Review and Analysis of Current and Future European e-ID Schemes

Siddhartha Arora

Technical Report
RHUL-MA-2008-07
15 January 2008

Department of Mathematics
Roal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

Review and Analysis of Current and Future European e-ID Card Schemes

Siddhartha ARORA – sarora@ieee.org
Supervisor: Dr. Michael J Ganley

Royal Holloway, University of London

Submitted as part of the requirements for the award of the MSc in Information Security of the University of London.
Note: After submission of this document, minor typographical changes were made on August 3rd 2007.

CONTENTS

1. EXECUTIVE SUMMARY 6

2. INTRODUCTION 7

2.1 SCOPE & OBJECTIVES 8
2.1.1 SCOPE RELATING TO E-ID CARDS 8
2.1.2 PROJECT OBJECTIVES 8
2.1.3 OUT OF SCOPE 8
2.2 MOTIVATION FOR E-ID CARD IMPLEMENTATIONS 9
2.2.1 E-GOVERNMENT SERVICES 9
2.3 INFORMATION SECURITY & E-ID CARDS 10

3. INTRODUCING IDENTITY 12

3.1 IDENTITY 12
3.2 ALLEGIANCE, CITIZENSHIP & NATIONALITY 13
3.3 IDENTITY DOCUMENTS 14
3.3.1 THE PASSPORT 14
3.3.2 SEED IDENTITY DOCUMENTS 15
3.4 THE ELECTRONIC IDENTITY (E-ID) 15
3.5 THE NATIONAL E-ID CARD 16
3.5.1 SECURE SIGNATURE CREATION DEVICES (SSCD) 17

4. E-ID CARD APPLICATIONS 18

4.1 APPLICATION USERS 18
4.2 BASE FUNCTIONALITY 18
4.3 GOVERNMENT APPLICATIONS 18
4.3.1 DEPLOYED E-GOVERNMENT APPLICATIONS 19
4.3.2 NON-GOVERNMENTAL AND OTHER APPLICATIONS 21
4.4 POSSIBLE FUTURE/OTHER APPLICATIONS 21
4.4.1 IDENTITY MIXER 22

5. NATIONAL E-ID CARD IMPLEMENTATIONS 23

5.1 AUSTRIAN BÜRGERKARTE 23
5.1.1 THE AUSTRIAN CITIZEN CARD CONCEPT 23
5.2 BELGIAN PERSONAL IDENTITY CARD (BELPIC) 27
5.3 UNITED KINGDOM 30
5.4 MALAYSIAN MYKAD 32

6. NATIONAL REGISTRIES & BACK-END DATABASES 34

6.1 NATIONAL DATABASES 34
6.1.1 THE UK NATIONAL IDENTITY REGISTER (NIR) 34
6.2 PAN-EUROPEAN CENTRAL DATABASES 35
6.2.1 EURODAC 35
6.2.2 EUROPEAN VISA INFORMATION SYSTEM (VIS) 36

7. KEY COMPONENTS OF E-ID CARDS 37

7.1 CARD LIFECYCLE 37
7.2 CARD MATERIALS 38
7.3 SMARTCARDS 38
7.3.1 CENTRAL PROCESSING UNIT (CPU) 39
7.3.2 MEMORY 39
7.3.3 MULTI APPLICATION CARD OPERATING SYSTEMS (MACOS) 40
7.3.4 CARD COMMUNICATION: CONTACT VS. CONTACTLESS 41
7.4 OTHER CARD OPTIONS 43
7.4.1 MAGNETIC STRIPS 43
7.4.2 2-D BARCODES 43
7.4.3 OPTICAL STORAGE 44

8. CARD SECURITY MECHANISMS 45

8.1 BIOMETRICS 45
8.1.1 OVERVIEW 45
8.1.2 BIOMETRIC SYSTEM MODEL 46
8.1.3 MEASURING BIOMETRIC ACCURACY 48
8.1.4 FINGERPRINT BIOMETRICS 48
8.1.5 FACIAL BIOMETRICS 49
8.1.6 HYBRID – MULTIMODE BIOMETRICS 49
8.1.7 OTHER FORMS OF BIOMETRICS 49
8.2 PKI INTEGRATION 50
8.2.1 PKI INTEROPERABILITY 50
8.2.2 FUNCTIONS OF PKI FOR E-ID CARDS 50
8.3 PHYSICAL PROTECTION MECHANISMS 51

9. RISK ASSESMENT 53

9.1 SOURCES OF REQUIREMENTS (LEGAL & BUSINESS) 53
9.2 ASSETS REQUIRING PROTECTION 53
9.3 VALUATION OF ASSETS 55
9.4 THREATS, VULNERABILITIES & CONTROLS 55
9.4.1 MASQUERADING / FALSE ACCEPTS 55
9.4.2 DENIAL OF SERVICE / FALSE REJECTS / LACK OF ACCEPTANCE & AVAILABILITY 56
9.4.3 HUMAN ERROR 57

