owner, aid user accessibility or introduce barriers, including operating costs, to users?	[95] (A.17.6.)
User Confidence	To what extent will the User hold the firm belief that the APIM will protect their interests, e.g. privacy, safety within the specified operational context? Does the APIM demonstrate: –explicit authorisation (The system does not become unsafe automatically); –visibility (The system reports the security status); –revocability (The user may undertake tasks to change the security status); –path of least resistance (The user does not inadvertently choose to make the security status unsafe); –expected ability (The user should be aware of all the systems' abilities); –appropriate boundaries (The user should be able to distinguish what aspects are relevant); –expressiveness (The user should be able to instruct the system what tasks are to be performed); –clarity (The user should understand the all the system's tasks); and –dependability (The system protects the user from being fooled)?	[327] (A.17.7.)
User Duress	Does the context warrant the inclusion of a feature in the APIM to indicate that the user is being forced or coerced to act involuntarily? Would the inclusion of a surreptitious "panic button" instrument likely to cause harm to the user or potentially be exploited or is it unnecessary for the application context?	[247] (A.17.8.)

Table A.17: User Accessibility Evaluation Theme

Factors	Criteria Questions	Source/Identifier
Implementation Costs	What are the total APIM project fulfilment costs? Does this estimate include installing devices computer, networks, software etc and new or changes to deployed infrastructure? To what extent might a modular approach, particularly the application interface design, control expenditure?	[252] (A.18.1.)
Maintenance Costs	What are the actual operational and support costs in relationship to the business case's estimations? Do these costs include support costs of hardware; software; maintenance processes; personnel; and training costs? What is the cost impact to change existing procedures?	[238] (A.18.2.)
Cost of Input Devices	What is the unit cost of signal input device including firmware and its protection, in the event it was stolen or to prevent its internal operation from being examined?	[238] (A.18.3.)
Cost of Artefacts	What is the unit cost of the artefact, e.g. an integrated circuit card and its protection, if it was stolen, or in order to prevent its internal operation from being examined?	[177] (A.18.4.)
Management Costs for Input Devices or Artefacts	What are the estimated costs for distributing and logistical support for any devices and/or artefacts associated with the APIM?	[238] (A.18.5.)
Infrastructure Processing Costs	What is the cost of the proposed solution for introduction of new or integrating the APIM technology into existing infrastructure in terms of network, hardware, software, support, personnel and training?	[238] (A.18.6.)
Costs Recovery	What are the likely costs for making the APIM mandatory to all users in the community, as opposed to making the use of the APIM optional? Is there capacity to recover some costs?	[238] (A.18.7.)
Other Parties' Costs	What are the total costs and/or effort for each party involved, excluding users' costs, in the use of the APIM, including hardware and software, to ensure its compatibility with the users' processes and the need to revise supporting infrastructures?	[238] (A.18.8.)

Table A.18: Owners' Costs Evaluation Theme

Appendix B – EU State's eID Card Programme Case Study: Questions for Interviewees

---

This appendix contains the interview questions posed to the interviewees involved in the EU State's eID Card Programme.

Interview Questions *Interview Questions for Interviewees Involved with eID Card Programme in the EU state.*

1. What was the approach adopted within the ID Card Programme to determine the most suitable mechanism to identify citizens? Please describe it.
2. If there was not a formal approach, please outline or describe the methods or development approach employed within the Programme that addressed the problems of meeting the objectives of the programme with any social, organisational and technological issues. This may also include any usability or user accessibility and handling of biographical and biometric data.
3. How were stakeholders identified in the Programme and their objectives accommodated?
4. Were there clear objectives for the ID Card at the outset?
5. What was the method used to gather the requirements of the APIM?
6. What were the main factors that affected the requirements documented and how well did these map to the objectives?
7. What were the critical factors that affected the selection of the identification mechanism (biometric modality and or user authentication mechanism)?

8. In retrospect, what characteristics of the Programme would you choose now to include in your requirements?

9. In hindsight how could your approach have identified these requirements?

10. In retrospect, what characteristics of the implemented mechanism would you change?

11. In retrospect, what factors at the strategic level or stakeholder objectives were not fully researched or understood?

12. How did these factors impact upon the decisions made at the time in terms of the requirements documented and decisions made on the identification mechanism actually selected?

13. If a formal approach was available as a decision-tool would this have been of benefit or likely to have changed any of the decisions made?

14. What characteristics would you expect to be included in such a decision-tool for selecting identification mechanisms?

July 2009

Appendix C – Evaluation Themes and Factors (Stage B)

This appendix contains 25 evaluation theme tables relating to the factors for evaluating an APIM as at Stage B of our factor validation effort, representing Step 6 of our research implementation plan.

The tables show the status of our factors following our validation efforts using the data from our EU State eID Card Programme Case Study. The status also indicates which evaluation factors were grounded, deduced and Not-grounded in our data. We show relabelled factors as 'RF' and criteria questions which required amendment as 'AQ'.

We assign an identifier to a new factor identified in Stage B, e.g. B.4.1, to denote stage created, evaluation theme and factor reference number, to enable each factor and its criterion question to be tracked through each subsequent validation.

The tables in this appendix contain the following evaluation themes:

Table C.1 Stakeholders' Objectives Evaluation Theme (formerly Strategic Issues Evaluation Theme);

Table C.2 Stakeholders' Risks Evaluation Theme (formerly Risks Assessment Evaluation Theme);

Table C.3 Community's Characteristics Evaluation Theme (formerly Social Acceptability Evaluation Theme);

Table C.4 Task Environment Evaluation Theme (transferred from Effectiveness Perspective);

Table C.5 Constraints Evaluation Theme (new);

Table C.6 Polices Evaluation Theme (formerly Risks Controls Evaluation Theme);

Table C.7 Business Case Evaluation Theme;

Table C.8 Functional Requirements Evaluation Theme (formerly Functionality Evaluation Theme);

Table C.9 Privacy Compliance Evaluation Theme ;

Table C.10 Registration and Enrolment Evaluation Theme (formerly Credential Registration Evaluation Theme);

Table C.11 Performance Requirements Evaluation Theme (formerly Controls' Performance Evaluation Theme);

Table C.12 Assurance Requirements Evaluation Theme;

Table C.13 Task Dialogue Evaluation Theme (new);

Table C.14 Envisaged Issues Evaluation Theme (new);

Table C.15 Envisaged Vulnerabilities Evaluation Theme (new);

Table C.16 Forecasted Costs Evaluation Theme (new);

Table C.17 Security Architecture Evaluation Theme;

Table C.18 Identifier Management Evaluation Theme;

Table C.19 Reliability Results Evaluation Theme (formerly Reliability Testing Evaluation Theme);

Table C.20 Usability Results Evaluation Theme (formerly Usability Testing Evaluation Theme);

Table C.21 Technology Evaluation Theme;

Table C.22 Accessibility Results Evaluation Theme (formerly User Accessibility Evaluation Theme);

Table C.23 Solution's Issues Evaluation Theme (new);

Table C.24 Solution's Vulnerabilities Evaluation Theme (new);

Table C.25 Stakeholders' Costs Evaluation Theme (formerly Owners' Costs Evaluation Theme).

Factors	Criteria Questions	Status/Identifier
User Acceptability Rationale	What arguments support user acceptability or consent in terms of their responsibilities or liabilities to facilitate utilisation? What are the security controls to accomplish user privacy objectives? Do these controls negate the benefits of the customer proposition for potential users? Is the management of the users' private data under the immediate control of the APIM owner or that individual?	grounded RF AQ (A.3.2.)
Privacy Aims	What are the aims of the intended courses of action to protect user's private data? Does the protection or change in protection of a user's personal information fulfil a stated goal? Is the aim to retain Anonymity so that a user is not identifiable within a community? Is the aim to retain 'Undetectability' of an item of interest (IOI) so that an attacker cannot sufficiently distinguish whether it exists or not? Is the aim to retain 'Unlinkability' of two or more IOIs, e.g., subjects, messages, actions, etc.) so that an attacker cannot sufficiently distinguish whether these IOIs are related? Is the aim to retain 'Unobservability' of an item of interest (IOI) so that the undetectability of the IOI against all subjects uninvolved in is preserved and the anonymity of the users involved in the IOI even against the other subject(s) involved in that IOI cannot sufficiently distinguish by an attacker? Do these aims suggest the use of a pseudonym as an identifier of a user other than one of the individual's real names?	grounded RF AQ (A.4.5.)
Business Aims	What are the aims of the intended courses of action to protect information assets and resources ? Does this protection or change in protection fulfil a stated business target or goal which has been allocated a budget?	deduced RF AQ (A.4.4.)
Business Rationale	What arguments support the business aims of the Stakeholders, including the system owner, in respect of the considered need to instigate a change in protection of assets or facilitate a change to revise or introduce new business processes or delivery channels? Do the arguments incorporate the interests of all organisational entities, e.g. relying parties, trust service providers, which may rely on the APIM or may provide APIM related services?	grounded AQ (A.1.1.)
Security Benefits	Will the APIM be used to protect data and/or assets belonging to one or many entities? What are the types of entities, e.g. corporate or government, involved with the application context? Has consultation with entities been made with reference to a state or corporate policy for the appropriate security assurance?	Factor Deleted (A.1.2.) Duplicate of (A.1.1.)
Control Objectives	What are the proposed counter-measures, including the APIM, to minimise identified business risks and to achieve other business aims?	grounded (B.1.1.)

Table C.1: Stakeholders' Objectives Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Trust Between Stakeholders	What is the trust relationship between the APIM's owner or organisation and various supporting entities and could that lead, potentially, to a degree of reliance for users to operate an APIM as intended?	grounded RF AQ (A.7.8.)
Misfeasors' Threat Motivation	What are the underlying stimuli or goals that may lead to attacks to compromise the APIM? Do these motives include financial fraud, corporate espionage, intellectual challenge, error, state espionage or terrorism?	grounded RF (A.2.7.)
Attack and Compromise Probability	What is the likelihood of an attack or compromise event occurring? Does this projection incorporate an analysis of historical attacks and/or changes in threat intelligence? Are the probabilities foreseen confined to the system owner or do they include compromises relating to other stakeholders, including users?	Not-grounded (A.2.1.)
Impact Value Rating	What is the estimated impact value or severity score on the assets being protected if stolen or destroyed or modified? Does this estimate include losses, administrative costs as a result of a compromise and the indirect financial consequences of the entity's reputation being adversely affected?	grounded (A.2.2.)
Acknowledged Vulnerabilities	What are the known exploitable weaknesses in existing operations or conceptual vulnerabilities which have been explicitly accepted by stakeholders? Are these vulnerabilities published in the public domain?	grounded RF AQ (A.2.3.)
Compromise Scenarios	What types of deceptive user scenarios can be foreseen?	grounded (A.6.9.)
Impact on Upon Stakeholders	What are the likely consequences to all stakeholders, including users, if the APIM failed to detect unauthorised access or failed to verify or identify authorised users or subjects?	deduced (A.7.9.)
Privacy Impact Assessment	Has an impact assessment been made and documented in respect of the privacy issues that may impinge upon the requirements for the APIM?	Not-grounded (A.8.3.)
Users' Cooperation	What are the expectations that all individuals will cooperate voluntarily with an automated identification process? How have these expectation levels, in terms of legality, percentage coverage and utility, been substantiated?	grounded (A.7.11.)

Table C.2: Stakeholders' Risks Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Population Traits	Does the majority of the target user population have characteristics that could pose disadvantages or advantages for the possible APIM design options being considered? What is the particular mix of users with respect to impact upon the success of any APIM?	grounded (A.7.4.)
Privacy Assurance	What assurance is required to show that the technologies used in the implementation of the APIM allow for continuous auditing of compliance within stated privacy policies and practices governing the collection, use, and distribution of private information?	grounded (A.8.8.)
User Population Education	Is the user population likely to resist educational material supplied to assist in the introduction of a new or revised APIM? Has consideration been given to educating the users to allay their doubts/fears about utilizing a specific authentication or biometric mechanism?	grounded (A.7.2.)
User Obligations	Will potential users be required to provide their consent or acceptance to responsibilities or liabilities? To what extent do these obligations negate the benefits of the customer proposition for potential users?	grounded (B.3.1.)
Users' Relationship with Stakeholders	What is the relationship of the user to the APIM's owner, e.g. service provider, employer etc and any intermediaries, e.g. infrastructure provider, and could this trust lead to reliance on users to operate an APIM as intended?	grounded RF AQ (A.3.1.)
User Attitudes	What is known about the user population and the entities that operate the APIM? Has the user population been surveyed to determine their attitude towards using a biometric or authentication mechanism? Does a strong negative response indicate a need to reformulate plans or possibly the instigation of a proactive education programme?	Factor Deleted (A.7.1.) Duplicate to (A.3.3.)
Social Attitudes	What is the attitude of the intended user communities towards APIMs that address similar business or social problems? What are the social problems with these existing APIMs? To what degree does the existing method or intended way of identifying users cause difficulties? Do these issues include user perceptions which may restrict the use of an APIM to capturing biometric data that may be private and believed to be intrusive? Would an APIM be, or be perceived as, endangering health, safety or welfare (including inclusivity) of the user?	Not-grounded RF (A.3.3.)
Community Membership	Will the system and APIM be openly available to all parties? Are there membership restrictions or conditions for the intended user community?	grounded (A.3.4.)
Users' Trust	To what extent will the user community firmly believe in the competency of the APIM's system owner to act dependably, securely and reliably within the specified operational context?	grounded (A.3.5.)

Table C.3: Community's Characteristics Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Logical Usage Contexts	What are the applications and operational circumstances where the user is engaged with the APIM to perform tasks to access an asset and/or service? Who are the parties involved and what role do they perform with respect to the transactions or access to the asset? Will use involve parties in an enterprise only context, e.g. employer/employees? Will use involve parties in federated context - e.g. business partners/ customers/citizens? Will use involve parties in a heterogeneous context - e.g. State's citizens, Payment Cards? Have Use Cases been developed to aid in the scope and types of logical usage? Have scheme rules been established for the contexts involving multiple entities?	grounded (B.4.1.)
Physical Usage Contexts	Will the APIM also be used in applications for physical, e.g. visual inspection, identification purposes such as controlling access to a building or site, border crossing or to prove physical presence? Have use cases been developed to demonstrate physical usage?	grounded (B.4.2.)
Environment Characteristics	Where will the APIM operate? Will it be in public spaces, physically controlled environments, restricted networks or open networks? What are the physical conditions, devices, artefacts or other intelligent processing resources available? Does this description also include physical and social measures or conditions that limit or restrict access to information resources?	grounded (A.2.5.)
Operational Context	What are the operational circumstances where the user is engaged with the APIM to perform tasks to access an asset and/or service? Who are the parties involved and what role do they perform with respect to the transactions or access to the asset? For the APIM's owner will the parties involved be employees (private), business partners/customers (commercially confidential), state citizens (private) or a combination of these entities in a heterogeneous application?	Factor Deleted (A.2.6.) Split into (B.4.1.) and (B.4.2.)
Operational Logistics	How will the user operate devices or artefacts in the envisaged physical environments? Is the purpose of the APIM to identify the user controlling the APIM equipment, e.g. personal laptop computer, or will other individuals, e.g. police authority, use the artefacts to verify the subject and holder of the artefact?	grounded (B.4.3.)
Technical Control	To what degree does the operating environments, including remote sites, enable the APIM's owners (and user population) to control the technology processes and, where relevant, to monitor user behaviour?	grounded RF AQ (A.6.8.)

Table C.4: Task Environment Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Signal Data Exchange	Will there be a need to exchange user signal data between other organisations with similar mechanisms utilising the same user signal data or human characteristic? Do interoperability specifications exist?	grounded (A.5.6.)
External Performance Benchmarks	Have there been any performance or security tests or evaluations of biometric or authentication mechanisms similar to the intended application context and business problem? What are the learning outcomes?	grounded (A.5.7.)
Users' Signal Enrolment	What are the constraints that would determine how the APIM captures the user's initial input signal? Is there an existing user enrolment policy? Is the user required to be present, undertake the process remotely or are the processes combined? What other user data, e.g. autobiographical, are required at enrolment?	grounded AQ (A.10.2.)
Regulatory Constraints	What legislation will affect the data that the entity may store for the intended user population, e.g. Data Protection Acts, Privacy Laws?	grounded (A.1.6.)
Legal Imperatives	What legal issues could hinder or support a change programme (privacy, data access etc.) to deploy an APIM?	grounded (A.1.7.)
Contextual Legacies	What existing technical constraints or social norms or internal organisational issues (employee rights, privacy, etc.) could hinder a change programme or project to introduce or revise an APIM? Are there any legacy systems or commonly established procedures or adopted rules that could place restrictions on the requirements to introduce or revise an APIM?	grounded RF AQ (A.5.4.)
Users' Costs	What are the potential costs and/or effort for each party involved in their use of the APIM that includes hardware and software, its compatibility with the user's processes and the need for supporting infrastructure?	grounded (A.3.6.)
Budget	What funds have been allocated by the organisations to minimise unacceptable risks? Do the aims include countermeasures to reduce direct financial losses and associated administrative costs as a result of a personal identification mechanism compromise, if sole or main control mechanism?	grounded (A.4.3.)
Standards	What standards impact the choice of an APIM, its use and or processes? Which information Security controls for user authentication, the use of cryptography or biometrics are required to be complied with?	grounded (A.5.5.)
Stakeholder Dynamics	What commercial or competitive or organisational issues could hinder or support a stakeholder's change programme (fraud, industry regulation alignment, staff privacy, data access etc.)? How do these issues affect entities' risks, e.g. profitability?	grounded RF (A.1.5.)
Compromise Recovery	What relationships exist (if any) between the users in the community and the APIM systems owner (e.g. service provider, employer etc..) and any intermediaries, e.g. infrastructure providers, to recover from occurrences where one or many individuals' mechanisms have been compromised? Are there procedures or scheme rules that enable the user to seek recourse for any damages or losses incurred?	grounded (B.5.1.)

Table C.5: Constraints Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Archiving Signal Data	What is the data retention period and retention rules for user signal data stored and used for authentication or identification?	grounded (B.6.1.)
Recognised Issues	What are the identified issues (if any) that have been explicitly accepted by Stakeholders, including users? Are these issues discussed in the public domain?	grounded (B.6.2.)
Authorised Identity Evidence Sources	Which entity is empowered to provide policy on the acceptable identity proof, sources and types of evidence, as part of the identity verification processes? Does the registration process dictate that the applicant is required to provide proof of identity? Will operatives and applicants be provided with a list of bodies that are considered as acceptable identity sources and the means to verify such evidence as valid seed identification documents?	grounded (B.6.3.)
Sanctions	What are the impositions of criminal or civil penalties or disciplinary reprisals for improper use of the APIM for authorised users? What are the criminal or civil consequences for misfeasors perpetrating violation acts to compromise the APIM or steal a person's digital identity	grounded (B.6.4.)
Requirements Gathering Methodology	How will the requirements for the APIM be established? Will this process involve prototyping or will they be established through formal requirements capturing procedures? Is the choice governed by the organisation's preferred system development methodology or restricted by tendering processes? How will the users be involved in stating their requirements (if at all)?	Not-grounded (A.5.3.)
Privacy Laws Compliance	Has an individual within the organisation, possibly a corporate governance function, been assigned responsibility to ensure privacy laws compliance? Do the legislative and regulatory aspects differ in each relevant jurisdiction?	grounded (A.8.2.)
Due Process	What is the means of settling or litigating disputes between the authorised users and the stakeholders as proprietors or custodians of information about those users?	grounded (B.6.5.)
User Duress Policy	Does the context warrant the inclusion of a feature in the APIM to indicate that the user is being forced or coerced to act involuntarily? Would the inclusion of a surreptitious "panic button" instrument likely to cause harm to the user or potentially be exploited or is it unnecessary for the application context?	Not-grounded RF (A.17.8.)
Policy Implementation Strategy	What is the strategy chosen to achieve the stakeholders' change programme objectives? Does the policy include the minimising of risks by introducing or revising controls given the operation context and strategic considerations?	deduced RF AQ (A.4.1.)
Privacy Laws and Privacy Policies	Which directives, international conventions, international and local laws and regulations are applicable to subjects' private data which could influence the requirements for an APIM? Are artefacts or credentials to indicate the subject's name? Are there guidelines on what is considered to be private data and how it is to be protected?	grounded (A.8.1.)

Table C.6: Policies Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Identity Approval/ Authorisation	Which organisations have been approved to supply an identifier or credential or provide authorisation against identity evidence submitted by the potential user, i.e. applicant seeking to obtain a user account and a credential?	grounded (A.9.1.)
APIM's Scope and Purpose	Why is the APIM being introduced or revised? Have goals been documented (e.g. Feasibility Study) which are set in terms of priority values of aspiration to be obtained from APIM's intended use?	grounded (B.7.1.)
Stakeholders' Benefits	Will the APIM be used to protect data belonging to one or many entities? Is the proposed APIM regarded as a business enabler to facilitate new service delivery channels e.g. eGovernment? What are the types of stakeholder organisation, e.g. Government or corporate entity, are involved? Has consultation been made with reference to the national policy or corporate policy for the appropriate security assurance?	grounded (B.7.2.)
Political and Economic Considerations	What political or economic matters may hinder or support organisational change? How does this impact upon the APIM selection?	deduced RF (A.1.4.)
Security Motivation of Authorised Users	What incentives could be employed to encourage appropriate use of the APIM? What are the possible disadvantages or liabilities that would apply if authorised users were found or proven to be negligent?	deduced (A.7.10.)
Expert Feasibility Opinion	Have the entities' applications been discussed with knowledgeable and independent members of respected information security professional group to assess technical feasibility.	grounded RF AQ (A.1.8.)
Programme Governance	What entities have authority for the decisions or authorisation processes relating to the selection of the APIM? Has a Steering Committee been formed to involve Multiple Stakeholders (Multiple Stakeholder Processes) with a consultation framework?	grounded (B.7.3.)
Alternatives Investigated	Has there been an investigation into the alternatives to the biometric or user authentication mechanisms to address the identification problem? Fundamentally, are biometrics really needed or desirable?	Not-grounded (A.6.4.)
Defined Business Problem	Is the personal identification problem fully understood and defined in terms of requirements and not solutions? To what degree are the existing mechanisms actually effective?	grounded RF AQ (A.5.1.)
Project Sponsorship	Is the APIM project initiation supported with a business case with a justification for expenditure by stakeholders?	deduced RF AQ (A.5.2.)
Identified Risks	What are the stakeholder' and possibly user risks that are to be controlled (potentially minimised) by the APIM?	grounded RF AQ (A.4.2.)
Risks Management	How does the organisation want to address the risks identified to provide access or entitlement to the intended user population? Do the options for risk mitigation include risk alleviation, e.g. by introducing or revising controls; risk transference, e.g. by taking out insurance against potential losses; risk avoidance, e.g. by terminating, user access or limiting some of the functionality; risk assumption, e.g. by performing due diligence in formally accepting the risks and monitoring the exposure or impact levels? Do the organisation's operating rules mandate an agreed approach to Risk Management within a cyclical framework to evaluate assets and their protection periodically?	deduced RF (A.2.8.)
Assurance Effectiveness Evidence	What evidence is required to demonstrate the APIM's ability to meet the security assurance requirements set by stakeholders?	Not-grounded RF AQ (A.2.4)

Table C.7: Business Case Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Positive or Negative Identification	Will the APIM be used for positive identification (proving a person is already enrolled) or negative identification (proving a person is not enrolled) or a consolidation of both to meet one or more requirements?	grounded (A.6.1.)
Overt or Covert Identification	Does the requirement entail the user being aware of the APIM? What legal issues and technical consideration apply if the requirement is for a covert APIM?	grounded (A.6.2.)
Multiple User Input Signals	If both positive and negative identification are required, is there a requirement to use same authentication or identification data, or is there potential for the combining of two or more separate user input signals, e.g. fingerprint and voice, face and voice, personal identification number, digital certificates and passwords etc?	grounded (A.6.5.)
Authorisation Attributes	What attributes need to be captured and passed to the access control system to enable verified users to have authorised permission to resources?	grounded (B.8.1.)
User Signal Storage Format	In what format should the APIM store the user's input signals for identification or verification purposes? Will data need to be converted into a format using a specific algorithm or protected using a cryptographic algorithm? How are the user's input signals to be captured to compare against those stored in the formatted or protected form? Does the solution require the identification data to be centralised in a database or involve an artefact, e.g. eID Card? What are security controls required to protect the storage and use of the user signal data in the proposed format?	grounded (B.8.2.)
Signal Capturing Device Interoperability	Are user signal capturing devices ubiquitous, e.g. keyboards, or are bespoke user signal reading devices and software required to support universal use with a range of user equipment, e.g. PDA, PC etc, or bespoke devices?	grounded (B.8.3.)

Table C.8: Functional Requirements Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Privacy Asset Register	What processes need to be put into place to write, publish, and maintain a clear and comprehensive document listing the types of information that may be collected, e.g. transactional information, personal data in an identifiable form? Does the document state the purpose of data collection, the data that may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency? Are applicants to be provided full disclosure of the intended uses of the credential and the related privacy implications?	grounded (A.8.4.)
Privacy Asset Appeals Procedure	What appeals procedures are to be maintained for those applicants who are denied a credential or for those authorised users whose credentials are revoked without explanation?	grounded (A.8.5.)
Privacy Asset Access Control	What processes are to be in place to ensure that only personnel with a legitimate need to access the privacy information, used within the APIM, are authorised? Does this safeguard include handling disputes relating to personal data stored and data maintained for purposes of applicant registration and credential issuance?	grounded (A.8.6.)
Privacy Asset Compromise	What processes are required to be in place to coordinate with approved entity, authority or agency officials to define consequences for the APIM or other systems violating privacy policies?	grounded (A.8.7.)
Privacy Security Controls	What are the security controls to be applied to accomplish privacy goals, where applicable? Is the management of the private data under the immediate control of the APIM owner or the individual? What are the technologies and infrastructures available to support these requirements?	grounded (A.8.9.)
Privacy Security Controls Erosion	What assurance is required to show that the technologies and controls used to implement the APIM does not erode privacy protections relating to the use, collection, and disclosure of private data in an identifiable form? Does this requirement include the protection against unauthorised access to users' private data or credential data stored on artefacts?	grounded (A.8.10.)

Table C.9: Privacy Compliance Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Proofing Clearance	How will the identity knowledge or documentary evidence presented by the user be verified?	grounded RF (A.9.2.)
Unacceptable Identity Evidence	What are the unacceptable identity source documents as determined by policy and visual/electronic identity inspection procedures?	Factor Deleted (A.9.3.) Duplicate of (A.9.9)
Acceptable Users	What does the policy stipulate in determining acceptable applicants as potential users?	grounded RF (A.9.4.)
Identity Proofing Rules	What are the identity registration processes and will interpretation guidance be made available for operatives?	grounded (A.9.5.)
Approved Registration Agencies	Which entities are to receive delegated powers to approve the issuance of an identifier and a credential to an applicant?	grounded (A.9.6.)
Identity Proofing and Registration	What is the registration process so that a credential can be issued to the genuine applicant, which has been assigned an identifier? How are artefacts containing credentials delivered to the genuine applicant?	grounded AQ (A.9.7.)
Remote or Local Registration	Is the applicant to appear in-person as part of the application and registration processes or are these processes to be undertaken separately? Can any of these processes be performed remotely with other controls?	grounded AQ (A.9.8.)
Acceptable Identity Evidence	What are the acceptable identity source documents as determined by policy? During identity proving, what evidence is the applicant required to provide in terms of forms of identity evidence in original form? Will operatives and applicants be provided with a list of acceptable issuing bodies identity source documents and the means to recognise or verify the authenticity of identity documents presented or identity data gathered?	grounded (A.9.9.)
Identity Proofing Compromise	Do risks dictate that the identity proving, registration and issuance process need to adhere to the principle of separation of duties to ensure that no single administrator has the capability to issue an APIM identifier or credential without the authorised cooperation of another authorised administrator?	grounded (A.9.10.)
Identity Proofing and Registration Accreditation	Does the identity proofing and registration processes used to verify the claimed identity of the applicant require accreditation?	grounded (A.9.11.)
Accreditation Processes Applicability	Which entities do the identity proofing and registration processes accreditation rules apply to?	Not-grounded (A.9.12.)
Approved Processes Adoption	What authorisation is required before the adoption and use of approved identity proofing and registration processes?	grounded (A.9.13.)
Credential Identifier	How will the enrolled user be uniquely recognised? Will the user require anonymity? Is there a need for pseudonymity, where the identifier masks the user's true identity?	grounded (A.6.3.)

Table C.10: Registration and Enrolment Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Operational Ergonomics	Will the APIM operate in consistent conditions or various environments? What are the non-standard conditions which reveal APIM constraints?	grounded (A.10.1.)
Input Signal Tolerations	During operational use, will the APIM be required to automatically flag poor quality signal input data? How much of the input can be reasonably tolerated to be flagged as poor quality data?	Not-grounded (A.10.3.)
Throughput Rates	What are the throughput rate requirements, i.e. timing maximums?	Not-grounded (A.10.4.)
User False Non-match Toleration	How many false non-match errors would the organisation accept and the user population tolerate as acceptable rates for user input signal false acceptance and false rejection?	grounded (A.10.7.)
Intervention Rate	What is the tolerable rate for false user input signal non-matches which require intervention by trained staff, if applicable?	Not-grounded (A.10.9.)
Impostor Detection	What is the acceptable probability that a false user input signal match setting being sufficiently low enough to deter deliberate compromise?	grounded (A.10.10.)
Combining Mechanisms	Would the acceptability of user input signal false matches or false acceptances become more palatable to the owner (or possibly the user) by combining two or more user input signals for the operational context?	grounded (A.10.11.)
Maximum Enrolment Time	What is the longest time permitted for successful user input signal enrolment?	grounded (A.10.14.)
Maximum Enrolment Attempts	How many attempts at signal enrolment should the user be allowed?	grounded (A.10.15.)
Template Protection	Are security controls required to protect the APIM's input signal data, e.g. authentication data, biometric images or template data?	grounded (A.10.19.)

Table C.11: Performance Requirements Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Attack Protection and Detection	What are the likely technology resources and/or social skills that will be used to compromise the APIM (either its entirety or at user level)? Is the APIM required to resist and detect attacks in order to protect information assets? What are experiences of past attacks and does this intelligence suggest changes in potential attacker's motivation? How closely does this assessment align with stated user signal performance to detect or deter an impostor being falsely accepted at least once in a number of attempts?	deduced AQ (A.11.1.)
Operational Quality Assurance	What test data are essential, as evidence, to assure the APIM's design will operate reliably, in line with the performance requirements? What are the operational qualities sought?	grounded (A.11.2.)
Documentation and Test Data Availability	What information are to made available to testers, including external or internal designs, to test assurance performance? Does the APIM design documentation need to be kept confidential?	grounded AQ (A.11.3.)
Functional Testing	What is the desired reliability to ensure the APIM implementation functions correctly? Is the implementation to be exposed only to documented attacks and which it is designed to counter? Is the implementation to be tested by external expertise? What are behavioural expectations in response to each attack test on the APIM?	grounded (A.11.4.)
Audit Logs	What audit information is required to fulfil legal obligations and risk management functions? Does the audit information need to include any or all of the following: the number of new biometric records accepted or new credentials issued, amended or revoked; the number of records verified, the number of users the APIM was unable to enrol; the quality measurements for the captured user signal data; the amount of APIM down time; the APIM errors by type; and the average enrolment processing time on a daily, weekly, and monthly basis?	Not-grounded RF (A.11.5.)
Performance Assessment Methodology	What is the evaluation approach, e.g. Common Criteria Evaluation Methodology, to test and evaluate candidate APIMs' performance in order to make an objective assessment (and repeatable results) based on the test data sets and substantiated results produced?	deduced (A.11.6.)
Assurance Test Regime	What are the tests required to prove the effectiveness of the APIM (holistic and within each component)? What is the test environment in which the evaluation will take place?	Not-grounded (A.11.7.)

Table C.12: Assurance Requirements Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Interaction Dynamics	Is the APIM to operate as a sub-process for the user as part of an overall task, e.g. cash machine transaction, or does it constitute the entire task, e.g. inspecting an ePassport? Where is the position of the identification process within the interaction to fulfil a user's task?	grounded (A.6.6.)
User Supervision	Is the user's interaction with the biometric device or other input device watched by authorised personnel or is it self-service and unobserved?	grounded (A.6.7.)
Multiplicity Impact	What are the number and similarity in operation to other APIMs used by the intended user population, i.e. multiple credentials (e.g. User Accounts and passwords)? Does the APIM require differentiation from other similar APIMs to avoid possible user confusion?	grounded (A.7.3.)
Task Sequence	What is the position of the APIM function within the user's task to achieve the desired goal? What impact could the potential APIM have upon the user in achieving the overall task including speed and accuracy? What outcomes need to be avoided from poor HCI design?	deduced (A.7.5.)
User Technical Expertise	To what extent would the user population have the capacity to acquire specific skills, if required?	deduced (A.7.6.)
Frequency of Use	Will the expected usage frequency or patterns of APIM usage lead to users becoming habituated or remaining non-habituated?	deduced (A.7.7.)

Table C.13: Task Dialogue Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Impostor Pass/ False Alarm Threshold	What is the acceptable decision threshold determined by the risks in the application context? How are these rates to be determined?	deduced RF (A.10.5.)
Multiple Attempts Limit	In the case of a user input signal false non-match how many additional attempts for identification should the user be permitted?	grounded (A.10.8.)
User Equipment	What are the operational devices which determine how an APIM captures the user's input signal during enrolment and live usage?	grounded AQ (A.10.12.)
Enrolment Supervision	Do security policies dictate that the enrolment process needs to be supervised in order to achieve the required user input signal quality?	grounded (A.10.13.)
Enrolment Failure Arrangements	What work-around measures are required should a user be unable to provide a valid input signal for enrolment, either temporarily or permanently?	grounded RF AQ (A.10.16.)
Vendor Support	What type of quality control and statistical evidence are vendors required to offer on the performance of the enrolment and identification processes?	grounded (A.10.17.)

Table C.14: Envisaged Issues Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Resources Allocated	What funds, personnel and tools will be committed to the change project or programme to design, implement, test, deploy and operate the APIM?	deduced (A.11.8.)
Environment Variance	What are the environmental factors that may affect user input signal enrolment and signal processing during live operation?	grounded (A.10.18.)
Impostor Pass Rate	What is the acceptable rate that a user input signal match is accepted erroneously by the matching component, possibly as a result of the threshold setting being too low to detect deliberate compromise, e.g. fraud attacks?	deduced RF AQ (A.10.6.)

Table C.15: Envisaged Vulnerabilities Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Backwards Compatibility	Is backward compatibility required to separate APIMs in different authorisation domains?	grounded (A.10.20.)
Application Flexibility	What are the potential factors which may influence stating suitability measurements for the APIM?	grounded (A.10.21.)
Scalability	What scalability is desired for the APIM? Is the user population forecasted to grow significantly during the APIM's projected life?	grounded (A.10.22.)
Upgrade Impact	What are the acceptable disruption, for the APIM owner and its users, if upgrades were to be possible to the APIM?	deduced (A.10.23.)
Costs Envisaged	What are the system owner's and stakeholders' estimated programme costs? Have these forecasts been based upon similar protection needs over a specified period? Do estimated costs draw on information from similar implementations, from initial system designs, from vendors' estimates or from suppliers' tender submissions?	deduced RF AQ (A.1.3.)

Table C.16: Forecasted Costs Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Identification/ Authentication Model	To what extent does the solution design or vendor proposals meet the requirements for the APIM and have specifications with validated test data been provided? Does the model align with policies and relevant standards? How does it align with the infrastructure that is used to implement the security policy in an organisation? Does it address physical, procedural and IT security controls in a holistic way?	grounded (A.12.1.)
Credential Storage	Where are the users' credential data stored? Does the APIM require the user to possess and use an artefact, e.g. a token, to store or to generate and protect users' signal data?	grounded AQ (A.12.2.)
User Input Signal Storage	Is the user's input signal data stored centrally or stored on an artefact or a combination of both?	grounded (A.12.3.)
Mechanism Processing Location	Will there be a centralised database or distributed storage medium, where a user will be required to carry his/her biometric or authentication data on a portable artefact to allow the APIM to operate universally?	grounded (A.12.4.)
Mechanism Processing Infrastructure	What are the network, systems, devices, software and processes required to support the APIM design? To what degree will the APIM owner have operational control over the components, e.g. the Internet, browser, or public key infrastructure, devices, to support the processing locations?	grounded (A.12.5.)
Processing Protection	How will the user input signal captured be protected during acquisition for either local processing or extracted and communicated for remote processing? How will the result be communicated to users and what preventative measures protect against compromising the result notified?	grounded (A.12.6.)
Alternative Identifier Types	Will a biometric feature or a name or code act as a unique identifier? Is that feature compatible, in terms of degradation, with the expected lifetime of the authorised access or recognition requirement?	grounded (A.12.7.)
Biometric Modality Selection	Where user input signals are based upon biometric features are all the elements, e.g. biometric modality template file size and storage medium elucidated in the detailed design?	Not-grounded (A.12.8.)
Knowledge Data Selection	Where user input signals are knowledge based are all the elements, e.g. data composition and user's cognitive actions, elucidated in the detailed design?	grounded (A.12.9.)
Mechanism Maintenance	Does the detailed design describe the tasks to support the APIM? How are users added or deleted from the APIM? How are user's data maintained? How is a user's claimed identity verified?	grounded (A.12.10.)
Maintenance Effort	How easy and often is it necessary to change or reissue authentication data, keys, tokens, and software or recapture of biometric samples?	grounded (A.12.11.)
Associated User Data	What associated user data are required to be stored, e.g. autobiographical data, with the identifier and identification data?	grounded (A.12.12.)
Signal Processing	Does the detailed design describe the APIM's functions, e.g. capturing the user's input signal, and how data are protected during all processes?	grounded (A.12.13.)
Combined User Input Signals	Does the design use multiple input signals or templates or data types related to each identifier? Will the user generate data from an artefact or token generation device or remote system?	grounded (A.12.14.)
Costs Influences	What factors in the security architecture are most likely to increase or decrease costs of the APIM?	Not-grounded (A.12.15.)
Security Training Needs	Is user interaction with the APIM intuitive or based on familiar designs? Will users require training on how to use the APIM, as designed? Is there a help desk facility for users?	grounded RF AQ (A.12.17.)
Performance Tests	Have there been any performance or evaluations of the APIM or similar mechanisms in a comparable application context?	grounded (A.12.18.)

Table C.17: Security Architecture Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Credential Lifetime	What is the intended life of the APIM's identifier, credential and artefacts to provide continued access or entitlement to the information asset?	grounded AQ (A.13.1.)
Credential Authenticity	What are the rules for officials or administrators to undertake credential issuance? Are these tasks automated? Is the verification of identity evidence a separate task undertaken independently during the applicant registration process?	grounded (A.13.2.)
Credential Integrity	What are the rules for officials or administrators to undertake other credential management processes, e.g. issuing replacements or revoking credentials? Are these tasks automated?	grounded (A.13.3.)
Credential Maintenance Process Adoption	What authorisation is required for entities and their officials to adopt and operate credential maintenance processes?	grounded (A.13.4.)
Credential Maintenance Tasks	What are the processes for issuing and maintaining identification credentials, including the processes for revocation and providing justification for credential withdrawal reasons to former users, if necessary?	grounded RF (A.13.5.)
Credential Delivery Verification	At the time of credential issuance, what are the processes to verify that the person to whom the credential is to be issued (and on whom the background verification was completed) is the same person as the intended applicant/recipient as approved by the authorised organisation during the person's registration?	grounded (A.13.6.)
Credential Use Locations	Where will the processing of the initial user input signal to the related credential take place? What are the conditions for normal operational use of the credential?	grounded (A.13.7.)

Table C.18: Identifier Management Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Sampling Normalisation	Will the APIM use more than one instance of captured user signal or biometric input data to create the enrolment template?	Not-grounded (A.14.1.)
Signal Entropy	Is there sufficient inherent variation or randomness in the user's input signal to avoid candidate identification collisions?	Not-grounded (A.14.2.)
Threshold Performance	Does the accuracy of the APIM comparison results meet the required Impostor Pass/False Alarm decision threshold? What is the impact upon performance from the adjustment of the threshold setting?	deduced (A.14.3.)
Deceit Resistance	What is the difficulty, in terms of knowledge and resources, to synthesise an unauthorised entity of generating valid/correct user input signals?	deduced (A.14.4.)
Artefact Counterfeiting	What is the difficulty, in terms of knowledge and resources, to deceive an APIM by producing a counterfeit copy of an artefact?	deduced (A.14.5.)
Device Maintainability	What is the probability that an APIM related device will perform its intended function over a specified interval of operation?	grounded (A.14.8.)
Device Interfacing	Are supporting devices and artefacts functioning correctly for their intended purposes in a way that meets the APIM's requirements which prevents them being disabled or the APIM being circumvented? Is the installation to be tamper-evident with physical integrity and use sensors to detect attempts at circumvention or possess similar controls?	grounded (A.14.9.)
Signal Privacy	Does the APIM's signal data contain the user's private details, e.g. iris? Does the user approve the use of this private data and its protection?	deduced (A.14.14.)
Signal Data Protection	What are the technological safeguards to protect the integrity and and confidentiality of the user's signal data captured, stored, processed and transmitted?	grounded RF AQ (A.14.15.)
Failure to Enrol Rate	Average number of users in the test case that are unable to provide an input signal of sufficient quality for identification or authentication?	Not-grounded (A.14.17.)
Average Time of Impostor Try	Time to detect impostor attempts, including repeated tries averaged, regardless of successful verification over all impostor attempts?	Not-grounded (A.14.19.)
Average Time of Verification Try	Time to achieve correct user verification including repeat attempts averaged over all attempts and tests?	deduced (A.14.20.)
Average Number of Impostor Capture Failures	Number of failures in capturing user signal data averaged over all impostors' attempts?	deduced AQ (A.14.21.)
Average Number of Genuine Capture Failures	Number of failures in capturing signal data from genuine subjects averaged over all genuine subjects‘ attempts?	Not-grounded (A.14.22.)
Artefact Accreditation	What processes are to be established to issue an artefact and/or other related devices to users from approved suppliers whose reliability has been vetted by the APIM owner or agency and so approved or authorised in writing, i.e. accredited?	grounded RF AQ (A.13.8.)
Tamper Protection	Are there tamper deterrent and tamper indicative technologies available to notify errors in the APIM?	deduced (A.16.18.)
Template Update Notifications	Will the audit trail flag changes to data relating to an enrolled template; or the template itself; or any changes in user access rights as safeguards to detect unauthorised tampering?	Not-grounded (A.16.19.)

Table C.19: Reliability Results Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Interface Use	What data have been generated from the APIM's usability tests? Do the results provide evidence that both the authorised users and the APIM's administrators usage of the APIM's Human Computer Interface, artefacts, tokens or devices' interactions are as intended? Are there identified usability issues which introduce adverse or undesirable user behaviour that may compromise the effectiveness of the APIM?	Not-grounded (A.15.1.)
Convey Security Features	Does the APIM's human computer interface convey the available security features to the user?	Not-grounded (A.15.2.)
Visibility of Mechanism Security Status	Does the APIM's human computer interface have the ability for the user to observe the security status of internal operations?	Not-grounded (A.15.3.)
Intuitive Interface	To what extent is the APIM's human computer interface comforting and naturally easy to learn?	Not-grounded (A.15.4.)
Aesthetic and Minimalist Design	Does the APIM's human computer interface convey or display only relevant security information?	Not-grounded (A.15.5.)
Error Reporting and Assistance	Does the APIM's human computer interface show error messages that are detailed and state, if necessary, where to obtain help?	Not-grounded (A.15.6.)
User Satisfaction	Does the APIM's human computer interface aid the user in having a satisfactory experience with the APIM and other related components?	Not-grounded (A.15.7.)
Depth of Cognitive Processing at Enrolment	Does the user require cursory rehearsal, visual co-ordination, cognitive activity or no effort in order to provide user signal data?	deduced (A.15.8.)
Signal Retrieval Strategy	Is recall of the signal (authentication data) from the user's memory to use the APIM with or without cues or recognition focused? Does the APIM support or prompt the user to recall their input signal data supplied upon enrolment and the procedures for using the APIM's interactive design?	Not-grounded (A.15.9.)
Signal Meaningfulness	Is the user signal used by the APIM system assigned, self-assigned by the user, meaningful to the user or deducible only by the user?	Not-grounded (A.15.10.)
Task Convenience	Is the APIM likely to be operationally acceptable aligning with the user's task or duties? Is the APIM easy to learn within that task? Do the APIM's interaction processes and signal data need to be memorised? Are allowances made for human error or limitations?	Not-grounded (A.15.11.)
User Signal Preference	What is the users' preference for signal type? Is the biometric modality chosen likely to be accepted against other modalities which may be more familiar or less intrusive?	Not-grounded (A.15.12.)
User Training	Do users require training on how to use the APIM properly? Is the APIM supported by tools, e.g. wizards? Is the interaction intuitive?	grounded (B.20.1.)

Table C.20: Usability Results Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Database Contingency	Is database backed-up and restore required if the identifiers and user template or data for the APIM are lost, amended or destroyed?	Not-grounded (A.12.16.)
System Resources	What are the computer system and network resources envisioned to support the overall APIM?	Not-grounded (A.16.1.)
System Functionality	Has full consideration been given to all functions and components to support the APIM? Does this description include: user data collection; user input signal data capture and parameter extraction; data transmission; data translation; signal processing; template or image storage;and user security management features and training information?	deduced (A.16.3.)
Technology Impact	What is the impact of the proposed APIM in terms of hardware, software, personnel and training upon existing infrastructure?	deduced (A.16.4.)
Existing Technologies Utilisation	Is there a list of the available hardware and software in the architectural designs to support the APIM? To what extent does the design utilise existing legacy systems and infrastructure?	deduced RF AQ (A.16.5.)
Technical Interoperability	Will interoperability of the APIM with other existing, possibly alternative APIMs, in the intended application context be an issue?	Not-grounded RF (A.16.6.)
Processing Capacity	What is the processing power and media storage needed to support the APIM locally and/or a server at a central location?	Not-grounded (A.16.7.)
Back-up Methods	What are the back-up procedures should the APIM fail totally or partially in resulting in the total or temporary unavailability of all users' signal data?	Not-grounded (A.16.8.)
Roles Assignment	What are the roles and responsibilities for the various parties involved with the APIM? Has an operational role been assigned for a security officer, security operator, an auditor, an administrator, an APIM manager, a standard user, and privileged users?	grounded (A.16.11.)
Personnel Support	Are technical support personnel, or substitutes, critical to the operation of the APIM available?	Not-grounded (A.16.12.)
Continual Training	What are the training requirements for users and the administrators, of the APIM for the initial usage also for ongoing operations?	deduced (A.16.13.)
Device Calibration	Are the user input signal capture devices capable of performing automatic self-diagnostic and calibration tasks continually?	Not-grounded (A.16.14.)
Lockout/ Thresholds Maintenance	How does the APIM support a lockout or threshold for excessive invalid access attempts by authorised users? How are these lockouts and thresholds changed securely?	grounded (A.16.15.)
Subject Supervision	What competencies and involvement are acceptable for administrators to supervise subject enrolment?	Not-grounded (A.16.16.)
Enrolment Process Support	Is it required that a supervisor has the ability to intervene in the enrolment process to improve the quality of the user's signals?	Not-grounded (A.16.17.)
Data Protection	What technological safeguards have been implemented to safeguard the integrity and confidentiality of the user signal and privacy data the APIM captures, stores, processes and transmits?	deduced (A.16.20.)

Table C.21: Technology Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Operational Enablers	Does the user require any special technical expertise, particular artefacts or devices, special software or hardware devices to use or access the APIM?	grounded (A.17.1.)
Subject Inclusiveness	Are there any sensory, physical, cognitive disabilities that prohibit or restrict impaired users from using the APIM as designed?	grounded RF AQ (A.17.2.)
Maintainability Effort	What is the time and effort spent in fulfilling these following tasks: –application and enrolment processes –authentication processes –replacement of authentication data –replacement of keys and X.509.3 certificates –securing of authentication data or keys – biometric template updates –other administrative functions relating to hardware or software?	deduced AQ (A.17.3.)
Use Maintenance Effort	What are the likely users effort involved with managing: –APIM and associated devices or artefacts; –back-ups and expiration or retraction of authentication access; or –loss of authentication data or keys?	deduced (A.17.4.)
Use Convenience Comparison	Is the user's time consumed at replacement, enrolment and operational use together with maintenance functions commensurate to the importance, responsibilities or liabilities, of users performing their task?	Not-grounded (A.17.5.)
Technology Provisioning	Does the APIM operate using commonly available technology or are the components specialised dedicated to that APIM or underlying service? Is processing performed centrally and shared with ubiquitous devices? Does device provisioning, and contributions made by the owner, aid user accessibility or introduce barriers, including operating costs, to users?	grounded RF (A.17.6.)

Table C.22: Accessibility Results Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Privacy Impact	Does the use of the APIM affect user's feelings or beliefs?	grounded (A.15.13.)
Assurance Evidence	What evidence demonstrates the APIM's ability to meet the assurance requirements set?	Not-grounded (A.14.18.)
Costs Recovery	What are the likely costs for making the APIM mandatory to all users in the community, as opposed to making the use of the APIM optional? Is there capacity to recover some of these costs?	grounded (A.18.7.)
Identification Time	What is the time to: activate the sensing device; capture user input signals; extract signal parameters; retrieve files and other ancillary processing; compare the input signals against those stored; communicate between the various APIM components; and effect notification of acceptance or rejection or other results? What are the possibilities to shorten the overall processing timescales? to improve the acceptability for users and other stakeholders?	grounded (A.14.7.)
Practical Experience	What are the experiences from owners/users/administrators from using this APIM in environment similar to the context application?	grounded (A.12.19.)
User Confidence	To what extent will the user hold the firm belief that the APIM will protect their interests, e.g. privacy, safety within the specified operational context? Does the APIM demonstrate: –explicit authorisation (The system does not become unsafe automatically); –visibility (The system reports the security status); –revocability (The user may undertake tasks to change the security status); –path of least resistance (The user does not inadvertently choose to make the security status unsafe); –expected ability (The user should be aware of all the systems' abilities); –appropriate boundaries (The user should be able to distinguish what aspects are relevant); –expressiveness (The user should be able to instruct the system what tasks are to be performed); –clarity (The user should understand the all the system's tasks); and –dependability (The system protects the user from being fooled)?	Not-grounded (A.17.7.)
Criticality of Contingency Plan	Is there an appropriate contingency plan and disaster recovery policy to ensure continued operations in the event of an APIM failure, partially or totally?	Not-grounded (A.16.9.)
Repair Response Times	What are the proposed repair response times and the planned delivery of replacement parts? Is this acceptable to the system owner and the user community?	deduced (A.16.10.)
Liabilities and Responsibilities	Are the APIM's stakeholder responsibilities clearly defined and delineated so that stakeholders may determine their respective liabilities?	grounded (B.23.1)

Table C.23: Solution's Issues Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Components Integration	Are devices and/or artefacts, hardware and software components, integrated to function correctly, as designed, in a manner that meets the APIM's requirements?	grounded (B.24.1.)
Circumvention Susceptibility	What is the difficulty, in terms of knowledge and resources, to circumvent the APIM, without the need to deceive the processing logic?	grounded (A.14.6.)
Signal Predictability	Is the APIM's signal authentication data sufficiently disguised to prevent strangers, friends and family etc. from determining it?	Not-grounded (A.14.10.)
Signal Abundance	What is the APIM's number of possible user input signal or signal extraction permutations or total key space?	grounded (A.14.11.)
Signal Disclosure	Is the APIM's authentication or key or verification data easy to record or transfer, easily observed at entry or almost impossible to disclose?	grounded (A.14.12.)
Signal Robustness	Does the APIM's signal data capture device withstand various known attacks, e.g. keyboard loggers, brute force attacks, theoretical attacks?	grounded (A.14.13.)
Exploitable Vulnerabilities	What are the known exploitable weaknesses in deployed or candidate APIMs?	grounded RF AQ (A.14.16.)
Vendor Assessment	What is known about the potential vendors/integrators experience and capabilities for delivering the APIM to the proposed design?	grounded (A.12.20.)

Table C.24: Solution's Vulnerabilities Evaluation Theme

Factors	Criteria Questions	Status/Identifier
Implementation Costs	What are the total APIM project fulfilment costs? Does this estimate include installing devices computer, networks, software etc and new or changes to deployed infrastructure? To what extent might a modular approach, particularly the application interface design, control expenditure?	deduced (A.18.1.)
Maintenance Costs	What are the actual operational and support costs in relationship to the business case's estimations? Do these costs include support costs of hardware; software; maintenance processes; personnel; and training costs? What is the cost impact to change existing procedures?	Not-grounded (A.18.2.)
Mechanism Anticipated Lifespan	What is the APIM's and its components predicted life expectancy? Will it allow upgrade or migration or replacement of the APIM? How do these aspects impact upon the costs of using different user input signals or vendors?	Not-grounded RF AQ (A.16.2.)
Cost of Input Devices	What is the unit cost of signal input device including firmware and its protection, in the event it was stolen or to prevent its internal operation from being examined?	deduced (A.18.3.)
Cost of Artefacts	What is the unit cost of the artefact, e.g. an integrated circuit card and its protection, if it was stolen, or in order to prevent its internal operation from being examined?	grounded (A.18.4.)
Management Costs for Input Devices or Artefacts	What are the estimated costs for distributing and logistical support for any devices and/or artefacts associated with the APIM?	Factor Deleted (A.18.5.) Merged with (A.18.2.)
Infrastructure Processing Costs	What is the cost of the proposed solution for introduction of new or integrating the APIM technology into existing infrastructure in terms of network, hardware, software, support, personnel and training?	Not-grounded (A.18.6.)
Other Stakeholders' Costs	What are the total costs and/or effort for each party involved, excluding users' costs, in the use of the APIM, including hardware and software, to ensure its compatibility with the users' processes and the need to revise supporting infrastructures?	Not-grounded RF AQ (A.18.8.)

Table C.25: Stakeholders' Costs Evaluation Theme

Appendix D – EU State's eGates Programme Case Study: Questions for Interviewees

---

This appendix contains the questions posed to the interviewees involved in the EU State's Airport eGates Programme.

Interview Questions for Interviewees Involved with eGates Programme for Airports in the EU state.

The inquiry into Automated Personal Identification is building a theory(ies) regarding when a project should adopt a systematic methodology to select the optimum human recognition system or alternatively use an unstructured, yet flexible approach.

The research questions for this case study, therefore, focus on the approach as to how eGates were selected for the various airports, which assumes that an evaluation of many different factors was undertaken during the project. The research is not an assessment or judgment of the actual eGates that were selected or criticism of the processes involved in the selection; however, it seeks to gain insight into the way the eGates were considered and eventually selected.

The following questions will be used in an open interview and it is acknowledged that as an interviewee you may have contributed with limited knowledge of certain aspects of the projects.

1. When did you first become involved with the eGates projects and please describe your role?

2. Please describe the approach adopted to select the eGates?

3. How were the following project deliverables formulated or achieved:
4. objectives for the eGates?
5. operational requirements?
6. constraints and any policy directives, e.g. budget, health and safety regulations respectively?
7. key performance indicators upon which to base an assessment?
8. the suppliers and their solution together with its configuration chosen?
9. the results of the pilot exercises assessed?
10. Are there outstanding issues relating to eGates, in respect of cost implications, vulnerabilities and operational issues, e.g. usability, accessibility, reliability?;
11. In retrospect, is there any part of the approach adopted that you would recommend doing differently? Why?

The research seeks to gather information about your contribution or knowledge of how the project deliverables were established. Information on the deliverables is not required: the research concentrates on the decision processes only.

June 2011

Appendix E – Evaluation Themes and Factors (Stage C)

This appendix contains 25 evaluation theme tables showing the factors for evaluating an APIM as at Stage C of our factor validation effort, representing Step 9 of our research implementation plan.

The tables show the status of the evaluation factors following our validation efforts using the data from our EU State's eGates Programme Case Study. The status also indicates which evaluation factors were Grounded (G), Deduced (D) and Not-grounded (N) in our data. We show relabelled factors as 'RF' and criteria questions which required amendment as 'AQ'.

We assign an identifier to a new factor identified in Stage C, e.g. C.8.1., to denote stage created, evaluation theme and factor reference number, to enable each factor and its criterion question to be tracked through each subsequent validation.

The tables in this appendix contain the following evaluation themes:

Table E.1 Business Case Evaluation Theme;

Table E.2 Stakeholders' Objectives Evaluation Theme;

Table E.3 Stakeholders' Risks Evaluation Theme;

Table E.4 Community's Characteristics Evaluation Theme;

Table E.5 Usage Environment Evaluation Theme (formerly Task Environment Evaluation Theme);

Table E.6 Constraints Evaluation Theme;

Table E.7 Policies Evaluation Theme;

Table E.8 Functional Requirements Evaluation Theme;

Table E.9 Privacy Compliance Evaluation Theme;

Table E.10 Registration and Enrolment Evaluation Theme;

Table E.11 Performance Requirements Evaluation Theme;

Table E.12 Assurance Requirements Evaluation Theme;

Table E.13 Task Dialogue Evaluation Theme;

Table E.14 Envisaged Issues Evaluation Theme;

Table E.15 Envisaged Vulnerabilities Evaluation Theme;

Table E.16 Predicted Costs Evaluation Themes (formerly Forecasted Costs Evaluation Theme);

Table E.17 Security Architecture Evaluation Theme;

Table E.18 Identifier Management Evaluation Theme;

Table E.19 Reliability Results Evaluation Theme;

Table E.20 Usability Results Evaluation Theme;

Table E.21 Technology Management Evaluation Theme (formerly Technology Evaluation Theme);

Table E.22 Accessibility Results Evaluation Theme;

Table E.23 APIM's Issues Evaluation Theme (formerly Solution's Issues Evaluation Theme);

Table E.24 APIM's Vulnerabilities Evaluation Theme (formerly Solution's Vulnerabilities Evaluation Theme); and

Table E.25 Stakeholders' Costs Evaluation Theme.

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Feasibility Outlook (A.1.8.) D RF	The likelihood of an APIM fulfilling its purpose from a business, legal, operational and technological standpoints should be ascertained at the outset.	Are there similar deployments precedents, a conceptual prototype or independent expert opinion that could provide indications on the potential of an APIM fulfilling its purpose?
Risks Identified (A.4.2.) D AQ	Stakeholder risks need to identified, understood and articulated in order to determine the mitigating controls provided by the APIM.	What are the stakeholders' business risks which require control? What vulnerabilities and threats have been identified which may impact the assurance sought from the deployed?
Defined Business Problem (A.5.1.) D	If the business problem is not fully understood and resolution objectives articulated then solution cannot be evaluated for its utility to resolve that stated business problem.	Is the personal identification problem fully understood and expressed as a high-level problem description and not attributes from potential solutions? How effective and efficient are existing mechanisms?
Project Sponsorship (A.5.2.) N AF AQ	The basis for the approved investment for effort to introduce or revise an APIM needs to be stated at the outset.	Is the business analysis of stakeholders' objectives for an APIM supported by a business case with justification for expenditure?
Alternatives Investigated (A.6.4.) D AQ	Previous investigations should reveal the issues and costs related to resolving the business problem. Using biometrics or hardware tokens need due consideration.	What are the learnings from investigations of possible solutions, including biometrics, or similar APIM deployments to address the human identification problems?
Security Motivation of Authorised Subjects (A.7.10.) G	The authorised subjects may not derive benefits for using the APIM. The incentives or penalties that should persuade subjects to manage credentials in an acceptable way need to be stated.	What are the incentives to encourage subjects to use the APIM as designed? What are the disadvantages or liabilities that may apply for inappropriate subject behaviour or neglect?
Entity Relationships (A.7.8.) G RF AQ	Stakeholders interact in through informal arrangements or through scheme rules to ensure the APIM provides an acceptable and viable proposition to resolve a stated business problem.	What is the relationship between the APIM's issuing authority and relying party entities and other stakeholders, including the subjects themselves. Is a formal usage agreement or contract in place?
Identity Authorisation Model (A.9.1.) D RF AQ	A description of the direct and indirect stakeholder entities, including the subjects, in the application context helps to establish the role of each entity and its relationships with other entities.	Who are the stakeholder entities involved with the application context? Which entities may use subject identifiers and/or credentials for identification or authentication purposes?
Contextual Purpose (B.7.1.) G	The purpose of the APIM needs to be fully understood and communicated in terms of desired outcomes or objectives to direct effort to evaluate and select the optimal APIM.	Why is the APIM being introduced or revised? What are the business goals that describe the business problem or opportunity, priority values of aspiration to be achieved in the scope of the APIM's intended usage?
Stakeholders' Benefits (B.7.2.) G	The benefits, tangible and non-tangible, to revise or introduce an APIM need to be stated at the outset. Some benefits should be derived from investing resources to introduce or revise an APIM.	Will the APIM be used to protect data assets or enhance the operations of one or many stakeholders? What are the advantages to the direct and indirect stakeholders to introduce or revise the APIM?
Programme Governance Framework (B.7.3.) G	The decisions processes between the stakeholders need to be stated, particularly the entity empowered to make changes to consultation or decision processes or representative body membership.	What entity or group has the authority for decisions or authority to change processes to select an APIM? How does the governance framework operate for decision-making amongst its stakeholders?
Assurance Effectiveness	This factor is a replication of Assurance Results Evaluation Theme.	(A.2.4.) deleted

Table E.1: Business Case Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Subject Privacy Protection Aims (A.4.5.) N RF AQ	Clarification is needed on how subjects' private data are to be protected in line with legal, contractual and ethical obligations.	What are the intended courses of action to protect subject's private information?
Sponsorship Aims (A.4.4.) G RF AQ	The sponsor's goal or prime objectives need to be clear to introduce an APIM or revise a deployed APIM, which may align or conflict with other stakeholders' or subjects' objectives.	What are the aims of the sponsor stakeholder in terms of asset protection and business enhancements? How do these aims align with the objectives of other stakeholders, including subjects and users?
Stakeholders' Business Rationale (A.1.1.) D RF AQ	A description of stakeholders' benefits is needed to support the introduction of an APIM or changes to current protection.	What arguments support stakeholders' aims to instigate the introduction of an APIM or changes to a deployed APIM? Are all stakeholders interests included?
Subject / User Acceptability Rationale (A.3.2.) N RF AQ	The reasons for subjects and users willingness to use the APIM in the application context should be explained.	What are the stakeholders' arguments that describe the reasons for subjects' acceptance an APIM for its intended usage?
Control Objectives (B.1.1.) G	The impact on annual loss expectancy by introducing or revising an APIM access should be described as an aim.	What are the desired risks control outcomes sought by introducing or revising an APIM to the current situation?

Table E.2: Stakeholders' Objectives Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Risks Treatment Strategy (A.2.8.) D RF AQ	Stakeholders may have different risks and alternative risk appetites to manage identified risks and residual risks.	What are the stakeholders' risks management strategies (alleviation, transference, avoidance, acceptance) for treating identified risks and the remaining residual risks?
Impact on Stakeholders (A.7.9.) D	The consequences of an APIM failure need to be determined for all stakeholders, including subjects.	What are the likely consequences if an APIM failed, which includes unauthorised access to an asset and the unavailability of an asset?
Compromise Scenarios (A.6.9.) N	Social engineering attacks on subjects and technological based attacks need to be articulated.	What types of APIM user deception attacks can be foreseen? What are the known technological or social based attacks?
Privacy Impact Assessment (A.8.3.) D AQ	Organisational stakeholders may have legal and contractual obligations to protect subjects' private data.	What is the impact on each stakeholder and related subjects if subjects' private data are compromised? how does this impact influence the requirements for the APIM?
Attack and Compromise Probabilities (A.2.1.) D AQ	The probability of compromise helps to determine appropriate security controls given the value of the assets and known vulnerabilities and threats.	What is the likelihood of a deliberate attack on the APIM? Also what is the probability of errors occurring? Do these projections include an analysis of historical events from all stakeholders?
Vulnerabilities Identified (A.2.3.) G RF	The known vulnerabilities help to determine the current levels of assurance in the application context and also identifies the desired assurance of an APIM.	What are the known exploitable weaknesses in existing operations or potential flaw in new operations which may include technological, operational and human error aspects?
Impact Value Rating (A.2.2.) G AQ	The value of damages or consequences to business operations needs to be established in order to determine the appropriate security controls, including the optimal APIM.	What are the estimated impact costs or impact ratings if stakeholders' assets and resources were to be stolen, destroyed or modified in the event of an APIM failure?
Threat Motivation (A.2.7.) G RF	The motivation behind the threats with the rewards and deterrent penalties to miscreants help determine APIM's objectives as countermeasure.	What is underlying stimuli or goals of miscreants that lead to attacks on the APIM? Are deterrents proportionate to potential rewards? What are attackers' motives?

Table E.3: Stakeholders' Risks Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Subject Proposition (A.3.1.) G RF AQ	The general acceptance of an APIM type does not immediately validate its usage for a particular application context.	What are the stakeholders' expectations relating to subject community's adoption of an APIM? Do subjects derive sufficient benefit to encourage the proper use of an APIM?
Social Attitudes (A.3.3.) G AQ	The acceptability of an APIM for its intended purpose to the subject community gives an indication on subjects' motivation to use the APIM as designed.	What subject attitudes have been established from surveys on similar APIM deployments? How do these surveyed responses support or negate effort to introduce or revise an APIM?
Community Membership (A.3.4.) G AQ	The categorisation of community members informs the scope for the APIM. Membership characteristics provide differentiators and indications on the nature of the community together with expansion or contraction rates.	Who are the subjects and/or users in the context's community? Are the subjects direct operators of the APIM? Is community membership open to all individuals or restricted and what are those restrictions?
Subjects' Trust (A.3.5.) D RF AQ	The degree of reliance and acceptability of the APIM may be based upon existing relationships and perceptions of trustworthiness of public and private organisations. Without trust subjects may not co-operate or use the APIM as intended. Trust may also develop from a contractual agreement or legislation.	What is trust relationship between the APIM's issuing authority and the subject? Is it a new relationship? What is the trust relationship between the relying party and the subject? Are there any issues that would enhance or limit existing relationships or inhibit relationships from developing?
Subject and User Training (A.7.2.) G RF AQ	The subject community's capability and motivation to absorb technical and operational skills could help to widen the options of credentials and/or other devices.	Is the subject community capable of absorbing knowledge from educational material supplied relating to the proper usage of credentials or other devices?
Population Traits (A.7.4.) G	The subjects' characteristics are important to avoid exclusion from the community and provides traits upon which requirements may be specified and designs may be evaluated.	What are the main characteristics of the subject community, in terms of population demographics, physiology, behaviour, appearance that pose disadvantages or create advantages for the APIM selection options?
Users' Cooperation (A.7.11.) D	The subject community which is to use an APIM may impact, inadvertently, its effectiveness and efficiency.	What are the expectations that all individuals will cooperate voluntarily with an automated identification process in this application context?
Privacy Assurance (A.8.8.) D AQ	Evidence is needed to substantiate claims of compliance with privacy legislations and the commitments provided to the subject community.	What assurance is required to demonstrate anonymity, unlinkability, unobservability and anonymity compliance to data privacy legislation and security policies?
User Obligations (B.3.1.) G	The disadvantages or liabilities of the usage terms for the APIM may outweigh any potential benefit or proposition to the subject or user. Some APIMs contain terms and conditions or are mandatory.	What subject consent or acceptance is needed for user and/or subjects to acknowledge their responsibilities or liabilities for the APIM? To what extent do these obligations negate their benefits of using the APIM?

Table E.4: Community Characteristics Evaluation Theme

Factor, Identifier and Status	**Factor Explanation**	**Criteria Questions**
Environment Ergonomics (A.2.5.) G RF AQ	The environment's characteristics may impact upon the ergonomic operation of the APIM.	How will the APIM operate in the intended physical usage settings? Will it be required to operate in consistent environments? What attributes differentiate its usage in the envisaged usage settings?
Technical Control (A.6.8.) G AQ	Subjects' control of technical devices may impact the requirements for an APIM and may influence the subject's acceptance and usage of a device, particularly. if they are unfamiliar.	Does the subject utilise a ubiquitous device or is technology supplied by the APIM issuing authority or relying party? What physical control should stakeholders have over the APIM and its components? To what extent should users control devices' logical operations?
Logical Usage Settings (B.4.1.) G	The information systems that the APIM supports need to be described together with the supporting devices, infrastructure and operating systems.	What are intended logical applications for the APIM, the types of operating devices and operating systems?
Physical Usage Settings (B.4.2) G	The physical location may adversely impact or enhance the subject's ability to use the APIM.	Where will the APIM operate? What are physical environmental characteristics of these locations?
Usage Logistics (B.4.3.) G	The usage scenarios for automated identification requires clarification to ensure the scope and purpose for the APIM is articulated and understood.	Will the APIM be used for physical identification, logical identification or both? Have usage cases been developed?

Table E.5: Usage Environments Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Political Considerations (A.1.4.) G RF AQ	The politics and economics relating to the application context may influence the requirements for the APIM.	What political or economic matters may hinder or support organisational change? How does this change impact the APIM selection?
Stakeholder Relationships (A.1.5.) G RF AQ	The relationships between the stakeholders and subjects together with implicit understandings could influence stakeholder collaboration.	What commercial, organisational or political stakeholder relationship issues hinder or support a proposition to introduce an APIM or revise an APIM deployment?
Regulatory Imperatives (A.1.6.) G RF AQ	Regulation may place restrictions or additional tasks on stakeholders to comply and to demonstrate compliance.	How does legislation and industry guidelines impact the stakeholder aims for an APIM in the proposed usage settings?
Budget Allocated (A.4.3.) N RF AQ	The budgetary capital and operational investments that stakeholders' commit influence requirements and choices on APIM solution candidates.	What funds and resources have allocated by stakeholders, to introduce an APIM or review / revise an APIM deployment, in order to minimise risk?
Contextual Legacies (A.5.4.) G AQ	The restrictions of the application context influence the proposition for the APIM. It is assumed that the APIM proposition does not start from a neutral historical state, whether technological or social norms.	What external existing issues relating to the application context could impact the stakeholders' and subjects' propositions, which include organisational issues, current practices, social norms, existing infrastructures and deployed information systems?
Subject Application and Signal Enrolment (A.10.2.) G RF	The application context may require that a subject's application and enrolment must be a face-to-face interaction. Alternatively, either or both activities are self-service or remote.	What are the restrictions in terms of the logistics or procedural activities that dictate where and how subject signals are acquired, generated and distributed?
External Performance Benchmarks (A.5.7.) G AQ	The reality of the environment influence the APIM's performance capabilities and reliability.	What are the performance limitations of the usage settings in which the APIM is designed to operate? What are the learnings from similar deployments?
Specifications and Information Technology Standards (A.5.5.) G RF AQ	Specifications for application contexts are designed to ensure technical and procedural interoperability and are also a claim to a specific quality.	What specifications are applicable to the APIM to ensure interoperability and requisite quality in the application context? Which standards are these specifications based upon?
Users' Costs (A.3.6.) G AQ	The APIM's design may utilise ubiquitous or special devices and costs to ensure compatibility may be incurred by subjects rather than stakeholders.	What are the potential costs for users to use the APIM, in terms of hardware, software, infrastructure service purchases and compatibility with users' processes?
Signal Data Exchange Interoperability (A.5.6.) G RF AQ	Data may need to be exchanged between relying party stakeholders and credential issuing authorities.	Is there a need to exchange subjects' signal data or other attributes with other organisational entities for the APIM's application context? Do interoperability specifications exist?
Auditing Subject Data Usage (A.1.7.) N RF AQ	The periodicity and measures for using and storing signal data may impact potential investigations or efforts to comply with legal or contractual obligations.	What is the retention period and archive storage rules for data used by the APIM to automatically identify a subject and what are the legal and risks associated auditing requirements for these data?
Compromise Recovery Inhibitors (B.5.1.) G RF AQ	The obstacles which may affect recovery of an APIM should be articulated.	How will stakeholders recover the APIM in the event of failure? Are there technology, procedures or scheme rules which inhibit recovery actions?

Table E.6: Constraints Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Archiving Data Policies (B.6.1.) G RF	The stakeholder policy on data or audit log retention may differ to that required by privacy regulation or rules of the context in which the APIM operates.	What are the stakeholders' policies on retaining and archiving data generally? How do these policies relate to the APIM subject signal and other private data in usage transactions?
Organisational Policies (A.8.1.) G RF	The stakeholder organisational policies may give direction on issues relating to an organisation's governance.	How do stakeholder organisation policies, including privacy policies, impact the automated identification of employees, customers, agents or partners?
Recognised Issues (B.6.2.) G AQ	Contextual issues should be articulated and researched as knowledge of their impact may affect the requirements for an APIM.	Are there issues relating to the application context explicitly accepted by stakeholders, including users? Are these issues discussed in the public domain?
Authorised Identity Evidence Sources (B.6.3.) G	The stakeholders must provide direction as to which entity or group determines the policies on the proof identity evidence, registration and enrolment processes.	Which entities are empowered to provide policy on acceptable proof of identity evidence, registration and enrolment?
Privacy Laws Compliance (A.8.2.) N AQ	The individual or accountable group assigned with the responsibility of compliance with legislation needs to provide direction on privacy issues.	Have stakeholders assigned the responsibility of complying with privacy laws to a specific entity with responsibility to manage this corporate governance issue?
Programme Implementation (A.4.1.) D RF AQ	How does each stakeholder go about implementing agreed organisational change policies?	What is the stakeholders' strategy and governance framework to implement organisational changes?
Requirements Gathering Methodology (A.5.3.) D AQ	The methodology used by stakeholders programme may influence the requirements for the APIM.	How will the development programme gather and articulate their business requirements for an APIM?
Stakeholders' Resolution Processes (B.6.5.) G RF	Stakeholders should have the means and procedures for settling disputes with other stakeholders and subjects.	What are the stakeholders' policies for settling disputes with partners, customers and other entities and also subjects?
Subject Duress (A.17.8.) N RF	The context may dictate that subjects should be able to use a 'panic button' to notify duress while using the APIM.	Does the application context warrant the inclusion of a notification alarm to indicate coercion of a subject while using the APIM?
Imposing Sanctions (B.6.4.) G	Stakeholders may choose to seek criminal damages for miscreants or impose disciplinary reprisals.	What is the stakeholder policy for dealing with miscreants or authorised users which improperly use the APIM?

Table E.7: Policies Evaluation Theme

Factor, Identifier and Status	**Factor Explanation**	**Criteria Questions**
Subject Signals Enrolment (C.8.1.) G	The processes to enrol subjects' signals must be specified. Some subjects' signals may be acquired remotely or generated remotely.	What functions are required to capture subjects' signals or generate authentication data during local or remote enrolment?
User Authorisation Model (C.8.2.) G	The user authorisation model between the user and stakeholder entities need to be understood.	What entities are involved with the identification or entification? What are their roles within the automatic identification and authorisation processes?
Administration Processes (C.8.3.) G	The entity assigned with responsibility of administering the APIM must have access to the required system functionalities in order to execute their tasks.	What are the required processes to enable administration personnel to perform duties to fulfil all the life-cycle tasks to support the APIM and its users? What safeguards are required to prevent access to private data and processes?
Signal Capturing Device Interoperability (B.8.3.) G	The devices for the APIM may be bespoke or ubiquitous and may also need enhancement to comply with interoperability specifications.	What specifications are the devices and software required to adhere to? What is required to ensure these devices operate universally?
User Authentication Attributes (B.8.1.) G	Identification and authentication may be linked to access control mechanisms, which may require attribute data from the APIM to function properly.	What attributes need to be captured from the APIM to enable verified users to have access to functions and data in the user authorisation model?
Identification Mode (A.6.1.) G RF AQ	Positive identification proves that a subject is enrolled whereas negative identification proves that a subject is not enrolled or known.	Is the purpose of the APIM to positively identify an enrolled subject or to ensure that a person is not enrolled? Is there a need to consolidate both functions?
Multiple Subject Signals (A.6.5.) G RF AQ	The assurance requirement based upon risks dictate whether a single signal is adequate or that fusion of biometrics, knowledge based or computed signals using an ICC are required.	Do the risks and assurance requirements suggest the use of a single subject signal or necessitate the fusion of multiple subject signals possibly using calculated data from artefacts or generated by other sources?
Identification Transparency (A.6.2.) G RF AQ	Covert identification rules out some APIM types, particularly based user knowledge. Most APIMs require overt subject participation. An application context may permit both covert and overt verification.	Does the requirement entail the subject being unaware of the APIM? If so, what are the legal and technological constraints that apply to a covert APIM? Does the requirement allow for covert and overt flexibility of transparency?
Subject Signal Storage (B.8.2.) G	The requirement for the signal's format(s), its storage location(s) and its required protection dictates how the identification or entification processes are to operate.	What format will the subject signal be stored for identification or entification? Where should that data be stored? How should that stored data be protected?

Table E.8: Functional Requirements Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Approved Privacy Asset Registrars (A.8.4.) G RF AQ	The entities that are authorised to verify and maintain subjects' private data in a repository. This function may differ to registration authorities and enrolment agencies or identity service providers.	What entities have been delegated powers to acquire subjects' private data, store, maintain and use it and possible to issue credentials? Does this agency gain approval to register, to enrol subjects and to issue credentials?
Privacy Assets Appeals Procedure (A.8.5.) N	The stakeholders may be required to deal with events where subjects' may not be entitled to access an asset or may not be able to produce the required biometric feature or may dispute stakeholder claims of improper usage.	What procedures are to be put in place for those applicants who are denied access to an information system or have their access revoked, either legitimately or erroneously?
Privacy Asset Access Controls (A.8.6.) D RF AQ	Private data are assets belonging to subjects that are maintained by a custodian or approved entities that comply with privacy legal requirements.	What documentation describes the processes to ensure that only authorised users may collect, use, maintain, disclose and protect subjects' private data for the APIM?
Privacy Asset Compromise (A.8.7.) G	Stakeholders should have the processes and necessary resources to manage privacy compromise incidents.	What processes are required to co-ordinate with authorised entities, responses to notifications of suspected privacy violations?
Privacy Asset Inspection (A.8.9.) N	Auditors or government bodies may require to ensure that data are held in compliance to law and contractual obligations.	What processes need to be put into place to allow inspection of the privacy asset register generally which also allows subjects to access to their personal information held?
Privacy Controls Erosion (A.8.10.) N AQ	Stakeholders need to demonstrate that controls to maintain subjects' private data continue to be effective.	What processes are necessary to prevent the existing controls on maintaining subjects' private data from being eroded? Should these processes include subject data held on an artefact?

Table E.9: Privacy Compliance Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identity Proofing Methods (A.9.2.) G RF AQ	The methods by which administrative personnel verify presented evidence are important to detect fraudulent identity applications.	How should the identity knowledge or documentary evidence presented by the applicant be verified as authentic for the genuine subject?
Identity Proofing Rules (A.9.5.) G AQ	These rules determine who is entitled to be a community member, the evidence to support that entitlement and the authorising entity empowering that entitlement.	What are the identity verification processes and the required evidence and authorisation which entitles a subject access to a resource or asset? What attributes entitle or prohibit a user from being a subject member of the community?
Approved Registration Agencies (A.9.6.) G	The entities authorised to check subjects' entitlement to assets, which performs the verification of seed identification evidence, subject's application data, issuing identifiers and delivering credentials.	What entities have been delegated powers to register, issue identifiers, acquire subjects' signal data and issue and maintain credentials for the APIM? Does this entity also have authority to store and use subjects' data?
Application and Registration Processes (A.9.7.) G RF AQ	The entity to perform the registration of an authorised subject and the rules that govern the registration processes require articulation.	What are the application, registration and enrolment processes for authorised subjects. What are the complete end-to-end processes, including artefacts to subjects?
Identity Proofing and Registration Accreditation (A.9.11.) N	The may be a requirement for the identity verification and registration processes to be independently scrutinised to address risks identified or to control access to subjects' private data.	Does the identity proofing and registration processes require accreditation by an independent body?
Accredited Processes Applicability (A.9.12.) D AQ	The accreditation is to ensure that an identity checking service provider's processes meet a particular specification to offer an accredited identity checking service.	What entities provide the identity verification functionality and is there a requirement for their processes to be accredited? Does the provider also register individuals or carry out enrolment tasks?
Approved Processes Adoption (A.9.13.) D AQ	The approval relates to whether the identification checking service has to obtain the necessary authorisation to perform and provide such services.	What authorisation is required before the adoption and operation of an approved identity verification service operates on behalf of stakeholder entities, including relying parties?
Credential Identifier or Entifier (A.6.3.) G RF AQ	The requirement to link the identification process to a unique identifier impacts the APIM mode of operation. An identifier enables 1–1 authentication. Entification involves 1–many searching.	Is a unique identifier assigned to authenticate the subject or entification using the subject's attributes? Is there a need for subject anonymity or the use of a pseudonym to mask the subject's declared identity?
Acceptable Subjects (A.9.4.) G RF AQ	The rules to implement the policy for distinguishing between subjects entitled to access assets or resources and those individuals that are not authorised.	What does the policies stipulate in terms of determining acceptable members or acceptable characteristics of the subject community? Are there differing interpretations to the rules which constitutes stakeholders acceptability?
Enrolment and Credential Issuance (A.9.8.) G RF AQ	Registered subject's signals upon which subjects will be entified or authenticated must be captured, generated and distributed securely. Signals may need captured directly from the subject and generated to a specific standard.	What are the processes to capture the subjects' signals for the APIM? Does this process require the subject to attend an enrolment facility or generate initial authentication data remotely or is the data generated by other entities and sent to the subject?
Acceptable Identity Evidence (A.9.9.) G AQ	The seed documentation and its sources validate the veracity of the claimed identity. Issuing authorities and relying parties rely on this evidence.	What are the acceptable identification source evidence for proof of identity processes? How is that evidence itself validated or cross-referenced?

Table E.10: Registration and Enrolment Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Maximum Identification Attempts Limit (C.11.1.)	Limiting the number of user attempts may reduce demands on system resources and may limit replay attacks at the expense of denying genuine users access to assets.	How many attempts are users allowed to identify or to entify a subject ? What is the maximum attempts before access is disabled?
Maximum Identification Time Limit (C.11.2.)	The identification transaction time may need to be responsive to operational tasks and risks?	What is the maximum time permitted for each subject identification or entification attempt before another try may be attempted?
Operational Ergonomics (A.10.1.) G AQ	The nature of the environments impacts the ability of an APIM to operate consistently, e.g. lighting variations.	Is the APIM to operate in consistent conditions or variable environments? What are the variable conditions which may impact performance?
Subjects' Signal Tolerations (A.10.3.) G AQ	This rate focuses on the input devices and the need for calibration, both initially and continually.	Will the APIM need to flag poor quality subject signals captured? What is the toleration rate before further subject signals or additional data are acquired?
Subject Throughput Rates (A.10.4.) G	The timing impacts usability and security and vulnerabilities stemming from repeated attempts or long feedback response times.	What are the required throughput rate requirements expressed in terms of minimum numbers in a specific time? What is the maximum queuing timescales?
Subject False Non-match Tolerations (A.10.7.) G	The requirements of the application context may necessitate that genuine subjects are rejected at the expense of detecting impostors, or vice versa.	How many false non-match errors are tolerable or acceptable for subject signals, i.e. false accept rates and false reject rates, which are commensurate to the risks of the application context.
Intervention Rate (A.10.9.) G	The subjects may need assistance and interventions may improve unsupervised throughput over a period of time.	What is tolerable error rate before assistance to a subject is offered by a trained operative? Does this rate allow for user familiarisation of the APIM?
Impostor Detection Rate (A.10.10.) G	The risks in the application context determine the rate at which an APIM is required to perform to detect an impostor.	In respect of the risks identified, what is the acceptable probability that an APIM fails to detect an impostor?
Maximum Enrolment Time (A.10.14.) G	The enrolment time should not be protracted in respect of the context its risks and assurance requirements.	What is the maximum time permitted for each subject's signal enrolment attempt?
Maximum Enrolment Attempts (A.10.15.) G AQ	The number of enrolment attempts may inadvertently reduce the size of the subject community.	How many attempts is a subject allowed to enrol their signals? Would supervision increase or reduce the number of attempts?
Signals and Template Protection (A.10.19.) G	The data upon which identification and/or authentication decisions take place must be reliable.	What are the security controls required to protect the subject's signal data so that these data may be used for identification and/or authentication purposes?

Table E.11: Performance Requirements Evaluation Theme

Factor, Identifier and Status	**Factor Explanation**	**Criteria Questions**
Attack Protection and Detection (A.11.1.) G	The resources and skills to successfully compromise an APIM should be significant in order to deter misfeasance.	What are the technology resources and skills needed to successfully attack an APIM? Are attacks to be detected?
Assurance Test Tools and Methods (A.11.2.) G	The required tools and utilities need description to enable assessors to carry out the tests and evaluate result data.	What tools and facilities are required to perform functional and assurance tests described in the testing plan?
Documentation and Test Data Availability (A.11.3.) G	Lack of documentation should make it harder for attackers to acquire the relevant knowledge to attack the APIM. Evaluators either test the APIM with or without this knowledge.	What information are to be made available to assessors to test the APIM? What documentation will remain confidential and which elements will be in the public domain for attackers to interrogate?
Functional Testing (A.11.4.) G	These statements inform potential suppliers and developers of APIMs on the various types of attacks envisaged and how the APIM should respond to each type of attack.	What is the desired reliability to ensure the APIM functions correctly? Are assurance tests to be performed on documented attacks and/or tested by external expertise? What are the behavioural expectations in response to each type of attack?
Audit Logs (A.11.5.) D	Data are required to demonstrate compliance but also assist in gaining an understanding on performance and to investigate security breaches.	What data are required to meet regulatory reporting and risk management functions? Are assurance data required for operational management and investigation purposes?
Assurance Assessment Methodology (A.11.6.) G	The way the assessment is performed should be objective, repeatable and auditable based upon substantiated result data and a testing plan.	What is the assessment framework to test the APIM? Has a testing plan and test resources been allocated to carry out assurance assessments?
Assurance Tests (A.11.7.) D AQ	The requirements for proposed devices and artefacts need to be described together with the test data needed in order to test for assurance. The tests may be incorporate functionality from internal or external designs.	What are the operational qualities for any required physical devices or artefacts that subjects may need to use? How are these artefacts to be protected? What test data are required, as evidence, on the devices' assured operation?
Combining Signals (A.10.11.) G RF AQ	The fusion of two or more subject signals may improve the identification or authentication of the genuine subject.	Do risks dictate the requirement for two or more subject signals to improve the identification or authentication of the genuine subject?

Table E.12: Assurance Requirements Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Interaction Dynamics (A.6.6.) G AQ	The usage settings will determine how the subjects' signals are to be captured, through the types of device, which may be operationally conducive. A poorly HCI design may be a disincentive to potential users.	Is the APIM interaction to operate as a sub-process in a subjects' system usage task? Does the interaction use ubiquitous devices? Do these devices need to work in particular ergonomic, physical or logical conditions? What outcomes need to be avoided from poor HCI design?
Interaction Supervision (A.6.7.) G RF AQ	The degree of subject supervision or control needed to ensure the subjects' signals are sensed properly.	Do the signal input devices require subject involvement, subject supervision or should the APIM be designed for self-service?
Multiple Credential Impact (A.7.3.) G RF AQ	The similarity of input devices may lead to user confusion, errors or undesired behaviour. Multiple APIMs in similar usage settings may introduce usability difficulties and errors.	What are the input devices normally adopted for the types of usage settings envisaged? Does the proposed APIM need differentiate itself from other similar types of APIMs to avoid user confusion, error or behaviour?
Task Sequence (A.7.5.) G	The APIM interaction may appear at the start of the users' task, during and/or at the completion of the transaction. The logic of where to place the APIM interaction is dictated by how the user would habitually complete the task.	Does the APIM interaction comprise entire user's task or it is part of a transaction? What is the position(s) of the APIM interaction in the overall transaction? What usability impact should the APIM interaction avoid in relation to the user's successful completion of the overall transaction?
User Technical Expertise (A.7.6.) D AQ	The extent to which a subject population is able or willing to use a new device or process may impact the types of input devices and the nature of the APIM interaction.	What skills do the subjects or users need to learn to use the input device to record subjects' signals? Does the subject population have the capability and motivation to acquire such skills?
Usage Frequency (A.7.7.) D	The regular usage of an APIM may reinforce subjects' habits. Irregular usage may suggest that subject learning should be minimised.	What is the expected subject usage pattern for the APIM and could this pattern lead to habitual usage? Does this usage pattern apply right across the subject population?

Table E.13: Task Dialogue Evaluation Theme

Factor, Identifier and Status	**Factor Explanation**	**Criteria Questions**
Impostor Pass/ False Alarm Threshold (A.10.5.) D	The setting of the threshold depends upon the risks of the application context. The method to establish the acceptable rate should be articulated.	What is the acceptable identification decision threshold as determined by the risks in the application context? How is this rate to be determined?
Multiple Attempts Limit (A.10.8.) G AQ	A genuine subject may receive a false rejection erroneously. The increase in number of attempts, however, gives opportunities for impostors.	In the case of subject signal false non-match for a subject how many additional attempts for identification should the subject be permitted before an action is instigated?
User Equipment Needed (A.10.12.) G RF AQ	The costs and effort for users to set up the APIM may not be commensurate to users' potential benefits.	What equipment, including costs, and effort is required by users to set up the APIM in comparison to users' potential benefits?
Enrolment Supervision (A.10.13.) G AQ	The quality of data required may necessitate intervention to ensure that signals are sufficient for intended purpose.	What quality do the subjects' initial signals need to meet for automated identification before invoking operative intervention?
Enrolment Failure Arrangements (A.10.16.) G	Some subjects may be excluded and alternative measures may be needed to enable accessibility. Some subjects subject may try to exploit exemptions.	What measures are required should subjects be unable to produce the signals to the required quality, either temporary or permanently?
Vendor Capabilities Evidence (A.10.17.) G RF AQ	Data showing a track record provides an indication on a supplier's potential to deliver and perform to the terms of a contract. Financial standing and local representation may also have a bearing on acceptability.	What type of evidence is required from potential suppliers that shows they can supply the APIM provided in their proposals? Do they need to supply references to deployments in similar application contexts or geographic locations?

Table E.14: Envisaged Issues Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identity Proofing Comprise (A.9.10.) G	There should be the means to detect fraudulent identity claims and prevent false registration applications. A credential could be issued to an individual who is not entitled erroneously or unwittingly.	What are the processes that detect fraudulent identity claims or false registration? Do the risks dictate that the identity verification, registration and enrolment require the segregation of operatives' duties?
Genuine Failure Impact (C.15.1.)	The impact of the failure of an APIM to correctly identify a subject needs to be understood and quantified.	What is the impact of an APIM failure to correctly identify genuine subjects?
Acknowledged Conceptual Vulnerabilities (C.15.2.)	The requirements acquisition processes should reveal vulnerabilities that cannot be resolved. Data are required required as an explicit acknowledgment.	What are the conceptual vulnerabilities that have been accepted by stakeholders in terms of partial or total failure or compromise?
Availability Goals (C.15.3.)	The availability of the APIM is critical to support the business operations. Slack periods may allow maintenance tasks to be performed.	What are the availability requirements for the APIM? Are there peak processing periods or time slots when maintenance may be carried out?
Resource Limitations (A.11.8.) D RF	Insufficient resources, technical competencies and available infrastructure may restrict the choice of APIM.	What personnel, facilities and infrastructure are committed to design, test, deploy and operate the APIM?
Receiver Operating Characteristics and Influences (A.10.18.) G RF AQ	Each point on the ROC curve defines the acceptable vulnerabilities of the APIM. It is an acknowledgment of these vulnerabilities and influences.	What are the acceptable vulnerabilities of false rejects to false acceptance across all operating points? What influences the variations of these points across the threshold curve?
Impostor Pass Impact (A.10.6.) D RF	The impact of the failure of an APIM or its circumvention due vulnerabilities needs to be understood and quantified.	What is the impact of an APIM's failure to correctly identify impostors, particularly setting the rate too low to detect deliberate attacks?

Table E.15: Envisaged Vulnerabilities Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Expected Lifetime (C.16.1.) G	The stakeholders expectations regarding the return on investments need to be ascertained.	What is the expected lifetime usefulness of the APIM for the application context based on Return of Investment (ROI) calculations?
Backward Compatibility (A.10.20.) G AQ	The reuse of existing infrastructure existing procedures necessitate accommodating existing capabilities.	Is backward compatibility required to existing APIMs or accepted operating norms or existing capabilities or infrastructures?
Usage Flexibility (A.10.21.) G AQ	The costs associated with a single purpose may not bring sufficient returns on stakeholders' investments.	Is the APIM designed for a single purpose or is it ubiquitous in design to be used for a number of approved applications?
Scalability (A.10.22.) G RF AQ	The take up of services and an APIM may be difficult to predict. All projections should be validated as over or under capacity may impact costs and performance.	What scalability is required in terms of responding to population growth or decrease? How quickly should a response be required in terms of numbers and timescales to ensure sufficient capacity?
Systems Upgrade Impact (A.10.23.) D RF	While it may be desirable to upgrade an APIM's components the effort, disruption and costs of revising deployed systems needs to be estimated.	What are the acceptable disruption, for the APIM owner, stakeholders and its users, and infrastructure, if upgrades were possible, to a deployed APIM?
Programme Costs (A.1.3.) G RF AQ	The programme costs need to be ascertained, which may include many assumptions and calibrated predictions.	What are the predicted sponsor entity costs? Are stakeholders' costs based upon similar requirements and application contexts? Have any initial designs been produced to facilitate cost comparisons with similar deployments?

Table E.16: Predicted Costs Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identification/ Authentication Model (A.12.1.) G AQ	A diagrammatic representation assists in determining the extent to which the security architecture, including the APIM, maps to articulated requirements.	How does the APIM integrate into the overall security architecture? What are the controls for interactions between technology, processes and people?
Subject Signal Storage Locations (A.12.2.) G RF	The locations where the identifier and credentials determine how that data may be used by the APIM.	Where are the identifier and subject's signals be stored? Are the data for usage stored centrally, on a distributed artefact or on a device or at other locations?
Subject Signal Storage Format (A.12.3.) G	The data may be stored in its original form or in a transformed state. e.g. template. The cryptographic protection needs description.	How are the subject signal data stored? Are all data stored in the same format? What are the size of the data signals and how are data protected?
Mechanism Processing Locations (A.12.4.) G AQ	The comparison of the subject's identifier and /or credentials may take place locally, remotely or hybrid solution.	On what device does the signals matching take place and where do those data reside? What are the roles of each physical device and application software in the APIM?
Mechanism Processing Infrastructure (A.12.5.) G	The comparison of the subject's identifier and /or credentials may take place locally, remotely or hybrid solution.	Is there a centralised database on-line or distributed storage medium, e.g. smart card, which require network connectivity? What are the networks, systems and software?
Processing Protection (A.12.6.) G AQ	The confidentiality of subject's signals are paramount to minimise replay attacks.	How are the subject's signals and data protected during usage?
Subject Signal Data (A.12.8.) G AF AQ Merger of (A.12.8.) and (A.12.9.)	The signals that are used by the matching processor to entify or verify the subject together with a description of the device used to capture subject's signals or data from other devices. A description of how these signals are captured and processes is fundamental for evaluation.	What subject signals, from biometric modalities or user knowledge or certificates or device identifiers or other data, are used to entify or identify the subject? Does it involve the use of an identifier? How are various data elements fused? What devices and processes are used to capture signal data and other related data ?
Mechanism Maintenance Effort and Reactivation (A.12.10.) D RF AQ	The effort involved to distribute components or revise subject's signals as portrayed by APIM's design, or in the event of error, compromise or faulty devices.	How easy and how often is it necessary to change or reissue data, devices, artefacts subject signals associated with the APIM? Does this reinstatement involve the subject seeking assistance from a support team?
Artefacts Maintenance (A.12.11.) D RF AQ	The credential data may be revised by the subject, the administrator or automatically.	How are credential data on artefacts updated, replaced or replenished in normal, compromise or failure states?
Subject Signals Processing (A.12.13.) D AQ	The process to capture the subject's signal to entify or identify must be described.	What are the processes to capture, transform, compare captured signals and outputs results to the subject and intermediary devices and systems?
Combined User Input Signals (A.12.14.) G AQ	The processes to capture multiple subject's and fuse these signal to entify or identify must be described.	Does the design capture multiple subject signals and how are these signals fused within the authentication model, which should explain the use of intermediary devices and systems?
Mechanism Training and Awareness (A.12.17.) D AQ	The subjects may need guidance on how to use, maintain the credentials. Advice facilitates desired behaviour.	How are subjects' trained to use the the APIM and its devices or artefacts? Are users provided with security awareness information regularly?

Table E.17: Security Architecture Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identity Proofing Processes (C.18.1.) G	The processes to check the subjects' proof of identity evidence must be validated. The acceptable breeder documents and/or identity attributes need to be stated in order to enable the registration of an applicant.	What are the processes for the authorised entities in order to check identification evidence gathered or supplied by the subject applicant? How do these processes merge with the registration and enrolment processes?
Prime Identifier Data (C.18.2.) G	A unique identifier enables the APIM to link to the genuine subject in the community of subjects.	What is the identifier or entifier assigned to the subject for authentication or entification purposes? Are subject identifiers assigned or randomly generated?
Credential Life Expectancy (A.13.1.) G RF	The life expectancy of the APIM and its components determines the replacement strategy, which may impact costs and performance.	What is the intended life expectancy of the APIM including infrastructure components, devices or artefacts, e.g. ICC, or data persistence, e.g. biometric?
Credential Authenticity (A.13.2.) G	The provision of identifiers and/or credentials should be undertaken with controls to ensure the genuine subject receives their identifier data or artefact.	What are the rules for issuing identifiers and/or credentials, whether processes automatically, or through officials or administrators?
Credential Integrity (A.13.3.) G	The integrity of the entifier and identifier data and the credentials form the basis of the APIM's assurance.	How are the integrity of identifiers and/or subject credential data protected by issuing authorities and by relying parties?
Credential Maintenance Empowerment (A.13.4.) G RF AQ	The maintenance of the credentials may need to be authorised entities to carry out these functions.	Do entities require authorisation to entitle them to operate credential maintenance, replacement or destruction processes of identification data? Does this include the revoking of credentials?
Identifier and Credential Maintenance Tasks (A.13.5.) G RF AQ	The life-cycle management of the identifiers and entifiers and/or credentials need to be stated for assurance purposes.	What are the processes for the issuance, maintenance and destruction of data relating to entifiers, to identifiers and/or credentials? entifiers, to identifiers and/or credentials? Is justification needed to revoke subjects' credentials?
Credential Delivery Verification (A.13.6.) G	The issuer of the identifier and/or the credential needs to know that the genuine user has received these items.	Is the acknowledgment of the receipt of an identifier and /or credentials by the subject reconciled and what is the verification process?
Credential Creation Locations (A.13.7.) D RF	The method to enrol the initial subject signal or to generate subsequent signals need to be described. Are these signals system generated in whole or in part?	How will the initial and subsequent subject signals be captured or generated? What are the conditions for delivering artefacts to the genuine subject?
Alternative Identifiers (A.12.7.) N	The use of other forms of identifiers or pseudonyms may be required for anonymity or privacy purposes.	Are there alternative identifiers or entifiers to protect or mask the identity of the subject?
Subject Autobiographical Data (A.12.12.) G	Additional data relating to the person may be used for out of bounds identification purposes. Does its purpose align with privacy legislation?	What associated subject data are stored with the identifier and subject signal identification data? Why is it necessary to acquire this additional data?

Table E.18: Identifier Management Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Sampling Normalisation (A.14.1) D AQ	The signals should be of sufficient quality to meet performance accuracy and speed requirements.	How many instances of subject signals are captured at enrolment and during usage to create signals templates or to update profiles?
Signal Entropy (A.14.2.) G	The differentiation of signals enables accurate entification of subjects.	Is there sufficient inherent variation or randomness in subjects' signals to avoid identification collisions?
Performance Indications (A.14.3.) D RF AQ	The False Acceptance Rates and the False Rejection Rates should be compared to accuracy requirements and impact upon throughput.	Does the accuracy of the comparison meet stated entification and identification requirements? What is the impact on timings from adjusting configured threshold settings?
Deceit Resistance (A.14.4.) G AQ	The extent of the deceit resistance on theoretical and practical exploitation informs vulnerability and liability considerations.	What is the difficulty, in required knowledge and resources, for an attacker to deceive an APIM? How well does the APIM withstand brute force attacks?
Artefact or Credential Counterfeiting (A.14.5.) G RF	The theoretical or practical difficulty in producing a counterfeit artefact or credential informs vulnerability and liability considerations.	What is the difficulty, knowledge and resources, to counterfeit an artefact or credential to ascertain subjects' signals or extracted parameters?
Signal Confidentiality (A.14.14.) G RF AQ	Revealing subjects' signals may enable attackers to gather data to perform replay attacks.	Are subjects' signals exposed during capture, transformation, transmission or in comparison processing in full or partially?
Signal Data Protection (A.14.15.) D	Changing subjects' signals may enable attackers to gather data to launch denial of service attacks.	What are the technological safeguards to protect the integrity of the subject's signal data captured, stored, processed and transmitted?
Average Failure to Enrol Rate (A.14.17.) D RF AQ	Predicting the percentage of subjects that may be unable to provide signals of sufficient quality informs accessibility considerations.	What is the predicted percentage of subjects that are unable to provide signals of sufficient quality at enrolment? How do these indications compare with other subject communities?
Average Time of Impostor Try (A.14.19.) D	The repeated attacks by impostors may severely impact the APIM to perform correctly	Time to detect impostor attempts, including repeated tries averaged, over all impostor attempts, regardless of successful verification?
Average Time of Verification (A.14.20.) D	The average time to entify or identify a subject in proportion to the users task impacts usability.	What is the time to achieve correct subject entification or identification which includes repeat attempts averaged over all attempts?
Average Impostor Failure Rate (A.14.21.) D AQ	The average number of impostor attempts before the APIM is rendered invalid or obsolete informs reliability.	What is the impostor failure rate averaged against all subject signals which have failed?
Signal Capture Failure Rates (A.14.22.) D	Predicting the percentage of subjects that may be unable to provide signals of sufficient quality informs accessibility considerations.	What is the percentage of genuine subjects which are unable to provide signals of sufficient quality during usage? How do these indications compare with other subject communities?
Artefact / Device Accreditation (A.13.8.) G AQ	The accreditation or approval by an agency that credentials and devices conform to specifications provides reliability assurance.	What processes are to be established to issue credentials or devices from approved suppliers? Which agency accredits or approves these elements?
Tamper Protection (A.16.18.) N	The capabilities of devices or software provides evidence of unauthorised interference attempts.	Are there tamper deterrent or tamper indicative technologies to notify parties of an attack?
Template Update Notifications (A.16.19.) N AQ	These activity logs enable the detection or investigation of compromise attempts or changes to subject's signals.	What log entries flag changes to an enrolled subject signal or template, user access rights or changes in user behaviour?

Table E.19: Reliability Results Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Multiplicity Errors (C.20.1.) G	Similar APIMs from other application contexts may confuse subjects.	Are there similar APIM deployments that could confuse the subject in the community and cause errors?
Interface Usage Data (A.15.1.) G RF AQ	Test data may include timing user tasks or video data using the APIM.	What test data provides evidence that that subjects' usage of the APIM are as intended?
Security Features Conveyed (A.15.2.) G	Visible security features enables the user to manage security tasks.	What features convey the available security features to the user?
Visibility of Security Status (A.15.3.) D	The interface should advise the user when they have made a mistake or provide feedback on normal status.	Does the APIM's interface provide feedback to the user on the APIM's security status?
Intuitive Interface (A.15.4.) G	Awkward interfaces may make the APIM difficult to learn and use.	Is the APIM's interface comforting and naturally easy to learn? Is the design sufficiently intuitive to facilitate habitual usage?
Aesthetic and Minimalist Design (A.15.5.) G	Too much information may confuse the user, which may lead to errors.	Does the APIM's interface convey or display only relevant security information?
Error Reporting (A.15.6.) G	The user should be notified of errors and given guidance on how to rectify the error safely.	Does the APIM's interface provide error messages that are sufficiently detailed to advise users where to obtain help?
User Satisfaction (A.15.7.) G	An unsatisfactory experience may may indicate HCI design flaws.	Does the APIM's interface provide a satisfactory experience?
Cognitive Activity (A.15.8.) D	Enrolment processes may be complex and require significant focus to ensure signal data, are of an adequate quality.	Does the user require cursory rehearsal, visual co-ordination, in depth cognitive processing in order to produce signal data of sufficient quality for authentication or entification purposes?
Signal Retrieval Strategy (A.15.9.) N AQ	Remembering random authentication data or methods may be overcome by using visual or audio cues.	What cues are provided to the user to recall data or methods to use the APIM as designed?
Signal Meaningfulness (A.15.10.) N AQ	Letting subjects choose data that have significant value to them may assist their recall of authentication data.	Are subjects' signal data assigned by a system, acquired automatically or created by the subject to make the signal deducible to the subject?
Tasks Alignment (A.15.11.) G RF AQ	The APIM interaction should naturally fit at the appropriate point in the users task and not be an awkward adjunct to the task. It should not be cumbersome to the task.	Does the APIM interaction align with users' mental models to perform the core underlying task? Is the user's effort on the APIM interaction proportionally convenient to the core operational task?
User / Subject Preference (A.15.12.) D AQ	Users may express a preference for a biometric modality or authentication data that is habitual to them.	What are user's preferred signal type or APIM for this type of application context? Why is this preference more acceptable?
User Training (B.20.1.) G	The APIM may require users to learn how to use unfamiliar devices or processes that are not intuitive.	What training do users need to use the APIM as designed? How is that training delivered?

Table E.20: Usability Results Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Database Contingency (A.12.16.) G	The continuity of the APIM may be vital to stakeholders' business operations and provision of services. Security incidents may cause severe operating problems.	What are the database contingency plans for the identifiers and subject signal data should this data become compromised or unavailable? How can recovery be achieved to match availability goals?
Systems' Resources (A.16.1.) G	The APIM's processing needs to rely on different infrastructures, which may be under the stakeholders' control.	What network, systems, software, devices, form part of the APIM's infrastructure? Does it involve a Public Key Infrastructure?
System Functionality Description (A.16.3.) D RF AQ	Reviewing stakeholders' systems ensures the completeness of the APIM and that interfaces are specified.	What evidence demonstrates that the APIM description is complete for all functions and components?
Legacy System Impact (A.16.4.) D RF	The introduction of systems and processes may adversely impact existing operations. Extra costs and effort may be absorbed.	What is the impact of the proposed APIM, in terms of processing, on existing hardware, software, personnel, infrastructure and systems? What are the effects on current operations?
Legacy System Reuse (A.16.5.) G RF AQ	Reusing existing networks, systems or operational procedures may assist in containing costs and minimising impacts to operations and subjects.	To what extent can existing network, information systems, infrastructure and processes be reused or enhanced for this candidate APIM?
Processing Capacity (A.16.7.) D AQ	The processing capacity needed to operate the APIM, both centrally on servers and on users' devices need to be quantified.	What is the processing power needed to support the APIM for stakeholder's and users? To what extent are these computations processed on local devices or artefacts?
Back-up Methods (A.16.8.) N	The reliability of these methods may impact stakeholders' ability to recover normal operations quickly.	What are the back-up procedures to respond to a total or partial failure of the APIM, including access to subjects signal data stored?
Administration Support Roles (A.16.11.) G RF AQ	The roles and tasks need to be clarified to ensure clarification of authorised responsibilities.	What are the roles and responsibilities of the administration entities or staff involved in supporting the APIM?
Expert Support (A.16.12.) G RF AQ	The APIM may require specialist knowledge to perform core duties, may increase reliance on suppliers.	Are unique skills or competencies required to operate the APIM, in normal, compromised or failure states?
Administration Personnel Training (A.16.13.) G RF AQ	The competencies of existing personnel may need to be enhanced continually to support the APIM.	What are the training requirements for administrative personnel, both initially and continually?
Device Calibration (A.16.14.) G AQ	Some signal capture devices operate discretely; however, some sensing devices may need periodic recalibration.	Does the user's device need to be calibrated regularly so that the APIM functions and performs correctly?
Lockout/Threshold Maintenance (A.16.15.) G	Some genuine users may exceed set retry limits. Users accounts should be reactivated securely.	How does the APIM support lockout thresholds on excessive invalid attempts? How are user lockouts or thresholds reset securely?
Subject Supervision (A.16.16.) G	The need to supervise subjects may impact subject usage of the APIM.	Are subjects supervised during their usage of the APIM?
Enrolment Supervision (A.16.17.) G	The skills required and the authority to perform such duties to reduce enrolment failures or inadequate data.	What are the competences required for staff to supervise subject enrolment? How are quality of captured data improved?
Processing Protection (A.16.20.) D RF AQ	The signal data must be protected to ensure validity of the identification or authentication processes.	What technological safeguards protect the integrity and confidentiality of subjects' signal data captured, stored, processed and the identification result transmitted?

Table E.21: Technology Management Evaluation Theme

Factor, Identifier and Status	**Factor Explanation**	**Criteria Questions**
Subject Signal Linkage (C.22.1.) G	The strength of the binding may vary between weak password data and cryptographic computations.	What is the strength of the binding between the subject and the signals acquired for identification / authentication?
Operational Enablers (A.17.1.) G	The APIM should not be so complex as to require special skills, which exclude some users.	Does the user need technical expertise or equipment to use the APIM or its associated artefacts or credentials?
Subject Inclusiveness (A.17.2.) G	Disabilities may exclude the user from operating the APIM as designed.	Are there any sensory, physical or cognitive skills that would prohibit or limit users from operating the APIM?
User Maintenance Tasks (A.17.3.) D RF AQ (A.17.3.) and (A.17.4.) merged	Some devices may require cleaning, recalibration or software may require updates in order to function correctly. The inability to perform these tasks may exclude some users. The interference of some components may render them ineffective.	What maintenance tasks does the user undertake to keep the APIM functioning as designed? How will the user be notified or become aware of malfunction or rendering the device vulnerable?
Usage Convenience (A.17.5.) D RF AQ	The amount of time and effort to use and maintain the APIM may be disproportionate to that of the risks and liabilities of the task.	What actions and effort are needed to use the APIM when compared with the user's responsibilities and liabilities related to the underlying task?
Technology Provisioning (A.17.6.) G	Some devices or software licences may be prohibitively expensive to buy which may exclude some subjects.	What technical components are required, including devices, drivers, software to operate the APIM? Are these components ubiquitous?

Table E.22: Accessibility Results Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Availability Indicators (C.23.1.) G	The failure of the APIM function may cause service delivery problems or other issues for relying parties.	How often does the APIM suffer from partial or total outages? What are the recovery processes?
Assurance Evidence (A.14.18.) D	The basis of on which test data are acquired and its relevance to the live environment informs assurance testing.	What evidence demonstrates the APIM's ability to meet assurance requirements? How was it produced and by which entity?
Practical Experience (A.12.19.) G	Lessons from others entities using this type of APIM to address their problems are useful input.	What is the experience of owners, users and administrators using this APIM or similar designs in the application context?
Identification Time Profile (A.14.7.) G RF AQ	Elapsed time may be more acceptable by re-engineering the signal sensing, capturing, extraction, transformation comparison and results processes.	What is the possibility of reducing the overall entification or identification time? Have timings on all sub-processes been ascertained so as to consider re-engineering the logic?
Liabilities and Responsibilities (B.23.1.) G	Onerous responsibilities or disproportionate liabilities may outweigh benefits, notwithstanding costs.	What are the responsibilities and liabilities associated with the APIM for each stakeholder?
Privacy Impact (A.15.13.) G	Revealing social acceptability issues may expose trust problems with the technology and/or service provider.	What is the APIM's effect upon subject's feelings about their privacy and their risks?
Criticality of Contingency Plan (A.16.9.) D	Business continuity and the risks of disaster must be weighed against recovery plan costs.	What is the criticality of a contingency plan to ensure business as usual operations in the event of an APIM failure?
Repair Response Times (A.16.10.) G	The time to repair elements of the APIM should be recorded and be included in a Service Level Agreement.	What is the proposed repair response times for central servers and/or users' devices? Are these timescales acceptable to all parties?
User Confidence (A.17.7.) D	A lack of trust in the devices may affect the users' usage of the APIM.	To what extent does the user community hold the belief that the APIM will protect their interests? What evidence supports these findings?
Stakeholder Costs Recovery (A.18.7.) D	Stakeholders may consider the use of ubiquitous as a way of reducing costs, which offer adequate protection and functionality.	What is the possibility of subjects or users absorbing APIM devices costs? Is enabling ubiquitous device usage a viable strategy?
Ubiquity (A.16.6.) G RF AQ	The APIM may need to operate with an existing mechanisms or use ubiquitous components.	Are the APIM's components universal enabling interoperability with alternative APIMs, in the intended application context?
Performance Comparisons (A.12.18.) G RF	The performance results from other deployments may highlight performance discrepancies.	How does the indicative performance of this APIM in this application context compare with similar deployments?

Table E.23: APIM's Issues Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Components Integration (B.24.1.) G	The integration of disparate components may introduce technical vulnerabilities or usability deficiencies.	To what extent do the APIM's components integrate into a coherent solution to meet the operational requirements?
Mechanisms' Consistency (A.14.8.) D RF	Knowledge of the APIM's capability to perform reliably, without degradation, is essential to manage risks.	What is the probability that an APIM will perform its intended functions over a specified interval of operation?
Device Interfacing (A.14.9.) G	The integration of signal sensing devices, their firmware and integration to the application should ensure that the security of the APIM is not circumvented.	Are supporting devices and artefacts functioning coherently for their intended purposes in a way that meets the requirements for an APIM, in order to detect attempts at circumvention?
Circumvention Susceptibility (A.14.6.) N	The probability of theoretical based attacks need to be clarified.	What is the difficulty, in terms of knowledge and resources, to circumvent the APIM without the need to deceive the processing logic?
Signal Predictability (A.14.10.) G AQ	The unpredictability of a signal reduces guessing attacks.	Are the subjects' signals sufficiently disguised to prevent attackers from determining these data or succeeding signals?
Signal Abundance (A.14.11.) G	A significantly large key space should deter impostors from brute force attacks and subject signal collisions.	What is the APIM's number of possible subjects' signal permutations or total key space? To what extent are subject signal collisions, in entification mode, possible?
Subject Signal Exposure (A.14.12.) G RF AQ	Safeguards are needed to ensure subjects' signal data are not exposed to unauthorised parties during storage or during transactions.	Is the subject's signal data easy to record or acquire during storage, capture, transmission, extraction or identification or authentication comparison processes?
Signal Robustness (A.14.13.) G	The clarification of these capabilities may necessitate other controls to counter identified vulnerabilities.	To what extent does the signal capture device withstand known attacks or theoretical attacks?
Exploitable Vulnerabilities (A.14.16.) G	Vulnerabilities should be declared including those in the public domain and those confidential to suppliers.	What are the known exploitable weaknesses in the candidate APIM or in existing deployments?
Vendor Track Record (A.12.20.) G AQ	The stakeholders may gain comfort that the supplier has previously delivered in this context.	What experience and capabilities does the candidate vendor have in deploying APIMs in this type of application context?

Table E.24: APIM's Vulnerabilities Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Artefact Distribution Costs (C.25.1.) G	The logistics for distributing various elements securely may involve internal or external distribution channels.	What are the estimated costs for distributing devices, artefacts, initial authentication or data to subjects?
Implementation Costs (A.18.1.) G	The APIMs development costs need to be segregated from other types of costs.	What are the costs to develop or integrate the candidate APIM, which includes software implementation, testing or costs associated with obtaining accreditation?
Maintenance Costs (A.18.2.) G AQ	The introduction of new systems brings capital costs and operating support costs, which may be absorbed. partly into existing operations.	What are the operating and administrative costs for supporting the APIM, which includes costs of servers, networks, software, personnel, and impact upon existing operations?
Mechanism's Anticipated Life Expectancy (A.16.2.) G RF AQ	The anticipated life expectancy has implication on investments over the APIM's usefulness.	What is the life expectancy for the APIM, including sensors or ICC readers and/or ICCs or software? Does the APIM's design allow for device upgrade or migration?
Cost of Input Devices (A.18.3.) G	The costs of bespoke devices to capture subjects' signals is a major capital cost to be absorbed by stakeholders.	What is the cost of the signal input device including any firmware, the cost of tamper detection, including the protection of its internal logic from examination?
Cost of Artefacts (A.18.4.) G	The costs of smart cards together with the issuing of certificates needs to be segregated.	What is the unit cost of an artefact incorporating associated production and ICC personalisation or similar costs?
Infrastructure Processing Costs (A.18.6.) G AQ	The infrastructure costs may be separated from other operating costs; however, trust schemes may incur membership fees.	What are the costs associated with the supporting infrastructure, which includes communication networks or PKI based trust schemes?
Other Parties' Costs (A.18.8.) G AQ	The total cost to stakeholders should be ascertained to ensure that costs do not exceed predicted benefits.	What are the total costs for all stakeholders, including hardware, software, devices, artefacts to ensure its compatibility?
Costs Influences (A.12.15.) G	The isolation of specific cost elements may assist in identifying alternative technology configurations.	What elements are most likely to increase or decrease the APIM's costs?

Table E.25: Stakeholders' Costs Evaluation Theme

Appendix F – Evaluation Themes and Factors (Stage D)

This appendix contains 25 evaluation theme tables showing the factors for evaluating an APIM as at Stage D of our factor validation effort, representing Step 12 of our research implementation plan.

The tables show the status of the evaluation factors following our validation efforts using the data from our EU State's eGates Programme Case Study. The status also indicates which evaluation factors were Grounded (G) and Not-grounded (N) in our data. We show relabelled factors as 'RF', criteria questions which required amendment as 'AQ' and factor explanations which required revision as 'ER'.

We assign an identifier to a new factor identified in Stage D, e.g. (D.2.2.), to denote stage created, evaluation theme and factor reference number, to enable each factor and its criterion question to be tracked through each subsequent validation.

The tables in this appendix contain the following evaluation themes:

Table F.1 Business Case Evaluation Theme;

Table F.2 Stakeholders' Objectives Evaluation Theme;

Table F.3 Stakeholders' Risks Evaluation Theme;

Table F.4 Community's Characteristics Evaluation Theme;

Table F.5 Usage Environment Evaluation Theme;

Table F.6 Constraints Evaluation Theme;

Table F.7 Polices Evaluation Theme;

Table F.8 Functional Requirements Evaluation Theme;

Table F.9 Privacy Compliance Evaluation Theme;

Table F.10 Registration and Enrolment Evaluation Theme;

Table F.11 Performance Requirements Evaluation Theme;

Table F.12 Assurance Requirements Evaluation Theme;

Table F.13 Task Dialogue Evaluation Theme;

Table F.14 Envisaged Issues Evaluation Theme;

Table F.15 Envisaged Vulnerabilities Evaluation Theme;

Table F.16 Predicted Costs Evaluation Themes;

Table F.17 Security Architecture Evaluation Theme;

Table F.18 Identifier Management Evaluation Theme;

Table F.19 Reliability Results Evaluation Theme;

Table F.20 Usability Results Evaluation Theme;

Table F.21 Manageability Evaluation Theme (formerly Technology Management Evaluation Theme);

Table F.22 Accessibility Results Evaluation Theme;

Table F.23 APIM's Issues Evaluation Theme;

Table F.24 APIM's Vulnerabilities Evaluation Theme; and

Table F.25 Stakeholders' Costs Evaluation Theme.

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Feasibility Outlook (A.1.8.) G	The likelihood of an APIM fulfilling its purpose from a business, legal, operational and technological standpoints should be ascertained at the outset.	Are there similar deployments precedents, a conceptual prototype or independent expert opinion that could provide indications on the potential of an APIM fulfilling its purpose?
Risks Identified (A.4.2.) G AQ	Stakeholder risks need to identified, understood and articulated in order to determine the mitigating controls provided by the APIM.	What are the stakeholders' business risks which require control? What vulnerabilities and threats relate to identification of persons, e.g. employees, customers, partners?
Defined Business Problem (A.5.1.) G	If the business problem is not fully understood and resolution objectives articulated then solution cannot be evaluated for its utility to resolve that stated business problem.	Is the personal identification problem fully understood and expressed as a high-level problem description and not attributes from potential solutions? How effective and efficient are existing identification systems?
Project Sponsorship (A.5.2.) G	The basis for the approved investment for effort to introduce or revise an APIM needs to be established at the outset.	Is the business analysis of stakeholders' objectives for an APIM supported by a business case with justification for expenditure?
Alternative APIMs Investigated (A.6.4.) G RF AQ	Previous investigations should reveal the issues and costs related to resolving the business problem. Using biometrics or hardware tokens need due consideration.	Have alternative APIMs been investigated and what were the learnings. Which biometric solutions were considered? How do similar application contexts address the same problem?
Security Motivation Authorised Subjects (A.7.10.)		Factor deleted as covered by factor (A.3.2)
Entity Relationships (A.7.8.) G AQ	Stakeholders interact in through informal arrangements or through scheme rules to ensure the APIM provides an acceptable and viable proposition to resolve a stated business problem.	What are the relationships between the direct and indirect stakeholder entities, particularly the subjects themselves and, where appropriate, users of an identification system. Do contracts or rules exist between the entities?
Identity Authorisation Model (A.9.1.) G AQ ER	A description of the direct and indirect stakeholder entities, including the subjects, in the application context helps to establish the role of each entity and its relationships with other entities.	Who are the stakeholder entities involved with the application context? Which entities may use subject identifiers and/or credentials, as relying parties, for person identification or for person authentication purposes?
Contextual Purpose and Scope (B.7.1.) G RF AQ ER	The purpose of the APIM needs to be fully understood and communicated in terms of desired outcomes or objectives to direct effort to evaluate and select the optimal APIM.	Why is the APIM being introduced or revised for the application context? What are the business goals that describe the priority values of aspiration to be achieved? What criteria defines the scope of the APIM's intended usage?
Stakeholders and Subjects' Benefits (B.7.2.) G RF AQ	The benefits, tangible and non-tangible, to revise or introduce an APIM need to be stated at the outset. Some benefits should be derived from investing resources to introduce or revise an APIM.	Will the APIM be used to protect data assets or enhance the operations of one or many stakeholders? What are the measurable and intangible benefits to direct and indirect stakeholders to introduce or revise the APIM?
Programme Governance Framework (B.7.3.) G AQ ER	The decision processes between the stakeholders need to be understood, also the entity empowered to make changes to an entity's organisation.	What entity or group have the mandated authority to make decisions for specifying the requirements for APIM and its selection? How does the governance framework operate for decision-making amongst these stakeholders?

Table F.1: Business Case Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Subject Privacy Protection Aims (A.4.5.) G AQ ER	Clarification is needed on how subjects' private data are to be protected in line with legal, contractual and ethical obligations and social norms.	What are the intended courses of action to protect subject's private data, biometric and autobiographical information, to comply with regulatory and organisation privacy policies?
Sponsorship Aims (A.4.4.) G AQ ER	The sponsor's prime objectives should be clearly stated to introduce an APIM or revise a deployed APIM, which may align or conflict with other stakeholders' or subjects' objectives, in order to gain stakeholders' acceptance.	What are the aims of the sponsor stakeholder in terms of asset protection and business enhancements? How do these aims align with the objectives of other stakeholders, including subjects? How are conflicting stakeholders' aims addressed in the application context?
Stakeholders' Business Rationale (A.1.1.) G AQ ER	A description of stakeholders' benefits is needed to support the introduction of an APIM or changes to a deployed APIM.	What arguments support stakeholders' aims to instigate the introduction of an APIM or changes to a deployed APIM? Have all stakeholders been consulted and their interests included?
Subject / User Acceptability Rationale (A.3.2.) G AQ ER	The reasons for subjects and users willingness to use the APIM in the application context should be validated supported with explanations.	What are the stakeholders' arguments that describe the reasons for subjects' acceptance to introduce or to revise a deployed APIM?
Impact on Assets/Resources (B.1.1.) G RF AQ ER	The desired impact on assets by introducing or revising an APIM should be understood.	What are the desired business outcomes sought by stakeholders, from introducing or revising an APIM, on assets and resources?
Impact on Stakeholders (A.7.9.)		Factor deleted expanded in new factors (D.2.1.), (D.2.2.), (D.2.3.), (D.2.4.) and (D.2.5.)
Risks Controls Outcomes (D.2.1.)	The impact on annual loss expectancy by introducing or revising an APIM access should be described as an aim.	What are the desired risks control outcomes sought by stakeholders, from introducing or revising a deployed APIM?
Productivity Impact (D.2.2.)	The impact on subject or users' tasks by introducing or revising an APIM should be described as an aim.	What are the desired productivity outcomes sought by introducing or revising an APIM to the current operational situation?
Regulatory Compliance Impact (D.2.3.)	The impact of an organisation's ability to comply with regulation by introducing or revising an APIM should be described.	What are the desired regulatory compliance outcomes sought by introducing or revising an APIM to the current operational situation?
Utilisation Impact (D.2.4.)	The expected utilisation of introducing or revising an APIM should be described.	What are the desired utilisation outcomes sought by introducing or revising an APIM to the current operational situation?
Investments Impact (D.2.5.)	The financial aims of investing to introduce or revise an APIM should be stated.	What are the desired financial outcomes sought by investing to introduce or revise an APIM to the current operational situation?

Table F.2: Stakeholders' Objectives Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Risks Treatment Strategy (A.2.8.) G ER	Stakeholders may have different risks appetites and alternative risk management approaches to address identified risks, including residual risks.	What are the stakeholders' risks management strategies (alleviation, transference, avoidance, acceptance) for treating identified risks and any remaining residual risks?
Compromise Scenarios (A.6.9.) G AQ ER	Social engineering attacks on subjects and technological based attacks on systems should be researched in order to feed into a risks assessment.	What types of identification system attacks are envisaged and why? What are the known technological or social based attacks in similar? application contexts?
Privacy Impact Assessment (A.8.3.) G AQ ER	Organisational stakeholders may have legal and contractual obligations to protect subjects' private data. These data form input into a risks assessment.	What is the impact on each stakeholder and related subjects if subjects' private data Personally Identifiable Information (PII) are compromised? How privacy risks influence the requirements for an identification system?
Attack and Compromise Probabilities (A.2.1.) G AQ ER	The probability of compromise helps to determine appropriate security controls, given the value of the assets and known vulnerabilities and threats, from a risks assessment.	What is the likelihood of a deliberate attack identification system? What is the likelihood that errors occur from subjects' usage or other events? Do these projections include historical events analysis for all stakeholders?
Vulnerabilities Identified (A.2.3.) G AQ ER	The known vulnerabilities help to determine the current levels of assurance in the application context and also informs a risks assessment.	What are the known exploitable weaknesses in existing operations or potential flaw in new operations which may include technological, procedural and human limitations?
Stakeholders' Impact Costs/ Value Ratings (A.2.2.) G RF AQ ER	The value of damages or consequences to business operations needs to be established in order to determine the security controls, which includes optimal APIM from a risk assessment.	What are the estimated impact costs or impact severity ratings to stakeholders' (including users) if their assets/resources were to be stolen, destroyed or modified or unavailable in the event of an APIM failure or compromise?
Threat Motivation (A.2.7.) G ER	The motivation behind the threats with the rewards and deterrent penalties to miscreants help determine APIM's countermeasures via a risks assessment.	What is underlying stimuli or goals of miscreants that lead to attacks on the APIM? Are deterrents proportionate to potential rewards? What are attackers' motives?
Assets and Resources Value (D.3.1.)	The value of the assets needs to be established in order to determine security controls.	What are the value of the assets or entitlement to resources to each stakeholder, including subjects, which an APIM should protect?
Privacy Data Assets (D.3.2.)	Private data are assets belonging to subjects that are maintained by a custodian or approved entities that are tasked with the compliance to privacy legislations.	What personal identity data are acquired from subjects and for what purposes? What are the processes to collect, use, maintain, disclose and protect subjects' private data utilised for personal identification?

Table F.3: Stakeholders' Risks Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Social Norms (A.3.3.) G RF ER	The acceptability of an APIM for its intended purpose to the subject community gives an indication on subjects' motivation to use the APIM in the application context.	What subject attitudes have been established from surveys on similar APIM deployments? How do these surveyed responses support or negate stakeholders' arguments to introduce or revise an APIM?
Community Membership (A.3.4.) G AQ	The categorisation of community members informs the scope for the APIM. Membership characteristics provide differentiators and indications on the nature of the community together with expansion or contraction rates.	Who are the subjects and users in the application context? Are users, direct operators, the subject to be identified? Is the community membership open to all individuals or restricted and what are those restrictions and how are they to be verified?
Subjects' Trust (A.3.5.) G	The degree of reliance and acceptability of the APIM may be based upon existing relationships and perceptions of trustworthiness of public and private organisations. Without trust subjects may not co-operate or use the APIM as intended. Trust may also develop from a contractual agreement or legislation.	What is trust relationship between the APIM's stakeholders and the subject/ users? Is it a new relationship? What is the trust relationship between potential relying parties and subjects? Are there any issues that would enhance or limit existing relationships or inhibit relationships from developing?
Subject and User Capabilities (A.7.2.) G RF AQ	The subject community's capability and motivation to absorb technical and operational skills could help to widen the options of credentials and/or other devices.	Is the subject community capable of absorbing knowledge of new identification devices from educational material to ensure the proper usage of credentials or other devices?
Populations' Characteristics (A.7.4.) G RF ER	The subjects' characteristics are important to avoid exclusion from the community and may provide distinguishing features upon which designs may be evaluated.	What are the distinguishing traits of the subject community, in terms of population demographics, physiology, behaviour, appearance that pose disadvantages or create advantages for certain biometric modalities or credentials?
Users' Cooperation (A.7.11.) G	The subject community which is to use an APIM may impact, inadvertently, its effectiveness and efficiency.	What are the expectations that all individuals will cooperate voluntarily with an automated identification process in this application context?
Privacy Assurance Evidence (A.8.8.) G RF ER	Evidence is needed to substantiate claims of compliance with privacy legislations and the commitments provided to the subject community by stakeholders.	What assurance is required to demonstrate anonymity, unlinkability, unobservability and anonymity compliance to data privacy legislation and security policies?
User Obligations and Liabilities (B.3.1.) G RF ER	The responsibilities and/or liabilities of the usage terms for the APIM may outweigh any potential benefit or proposition to the subject or user. Some APIMs contain terms and conditions or are mandatory.	What subject consent or acceptance is needed for user and/or subjects to acknowledge their responsibilities or liabilities to use an APIM? To what extent do these obligations negate their benefits of using the APIM?

Table F.4: Community Characteristics Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Environment Ergonomics (A.2.5.) G	The environment's characteristics may impact upon the ergonomic operation of the APIM.	How should the identification system operate in the intended physical usage locations? Will the APIM be required to operate in variable environments? What are the typical characteristics of the envisaged usage settings?
Physical and Logical Control (A.6.8.) G RF	Subjects' control of technical devices may impact the requirements for an APIM and may influence the subject's acceptance and usage of a device, particularly. if they are unfamiliar.	Does the subject utilise a ubiquitous device or is technology supplied by the artefact issuing authority and/or relying parties? What physical control should stakeholders have over physical devices and logical components? Should users manage the devices' logical operations?
Logical Usage Settings (B.4.1.) G ER	The information systems that the APIM supports need to be described together with the supporting devices, infrastructure and operating systems.	What are intended logical applications for the APIM, the types of operating devices and operating systems?
Physical Usage Settings (B.4.2) G ER	Physical usage locations may adversely impact or enhance the subject's ability to use the APIM and a stakeholder's ability to manage an APIM.	Where will the APIM operate? What are physical environmental characteristics of these locations?
Physical and/or Logical Identification (B.4.3.) G RF ER	The usage scenarios for identification system requires clarification to explain the nature of the personal identification transaction.	Will the identification system involve physical identification or remote logical identification or both? Have usage cases been developed?
Environmental Variances (D.5.1.)	The variability of a physical or logical environment may impact upon the capturing of the subjects' signals possibly resulting in many false rejections.	What are the key environmental factors that may affect the quality, the integrity and confidentiality of the captured signals? What impact could signal deterioration have on required genuine accept rates?
Subject Locale (D.5.2.)	The physical location of the subject and the localities in which identification are required to take place may impact the requirements for an identification system.	Where are subjects to be identified based? Are subjects to be authenticated remotely? Are subjects to be physically present at specified locations for logical authentication? Is enrolment to be performed remotely?

Table F.5: Usage Environments Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Political and Economic Concerns (A.1.4.) G RF	The politics and economics relating to the application context may influence the requirements for the APIM.	What political agenda or economic matters may hinder or support organisational change? How does this change impact the requirements for an identification system?
Stakeholder Relationships (A.1.5.) G ER	Existing relationships between the stakeholders and subjects together with outstanding issues may hinder stakeholder collaboration.	What commercial, organisational or political stakeholder relationship issues hinder or support a proposition to introduce an APIM or revise an APIM deployment?
Regulatory Imperatives (A.1.6.) G	Regulations may place restrictions or additional tasks on stakeholders to comply and to demonstrate compliance.	How does legislation and industry guidelines impact the stakeholder aims for an APIM in the proposed usage settings?
Budget Allocated (A.4.3.) G AQ	The budgetary capital and operational investments that stakeholders' commit influence requirements and choices on APIM solution candidates.	What funds and resources have allocated by stakeholders, to introduce an APIM or review and possibly revise an APIM deployment, in order to minimise identified risk?
Contextual Legacies (A.5.4.) G	The restrictions of the application context influence the proposition for the APIM. It is assumed that the APIM proposition does not start from a neutral historical state, whether technological or social norms.	What existing and potential issues relating to the application context could impact the stakeholders' aims and subjects' propositions for an APIM, which include organisational issues, current practices, existing infrastructures, social norms and deployed information systems?
Subject Application and Enrolment (A.10.2.)		Factor deleted and replaced by factor (D.5.2.)
External Performance Benchmarks (A.5.7.) G ER	Data acquired on other APIMs in similar application contexts help to guide stakeholders' expectations on fulfilling their objectives.	What are the potential performance limitations of the envisage usage settings in which the APIM should be designed to operate? What are the learnings from similar deployments?
Specifications and Information Technology Standards (A.5.5.) G	Specifications for application contexts are designed to ensure technical and procedural interoperability together with a means to also claim compliance to a specific quality.	What specifications are applicable to the APIM to ensure interoperability and requisite quality in the application context? Which standards are these specifications based upon?
Users' Costs (A.3.6.)		Factor deleted as included in factor (A.3.1.)
Signal Data Exchange Interoperability (A.5.6.) G AQ	Data may need to be exchanged regularly between relying party stakeholders and credential issuing authorities.	Is there a need to exchange subjects' signal data or other attributes with other stakeholders in the application context? Do interoperability specifications exist and how are they enforced?
Auditing Subject Data Usage (A.1.7.) G ER	The periodicity and measures for using and storing signal data may impact potential investigations or efforts to comply with legal or contractual obligations.	What is the retention period and archive rules for data to be used by the APIM to automatically identify a subject? What are the legal and risks associated with auditing requirements for retaining these data?
Subject Proposition (A.3.1.) G	The general acceptance of an APIM type does not immediately validate its usage for a particular application context.	What are the stakeholders' expectations relating to subject community's adoption of an APIM? Do subjects derive sufficient benefit to outweigh expected costs and effort?
Compromise Recovery Methods (B.5.1.) G RF AQ	The obstacles which may affect the safe recovery of an APIM should be articulated.	How will stakeholders recover the APIM in the event of failure? Are there technology, procedures or scheme rules which inhibit or facilitate recovery actions?

Table F.6: Constraints Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Data Archiving Policies (B.6.1.) G	The stakeholder policy on data or audit log retention may differ to that required by privacy regulation or rules of the context in which the APIM operates.	What are the stakeholders' policies on retaining and archiving data generally? How do these policies relate to the APIM subject signal and other private data in usage transactions?
Organisational Policies (A.8.1.) G	The stakeholder organisational policies may give direction on issues relating to an organisation's governance.	How do stakeholder organisation policies, e.g. environmental policies, impact the requirements for an identification system for employees, customers, agents or partners?
Policies on Existing Contextual Issues (B.6.2.) G RF	Contextual issues should be articulated and researched as knowledge of their impact may affect the requirements for an APIM.	Are there issues relating to the application context explicitly accepted by stakeholders, including users? Are these issues discussed in the public domain?
Authorised Identity Evidence Sources (B.6.3.) G	The stakeholders must provide direction as to which entity or group determines the policies on the proof identity evidence, registration and enrolment processes.	Which entities are empowered to provide policy on acceptable proof of identity evidence, registration and enrolment?
Privacy Laws Compliance Accountability (A.8.2.) G RF	The individual or accountable group assigned with the responsibility of compliance with legislation needs to provide direction on privacy issues.	Have stakeholders assigned the responsibility of complying with privacy laws to a specific accountable entity with responsibility to manage this corporate governance issue?
Programme Implementation (A.4.1.) G	How does each stakeholder go about implementing agreed organisational change policies?	What is the stakeholders' strategy and governance framework to implement organisational changes?
Requirements Gathering Methodology (A.5.3.) G	The methodology used by stakeholders programme may influence the requirements for the APIM.	How will the development programme gather and articulate their business requirements for an APIM?
Stakeholders' Dispute Resolution Methods (B.6.5.) G RF	Stakeholders should have the means and procedures for settling disputes with other stakeholders and subjects.	What are the stakeholders' policies for settling disputes with partners, customers and other entities and also subjects?
Subject Duress Policy (A.17.8.) N	The context may dictate that subjects should be able to use a 'panic button' to notify duress while using the APIM.	Does the application context warrant the inclusion of a notification alarm to indicate coercion of a subject while using the APIM?
Imposing Sanctions (B.6.4.) G	Stakeholders may choose to seek criminal damages for miscreants or impose disciplinary reprisals.	What is the stakeholder policy for dealing with miscreants or authorised users who use the APIM improperly?
Stakeholders' Security Policies (D.7.1.)	These policies may help to inform stakeholders' considerations regarding the appropriate assurance for the APIM.	What are the stakeholder's security policies for identification and authentication? To what extent do they align with the stakeholders' objectives for the APIM?
Systems Development Methodology (D.7.2.)	Stakeholders may employ a formal approach to establish an architecture to support their business operations.	What is the development methodology, e.g. agile, for delivering integrated systems which are responsive to change and delivers the business information technology strategy?

Table F.7: Policies Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Subject Signals Enrolment (C.8.1.) G ER	Processes to capture subjects' signals should be outlined enable identification or authentication. Some subjects' signals may be acquired face-to-face or remotely.	What functions are required to capture subjects' signals or generate authentication data during local or remote enrolment? Are authentication data system generated?
Subject Signals Acquisition (D.8.1.)	The acquisition of subjects' signals may be performed during face-to-face interactions or remotely, through a network connection or a combination.	How are the subject's signals to be captured during usage transactions, from their physical presence or remotely or hybrid arrangement?
User Authorisation Model (C.8.2.) G	The user authorisation model between the user and stakeholder entities, including intermediaries, should be articulated.	What entities are involved with the identification or entification? What are their roles within the automatic identification or authorisation processes?
Administration Processes (C.8.3.) G ER	The entities assigned with responsibility of administering the APIM must have access to the required system functionality in order to execute their tasks. Some sensitive processes may require segregation of duties or dual control.	What are the required processes to enable organisation's administration personnel to perform duties to fulfil all the life-cycle to support the APIM? What safeguards are required to prevent access to private data and sensitive processes?
Subject Signal Capturing Device Interoperability (B.8.3.) G	The devices for the APIM may be bespoke or ubiquitous and may also need enhancement to comply with interoperability specifications.	Are specifications for devices and software and system interfaces available? How should components be verified to operate with other stakeholders' systems, e.g. relying party?
User Authentication Attributes (B.8.1.) G	Identification and authentication may be linked to access control mechanisms, which may require attribute data from the APIM to function properly.	What attributes need to be captured during transactions with the APIM so as to enable verified users to have access to functions and data in the user authorisation model?
Identification Mode (A.6.1.) G ER	Positive identification and authentication asserts that a subject is enrolled. Negative identification asserts that a subject is not enrolled and not known.	Is the purpose of the APIM to positively identify an enrolled subject or to ensure that a person is not enrolled? Is there a need to consolidate both functions?
Multiple Subject Signals (A.6.5.) G	The assurance requirement based upon risks dictate whether a single signal is adequate or that fusion of biometrics, or knowledge based, e.g. 2FA, or computed data combination are required.	Do the risks and assurance requirements suggest the use of a single subject signal or necessitate the fusion of multiple subject signals possibly using calculated data from artefacts or generated by other sources?
Identification Transparency (A.6.2.) G AQ	Covert identification rules out some APIM types, particularly based user knowledge. Most APIMs require overt subject participation. An application context may permit both covert and overt subject verification.	Does the requirement entail the subject being unaware or conscious of the identification process? What are the legal and technological constraints that apply to covert identification? Does the requirement need to allow for covert and overt flexibility of transparency?
Subject Signal Storage (B.8.2.) G	The requirement for the signal's format(s), its storage location(s) and its required protection dictates how the identification or entification processes are to operate.	What format should the subject signal be stored for the identification or entification processes? Where should that data be stored? How should that stored data be protected?

Table F.8: Functional Requirements Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Approved Privacy Asset Registrars (A.8.4.) G AQ	The entities that are authorised to verify and maintain subjects' private data in a central repository. This function may differ to registration authorities and enrolment agencies or identity service providers.	What entities have been delegated powers to acquire subjects' private data, store, maintain and to use it, and possibly, to issue artefacts or credentials? Does this agency need to gain approval to register, to enrol subjects and to issue artefacts and/or credentials?
Privacy Assets Appeals Procedure (A.8.5.) G AQ	The stakeholders may be required to deal with events where subjects' may not be entitled to access an asset or may not be able to produce the proposed biometric modality data or may dispute stakeholder claims of improper usage.	What procedures are to be put in place for those subject/user applicants who are denied access to an information system or have their access revoked, either legitimately or erroneously?
Privacy Asset Access Controls (A.8.6.) G	Private data are assets belonging to subjects that are maintained by a custodian or approved entities that comply with privacy legal requirements.	What documentation describes the processes to ensure that only authorised users may collect, use, maintain, disclose and protect subjects' private data for the APIM?
Privacy Asset Compromise (A.8.7.) G	Stakeholders should establish their capabilities together with resources in to order manage privacy compromise incidents.	What processes are required to co-ordinate with authorised entities, responses to notifications of suspected privacy violations?
Privacy Asset Inspection (A.8.9.) G AQ	Auditors or government bodies may be required to ensure that data are held in compliance to law and contractual obligations.	What processes need to be put into place to allow authorised inspection of the privacy asset register generally which also allows subjects to access to their personal information held?
Privacy Controls Erosion (A.8.10.) N	Stakeholders need to demonstrate that controls to maintain subjects' private data continue to be effective.	What processes are necessary to prevent any proposed controls on maintaining subjects' private data from being eroded? Should these processes also include subject's data held on an artefact?

Table F.9: Privacy Compliance Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identity Proofing Methods (A.9.2.) G ER	The methods by which administrative personnel verify presented data and documentary evidence are important to detect fraudulent identity applications.	How should the identity knowledge or documentary evidence presented by the subject applicant be verified as authentic for the genuine subject?
Identity Proofing Rules (A.9.5.) G ER	These rules determine who is entitled to be a community member, the data and evidence to support that entitlement and the authorising entity empowering that entitlement.	What are the identity verification processes and the required evidence and authorisation which entitles a subject access to a resource or asset? What attributes entitle or prohibit a user from being a subject member of the community?
Approved Registration Agencies (A.9.6.) G ER	The entities authorised to check subjects' entitlement to assets, which performs the verification of seed identification evidence, subject's application data, issuing identifiers and credentials.	What entities have been delegated powers to register, issue identifiers, acquire subjects' signal data and issue and maintain credentials for the APIM? Does this entity also have authority to store and use subjects' data?
Application, Registration and Enrolment Processes (A.9.7.) G RF AQ	The entity to perform the registration of an authorised subject and the rules that govern the registration processes require articulation.	What are the application, registration and enrolment processes for authorised subjects. What are the complete end-to-end processes, including distribution of artefacts or credentials to subjects or users?
Identity Proofing Detection (A.9.11.) G RF	The may be a requirement for the identity verification and registration processes to be independently scrutinised to address risks identified or to control access to subjects' private data.	What are the processes to detect fraudulent applicant identity claims during registration? Do the registration processes need to be approved by an authoritative body or independent body or to a standard?
Accredited Processes Applicability (A.9.12.) G AQ	The accreditation is to ensure that an identity checking service provider's processes meet a particular specification to offer an accredited identity checking service.	Which entities provide the identity verification functionality and is there a requirement for their processes to be accredited? Does the identity service provider also register individuals or carry out enrolment tasks?
Approved Processes Adoption (A.9.13.) G	The approval relates to whether the identification checking service has to obtain the necessary authorisation to perform and provide such services.	What authorisation is required before the adoption and operation of an approved identity verification service operates on behalf of stakeholder entities, including relying parties?
Credential Identifier or Entifier (A.6.3.) G	The requirement to link the identification process to a unique identifier impacts the APIM mode of operation. An identifier enables 1–1 authentication. Entification involves 1–many searching.	Is a unique identifier assigned to authenticate the subject or entification using the subject's attributes? Is there a need for subject anonymity or the use of a pseudonym to mask the subject's declared identity?
Acceptable Subjects (A.9.4.) G	The rules to implement the policy for distinguishing between subjects entitled to access assets or resources and those individuals that are not authorised.	What does the policies stipulate in terms of determining acceptable members or acceptable characteristics of the subject community? Are there differing interpretations to the rules which constitutes stakeholders acceptability?
Enrolment and Credential Issuance and Delivery (A.9.8.) G RF AQ ER	Registered subject's signals upon which subjects will be entified or authenticated must be captured, generated and distributed securely. Signals may need captured directly from the subject and generated to a specific standard.	What should the processes to capture subjects' signals for the APIM entail? Do these processes require the subject to attend an enrolment facility or produce their initial authentication data or is the data to be generated by other entities and delivered securely to the subject?
Acceptable Proof of Identity Evidence (A.9.9.) G RF AQ	The seed documentation and its sources validate the veracity of the claimed identity. Issuing authorities and relying parties rely on this evidence.	What are the acceptable identification source evidence for proof of identity processes? How is that documentary or data evidence itself verified or cross-referenced?

Table F.10: Registration and Enrolment Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Maximum Identification Attempts Limit (C.11.1.) G ER	Limiting the number of user attempts may reduce demands on system resources and may limit replay attacks at the expense of denying genuine users access to assets.	How many attempts are users allowed to identify or to entify a subject ? What is the maximum number of attempts before access is disabled for that user?
Maximum Identification Time Limit (C.11.2.) G AQ ER	The identification transaction time may need to be responsive to operational tasks and risks. The lack of time locks on repeated attempts may increase the vulnerability of the APIM.	What is the maximum time permitted for each subject identification or entification attempt before another try may be attempted? Is a timed lockout enforcement mechanism needed to prevent brute force attacks?
Operational Characteristics (A.10.1.) G RF	The nature of the environments impacts the ability of an APIM to operate consistently, e.g. lighting variations.	Is the APIM to operate in consistent conditions or variable environments? What are the variable conditions which may impact performance?
Subjects' Signal Tolerations (A.10.3.) G	This rate focuses on the input devices and the need for calibration, both initially and continually.	Will the APIM need to flag poor quality subject signals captured? What is the toleration rate before further subject signals or additional data are acquired from the subject?
Subject Throughput Rates (A.10.4.) G	The timing impacts usability and security and vulnerabilities stemming from repeated attempts or long feedback response times.	What are the required subject throughput rate requirements expressed in terms of minimum numbers in a specific time? What are the maximum queuing or delay timescales?
Subject False Non-match Tolerations (A.10.7.) G	The requirements of the application context may necessitate that genuine subjects are rejected at the expense of detecting impostors, or vice versa.	How many false non-match errors are deemed tolerable or acceptable for subject signals, i.e. false accept rates and false reject rates, which are commensurate to the risks of the application context.
Intervention Rate (A.10.9.) G	The subjects may need assistance and interventions may improve unsupervised throughput over a period of time.	What is tolerable error rate before assistance to a subject is offered by a trained operative? Does this rate allow for user familiarisation of the APIM?
Impostor Detection Rate (A.10.10.) G	The risks in the application context determine the rate at which an APIM is required to perform to detect an impostor.	In respect of the risks identified, what is the acceptable probability that an APIM fails to detect an impostor?
Maximum Enrolment Time (A.10.14.) G	The enrolment time for a subject should not be protracted in respect of the context, its risks and assurance requirements.	What is the maximum time permitted for each subject's signal enrolment attempt?
Maximum Enrolment Attempts (A.10.15.) G AQ AE	The number of enrolment attempts may inadvertently reduce the size of the subject community.	How many attempts is a subject or user allowed in order to enrol their signals? Could supervision reduce the number of enrolment attempts or improve the quality?
Subject's Signals and Template Protection (A.10.19.) G AQ ER	The data upon which identification and/or authentication decisions take place must be reliable.	What are the security controls required to protect the subject's signal data so that these data may be used reliably for subject identification and/or authentication purposes?

Table F.11: Performance Requirements Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Attack Protection and Detection (A.11.1.) G AQ ER	The resources and skills to successfully compromise an APIM should be significant in order to deter misfeasance.	What technology resources and skills should be needed to protect the APIM? To what extent should attacks to be detectable?
Assurance Test Tools and Methods (A.11.2.) G	The required tools and utilities need description to enable assessors to carry out the tests and evaluate result data.	What tools and facilities should be required to perform functional and assurance tests described in a proposed testing plan to meet the required assurance levels?
Documentation and Test Data Availability (A.11.3.) G	Lack of documentation should make it harder for attackers to acquire the relevant knowledge to attack the APIM. Evaluators either test the APIM with or without this knowledge.	What information are to be made available to assessors to test the candidate APIM? What documentation will remain confidential and which elements will be in the public domain for attackers to interrogate?
Functional Outcome Behaviours (A.11.4.) G RF ER	These statements inform candidate APIM suppliers and developers of APIMs on the types of attacks envisaged and how the APIM should respond to each type of attack.	What is the desired reliability to ensure the APIM functions correctly? Are assurance tests to be performed on documented attacks and/or tested by external expertise? What are the behavioural expectations in response to each type of attack?
Audit Logs (A.11.5.) G	Data are required to demonstrate compliance but also assist in gaining an understanding on performance and to investigate security breaches.	What data are required to meet regulatory reporting requirements and risk management functions? Are data required for operational management and investigation purposes?
Assurance Assessment Methodology (A.11.6.) G AQ	The way the assessment is performed should be objective, repeatable and auditable based upon substantiated result data and a testing plan.	How will candidate APIMs be tested? Has an accredited assessment framework been adopted to test candidate APIMs? How should the test plan be formulated for assurance assessments?
Assurance Tests (A.11.7.) G ER	The requirements for proposed devices and artefacts should be described together with the test data needed in order to test for assurance. The tests may be incorporate functionality from internal or external designs.	What are the operational qualities for any required physical devices or artefacts that subjects may need to use? How are these artefacts to be tested? What test data are required, as evidence, on the devices' assured operation?
Fusing Subject's Signals (A.10.11.) G RF AQ ER	The fusion of two or more subject signals may improve the identification or authentication, e.g. 2FA, of the genuine subject. Fusing biometric signals may be required according to the operating conditions, which may require additional identification or authentication assurance.	Do risks dictate the need to fuse two or more subject biometric signals or credentials to improve the identification of a genuine subject? At what performance point would additional subject signals be required to support the identification process? In which circumstances would extra signals or credential data be required?
Operational Accreditation (D.12.1.)	The application context may dictate that some or all components gain formal accreditation by independent assessors.	Does the application context necessitate prior accreditation of the APIM or its components to meet scheme rules or legislation?
Acceptable Usage Conditions (D.12.2.)	The scope of the tests need to be defined in terms of normal usage, likely attacks and possible errors.	What is the usage scope limitations of the candidate APIM assurance tests? Should the APIM be constrained from use in unacceptable environments and conditions?

Table F.12: Assurance Requirements Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Interaction Dynamics (A.6.6.) G	The usage settings will determine how the subjects' signals are to be captured, through the types of device, which may be operationally conducive. A poor HCI design may be a disincentive to potential users.	Is the APIM interaction to operate as a sub-process in a subjects' system usage task? Does the interaction use ubiquitous components? Do these components need to operate in specific ergonomic, physical or logical settings? What outcomes need to be avoided from poor HCI design?
Interaction Supervision (A.6.7.) G	The degree of subject supervision or control needed to ensure the subjects' signals are sensed properly.	Do the signal input devices require subject involvement, subject supervision or should the APIM be designed for self-service?
Multiple Credential Impact (A.7.3.) G	The similarity of input devices may lead to user confusion, errors or undesired behaviour. Multiple APIMs in similar usage settings may introduce usability difficulties and errors.	What are the input devices normally adopted for the types of usage settings envisaged? Does the proposed APIM need differentiate itself from other similar types of APIMs to avoid user confusion, error or behaviour?
Task Sequence (A.7.5.) G	The APIM interaction may appear at the start of the users' task, during and/or at the completion of the transaction. The logic of where to place the APIM interaction is dictated by how the user would habitually complete the task.	What is the position(s) of the identification transaction (s) in the user's task dialogue? What usability design issues should be avoided in order to enable a user's successful completion of their task. Should the user confirm their consent for their private data to be released to other parties for an identification transaction?
User Technical Expertise (A.7.6.) G ER	The extent to which a subject population is able or willing to learn and use a new device or process may impact the types of input devices and the nature of the APIM interaction.	What skills do the subjects or users need to learn to use the input device to record subjects' signals? Does the subject population have the capability and motivation to acquire such skills?
Usage Frequency (A.7.7.) G	The regular usage of an APIM may reinforce subjects' habits. Irregular usage may suggest that subject learning should be minimised.	What is the expected subject usage pattern for the APIM and could this pattern lead to habitual usage? Does this usage pattern apply right across the subject population?

Table F.13: Task Dialogue Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Impostor Pass/ False Alarm Threshold (A.10.5.) G AQ	The setting of the threshold depends upon the risks of the application context. The method to establish the acceptable rate should be articulated.	What is the acceptable identification decision threshold as determined by the risks and social norms of the application context? How was this threshold rate determined?
Multiple Attempts Limit (A.10.8.) G	A genuine subject may receive a false rejection erroneously. The increase in number of attempts, however, gives opportunities for impostors.	In the case of subject signal false non-match for a subject how many additional attempts for identification should the subject be permitted before an action is instigated?
User Equipment Needed (A.10.12.) G	The costs and effort for users to set up the APIM may not be commensurate to users' potential benefits.	What should the effort, including equipment and costs, be required by users to use the APIM in comparison to claimed benefits?
Enrolment Supervision (A.10.13.) G	The quality of data required may necessitate intervention to ensure that signals are sufficient for intended purpose.	What quality should subjects' signals need to meet for automated identification before invoking operative intervention?
Enrolment Failure Arrangements (A.10.16.) G	Some subjects may be excluded and alternative measures may be needed to enable accessibility. Some subjects subject may try to exploit exemptions.	What measures are required should subjects be unable to produce the signals to the required quality, either temporary or permanently?
Vendor Capabilities Evidence (A.10.17.) G	Data showing a track record provides an indication on a supplier's potential to deliver and perform to the terms of a contract. Financial standing and local representation may also have a bearing on acceptability.	What type of evidence is required from candidate APIM suppliers that shows they possess the capability to deploy and support their APIM? Do vendors need to supply references to deployments in similar application contexts or geographic locations?
Defined Effectiveness Metrics (D.14.1.)	The qualitative data and quantitative data that stakeholders require to determine the APIM's utility against their stated business objectives.	How is effectiveness of the APIM defined and to be evaluated for the application context? What data are to be acquired in order to measure and evaluate the APIM's effectiveness?
Defined Efficiency Metrics (D.14.2.)	The qualitative data and quantitative data that stakeholders require to determine the APIM's utility against their stated business objectives.	How is efficiency of the APIM defined and to be evaluated for the application context? What data are to be acquired in order to measure and evaluate the APIM's efficiency?

Table F.14: Envisaged Issues Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identity Theft Detection Impact (A.9.10.) G RF	There should be the means to detect fraudulent identity claims and prevent false registration applications. A credential could be issued to an individual who is not entitled erroneously or unwittingly.	What are consequences of failures to detect fraudulent application identity claims or false registrations? Do risks dictate that identity proofing, registration and enrolment processes require the segregation of operatives' duties and system privileges?
Genuine Failure Impact (C.15.1.) G	The impact of the failure of an APIM to correctly identify a subject needs to be understood and quantified.	What is the impact of an APIM's failure to correctly identify or authenticate genuine subjects?
Acknowledged Conceptual Vulnerabilities (C.15.2.) G	The requirements acquisition processes should reveal vulnerabilities that cannot be resolved. Data are required required as an explicit acknowledgment.	What are the conceptual vulnerabilities that have been accepted by stakeholders in terms of partial or total failure or compromise?
Availability Goals (C.15.3.) G	The availability of the APIM is critical to support the business operations. Slack periods may allow maintenance tasks to be performed.	What are the availability requirements for the APIM? Are there peak processing periods or time slots when maintenance may be carried out?
Manageability Limitations (A.11.8.) G	Insufficient resources, technical competencies and available infrastructure may restrict the choice of APIM.	What personnel, facilities and infrastructure are committed to design, test, deploy, operate and recover the APIM?
Receiver Operating Characteristics and Influences (A.10.18.) G	Each point on the ROC curve defines the acceptable vulnerabilities of the APIM. It is an acknowledgment of these vulnerabilities and influences.	What are the acceptable vulnerabilities of false rejects to false acceptance across all operating identification points? What influences the variations across the threshold curve?
Impostor Pass Impact (A.10.6.) G	The impact of the failure of an APIM or its circumvention due vulnerabilities needs to be understood and quantified.	What is the impact of an APIM's failure to correctly identify impostors, particularly setting the rate too low to detect deliberate attacks?
Upgrade Migration Impact (A.10.23.) G	The impact of migrating or upgrading an existing APIM in terms of continuity and costs may be prohibitive. The migration may introduce some temporary vulnerabilities.	What would be the acceptable disruption for stakeholders, users and subjects to migrate to a new APIM or upgrade a deployed APIM? How should any proposed migration counter temporary vulnerabilities?
Availability Goals (D.15.1.)	The availability of the APIM is critical to support the business operations. Slack periods may facilitate maintenance tasks.	What are the availability requirements for the APIM? Are there peak identification processing periods or time slots when maintenance may be carried out or is the APIM required to operate continuously without degradation?

Table F.15: Envisaged Vulnerabilities Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Expected Lifetime (C.16.1.) G	The stakeholders expectations regarding the return on investments need to be ascertained.	What is the expected lifetime usefulness of the APIM for the application context based on Return of Investment (ROI) predictions or other return, payback period on capital calculations?
Backward Compatibility (A.10.20.) G	The reuse of existing infrastructure existing procedures necessitate accommodating existing capabilities.	Is backward compatibility required to existing APIMs or accepted operating norms or existing capabilities or infrastructures?
Usage Flexibility (A.10.21.) G	The costs associated with a single purpose may not bring sufficient returns on stakeholders' investments.	Should the APIM be limited to a dedicated application or be ubiquitous in design to allow usage with other approved applications?
Scalability (A.10.22.) G	The take up of services and an APIM may be difficult to predict. All projections should be validated as over or under capacity may impact costs and performance.	What scalability is required in terms of responding to population growth or decrease? How quickly should a response be required in terms of numbers and timescales to ensure sufficient processing capacity?
Estimated Programme Costs (A.1.3.) G RF AQ	The programme costs need to be ascertained, which may include many assumptions and calibrated predictions.	What are the sponsor's predicted programme costs? Are all stakeholders' costs based upon similar requirements and application contexts? Have any initial designs been produced to facilitate cost comparisons with similar APIMs? Are predicted costs below budget allocated?
Estimated Operating Costs (D.16.1.)	The operating costs need to be ascertained, which may include many assumptions and calibrated predictions. A comparison with other similar application contexts may provide actual costs incurred.	What are the predicted sponsor and stakeholders' operating costs based upon similar requirements and application contexts? Have any initial designs been compared with budgets allocated for similar deployments over the anticipated lifetime for the APIM? How do these predicted costs compare with current operational budgets and expenditure constraints?

Table F.16: Predicted Costs Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identification/ Authentication Model (A.12.1.) G	A diagrammatic representation assists in determining the extent to which the security architecture, including the APIM, maps to articulated requirements.	How does the APIM's model fit stakeholders' overall security architectures? How well do candidate APIM's technology and processes match existing capabilities?
Subject Signal Storage Locations (A.12.2.) G ER	The locations where the subject's enrolled signal data are stored determine the processes which may be used by the APIM.	Where are the identifier and subject's signals be stored? Are the data for usage stored centrally, on a distributed artefact or on a device or at other locations?
Subject Signal Storage Format (A.12.3.) G AQ ER	The way the data is stored and its form e.g. biometric template, hashed PIN, determines the processes which may be accessed and used by the APIM.	How are subjects' signal data stored, e.g. directory? Are all data stored in the same structure and format? What are the size (bytes) of the data signals, credentials or templates?
Mechanism Processing Locale (A.12.4.) G RF AQ ER	The comparison of the subject's identifier and /or credentials may take place locally, remotely or distributed model. The intended usage locations should be described together with restrictions placed upon its controlled usage by genuine users and detection of unauthorised usage.	What system performs the identification decision and where does this system physically reside? What are the roles of each device and software components in the decision matching processes? Are the intended usage locations different to the signals matching location? What prevents the APIM being applied beyond its intended scope and purpose?
Mechanism Processing Infrastructure (A.12.5.) G AQ ER	The comparison of the subject's identifier and /or credentials may take place over public networks and may require a public key infrastructure.	Is there a centralised database on-line or distributed storage medium, e.g. smart card, or other components that require network access? Are all the APIM's components detailed?
Processing Protection (A.12.6.) G AQ ER	The confidentiality and integrity of subject's signals as data for identification are paramount for an APIM.	How are the subject's signals, data and processes protected during usage transactions and template updates?
Subject Signal Data (A.12.8.) G AQ ER	Data used by the matching decision process to entify or to verify the subject or user forms the core basis of the APIM's functionality.	What subject signals, from biometric modalities or user knowledge or certificates or device identifiers or other relevant data, are used to entify or identify the subject? Are subject's data associated with an identifier or pseudonym?
Combined User Input Signals (A.12.14.) G AQ ER	The processes to capture multiple subject's signals and how these signals are fused to entify or identify should be explained.	Does the design capture multiple subject signals and how are these signals fused in the identification model, which explain the use of intermediary devices and systems?
Maintenance Effort and Reactivation (A.12.10.) G AQ ER	The effort involved to distribute components or revise subject's signals as part of the APIM's normal operation, or in the event of error, compromise or faulty devices.	How easy and how often is it necessary to revise data and/or reissue data, devices, artefacts subject signals associated with the APIM? Does this reinstatement involve the subject seeking assistance from a support team?
Credential Maintenance (A.12.11.) G AQ	The credential data may be revised by the subject upon, an administrator to reset data or an automatic process.	How are credential data or artefacts updated, replaced or replenished in normal, compromise, recovery or failure states?
Subject Signals Processing (A.12.13.) G AQ	All processes to capture the subject's signals, data parameter extraction and transformations to entify or identify a subject should be explained.	What are the components which capture, transform, compare captured subjects' signals and output feedback, i.e. decision result, to the subject and intermediary systems?
Mechanism Training (A.12.17.) G AQ	The subjects may need guidance on how to use, maintain the credentials or to use sensing devices.	How are subjects' trained to use the APIM and its devices or artefacts? Are users to be given training in a security awareness programme?

Table F.17: Security Architecture Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Identity Proofing Processes (C.18.1.) G ER	The processes to verify the veracity of subjects' identity evidence should be commensurate to the risks. validated. Acceptable breeder documents and/or identity attributes should be stated in order to qualify the validity of the application and applicant for registration and enrolment.	What are the processes for the authorised entities in order to check identification evidence gathered or supplied by the subject applicant? How do these processes merge with the application, registration and enrolment processes?
Identifier Data (C.18.2.) G AQ	A unique identifier enables the APIM to link to the genuine subject in the community of subjects.	What is the identifier or entifier assigned to the subject for authentication or entification purposes? Are subject identifiers user defined or randomly generated? Does the identifier have a defined structure, e.g. name@addess? Are there alternative identifiers or entifiers to mask the genuine identity of the subject?
Alternative Identifiers (A.12.7.)		Factor deleted included in factor (C.18.2.)
Credential Life Expectancy and Persistence (A.13.1.) G RF AQ	The life expectancy of the APIM and its components determines the replacement strategy, which may impact costs and performance.	What is the intended life expectancy of the APIM including infrastructure components, devices or artefacts. How are data persistence problems , if relevant, overcome?
Unique Identifiers and Credential Authenticity (A.13.2.) G	The provision of identifiers and/or credentials should be undertaken with controls to ensure the genuine subject receives their identifier data or artefact.	What are the rules for issuing identifiers and/or credentials, whether processes automatically, or through officials or administrators?
Credential Protection (A.13.3.) G AQ ER	The integrity and the confidentiality of the identifier data and credential data form the basis of identity assurance.	How are the integrity of identifiers and/or subject credential data protected by issuing authorities, intermediaries and relying parties?
Credential Maintenance Empowerment (A.13.4.) G	The maintenance of the credentials may need to be authorised entities to carry out these functions.	Do entities require authorisation to entitle them to operate credential maintenance, replacement or destruction processes of identification data? Does this include the revoking of credentials?
Identifier and Credential Maintenance Tasks (A.13.5.) G	The life-cycle management of the identifiers and entifiers and/or credentials need to be stated for assurance purposes.	What are the processes for the issuance, maintenance and destruction of data relating to entifiers, to identifiers to credentials, including revocation of subjects' certificates?
Credential Delivery Verification (A.13.6.) G	The issuer of the identifier and/or the credential needs to know that the genuine user has received these items.	Is the acknowledgment of the receipt of an identifier and /or credentials by the subject reconciled and what is the verification process?
Credential Creation Locations (A.13.7.) G RF AQ ER	The entity and method to enrol subject signal or to generate subsequent signals need to be explained. These signals system may initiated by the subject or computer generated.	How will the initial and subsequent subject signals be captured or credential be generated? What are the processes and channels for delivering artefacts or data to the genuine subject?
Subject Autobiographical Data (A.12.12.) G AQ ER	Additional data relating to the person may be used for identity proofing purposes. The purpose of using the data should align with privacy laws.	What associated subject data are stored with the subject's identifier and subject signal data? Why is it necessary to acquire and retain these additional data?

Table F.18: Identifier Management Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Sampling Normalisation (A.14.1) G AQ	The subject's signals should be of sufficient quality to meet stated decision accuracy and speed requirements.	How many instances of subject signals are captured at enrolment and during usage to create and update subject signal templates?
Signal Entropy (A.14.2.) G ER	Significant differentiation of signals improves the identification accuracy of genuine subjects and also impostors.	Is there sufficient inherent variation or randomness in subjects' signals to avoid identification collisions?
Deceit Resistance (A.14.4.) G AQ	The extent of the deceit resistance on theoretical and practical exploitation informs vulnerability and liability considerations.	What is the difficulty, in required skills and resources, for an attacker to deceive an APIM? How well does the APIM withstand brute force and other common attack strategies?
Artefact or Credential Counterfeiting (A.14.5.) G AQ	The theoretical or practical difficulty in producing a counterfeit artefact or credential informs vulnerability and liability considerations.	What is the difficulty, knowledge and resources, to counterfeit an artefact or credential data or to ascertain subjects' signal data or determine extracted parameters?
Signal Confidentiality (A.14.14.)		Factor deleted as included in factor (A.14.15.)
Signal Data Protection (A.14.15.) AQ ER	Exposing subjects' signal data may enable attackers to gather data to launch denial of service attacks or to perform replay attacks.	How are subjects signals' authenticity, integrity and confidentiality protected during capture, encoding, transmission, and matching processes? How are the subject signal comparison decision result data protected?
Average Failure to Enrol Rate (A.14.17.) G AQ	Predicting the percentage of subjects that may be unable to provide biometric or data signals of sufficient quality informs accessibility and assurance evaluations.	What is the predicted percentage of subjects that will be unable to provide signals of sufficient quality at enrolment? How do these indications compare with other subject communities?
Average Time of Impostor Try (A.14.19.) G ER	The repeated attacks by impostors may severely impact the APIM to perform in terms of throughput speed.	Time to detect impostor attempts, including repeated tries averaged, over all impostor attempts, regardless of successful verification?
Average Time of Verification (A.14.20.) G ER	The average time to entify or identify a subject in proportion to the user's task may impact the APIM's acceptability.	What is the time to achieve correct subject entification or identification which includes repeat attempts averaged over all attempts?
Average Impostor Failure Rate (A.14.21.) G AQ	The average number of impostor attempts before a subject's access is rendered invalid or obsolete informs reliability.	What is the impostor failure rate averaged against all subject signals, including genuine subjects, which decide incorrectly?
Signal Capture Failure Rates (A.14.22.) G ER	Predicting the percentage of subjects that may be unable to provide signals of sufficient quality informs accessibility and usability considerations.	What is the percentage of genuine subjects which are unable to provide signals of sufficient quality during usage? How do these indications compare with other subject communities?
Artefact / Device Accreditation (A.13.8.) G AQ	The accreditation or approval by an agency that artefacts, credentials and devices conform to specifications provides reliability assurance.	What processes are to be established to issue artefacts, credentials or devices from approved agencies? Which authority accredits or approves selected agencies?
Tamper Protection (A.16.18.) G	The capabilities of artefacts, devices or software may provide evidence of unauthorised interference attempts.	Are there tamper deterrent or tamper indicative technologies to notify parties of an attack?
Template Updates (A.16.19.) G AQ ER	Activity logs enable the investigation and detection compromise attempts which may include changes to subject's signals.	What log entries flag changes to an enrolled subject signal or template, user access rights or modifications recognised in user behaviour?
Availability Evidence Submitted (D.19.1.)	Data from potential suppliers should indicate the availability of the APIM including maintenance operations.	What data is provided to assess the potential availability of the APIM and its components? When are maintenance tasks performed?

Table F.19: Reliability Results Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Multiplicity Errors (C.20.1.) G	Similar APIMs from other application contexts may confuse subjects.	Are there similar APIM deployments which may confuse subjects and/or users that could lead to the erroneous usage of the APIM?
Interface Usage Data (A.15.1.) G ER	Test data may include timing user tasks or video data using the APIM.	What test data provides evidence that subjects' usage of the APIM are as designed?
Security Features Conveyed (A.15.2.) G	Visible security features enables the user to manage security tasks.	What features convey the available security features and guidance to the user?
Visibility of Security Status (A.15.3.) G	The interface should advise the user when they have made a mistake or provide feedback on normal status.	Does the APIM's interface provide timely feedback to the user on the APIM's security status?
Intuitive Interface (A.15.4.) G AQ	Awkward interfaces may make the APIM difficult to learn and use.	Is the APIM's user interface comforting and naturally easy to learn? Is the interface's design sufficiently intuitive to facilitate habitual usage?
Aesthetic and Minimalist Design (A.15.5.) G ER	Excessive information communicated may confuse the user, which could lead to errors or delayed user actions.	Does the APIM's interface convey or display only relevant security information?
Error Reporting (A.15.6.) G	The user should be notified of errors and given guidance on how to rectify the error safely.	Does the APIM's interface provide error messages that are sufficiently detailed to advise users where to obtain help?
User / Subject Acceptability (A.15.7.) G AQ ER	An unsatisfactory experience may may indicate HCI design flaws. Users may express a preference for a biometric modality or authentication method that is habitual to them.	Does the APIM's interface provide a satisfactory usage experience? What are user's preferred signal type or APIM for this type of application context? Why is this preferred method more acceptable?
User / Subject Preference (A.15.12.)		Factor deleted included in factor (A.15.7.)
Cognitive Activity (A.15.8.) G	Enrolment processes may be complex and require significant focus to ensure signal data, are of an adequate quality for that candidate APIM.	Does the user require cursory rehearsal, visual co-ordination, in depth cognitive processing in order to produce signal data of sufficient quality for authentication or entification purposes?
Credential Data Retrieval Strategy (A.15.9.) G RF AQ	Remembering random authentication data or methods may be overcome by using visual or audio cues.	What cues are provided to the user to recall credential data or methods to use artefacts or devices to capture subject signals data?
Signal Meaningfulness (A.15.10.) G	Letting subjects choose data that have significant value to them may assist their recall of authentication data.	Are subjects' signal data assigned by a system, acquired automatically or created by the subject to make the signal deducible to the subject?
User Tasks Alignment (A.15.11.) G RF	The APIM interaction should naturally fit at the appropriate point in the users task and not be an awkward adjunct to the task. It should not be cumbersome to the task.	Does the APIM interaction align with users' mental models to perform the processes associated with the user's operational task? Is the user's effort proportionally convenient to complete the operational task?
User Knowledge (B.20.1.) G AQ	The APIM may require users to learn how to use unfamiliar devices or processes that are not intuitive.	What knowledge do subjects need to acquire in order to use the candidate APIM's components? How is that knowledge to be acquired?

Table F.20: Usability Results Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Systems' Resources (A.16.1.) G	The APIM's processing needs may rely on different infrastructures, which may not be under the stakeholders' control.	What network, systems, software, devices, form part of the APIM's infrastructure? Does it utilise a Public Key Infrastructure (PKI)?
System Functionality Description (A.16.3.) G	Reviewing stakeholders' systems ensures the completeness of the APIM and that interfaces are specified.	What evidence demonstrates that the description of the APIM is complete for all functions and components to enable performance and assurance assessments?
Legacy System Impact (A.16.4.) G	The introduction of new systems and new processes may adversely impact existing operations. Extra costs may need to be absorbed by stakeholders.	What is the impact of the proposed APIM, in terms of processing, on existing hardware, software, personnel, infrastructure and systems? What are the effects on current operations?
Legacy System Reuse (A.16.5.) G	Reusing existing networks, systems or operational procedures may assist in containing costs and/or minimising impacts to operations and subjects.	To what extent can existing network, information systems, infrastructure and processes be reused or enhanced for this candidate APIM?
Processing Capacity (A.16.7.) G	The processing capacity needed to operate the APIM, both centrally on servers and on users' devices and systems need to be quantified.	What computer processing power is needed to support the APIM for stakeholder's and users? To what extent are these computations processed on local devices or artefacts?
Back-up Methods (A.16.8.) G	The reliability of these methods may impact stakeholders' ability to recover normal operations quickly.	What are the back-up procedures to respond to a total or partial failure of the APIM, including access to stored subjects' signal data ?
Administration Support Roles (A.16.11.) G	The roles and tasks of staff need to be clarified to ensure clarification of authorised responsibilities.	What are the roles and responsibilities of the administration entities or stakeholders' employees involved in supporting the APIM?
Expert Support (A.16.12.) G	The APIM may require specialist skills and knowledge to perform core duties, which may increase reliance on suppliers.	Are unique skills or competencies required to operate the APIM, in normal, compromised failure and contingency states?
Administration Personnel Training (A.16.13.) G	The competencies of existing personnel may need to be enhanced continually to support the APIM.	What are the training requirements for administrative personnel, both initially and continually?
Device Calibration (A.16.14.) N	Some signal capture devices operate discretely; however, some sensing devices may need periodic recalibration.	Does the user's device need to be calibrated regularly so that the APIM functions and performs correctly?
Lockout/Threshold Maintenance (A.16.15.) G ER	Some genuine users may exceed set retry limits. Users' access should be reactivated by authorised personnel and/or authorised/authenticated processes.	How does the APIM support lockout thresholds on excessive invalid attempts? How are user lockouts or thresholds reset securely?
Subject Supervision (A.16.16.) G	The supervision of subjects may impact subject behaviour when using the APIM.	Are subjects supervised during their usage of the APIM's devices or applications?
Enrolment Supervision (A.16.17.) G	The skills required and the authority to perform enrolment duties to reduce subject signal data acquisition, if applicable.	What are the competences required for staff to supervise subject enrolment? How are quality of captured data improved?
Processing Protection (A.16.20.) G	The signal data must be protected to ensure validity of the identification or authentication processes.	What technological safeguards protect the integrity and confidentiality of subjects' signal data captured, stored, processed and the identification decision result transmitted?
Average Impact of Impostor Attempts (D.21.1.)	Continual brute force attacks may adversely impact systems' processing, which may degrade the APIM's throughput to identify genuine subjects.	What is the impact upon systems processing from repeated impostor attacks and also its impact on performance to authenticate genuine subjects?

Table F.21: Manageability Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Subject Signal Linkage (C.22.1.) G	The strength of the binding may vary between weak password authentication data and cryptographic computations.	What is the strength of the binding between the subject and the signals acquired for identification/authentication?
Operational Enablers (A.17.1.) G	The APIM should not be so complex as to require special skills, which may exclude some users.	Does the user need technical expertise or equipment to use the APIM or its associated artefacts or credentials?
Subject Inclusiveness (A.17.2.) G	Disabilities may exclude the user from using the APIM, via its devices or artefacts, as designed.	Are there any sensory, physical or cognitive skills that would prohibit or limit users from operating the APIM?
User Maintenance Tasks (A.17.3.) G	Some devices may require cleaning, recalibration or software may require updates in order to function correctly. The inability to perform these tasks may exclude some users. Interfering with some components may render them ineffective.	What maintenance tasks does the user undertake to keep the APIM functioning as designed? How will the user be notified or become aware of malfunction or rendering its devices or artefacts vulnerable?
Usage Convenience (A.17.5.) G	The amount of time and effort to use and maintain devices associated with the APIM may be considered disproportionate to the task's risks and liabilities.	What actions and effort are needed to use the APIM when compared with the user's responsibilities and liabilities related to the underlying task?
Technology Provisioning (A.17.6.) G	Some devices or software licences may be expensive to purchase or difficult to obtain, which may exclude some subjects in the community.	What technical components are required, including devices, drivers, software to operate the APIM? Are the user's components, e.g. keyboard, firmware and cryptographic utilities, ubiquitous?

Table F.22: Accessibility Results Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Availability Indicators (C.23.1.) G	The failure of the APIM function may cause service delivery problems or other issues for stakeholders.	How often does the APIM suffer from partial or total outages? What are the tested recovery processes?
Assurance Evidence (A.14.18.) G	The basis of on which test data are acquired and its relevance to the live environment informs assurance testing.	What evidence demonstrates the APIM's ability to meet assurance requirements? How was it produced and by which entity?
Performance Comparisons (A.12.18.) G	The performance results from other similar deployments may highlight performance discrepancies.	How does the indicative performance of this APIM in this application context compare with similar designs or deployments?
Practical Experience (A.12.19.)		Factor deleted as included in factor (A.12.20.)
Identification Time Profile (A.14.7.) G	Elapsed time may be more acceptable by re-engineering the signal sensing, capturing, extraction, transformation comparison and results processes.	What is the possibility of reducing the overall entification or identification time? Have timings on all sub-processes been ascertained so as to consider re-engineering the logic?
Liabilities and Responsibilities (B.23.1.) G	Onerous stakeholder responsibilities and/or disproportionate liabilities may outweigh claimed benefits, notwithstanding costs.	What are the responsibilities and liabilities associated with the APIM for each stakeholder, including users and/or subjects?
Privacy Impact (A.15.13.) G	Revealing social acceptability issues may potentially expose trust problems with the technology and/or service provider.	What is the APIM's effect upon subject's feelings about their privacy and their risks being adequately protected?
Database Contingency (A.12.16.)		Factor deleted included in factor (A.16.9.)
Business Continuity (A.16.9.) G RF AQ	Business continuity and the risks of natural disasters must be weighed against recovery plan costs. The continuity of the APIM may be vital to stakeholders' business operations and provision of services. Security incidents may cause severe operating problems.	What is the criticality of a contingency plan to recover operations to a normal state, in the event of an APIM failure? What are the database contingency plans for the identifiers and subject signal data should this data become compromised or unavailable? How can recovery be achieved to match availability goals?
Recovery Response Times (A.16.10.) G	The time to recover key elements of the APIM should be recorded and be included in a Service Level Agreement (SLA).	What is the repair/recovery response times for central servers and/or users' devices? Are these timescales acceptable to all parties?
User Confidence (A.17.7.) G	A lack of trust in the devices and the subject' signal data used to identify or authenticate the subject may impact the users' habitual operation of the APIM's devices.	To what extent does the user community hold the belief that the APIM will protect their interests and private data? What evidence supports subjects' preference for a specific biometric modality or credential.
Stakeholder Costs Recovery (A.18.7.) G	Stakeholders may consider the use of ubiquitous technologies as a way of reducing costs, which may offer adequate protection and functionality.	What is the possibility of subjects or users absorbing APIM devices costs? Is enabling ubiquitous device usage a viable deployment strategy?
Ubiquity (A.16.6.) G	The APIM may need to operate with an existing mechanism or infrastructure or use ubiquitous components.	Are the APIM's components universal enabling interoperability with alternative APIMs, in the intended application context?

Table F.23: APIM's Issues Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Components Integration (B.24.1.) G	The integration of disparate components may introduce technical vulnerabilities or usability deficiencies.	To what extent do the APIM's components integrate into a coherent solution to meet the stakeholders' operational requirements?
Performance Indications (A.14.3.) G	The False Acceptance Rates and the False Rejection Rates should be compared to accuracy requirements and impact upon throughput.	Does the accuracy of the identification decision meet stated entification and/or authentication requirements? What is the impact on timings from adjusting configured threshold settings?
Mechanisms' Consistency (A.14.8.) G	Knowledge of the APIM's capability to perform reliably, without degradation, is essential to manage risks.	What is the probability that the candidate APIM will perform its intended functions over a specified interval of operation?
Device Interfacing (A.14.9.) G	The integration of signal sensing devices, their firmware and integration to the application should ensure that the security of the candidate APIM is not circumvented.	Are supporting devices and artefacts functioning coherently for their intended purposes in a way that meets the requirements for an APIM, in order to serve genuine subjects and to detect attempts at circumvention?
Circumvention Susceptibility (A.14.6.) G ER	The probability of theoretical based attacks and also motivated attacks needs to be ascertained.	What is the difficulty, in terms of knowledge and resources, to circumvent the APIM without the need to deceive the processing logic?
Signal Predictability (A.14.10.) G	The unpredictability of subject's signal reduces the probability of successful guessing attacks.	Are the subjects' signals sufficiently disguised to prevent attackers from determining these data or succeeding signals?
Signal Abundance (A.14.11.) G	A significantly large key space should deter impostors from brute force attacks and subject signal collisions.	What is the APIM's number of possible subjects' signal permutations or total key space? To what extent are subject signal collisions, in entification mode, possible?
Subject Signal Exposure (A.14.12.) G	Safeguards are needed to ensure subjects' signal data are not exposed to unauthorised parties during storage or during transactions.	Is the subject's signal data easy to record or copy or acquire during storage, capture, transmission, extraction or identification or authentication comparison processes?
Signal Robustness (A.14.13.) G	The clarification of these capabilities may necessitate other controls to counter identified vulnerabilities.	To what extent does the signal capture device withstand known attacks or theoretical attacks?
Exploitable Vulnerabilities (A.14.16.) G	Vulnerabilities should be declared including those in the public domain and those confidential to suppliers.	What are the known exploitable weaknesses in the candidate APIM or in existing deployments?
Vendor Track Record (A.12.20.) G	The stakeholders may gain comfort that the supplier has previously delivered an APIM in this type of application context.	What experience and capabilities does the candidate vendor have in deploying APIMs in this type of application context?

Table F.24: APIM's Vulnerabilities Evaluation Theme

Factor, Identifier and Status	Factor Explanation	Criteria Questions
Artefact Distribution Costs (C.25.1.) G	The logistics for distributing various APIM components securely may involve internal or external distribution channels.	What are the estimated costs for distributing devices, artefacts, initial credential data, e.g. PIN, to subjects/users?
Implementation Costs (A.18.1.) G	The APIMs development costs may need to be segregated from other types of costs for stakeholders' accounting purposes.	What are the costs to develop or integrate the candidate APIM, which includes software implementation, testing and/or costs associated with obtaining security accreditation?
Maintenance Costs (A.18.2.) G	The introduction of new systems brings capital costs and administration support costs, which may be absorbed in full or partly into existing operational budgets.	What are the operating and administrative costs for supporting the APIM, which includes costs of servers, networks, software, personnel, and impact upon existing operations?
Mechanism's Anticipated Life Expectancy (A.16.2.) G ER	The anticipated life expectancy may have implications on investments relating to the APIM's usefulness and derived benefits.	What is the life expectancy for the APIM, including sensors or smartcard readers and/or smartcards or firmware? Does the APIM's design allow for the APIM's life expectancy to be extended to align with technological advancements?
Cost of Input Devices (A.18.3.) G	The costs of bespoke devices to capture subjects' signals is a major capital cost to be absorbed by stakeholders.	What is the cost of the signal input device including any firmware, the cost of tamper detection, including the protection of its internal logic from examination?
Cost of Artefacts (A.18.4.) G	The costs of smart cards together with the issuing of certificates needs to be segregated.	What is the unit cost of an artefact incorporating associated production and ICC personalisation or similar costs?
Infrastructure Processing Costs (A.18.6.) G	The infrastructure costs may be separated from other operating costs; however, trust schemes may incur membership fees.	What are the costs associated with the supporting infrastructure, which includes communication networks or PKI based trust schemes?
Other Parties' Costs (A.18.8.) G	The total cost to stakeholders should be ascertained to ensure that costs do not exceed predicted direct or indirect benefits.	What are the total costs for all stakeholders, including hardware, software, devices, artefacts to ensure its compatibility in the application context?
Costs Influences (A.12.15.) G	The isolation of specific cost elements may assist in identifying alternative technology configurations.	What elements are most likely to increase or decrease the APIM's costs?
Costs to Manage Issues and Vulnerabilities (D.25.1.)	An estimation of the costs to manage issues associated with an APIM and the costs incurred to counter identified issues and vulnerabilities need to be incorporated into the APIM's total operating costs.	What are the estimated costs to manage the issues associated with the APIM? What are the costs of the additional effort and controls to manage the APIM's identified issues and vulnerabilities respectively?

Table F.25: Stakeholders' Costs Evaluation Theme

Bibliography

[1] A. Adams and A. Blandford. Bridging the Gap Between Organisational and User Perspectives of Security in the Clinical Domain. *International Journal of Human-Computer Studies*, 63:175–202, 2005.

[2] A. Adams and M. Sasse. Users are not the Enemy: Why Users Compromise Security Mechanisms and How to Take Remedial Actions. In L. Cranor and S. Garfinkel, editors, *Security and Usability*, pages 639–649. O'Reilly Media Inc., California, USA, 2005.

[3] J. Adams. Cars, Cholera, and Cows - The Management of Risk and Uncertainty. Policy Analysis - No. 335, 1999. `http://www.cato.org/pubs/pas/pa335.pdf` [last checked July 2015].

[4] A. Al-Khouri. *Strategic and Large Scale Government IT Projects' Management: Innovation Report*. PhD thesis, University of Warwick, December 2007.

[5] A. Al-Khouri. Using Quality Models to Evaluate National ID Systems: The Case of the UAE. *International Journal of Social Sciences*, 1(2):117–130, 2007.

[6] V. Alagar. A Human Approach to the Technological Challenges in Data Security. *Computers & Security*, 5:328–335, 1986.

[7] M. Alavi and P. Carlson. A Review of MIS Research and Disciplinary Development. *Journal of Management Information Systems*, 8(4):45–62, 1992.

[8] K. Allendoerfer. Human Factors Considerations for Passwords and other User Identification Techniques, Part 1: Literary Review and Analysis. Technical Report DOT/FAA/TC - 05/20, Federal Aviation Administration, National Technical Information Service, Springfield, Virginia, January 2005. `http://hf.tc.faa.gov/technotes/dot_faa_ct_05_20.pdf` [last checked July 2015].

[9] K. Allendoerfer. Human Factors Considerations for Passwords and other User Identification Techniques, Part 2: Field Study, Results and Analysis. Technical Report DOT/FAA/TC - 06/09, Federal Aviation Administration U.S. Department of Transportation, National Technical Information Service, Springfield, Virginia, January 2006. http://hf.tc.faa.gov/technotes/dot_faa_tc_06_09.pdf [last checked July 2015].

[10] N. Alush-Aben. IdMology: Coherent Identity Management Methodology. Technical report, ID Focus, 2005. http://whitepapers.itbusinessnet.com/whitepaper398 [last checked July 2015].

[11] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems Second Edition*. Wiley Publishing, Inc, Indianapolis, USA, 2008.

[12] R. Anderson and T. Moore. The Economics of Information Security. *Science*, 314(5799):610–613, 2006.

[13] S. Angelo. Security Architecture Model Component Overview. Technical report, SANS Institute, 2001. http://www.sans.org/reading-room/whitepapers/basics/security-architecture-model-component-overview-526 [last checked July 2015.

[14] H. Armstrong. Managing Information Security in Healthcare – an Action Research Experience. In Sihan Qing and JanH.P. Eloff, editors, *Information Security for Global Information Infrastructures*, volume 47 of *IFIP The International Federation for Information Processing*, pages 19–28. Springer US, 2000. http://link.springer.com/content/pdf/10.1007{\%}2Fs12394-009-0027-1.pdf [last checked July 2015].

[15] J. Ashbourn. *Practical Biometrics – From Aspiration to Implementation*. Springer, 2004.

[16] M. Assel, S. Wesner, and A. Kipp. A Security Framework for Dynamic Collaborative Working Environments. *IDIS*, 2009. link.springer.com/content/pdf/10.1007{\%}2Fs12394-009-0027-1.pdf [last checked July 2015].

[17] Australian Government Department of Finance and Regulation. Identity Management for Australian Government Employees Framework (IMAGE). Technical report, Australian Government, 2008. http://www.finance.gov.au/files/2012/04/IMAGEv1-0.pdf [last checked July 2015].

[18] D. Avison and G. Fitzgerald. *Information Systems Development: Methodologies, Techniques and Tools*. McGraw-Hill Education, Maidenhead, UK, fourth edition, 2006.

[19] D. Avison, F. Lau, M. Myers, and P. Nielsen. Action Research. *Communications of the ACM*, 42(1):94–97, January 1999.

[20] D. Avison and H. Shah. *The Information Systems Development Life-cycle: a First Course in Information Systems*. McGraw-Hill International, Cambridge, UK, 1997.

[21] J. Backhouse and R. Halperin. Security and Privacy Perceptions of e-ID: A Grounded Research. In *ECIS Proceedings*, pages 1382–1393, 2008.

[22] D. Balfanz, G. Durfee, and D. Smetters. Making the Impossible Easy: Usable PKI. In *Security and Usability: Designing Secure Systems that People Can Use*, pages 319–334. O'Reilly, 2005.

[23] D. Barrett. *Bandits on the Information Superhighway*. Wiley, 2004.

[24] R. Baskerville. Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Comput. Surv.*, 25:375–414, December 1993.

[25] R. Baskerville. Investigating Information Systems with Action Research. *Communications of the Association for Information Systems*, 2(19), October 1999.

[26] R. Bernard. Information Lifecycle Security Risk Assessment: A Tool for Closing Security Gaps. *Computers & Security*, 26(1):26 – 30, 2007.

[27] E. Bertino and K. Takahashi. *Identity Management: Concepts, Technologies and Systems*. Airtech House, Norwood, MA,USA, 2011.

[28] J. Best. £9 million cost of eye scanning 'would have been better spent on immigration staff', April 2012. `http://central-government.governmentcomputing.com/news/2012/apr/11/iris-ukba-egates-eborders-report` [last checked July 2015].

[29] D. Birch. Victorian Values: Politicians and the Public Incorrectly See Security and Privacy as Opposites. *Information Security Technical Report*, 14:143–145, 2009.

[30] M. Bishop. *The Art and Science of Computer Security*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.

[31] N. Blaikie. *Approaches to Social Enquiry*. Polity Press, first edition, 1993.

[32] N. Blaikie. *Approaches to Social Enquiry: Advancing Knowledge*. Polity Press, second edition, 2007.

[33] B. Boehm. A Spiral Model of Software Development and Enhancement. *Computer*, 21(5):61–72, 1988.

[34] B. Boehm. Get Ready for Agile Methods, with Care. *Computer*, pages 64–69, January 2002.

[35] K. Boehner, P. Dourish R. DePaula, and P. Sengers. How Emotion is Made and Measured. *International Journal of Human-Computer Studies*, 65(4):275 – 291, 2007.

[36] P. Bresciani, P. Giorgini, F. Giunchiglia, J. Mylopoulos, and A. Perini. TROPOS: An Agent-oriented Software Development Methodology. Technical report, University of Trento – Department of Information and Communication, November 2002. Technical Report No DIT-02-0015.

[37] British Airports Authority. MiSense: Biometrically Enabled Access Control Trial at Heathrow Airport 2006/7 Summary Report, November 2007. `http://www.sita.aero/file/2815/misense-summary-report-jun07-pdf` [last checked April 2014].

[38] British Standards Institute. PAS92- Code of Practice for the Implementation of Biometric Systems. Technical report, British Standards Institute, 2011.

[39] BT Identity Management. Identity Management Quick Start Service, 2006. `http://www2.bt.com/static/i/media/pdf/security_healthcheck_br.pdf` [last checked July 2015].

[40] J. Bumgarner and S. Borg. The US-CCU Cyber Security Check-List. Technical report, U.S. Cyber Consequences Unit, 2007. `http://www.usccu.us/` [last checked July 2015].

[41] Bundesamt für Sicherheit in der Informationstechnik. Technical Guideline TR-03110-1 Advanced Security Mechanisms for Machine Readable Travel Documents Part 1 eMRTDs with BAC/PACEv2 and EACv1 v2.10, 2012. `https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html` [last checked July 2015].

[42] K. Cameron, R. Posch, and K. Rannenberg. Proposal for a Common Identity Framework: A User-Centric Identity Metasystem, October 2008. https://www.identityblog.com/wp-content/images/2009/06/UserCentricIdentityMetasystem.pdf [last checked July 2015].

[43] L. Camp. Designing for Trust. In R. Falcone, S. Barber, L. Korba, and M. Singh, editors, *AAMAS 2002 International Workshop - Trust, Reputation and Security: Theories and Practice*, pages 15–29. Springer-Verlag, 2003.

[44] S. Carlsson. Advancing Information Systems Evaluation Research: A Critical Realist Approach. *Electronic Journal of Information Systems Evaluation*, 6(2):11–20, 2003.

[45] A. Cavoukian. Privacy by Design - Take the Challenge, 2009. https://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf [last checked July 2015].

[46] D. Chadwick. Federated Identity Management. In A. Aldini, G. Barthe, and R. Gorrieri, editors, *FOSAD 2008/2009*, number 5705 in LNCS, pages 96–120. Springer-Verlag, Berlin, January 2009.

[47] K. Charmaz. *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. SAGE Publications Ltd, 2006.

[48] S. Chauhan, A. Arora, and A. Kaul. A Survey of Emerging Biometric Modalities. *Procedia Computer Science*, 2(0):213 – 218, 2010. Proceedings of the International Conference and Exhibition on Biometrics Technology.

[49] P. Checkland. *Systems Thinking, Systems Practice: Includes a 30-year Retrospective*. John Wiley & Sons, 1999.

[50] W. Chen and R. Hirschheim. A Paradigmatic and Methodological Examination of Information Systems Research from 1991 to 2001. *Information Systems Journal*, 14:197–235, 2004.

[51] W. Chua. Radical Development in Accounting Thought. *The Accounting Review*, 61(4):601–632, 1986.

[52] W. Chua. Theoretical Constructions Of and By the Real. *Accounting Organisations and Society*, 11(6):583–598, 1986.

[53] L. Church and A. Whitten. Generative Usability: Security and User Centred Design Beyond the Appliance. *NSPW09*, 2010. http://www.nspw.org/papers/2009/nspw2009-church.pdf [last checked July 2015].

[54] N. Clarke. *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*. Springer-Verlag London Limited, London, UK, 2011.

[55] N. Clarke and S. Furnell. Advanced User Authentication for Mobile Devices. *Computers & Security*, 26(2):109 – 119, 2007.

[56] R. Clarke. Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People*, 7(4):6–37, 1994.

[57] R. Clarke. Identification and Authentication Fundamentals, 2004. http://www.rogerclarke.com/DV/IdAuthFundas.html [last checked July 2015].

[58] R. Clarke. Terminology Relevant to 'Identity in the Information Society', 2008. http://www.rogerclarke.com/DV/IdTerm.html [last checked July 2015].

[59] R. Clarke. A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation, 2010. http://www.rogerclarke.com/ID/IdModel-1002.html [last checked July 2015].

[60] A. Coffey and P. Atkinson. *Making Sense of Qualitative Data: Complementary Research Strategies*. SAGE, 1996.

[61] L. Coles-Kemp. Information Security Management: An Entangled Research Challenge. *Information Security Technical Report*, 14(4):181 – 185, 2009. Human Factors in Information Security.

[62] Commission of the European Communities. A Common Immigration Policy for Europe: Principles, actions and tools - COM(2008) 359 final, 2008. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0359:FIN:EN:PDF [last checked April 2014].

[63] Common Criteria Biometric Evaluation Methodology Working Group. Common Methodology for Information Technology Security Evaluation - Biometric Evaluation Supplement. Technical report, Common Criteria Interpretation Management Board, 2002. www.cesg.gov.uk/publications/Documents/bem_10.pdf [last checked July 2015].

[64] Common Criteria Working Group. Common Methodology for Information Technology Security Evaluation. Technical report, Common Criteria Interpretation Management Board, September 2007. http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf [last checked July 2015].

[65] D. Cotroneo and S. Russo. Security Requirements in Service Orientated Architecture for Ubiquitous Computing. In *Proceedings of 2nd Workshop on Middleware for Pervasive and Ad hoc Computing*, pages 172–177, New York, NY, USA, 2004. ACM.

[66] Council of the European Union General Secretariat DG H. EU Schengen Catalogue - Schengen Information System (SIRENE): Recommendations and Best Practices, 2002. http://www.consilium.europa.eu/uedocs/cmsUpload/Cat.Sch.Vol.2EN.pdf [last checked July 2015].

[67] L. Coventry. Usable Biometrics. In L. Cranor and S. Garfinkel, editors, *Security and Usability*, pages 175–197. O'Reilly Media Inc., California USA, 2005.

[68] L. Coventry, A. De Angeli, and G. Johnson. Honest its Me! Self Service Verification. In *Presented at the CHI 2003 Workshop on Human-Computer Interaction and Security Systems*, 2003.

[69] A. Cresswell and S. Hassan. Organizational Impacts of Cyber Security Provisions: A Socio-technical Framework. In *Proceedings of the 40th Hawaii International Conference on System Sciences*. IEEE, 2007.

[70] J. Creswell. *Research Design: Quantitative and Qualitative Approaches*. Sage, First edition, 1994.

[71] J. Creswell. *Research Design: Quantitative, Qualitative, and Mixed Method Approaches*. SAGE, Third edition, 2009.

[72] J. Crosby. Challenges and Opportunities in Identity Assurance. Technical report, HM Treasury UK Government, 2008. http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/media/6/7/identity_assurance060308.pdf [last checked July 2015].

[73] J. Cunningham. Case Study Principles for Different Types of Case Studies. *Quality & Quantity*, 31:401–423, 1997.

[74] D. Bigo and J. Jeandesboz. Border Security, Technology and the Stockholm Programme, 2009. http://aei.pitt.edu/14993/1/

border-security-technology-stockholm-programme.pdf [last checked July 2015].

[75] D. Tziritis and A. Pur and F. Oliveri. SeBoCom Pre-Study: A Preliminary Study on Secure Border Communications, 2009. http://frontex.europa.eu/assets/Publications/Research/SeBoCom_Study.pdf [last checked July 2015].

[76] L. Dadayan. Measuring Return on Government IT Investments. In D. Remenyi and A. Brown, editors, *Proceedings of the 13th European Conference on Information Technology Evaluation*, 2006. http://www.ctg.albany.edu/publications/journals/ecite_2006_roi/ecite_2006_roi.pdf [last checked July 2015].

[77] T. Davenport, J. Harris, and R. Morison. *Analytics at Work: Smarter Decisions, Better Results*. Harvard Business Press, 2010.

[78] D. Denning. *Information Warfare and Security*. Addison-Wesley, 1999.

[79] Department of Internal Affairs. Evidence of Identity Standard. Technical report, New Zealand Government, June 2006. http://www.dia.govt.nz/diawebsite.nsf/Files/EOIStandard/$file/EOIStandard.pdf [last checked July 2015].

[80] G. Dhillon and J. Backhouse. Current directions in IS Security Research: Towards Socio-organisational Perspectives. *Information Systems Journal*, 11:127–153, 2001.

[81] I. Djordjevic, E. Scharf, D. Raptis, and B. Gran. Suitability of Risk Analysis Methods for Security Assessment of Large-scale Distributed Computer Systems. In *Proceedings of 6th Conference of International Association of Probabilistic Safety Assessment and Management (PSAM6)*, San Juan, Puerto Rico, 2002.

[82] E. Dobelis. Expert System for Business Decisions on Security Requirements. In R. Meersman, Z. Tari, and P. Herrero, editors, *On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops*, volume 4805 of *LNCS*, pages 46–47. Springer, 2007.

[83] P. Dobson. Critical Realism and Information Systems Research: Why Bother with Philosophy? *Information Research*, 7(2), 2002. http://InformationR.net/ir/7-2/paper124.html [last checked July 2015].

[84] P. Dourish, J. Delgado de la Flor, and M. Joseph. Security as a Practical Problem: Some Preliminary Observations of Everyday Mental Models, 2003. http://www.

andrewpatrick.ca/CHI2003/HCISEC/hcisec-workshop-dourish.pdf [last checked July 2015].

[85] P. Ducklin. Anatomy of a Password Disaster - Adobe's Giant-sized Cryptographic Blunder. Sophos nakedsecurity, 2013. https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized\-cryptographic-blunder/ [last checked July 2015].

[86] T. Dunstone and N. Yager. *Biometric System and Data Analysis: Design, Evaluation, and Data Mining*. Springer Science Business Media LLC, New York, USA, 2009.

[87] H. Ehtamo, M. Verkama, and R. Hamalainen. How to Select Fair Improving Directions in a Negotiation Model over Continuous Issues. *IEEE Transactions on Systems, Man and Cybernetics - Part C: Applications and Reviews*, 29(1):26–33, February 1999.

[88] A. Emigh. The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond. Technical report, US Department of Homeland Security Science and Technology Directorate and SRI International, October 2006. http://docs.apwg.org/reports/APWG_CrimewareReport.pdf [last checked July 2015].

[89] European Commission. Guidelines for Integrated Border Control Management in EC External Cooperation, 2010. http://capacity4dev.ec.europa.eu/ibm-eap/document/1-guidelines-integrated-border-management-european-commission\-external-cooperation-european [last checked July 2015].

[90] European Commission - Joint Research Centre (DG JRC). Biometrics at the Frontiers: Assessing the Impact on Society, 2006. http://ftp.jrc.es/EURdoc/eur21585en.pdf [last checked July 2015].

[91] D. Everett. Identity Verification and Biometrics. In K. Jackson, J. Hruska, and D. Parker, editors, *Computer Security Reference Book*, pages 37–73. CRC Press, Inc., Boca Raton, FL, USA, 1992.

[92] S. Faily. *A Framework for Usable and Secure System Design*. Dissertation, University of Oxford, 2011.

[93] S. Faily and I. Fléchais. A Meta-Model for Usable Secure Requirements Engineering. In *Software Engineering for Secure Systems, 2010. SESS '10. ICSE Workshop on*, pages 29–35, May 2010.

[94] S. Faily and I. Fléchais. Towards Tool-support for Usable Secure Requirements Engineering with CAIRIS. *International Journal of Secure Software Engineering*, 1(3):56–70, 2010.

[95] V. Fåk. Computer Verification of Human User's Identity: A Theoretical Model and Some Evaluation Criteria. *Computers & Security*, 10:626–636, 1991.

[96] B. Farbey and A. Finkelstein. Evaluation in Software Engineering: ROI, but More than ROI, 2001. http://eprints.ucl.ac.uk/843/1/4.8_edser3eval.pdf [last checked July 2015].

[97] B. Farbey, F. Land, and D. Targett. IS Evaluation: A Process for Bringing Together Benefits, Costs and Risks. In W. Currie and B. Galliers, editors, *Rethinking Management Information Systems: An interdisciplinary perspective*, pages 204–228. Oxford University Press, 1998.

[98] Federal Information Processing Standards Publication. Personal Identity Verification of Federal Employees and Contractors - FIPS201-1, 2006. http://www.nist.gov/manuscript-publication-search.cfm?pub_id=50836 [last checked July 2015].

[99] A. Ferreira, R. Cruz-Correia, L. Antunes, and D. Chadwick. Access Control: How Can it Improve Patients' Healthcare? *Studies in Health Technology and Informatics*, 127:65–76, 2007.

[100] B. Fitzgerald and D. Howcroft. Competing Dichotomies in IS Research and Possible Strategies for Resolution. In *Proceedings of the International Conference on Information systems*, ICIS '98, pages 155–164, Atlanta, GA, USA, 1998. Association for Information Systems.

[101] I. Fléchais. *Designing Secure and Usable Systems*. PhD thesis, University College, London, 2005. http://www.cs.ox.ac.uk/files/6345/thesis_final.pdf [last checked July 2015].

[102] I. Fléchais, C. Mascolo, and M. Sasse. Integrating Security and Usability into the Requirements and Design Process. *International Journal Electronic Security and Digital Forensics*, 1(1):12–26, 2007.

[103] I. Fléchais, M. Sasse, and S. Hailes. Bringing Security Home: A Process for Developing Secure and Usable Systems. In *Proceedings of the 2003 Workshop on New Security Paradigms*, pages 49–57. ACM Press, 2003.

[104] S. Friese. *Qualitative Data Analysis with ATLAS.ti*. SAGE, 2012.

[105] L. Fritsch. State of the Art of Privacy-Enhancing Technology - Report No. 1013. Technical report, Norsk Regnesentral (Norwegian Computer Centre), 2007. https://www.nr.no/publarchive?query=4589 [last checked July 2015].

[106] Frontex. BIOPASS I - Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate, 2010. http://frontex.europa.eu/assets/Publications/Research/Biopass_Study.pdf [last checked July 2015].

[107] Frontex. BIOPASS II - Automated Biometric Border Crossing Systems Based on Electronic Passports and Facial Recognition: RAPID and SmartGate, 2010. http://frontex.europa.eu/assets/Publications/Research/Biopass_Study_II.pdf [last checked July 2015].

[108] Frontex. Operational and Technical Security of Electronic Passports, 2010. http://frontex.europa.eu/assets/Publications/Research/Operational_and_Technical_Security_of_Electronic_Pasports.pdf [last checked July 2015].

[109] Frontex. Annual Risk Analysis 2011, 2011. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Annual_Risk_Analysis_2011.pdf [last checked July 2015].

[110] Frontex. Best Practice Guidelines in the Design, Deployment and Operation of Automated Border Control Crossing Systems, 2011. http://frontex.europa.eu/assets/Publications/Research/ABC_Best_Practice_Guidelines.pdf [last checked July 2015].

[111] Frontex. Beyond the Frontiers - Frontex: The First Five Years, 2011. http://frontex.europa.eu/assets/Publications/General/Beyond_the_Frontiers.pdf [last checked July 2015].

[112] Frontex. Frontex Risk Analysis Network Quarterly Issue 3 July-Sept, 2011. http://frontex.europa.eu/assets/Publications/Risk_Analysis/FRAN_Q3_2011.pdf [last checked April 2014].

[113] Frontex. Situational Overview on Trafficking Human Beings, 2011. http://frontex.europa.eu/assets/Publications/Risk_Analysis/Situational_Overview_on_Trafficking_in_Human_Beings.pdf [last checked July 2015].

[114] G. Ariely and R. Warnes and J. Bijak and R. Landesman. Futures of Borders: A Forward Study of European Border Checks, 2011. http://frontex.europa.eu/assets/Publications/Research/Futures_of_Borders.pdf [last checked July 2015].

[115] G. McLinden. World Bank - Collaborative Border Management : A New Approach to an Old Problem, 2012. https://openknowledge.worldbank.org/handle/10986/10044 [last checked July 2015].

[116] R. Galliers. In Celebration of Diversity in Information Systems Research. *Journal of Information Technology*, 26:299–301, September 2011.

[117] R. Galliers and F. Land. Choosing Appropriate Information Systems Research Methodologies. *Communications of the ACM*, 30(11):900–902, November 1987.

[118] M. Gerber and R. von Solms. Management of Risk in the Information Age. *Computers & Security*, 24:16–30, 2005.

[119] R. Germain. Large Scale Systems. In A. Jain, R. Bolle, and S. Pankanti, editors, *Personal Identification in a Networked World*. Kluwer Academic Publishers, 1999.

[120] D. Gollmann. *Computer Security*. Wiley, 2006.

[121] S. Gregor. The Nature of Theory in Information Systems. *MIS Quarterly*, 30(3):611–642, September 2006.

[122] J. Grijpink. Identity Fraud and Biometrics –An Assessment Model for the Use of Biometrics. *Computer Law & Security*, 22:316–319, 2006.

[123] R. Grinter and D. Smetters. Three Challenges for Embedding Security into Applications. In *CHI Workshop on Human-Computer Interaction and Security Systems*, Fort Lauderdale, April 2003.

[124] E. Guba and Y. Lincoln. Competing Paradigms in Qualitative Research. In N. Denzin and Y. Lincoln, editors, *Handbook of Qualitative Research*, pages 105–117. SAGE, first edition, 1994.

[125] M. Guel. A Framework for Choosing Your Next Generation Authentication / Authorisation System. *Information Security Technical Report*, 7:63–78, 2002.

[126] M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann, and M. Waidner. Privacy-Enhancing Identity Management. *Information Security Technical Report*, 9(1):35–44, 2004.

[127] M. Healy and C. Perry. Comprehensive Criteria to Judge Validity and Reliability of Qualitative Research within the Realist Paradigm. *Qualitative Market Research: An International Journal*, 3(3):118–126, 2000.

[128] M. Hemmati. *Multi-stakeholder Processes for Governance and Sustainability: Beyond Deadlock and Conflict*. Earthscan Publications, London, UK, 2002.

[129] R. Henning. Use of Zachman Architecture for Security Engineering, 1996. `http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper044/baltppr.pdf` [last checked July 2015].

[130] H. Highland. Passwords Revisited. *Computers & Security*, 6(6):451 – 452, 1987.

[131] R. Hirschheim. Information Systems Epistemology: An Historical Perspective. *London School of Economics*, 1991. `http://areadocenti.eco.unicas.it/virili/TerracinaRW/Kit/HirschheimISEpistemology.pdf` [last checked July 2015].

[132] R. Hirschheim, J. Iivari, and H. Klein. A Comparison of Five Alternative Approaches to Information System Development. *AJIS*, 5(1), 1997.

[133] J. Hitchings. Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology. *Computers & Security*, 14:377–383, 1995.

[134] C. Homburg. Hierarchical Multi-objective Decision-making. *European Journal of Operational Research*, 105(1):155–161, 1998.

[135] K. Howell. *An Introduction to the Philosophy of Methodology*. SAGE Publications Ltd, London, UK, 2013.

[136] D. Hubbard. *How to Measure Anything: Finding the Value of Intangibles in Business*. John Wiley & Sons, Inc., second edition, 2010.

[137] J. Hughes. An Identity Management Maturity Model. *Information Security Bulletin*, 11:99–105, April 2006.

[138] E. Hull, K. Jackson, and J. Dick. *Requirements Engineering*, volume 3. Springer, 2011.

[139] P. Hurst. Is Your Identity a Disposable Asset? https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CifasReports/Digital_Thieves_October2010.pdf [last checked July 2015].

[140] ICAO-New Technology Working Group. Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents. International Civil Aviation Organization, 2004. http://www.policylaundering.org/archives/ICAO/Biometrics_Deployment_Version_2.0.pdf [last checked July 2015].

[141] ICAO-New Technology Working Group. MRTDs Development of a Logical Data Structure for Optional Capacity Expansion Technologies V1.7. International Civil Aviation Organization, 2004. https://is.muni.cz/el/1433/podzim2014/PV181/um/sc4/LDS-technical_report_2004.pdf [last checked July 2015].

[142] ICAO-New Technology Working Group. Guide to Interfacing eMRTDs and Inspection Systems. International Civil Aviation Organization, 2005. http://www.icao.int/ [last checked June 2011].

[143] ICAO-New Technology Working Group. MRTDs RF Protocol and Application Standard for ePassports - Part 2 Tests for Air Interface, Initialisation and Anti-Collision and Transport Protocol. International Civil Aviation Organization, 2007. http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-17/TagMrtd17_WP015_b.pdf [last checked April 2014].

[144] ICAO-New Technology Working Group. MRTDs RF Protocol and Application Test Standard for ePassports - Part 3 Tests Application Protocol and Logical Data Structure . International Civil Aviation Organization, 2007. http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-17/TagMrtd17_WP015.pdf [last checked July 2015].

[145] ICAO-New Technology Working Group. MRTDs RF Protocol and Application Test Standard for ePassports - Part 4 e-Passport Reader Tests for Air Interface

Initialisation, Anti-collision and Transport Protocol. International Civil Aviation Organization, 2007. http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-17/TagMrtd17_WP015.pdf [last checked April 2014].

[146] ICAO-New Technology Working Group. Doc 9303 MRTDs Part 3 Machine Readable Official Travel Documents Volume 2 Specifications for Electronically Enabled MRTDs with Biometric Identification Capability. International Civil Aviation Organization, 2008. http://www.icao.int/publications/Documents/9303_p3_v2_cons_en.pdf [last checked July 2015].

[147] ICAO Technical Advisory Group. TAG Report on MRTDs for the TAG Twenty-First Meeting. International Civil Aviation Organization, 2012. http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-21/TagMrtd21-Report.pdf [last checked July 2015].

[148] ICAO Technical Advisory Group on Machine Readable Travel Documents. Electronic machine readable travel documents and passenger facilitation. International Civil Aviation Organization, 2008. http://www.icao.int/Security/mrtd/Downloads20Material/Machine20Readable20Travel20Documents20-20Passenger20Facilitation.pdf[last checked April 2014].

[149] International Air Transport Association. Simplifying passenger Travel: Ideal Process Flow Version 2.0, 2006. http://www.aci.aero/Media/aci/file/Freedocs/IPF_V20_30_Nov_06.pdf [last checked July 2015].

[150] International Civil Aviation Organization. ICAO MRTD Report - Global Standardization Vol. 7 No. 2, 2012. http://www.icao.int/publications/journalsreports/2012/MRTD_Report_Vol7_No2.pdf[last checked July 2015].

[151] International Telecommunication Union -Telecommunication Standardization Sector of ITU. Recommendation X.1252 - Series X: Data Networks, Open System Communications and Security, Cyberspace Security–Identity Management, Baseline Identity Management Terms and Definitions. Technical report, International Telecommunication Union -ITU-T, 2010. http://www.itu.int/rec/T-REC-X.1252/en [last checked July 2015].

[152] ISACA. COBIT 5 for Information Security - Preview Version. Technical report, 2012. http://www.isaca.org/COBIT/Documents/

COBIT-5-for-Information-Security-Introduction.pdf [last checked July 2015].

[153] ISO TC68 Financial Services. ISO 21188–Public Key Infrastructure for Financial Services: Practices and Policy Framework, 2006.

[154] ISO/IEC JTC1 SC17 WG3/TF1 for ICAO-New Technology Working Group. Machine Readable Travel Documents (MRTDs): History, Interoperability, and Implementation. International Civil Aviation Organization, 2007. http://www.icao.int/Security/mrtd/Downloads/TechnicalReports/ICAO_MRTD_History_of_Interoperability.pdf [last checked July 2015].

[155] ISO/IEC JTC1 Working Group SC27 Security Techniques. ISO/IEC 21827 Information technology: Security techniques – Systems Security Engineering – Capability Maturity Model (SSE-CMM), 2008.

[156] ISO/IEC JTC1 Working Group SC27 Security Techniques. ISO/IEC 24761 Information Technology: Security Techniques, Authentication Context for Biometrics, 2009.

[157] ISO/IEC JTC1 Working Group SC27 Security Techniques. ISO/IEC 24760 Information Technology: Security Techniques, Part 1 A Framework for Identity Management - Terminology and Concepts, 2011.

[158] ISO/IEC JTC1 Working Group SC27 Security Techniques. IISO/IEC 29115 Information Technology: Security Techniques, Entity authentication assurance framework, 2013.

[159] ISO/IEC JTC1 Working Group SC27 Security Techniques. ISO/IEC 29146 Information technology: Security techniques –A Framework for Access Management, 2014.

[160] ISO/IEC JTC1 Working Group SC37 Biometrics. ISO/IEC 19785 Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification, 2006.

[161] ISO/IEC JTC1 Working Group SC37 Biometrics. ISO/IEC 19795 Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework, 2006.

[162] A. Jain, R. Bolle, and S. Pankanti. Introduction to Biometrics. In A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in a Networked Society*, pages 1–41. Kluwer Academic, 1999.

[163] S. Jalaliniya and F. Fakhredin. Enterprise Architecture and Security Architecture Development. Master's thesis, Lund University, June 2011. `https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=1982454&fileOId=2018688` [last checked July 2015].

[164] A. Jaquith. *Security Metrics: Replacing Fear, Uncertainty and Doubt*. Addison-Wesley, 2007.

[165] N. Jayaratna. *Understanding and Evaluating Methodologies: Normative Information Model-based System Analysis and Design (NIMSAD)–a systemic framework*. McGraw-Hill, Maidenhead, UK, 1997.

[166] N. Jayaratna and P. Holt. Selection Criteria for Methodologies. *International Journal of Information Management*, 16(1):75 – 76, 1996.

[167] J. Johnston, J. Eloff, and L. Labuschagne. Security and Human-Computer Interfaces. *Computers & Security*, 22(8):675–684, 2003.

[168] J. Jürjens. Model-based Security Testing Using UMLsec: A Case Study. In *Proceedings of the Fourth Workshop on Model Based Testing (MBT 2008)*, volume 220, pages 93 – 104, 2008.

[169] M. Kailay and P. Jarratt. RAMeX: A Prototype Expert System for Computer Security Risk Analysis and Management. *Computers & Security*, 14(5):449 – 463, 1995.

[170] Y. Kalfoglou, T. Menzies, K-D. Althoff, and E. Motta. Meta-knowledge in Systems Design: Panacea or Undelivered Promise? *The Knowledge Engineering Review*, 15(04):381–404, 2000.

[171] P. Karger. Privacy and Security Threat Analysis of the Federal Employee Personal Identification (PIV) Program. In *Proceedings of the 2nd Symposium on Usable Privacy & Security (SOUPS)*, pages 114–121. ACM Press, 2006.

[172] M. Karyda and S. Kokolakisand E. Kiountouzis. Redefining Information Systems Security: Viable Information Systems. In Michel Dupuy and Pierre Paradinas, editors, *Trusted Information*, volume 65 of *IFIP International Federation for Information Processing*, pages 453–467. Springer US, 2001.

[173] R. Keeney, H. Raiffa, and R. Meyer. *Decisions with Multiple Objectives: Preferences and Value Trade-offs*. Cambridge University Press, 1993.

[174] S. Kim and H. Lee. A Study on Decision Consolidation Methods Using Analytic Models for Security Systems. *Computers & Security*, 26:145–153, 2007.

[175] S. Kokolakis, A. Demopoulos, and E. Kiountouzis. The Use of Business Process Modelling in Information Systems Security and Design. *Information Management & Computer Security*, 8(3):107–116, 2000.

[176] S. Körting and D. Ombelli. Mapping Security Services to Authentication Levels. Technical report, European Network and Information Security Agency, November 2010. `https://www.eid-stork.eu/dmdocuments/public/mapping.pdf` [last checked July 2015].

[177] J. Kreps and B. Ancker-Johnston. FIPS 48 - Guidelines on the Evaluation of Automated Personal Identification. Technical report, National Bureau of Standards, U.S. Department of Commerce, 1978.

[178] B. Krishnamurthy, D. Malandrino, and C. Wills. Measuring Privacy Loss and the Impact of Privacy Protection in Web Browsing. In L. Cranor, editor, *Symposium on Usable Privacy and Security (SOUPS2007)*, 2007.

[179] Y. Lai and C. Hwang. *Fuzzy Multiple Objective Decision Making: Methods and Applications*. Springer-Verlag, Berlin, 1994.

[180] F. Land. Evaluation of System Goals in Determining a Design Strategy for a Computer Based Information System. *The Computer Journal*, 19, 1976.

[181] M. Landry and C. Banville. A Disciplined Methodological Pluralism for MIS Research. *Accounting, Management & Information Technology*, 2(2):77–97, 1992.

[182] J. Leach. Improving User Security Behaviour. *Computers & Security*, 22(8):685 – 692, 2003.

[183] S. Lee. A Scientific Methodology for MIS Case Studies. *MIS Quarterly*, 13(1):pp. 33–50, 1989.

[184] A. Lewins and C. Silver. Choosing a Working CAQDAS Package. `http://eprints.ncrm.ac.uk/791/1/2009ChoosingaCAQDASPackage.pdf` [last checked July 2015], April 2009.

[185] B. Lewis. NVivo 2.0 and ATLAS.ti 5.0: A Comparative Review of Two Popular Qualitative Data Analysis Programs. *Field Methods*, 16(4):439–464, 2004.

[186] S. Li and A. Jain. *Encyclopedia of Biometrics*. Springer, 2009.

[187] S. Lichtenstein. Factors in the Selection of a Risk Assessment Method. *Information Management & Computer Security*, 4(4):20–25, 1996.

[188] J. Lopez, R. Oppliger, and G. Pernul. Authentication and Authorisation Infrastructures: A Comparative Study. *Computers & Security*, 23:578–590, June 2004.

[189] M. King. Rebus Passwords. In *Proceedings of the 7th Annual Computer Security Applications Conference*, pages 239–241. IEEE, 1991.

[190] J. Mace, S. Parkin, and A. van Moorsel. A Collaborative Ontology Development Tool for Information Security Managers. In *Proceedings of the 4th Symposium on Computer Human Interaction for the Management of Information Technology*. ACM, 2010.

[191] V. MacLeod and B. McLindin. Methodology for the Evaluation of an International Airport Automated Border Control Processing System. In L. Jain, E. Aidman, and C. Abeynayake, editors, *Innovations in Defence Support Systems*, pages 115–145. Springer-Verlag, Berlin, 2011.

[192] M. Makowski and A. Wierzbicki. Modelling Knowledge: Model-based Decision Support and Soft Computations. In X. Yu and J. Kacprzyk, editors, *Applied Decision Support with Soft Computing*, pages 3–60. Springer, 2003.

[193] A. Mansfield. Biometric Authentication in the Real-world. Technical report, Centre for Mathematics and Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, UK, 2003.

[194] A. Mansfield and J. Wayman. Best Practices in Testing and Reporting Performance of Biometric Devices. Technical Report 2.01, Centre for Mathematics and Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, UK, August 2002. NPL Report CMSC 14/02.

[195] A. Martins and J. Eloff. Assessing Information Security Culture, 2007. `http://icsa.cs.up.ac.za/issa/2002/proceedings/A026.pdf` [last checked July 2015].

[196] S. Mason. Validating Identity for the Electronic Environment. *Computer Law and Security Report*, 20(3):164–170, 2004.

[197] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of Artificial "Gummy" Fingers on Fingerprint Systems. In R. van Renesse, editor, *Proceedings of Optical Security and Counterfeit Deterrence Techniques IV*, volume 4677. SPIE, 2002.

[198] J. Maxwell. *A Realist Approach for Qualitative Research*. SAGE, 2012.

[199] Industrieanlagen-Betriebsgesellschaft mbH (IABG). Fundamentals of the v-modell xt, September 2007. `http://v-modell.iabg.de/v-modell-xt-html-english/index.html` [last checked July 2015].

[200] J. McNiff and J. Whitehead. *Doing and Writing Action Research*. SAGE, 2009.

[201] Meta Group for Danish Ministry of Science Technology and Innovation. Privacy Enhancing Technologies, 2005. `https://danskprivacynet.files.wordpress.com/2008/07/rapportvedrprivacyenhancingtechlologies.pdf` [last checked July 2015].

[202] R. Michaels, P. Grother, and P. Phillips. The NIST Human ID Evaluation Framework. In J. Kittler and M. Nixon, editors, *Proceedings of the Fourth International Conference on Audio Visual Biometric Person Authentication*, pages 403–411. Springer-Verlag, 2003.

[203] M. Miles and A. Huberman. *An Expanded Sourcebook for Qualitative Data Analysis*. SAGE Publications Ltd, second edition, 1994.

[204] A. Milgate. Identity and access management - the identity dictionary, 2006. `http://identityaccessman.blogspot.co.uk/2006/08/identity-dictionary.html` [last checked July 2015].

[205] J. Mingers. Combining IS Research Methods: Towards a Pluralist Methodology. *Information Systems Research*, 12(3):240–259, September 2001.

[206] K. Mitnik, L. Simon, and W. Simon. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc, 2002.

[207] M. Mont, Y. Beresnevichiene, D. Pym, and S. Shiu. Economics of Identity and Access Management: Providing Decision Support for Investments. In *Network Operations*

and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, pages 134–141, 2010.

[208] H. Mouratidis and P. Giordini. Secure TROPOS: A Security-Oriented Extension of the TROPOS Methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(2):285–309, 2007.

[209] H. Mouratidis and J. Jürjens. From Goal Driven Security Requirements Engineering to Secure Design. *International Journal of Intelligent Systems*, 25:813–840, 2010.

[210] E. Mumford. A Socio-technical Approach to Systems Design. *Requirements Engineering*, 5:125–133, 2000.

[211] M. Myers. A Disaster for Everyone to See: An Interpretive Analysis of a Failed IS Project. *Accounting, Management and Information Technologies*, 4(4):185 – 201, 1994.

[212] M. Myers. Investigating Information Systems with Ethnographic Research. *Communications of the Association for Information Systems*, 2(23), 1999. `http://www.qual.auckland.ac.nz/MyersCAISarticle.pdf` [last checked July 2015].

[213] M. Myers. *Qualitative Research in Business and Management*. Sage, 2009.

[214] K. Nandakumar, A. Jain, and A. Ross. *Handbook of Multibiometrics*. Springer, New York, US, 2006.

[215] National Institute of Science and Technology, U.S. Department of Commerce. Biometric Specifications for Personal Identity Verification Special Publication 800-76-2. Technical report, National Institute of Science and Technology, U.S. Department of Commerce, 2012. `http://www.nist.gov/manuscript-publication-search.cfm?pub_id=914224` [last checked July 2015].

[216] National Institute of Standards and Technology (NIST). Special Publication 800-103 Draft An Ontology of Identity Credentials Part 1: Background and Formulation. Technical report, U.S. National Institute of Standards and Technology, 2006. `http://csrc.nist.gov/publications/drafts/sp800-103-draft.pdf` [last checked July 2015].

[217] National Institute of Standards and Technology (NIST). Special Publication 800-63-2 Electronic Authentication Guideline. Technical report, U.S. National Insti-

tute of Standards and Technology, 2013. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf [last checked July 2015].

[218] S. Nerur, R. Mahapatra, and G. Mangalaj. Challenges of Migrating to Agile Methodologies. *Communications of the ACM*, 48(5):73–78, May 2005.

[219] B. Niehaves. Epistemological Perspectives on Multi-Method Information Systems Research. *ECIS 2005 Proceedings Paper 120*, 2005. http://aisel.aisnet.org/ecis2005/120 [last checked July 2015].

[220] NIST Computer Security Division. Federal Information Security Framework prepared for Security, Privacy and Critical Infrastructure Committee. Technical report, CIO Council, November 2000. http://csrc.nist.gov/drivers/documents/Federal-IT-Security-Assessment-Framework.pdf [last checked July 2015].

[221] National Institute of Science and U.S. Department of Commerce Technology. Security metrics guide for information systems. Technical Report Special publication 800-55, National Institute of Science and Technology, U.S. Department of Commerce, 2003.

[222] New Zealand Office of the Privacy Commissioner. Privacy Impact Assessment Handbook. Technical report, Privacy Commissioner, New Zealand Government, 2007. http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf [last checked July 2015].

[223] L. O'Gorman. Comparing Passwords, Tokens and Biometrics for User Authentication. *Proceedings of the IEEE*, 91:2021–2040, December 2003.

[224] W. Orlikowski and J. Baroudi. Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, 2(1):1 – 28, 1991.

[225] L. Palen and P. Dourish. Unpacking "Privacy" for a Networked World. In *CHI2003*, volume 3, pages 605–638, 2003.

[226] A. Palmer. Criteria to Evaluate Automated Personal Identification Mechanisms. *Computers & Security*, 27:260–284, November-December 2008.

[227] A. Palmer. Approach for Selecting the Most Suitable Automated Personal Identification Mechanism (ASMSA). *Computers & Security*, 29(7):785–806, 2010.

[228] S. Parkin, A Morsel, P. Inglesant, and M. Sasse. A Stealth Approach to Usable Security: Helping IT Security Managers to Identify Workable Security Solutions, July 2010. http://www.cs.ncl.ac.uk/publications/trs/papers/1209.pdf [last checked July 2015].

[229] H. Patel. *Guidelines on Research Governance, Research Ethics and Good Research Practice*. Royal Holloway, University of London, Egham, Surrey, UK, third edition, February 2008. http://www.ohs.org.uk/ethics/codeofgoodresearchpractice.pdf [last checked July 2015].

[230] J. Pato and L. Millett. Biometric Recognition: Challenges and Opportunities. Technical report, Whither Biometrics Committee, US National Research Council, September 2010. http://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities [last checked July 2015].

[231] M. Patton. *How to Use Qualitative Methods in Evaluation*. SAGE Publications, London, 1989.

[232] M. Patton. *Qualitative Research and Evaluation Methods*. Sage Publications, London, third edition, 2002.

[233] R. Pawson and N. Tilley. *Realistic Evaluation*. Sage Publications, London, UK, 1997.

[234] T. Peltier, J. Peltier, and J. Blackley. *Information Security Fundamentals*. CRC Press LLC, 2005.

[235] G. Peterson. Security Architecture Blueprint. Technical report, Arctec Group, 2001. http://arctecgroup.net/pdf/ArctecSecurityArchitectureBlueprint.pdf [last checked July 2015].

[236] A. Pfitzmann and M. Hansen. A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. v0.34, Aug 2010. https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf [last checked July 2015].

[237] U. Piazzalunga, P. Salvaneschi, and P. Coffetti. The Usability of Security Devices. In L. Cranor and S. Garfinkel, editors, *Security and Usability*, pages 199–220. O'Reilly Media Inc., California, USA, 2005.

[238] D. Polemi. Biometric techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal Where They are Most Applicable. Technical report, Institute of Communication and Computers, National Technical University of Athens, 1997. http://cordis.europa.eu/infosec/src/stud5fr.htm [last checked July 2015].

[239] D. Power. What is a DSS? *The On-line Journal for Data-intensive Design*, 1(3), 1997. http://www.tgc.com/dsstar/971021/100015.html [last checked July 2015].

[240] G. Prasad and U. Rajbhandari. *Identity Management on a Shoestring: Architectural Lessons from a Real World Implementation*. C4 Media Inc., 2010.

[241] A. Preston. The Problem in and of Management Information Systems. *Accounting, Management and Information Technologies*, 1(1):43 – 69, 1991.

[242] G. Price. The Benefits and Drawbacks of Using Electronic Identities. *Information Security Technical Report*, 13(2):95 – 103, 2008.

[243] C. Probst and J. Hunker. The Risk of Risk Analysis And its Relation to the Economics of Insider Threats. In T. Moore, D. Pym, and C. Ioannidis, editors, *Economics of Information Security and Privacy*, pages 279–299. Springer US, 2010.

[244] A. Rahaman and M. Sasse. A Framework for the Lived Experience of Identity. *IDIS*, 3(8):605–638, 2010.

[245] K. Rannenberg. Recent Developments in Information Security Evaluation - The Need for Evaluation Criteria for Multilateral Security. In R. Sizer, L. Yngstrom, H. Kaspersen, and S. Fischer-Hubner, editors, *Security and Control of Information Technology in Society - Proceeding of the IFIP TC9/WG9.6*, pages 113–128, Amsterdam, The Netherlands, 1994. North-Holland.

[246] K. Rannenberg. Multilateral Security - A Concept and Examples for Balanced Security. In *NSPW '00: Proceedings of the 2000 Workshop on New Security Paradigms*, pages 151–162, New York, NY, USA, 2000. ACM.

[247] D. Raphael and J. Young. Automated Personal Identification. Technical report, Stanford Research Institute, 1974.

[248] J. Raskin. The Humane Interface: New Directions for Designing Interactive Systems. *ACM Press*, 2000.

[249] K. Renaud. Quantifying the Quality of Web Authentication Mechanisms –A Usability Perspective. *Journal of Web Engineering*, 3(2):95–123, 2004.

[250] K. Renaud. Evaluating Authentication Mechanisms. In L. Cranor and S. Garfinkel, editors, *Security and Usability: Designing Secure Systems that People Can Use*, pages 103–128. O'Reilly Media, Inc, California, USA, 2005.

[251] T. Renkema. *The IT Value Quest: How to Capture Business Value of IT Based Infrastructure*. John Wiley, New York, 2000.

[252] K. Rhodes. Information Security Challenges in Using Biometrics: Applied Research and Methods. Technical Report GAO-03-1137T, General Accounting Office of the United States, 2003. `http://www.gao.gov/assets/120/110297.pdf` [last checked July 2015].

[253] L. Richards. *Handling Qualitative Data: A Practical Guide*. Sage, second edition, 2009.

[254] T. Richards and L. Richards. Using Computers in Qualitative Research. In N. Denzin and Y. Lincoln, editors, *Handbook of Qualitative Research*, pages 445–462. SAGE, first edition, 1994.

[255] C. Roberts. Biometric Attack Vectors and Defences. *Computers & Security*, 26:14–25, 2007.

[256] D. Royer. Development of a Theoretical Model for Explaining and Predicting the Impacts of Enterprise Identity Management Introductions. In T. Alexander, M. Turpin, and J. van Deventer, editors, *18th European Conference on Information Systems*, 1793-1805, Department of Informatics, Pretoria, South Africa, 2010. ECIS. ISBN 978-0-620-47172-5.

[257] D. Royer. *Enterprise Identity Management: Towards an Investment Decision Support Approach*. Springer, Ely, USA, 2013.

[258] D. Royer and M. Meints. Enterprise Identity Management (EIdM) - Towards a Decision Support Framework Based on the Balanced Scorecard Approach. In *ARES 2008 –Proceedings of the 3rd International Conference on Availability, Security and Reliability*. Springer, 779-786 2009.

[259] J. Saldaña. *The Coding Manual for Qualitative Researchers*. SAGE Publications Ltd, 2009.

[260] K. Sallhammar, B. Helvik, and S. Knapskog. A Framework for Predicting Security and Dependability Measures in Real-time. *International Journal of Computer Science and Network Security*, 3(7):169–183, March 2007.

[261] M. Sasse. Computer Security: Anatomy of a Usability Disaster, and Plan for Recovery. In *Proceedings of the 2003 Workshop on Human-Computer Interaction and Security Systems*, CHI 2003.

[262] M. Sasse, S. Brostoff, and D. Weirich. Transforming the Weakest Link - a Human/Computer Interaction Approach to Usable Effective Security. *BT Journal*, 19(3):122–133, 2001.

[263] J. Sherwood, A. Clark, and D. Lynas. *Enterprise Security Architecture: A Business Driven Approach*. CMP Books, San Francisco, US, 2005.

[264] A. Shostack and A. Stewart. *The New School of Information Security*. Pearson Education, 2008.

[265] D. Silverman. *Interpreting Qualitative Data*. SAGE Publications, 2006.

[266] M. Siponen. Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods. *Information and Organization*, 15:339–375, 2005.

[267] M. Siponen, R. Baskerville, and T. Kuivalainen. Integrating Security into Agile Development Methods. In *Proceedings of the 38th Hawaii Conference on System Sciences*. IEEE, 2005.

[268] M. Siponen and H. Oinas-Kukkonen. A Review of Information Security Issues and Respective Research Contributions. *The Database for Advances in Information Systems*, 38(1):60–80, February 2007.

[269] S. Sloan. Identity Management: A White Paper. Technical report, The Open Group, 2004.

[270] D. Smetters and R. Grinter. Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications. In *New Security Paradigms Workshop*, Virginia Beach, VA, September 2002.

[271] R. Smith. *Authentication: From Passwords to Public Keys*. Addison-Wesley, 2002.

[272] S. Smithson and R. Hirschheim. Analysing Information Systems Evaluation: Another Look at an Old Problem. *European Journal of Information Systems*, 7:158–174, 1998.

[273] J. Sowa. *Knowledge Representation: Logical, Philosophical and Computational Foundations*. Brooks Cole, 2000.

[274] L. Spencer, J. Ritchie, and W. O'Connor. Analysis: Practices, Principles and Processes. In J. Ritchie and J. Lewis, editors, *Qualitative Research Practice*, pages 199–218. SAGE Publications Ltd, 2003.

[275] M. Spruit and P. Samwel. Risk Analysis on Internet Connection. In *Proceedings of the IFIP TC11 WG11.1/WG11.2 Seventh Annual Working Conference on Information Security Management &Amp; Small Systems Security*, pages 89–102, Deventer, The Netherlands, The Netherlands, 1999. Kluwer, B.V.

[276] T. Stevens. Identity, Identity, Identity. Technical report, British Computer Society, April 2007. `http://www.bcs.org/content/conWebDoc/11113` [last checked July 2015].

[277] S. Stolfo, M. Bellovin, and D. Evans. Measuring Security. *Security & Privacy*, 9(3):60–65, May 2011.

[278] D. Straub and R. Welke. Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4):441–469, 1998.

[279] D. Stufflebeam. Meta-evaluation. *Journal of Multi Disciplinary Evaluation*, 7(15):99–158, February 2011.

[280] R. Sullivan. *Your Evil Twin Behind the Identity Theft Epidemic*. O'Reilly, 1996.

[281] C. Sylla and H. Wen. A Conceptual Framework for the Evaluation of Information Technology Investments. *International Journal of Technology Management*, 24(2):236–261, 2002.

[282] Synovate for the US Federal Trade Commission. The 2006 Identity Theft Survey Report, November 2007. `https://www.ftc.gov/reports/federal-trade-commission-2006-identity-theft-survey\-report-prepared-commission-synovate` [last checked July 2015].

[283] M. Teltzrow and A. Kobsa. Impacts of User Privacy Preferences on Personalised Systems. In C. Karat, J. Blom, and J. Karat, editors, *Designing Personalized User Experiences for eCommerce*, pages 315–332. Kluwer Academic, 2004.

[284] The British Bankers Association. Proving Your Identity, 2009. https://www.bba.org.uk/publication/leaflets/proving-your-identity/ [last checked July 2015].

[285] The Norwegian Centre for Information Security. Password 12: Passport Survey in Norway, 2012. http://passwords12.at.ifi.uio.no/NorSIS/NorSIS_Passwords12.pdf [last checked July 2015].

[286] The Open Group. Identity Management Business Scenario. Technical report, The Open Group, July 2002. http://www.opengroup.org/downloads/bus-scenario-IM.pdf [last checked July 2015].

[287] D. Todorov. *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Auerbach Publications, Boca Raton, New York, 2007.

[288] D. Toledano, R. Pozo, A. Trapote, and L. Gomez. Usability Evaluation of Multi-modal Biometric Verification Systems. *Interacting with Computers*, 18:1101–1122, 2006.

[289] M. Toure. Intelligent Framework for Security. In G. Rzevski, R. Adey, and D Russell, editors, *Proceedings of the Ninth International Conference on Applications of Artificial Intelligence in Engineering*. Computer Mechanical Publications, 1994.

[290] E. Trauth. Choosing Qualitative Methods in IS Research: Lessons Learned. In E. Trauth, editor, *Qualitative Research in Information Systems*, pages 271–288. Idea Group Publishing, 1991.

[291] E. Trauth. The Choice of Qualitative Methods. In E. Trauth, editor, *Qualitative Research in Information Systems*, pages 1–19. Idea Group Publishing, 1991.

[292] E. Trauth and D. Howcroft. Critical Empirical Research in IS: An Example of Gender and the IT workforce. *Information, Technology & People*, 19(3):272–292, 2006.

[293] T. Tryfonas, E. Kiountiuzis, and A. Poulymenakou. Embedding Security Practices into Contemporary Information Systems Development Processes. *Information Management & Computer Security*, 9(4):183–197, 2001.

[294] E. Turban and H. Watson. Integrating Expert Systems, Executive Information Systems and Decision Support Systems. In *Decision Support Systems-89 Transactions*, pages 151–162, New York, NY, USA, 1989. ACM.

[295] UK Biometrics Working Group. Use of Biometrics for Identification and Authentication - Advice on Product Selection. Technical report, UK Government - Office of the e-Envoy, 2002. http://www.cesg.gov.uk/publications/Documents/biometricsadvice.pdf [last checked July 2015].

[296] UK Home Office. IRIS Scheme Definition Document, 2005. http://webarchive.nationalarchives.gov.uk/20140110181512/http://www.ukba.homeoffice.gov.uk/sitecontent/documents/managingourborders/eborders/irisdownloads/schemedefinitiondocument.pdf [last accessed July 2015].

[297] UK House of Lords European Union Committee. FRONTEX: the EU External Borders Agency Report with Evidence, 2008. http://www.publications.parliament.uk/pa/ld200708/ldselect/ldeucom/60/60.pdf [last checked July 2015].

[298] UK Information Commissioner's Office prepared by Trilateral Research & Consulting. Privacy Impact Assessment and Risk Management. Technical report, UK Information Commissioner's Office, 2013. https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf [last checked July 2015].

[299] UK Parliament - Home Affairs Committee. Work of the UK Border Agency (August-December 2011), 2012. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmhaff/1722/172202.htm [last checked July 2015].

[300] United States of America Homeland Security Presidential Directive. Policy for a Common Identification Standard for Federal Employee and Contractors HSPD-12, 2004. https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf [last checked July 2015].

[301] University of Birmingham for Frontex. Ethics of Border Security, 2010. http://frontex.europa.eu/assets/Publications/Research/Ethics_of_Border_Security_Report.pdf [last checked July 2015].

[302] A. Uzunov, E. Fernandez, and K. Falkner. Engineering Security into Distributed Systems: A Survey of Methodologies. *Journal of Universal Computer Science*, 18(20):2920–3006, 2012.

[303] S. Vanamali. Identity Management Framework: Delivering Value for Business. Technical report, The Information Systems Audit and Control Association

(ISACA), 2004. http://www.isaca.org/Journal/archives/2004/Volume-4/Documents/jpdf044-IdentityManagement.pdf [last checked July 2015].

[304] W3C Workshop Participants. W3C Workshop on Identity in the Browser. Technical report, World Wide Web Consortium, 2011. http://www.w3.org/2011/identity-ws/report.html [last checked July 2015].

[305] N. Walliman. *Social Research Methods*. SAGE, 2006.

[306] H. Walther, A. Brömme, and A. Netzer. An Approach to Model the Generic Identity and Access Management Process "approve-request". Technical report, NIFIS, 2008. http://www.genericiam.org/doc/2008-04-17_Exploring_Generic_IAM_Processes_(NIFIS).pdf [last checked July 2015].

[307] G. Warfel. *Identification Technologies: Computer, Optical and Chemical Aids to Personal ID*. Charles Thomas, Springfield, Illinois, USA, 1979.

[308] A. Warren, R. Bayley, C. Bennett, A. Charlesworth, R. Clarke, and C. Oppenheim. Privacy Impact Assessment: International Experience as a Basis for UK Guidance. *Computer Law & Security*, 24:233–242, 2008.

[309] K. Warren. Security Controls in Service Management. Technical report, SANS Institute InfoSec Reading Room, 2010. http://www.sans.org/reading-room/whitepapers/iso17799/security-controls-service-management-33558 [last checked July 2015].

[310] M. Warren and W. Hutchinson. A Security Risk Management Approach for e-commerce. *Information Management & Computer Security*, 11(5):238–242, 2003.

[311] J. Wayman, A. Jain, D. Maltoni, and D. Maio. An Introduction to Biometric Authentication Systems. In J. Wayman, A. Jain, D. Maltoni, and D. Maio, editors, *Biometric Systems: Technology, Design and Performance Evaluation*, pages 1–20. Springer, 2005.

[312] J. Wayman, A. Possolo, and A. Mansfield. Fundamental Issues in Biometric Performance Testing: A Modern Statistical and Philosophical Framework for Uncertainty Assessment, 2010. http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/FundamentalIssues_Final.pdf [last checked July 2015].

[313] S. Weingart, S. White, W. Arnold, and G. Double. An Evaluation System for the Physical Security of Computing Systems. In *Proceedings of the 6th Annual Conference Computer Security Applications Conference*, pages 232–243. IEEE, 1990.

[314] C. Weir, G. Douglas, M. Carruthers, and M. Jack. User Perceptions of Security, Convenience and Usability for eBanking Authentication Tokens. *Computers & Security*, 28(1-2):47 – 62, 2009.

[315] D. Weirich and A. Sasse. Pretty Good Persuasion: A First Step Towards Effective Password Security in the Real World. In V. Raskin, editor, *NSPW '01: Proceedings of the 2001 Workshop on New Security paradigms*, pages 137–143, New York, NY, USA, 2002. ACM. 537011.

[316] D. White. *Decision Methodology*. John Wiley and Sons Ltd, 1975.

[317] E. Whitley. The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications. Technical Report Version 1.09, London School of Economics, June 2005. `http://eprints.lse.ac.uk/29117/1/identityfullreport.pdf` [last checked July 2015].

[318] J. Whittaker and H. Thompson. *How to Break Software Security*. Pearson Education Inc, 2004.

[319] A. Whitten and J. Tygar. Why Johnny Can't Encrypt. In L. Cranor and S. Garfinkel, editors, *Security and Usability*, pages 669–692. O'Reilly, 2005.

[320] G. Williamson, D. Yip, I. Sharoni, and K. Spaulding. *Identity Management: A Primer*. MC Press Online, Lewisville, TX, USA, 2009.

[321] P. Windley. *Digital Identity*. O'Reilly, 2005.

[322] C. Wood, W. Banks, S. Guarro, A. Garcia, V. Hampel, and H. Sartorio. *Computer Security - A Comprehensive Controls Checklist*. John Wiley, Chichester, 1987.

[323] J. Woodward. An Introduction to Biometric Authentication Systems. In J. Woodward, N. Orlans, and P. Higgins, editors, *Biometrics: Identity Assurance in the Information Age*. McGraw-Hill Osborne, 2003.

[324] J. Yan, A. Blackwell, R. Anderson, and A. Grant. The Memorability and Security of Passwords - Some Empirical Results. Technical Report UCAM-CL-TR-500, University of Cambridge, Computer Laboratory, September 2000. `http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf` [last checked July 2015].

[325] Z. Yazar. A Qualitative Risk Analysis and Management Tool - CRAMM. Technical report, SANS Institute, 2002. http://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83 [last checked July 2015.

[326] Z. Ye, S. Smith, and D. Anthony. Trusted Paths for Browsers. *ACM Transactions on Information and System Security*, 8(2):153–186, 2005.

[327] Ka-Ping Yee. User Interaction Design for Secure Systems. In *Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290. Springer-Verlag, 2002.

[328] Ka-Ping Yee. Aligning Security and Usability. *IEEE Security & Privacy*, 2(5):48–55, 2004.

[329] Ka-Ping Yee. Guidelines and Strategies for Secure Interactive Design, 2005. http://labs.toolness.com/temp/sid/ch13yee.pdf [last checked July 2015].

[330] R. Yin. *Case Study Research: Design and Methods*. SAGE, fourth edition, 2009.

[331] J. Zachman. A Framework for Information Systems Architecture. *IBM Systems Journal*, 26(3):276–292, February 1987. http://www.zachmanframework.com/images/ZI_PIcs/ibmsj2603e.pdf [last checked July 2015].

[332] J. Zackman. Concepts of the Framework for Enterprise Architecture. Technical report, Zackman International, 2004. http://links.enterprisearchitecture.dk/links/files/Zachman_ConceptsforFrameworkforEA.pdf [last checked July 2015].

[333] M. Zurko. User-centred Security: Stepping up to the Grand Challenge. In *Proceedings 21st Annual Computer Security Applications Conference (ACSCA)*, pages 187–202, 2005.

[334] M. Zurko and R. Simon. User-centered Security. In *Proceedings of the 1996 Workshop on New Security Paradigms*, NSPW '96, pages 27–33, New York, NY, USA, 1996. ACM.