10. STANDARDS & LEGISLATION 58

10.1 INTEROPERABILITY 58
10.2 TECHNOLOGICAL STANDARDS 59
10.2.1 INTERNATIONAL ORGANISATION FOR STANDARDISATION (ISO) / INTERNATIONAL ELECTROTECHNICAL COMMISSION (IES) 59
10.2.2 EUROPEAN COMMITTEE FOR STANDARDISATION (CEN) 59
10.2.3 INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO) 60
10.2.4 OTHER TECHNOLOGICAL STANDARDS 61
10.3 FORMAL (LEGAL) STANDARDS 61
10.3.1 EUROPEAN DIRECTIVE ON ELECTRONIC SIGNATURES – 1999/93/EC 61
10.3.2 DATA PROTECTION AND PRIVACY 62
10.3.3 EUROPEAN COMMISSION TREATY ARTICLE 18 62
10.3.4 OTHER EUROPEAN LEGISLATION 63
10.4 NATIONAL LEGISLATION 64

11. CONCLUSION 66

12. BIBLIOGRAPHY 68

LIST OF FIGURES

Figure 1: Growth Rates in Online Sophistication 2001-2004 10
Figure 2: Stages of Online Sophistication [11] 10
Figure 3: British Nationality Types [14] 14
Figure 4: Generating the Source PIN (sPIN) [30] 25
Figure 5: Generating the Sector Specific PIN (ssPIN) [30] 26
Figure 6: Generation of sPINs from foreign e-IDs [30] 27
Figure 7: Belgian e-ID Front and Back [31] 28
Figure 8: Malaysian MyKad e-ID Card (front) [36] 32
Figure 9: Some Key Components of an e-ID Card [41] 37
Figure 10: Smartcard components (without antenna) [45] [46] 39
Figure 11: Optical Storage Card [53] 44
Figure 12: Biometric System Model [55] 46
Figure 13: Modified TFI model, influenced by the Open Systems Framework of Social Interaction [2] 58

LIST OF TABLES

Table 1: Three Levels of Protection [6] 7
Table 2: Means of Identification [13] 12
Table 3: e-ID Attributes [9] 16
Table 4: e-ID Users 18
Table 5: Public Services [11] 19
Table 6: Online Services Clusters 19
Table 7: Deployed Application Landscape [20], [21], [22] 20
Table 8: Austrian Identity Types [29] 24
Table 9: National Registers in Austria [29], [30] 24
Table 10: BELPIC Chip components [16] 29
Table 11: UK e-ID Card Authentication Services [19] 31
Table 12: Database Key Components 34
Table 13: Variables affecting card lifecycle 38
Table 14: Common materials for e-ID cards 38
Table 15: Biometric Accuracy Measurement Criteria [56] [57] 48
Table 16: Physical Protection Mechanisms [43] 52
Table 17: e-ID Card Drivers 53
Table 18: Relevant Assets for e-ID cards 55
Table 19: Asset Valuation Scale 55
Table 20: ISO/IEC Standards 59
Table 21: CEN ECC Standards 60
Table 22: Three parts to ICAO Doc 9303 [18] 61
Table 23: Other relevant European legislation 64
Table 24: Legislation at National Level 65

ACKNOWLEDGEMENTS

I would like to take this opportunity to thank the following persons for their input, lively dialogue and support:

- At IBM's Zurich Research Lab: Dieter Sommer, Thomas Gross, Tamas Visegrady and the "3 Michaels": Baentsch, Osborne and Kuypers
- At KU Leuven: Danny De Cock
- My project supervisor at Royal Holloway: Dr. Michael J Ganley
- Fellow colleagues in the MSc programme at RHUL, especially Matt Palmer, Roman Yashin, Victor Fieldhouse and Leo Kolbeinsson
- At Zurich Financial Services: Luke O'Connor
- The moderator of the "Interop e-ID" mailing list and e-ID specialist at the Comune di Grosseto: Bud P. Bruegger
- Last, but not least, my parents for their kindness, support and encouragement.

1. EXECUTIVE SUMMARY

The purpose of this report is to accomplish the following objectives:

1. Review and analysis of existing and future e-ID standards and technologies

2. Review and analysis of national e-ID card schemes (in Europe), including their objectives and the policy drivers (motivation).

3. A review of the applications that e-ID cards enable, both for public policy purposes and commercial usage (planned & actual).

4. Lessons learned from existing e-ID card schemes (successes and failures) and determine whether new international schemes/standards will address past short-comings or not.

As a result of attempting to accomplish these objectives, it became apparent that across Europe we are still in a fairly early stage of development. More importantly, there is no coordinated effort across Europe to implement e-ID cards. Leading e-ID card schemes to be designed and implemented at a national level has lead to a heterogeneous collection of scheme types. Not only is there an inconsistency in the primary objectives of e-ID cards, the use of different standards and technologies has lead to a lack of interoperability between schemes.

2. INTRODUCTION

In addition to considerable press coverage [1], electronic identity (e-ID) Cards have recently been a topic both at a European Union [2], and at national levels [3]. In addition, the technologies underlying e-ID Cards, many of which will be reviewed in this project, are also technologies with varying levels of maturity and certainly all of which are still actively being studied in the research community [2].

At a very high level, there probably are three key reasons why e-ID cards have received prominent attention:

- Political and legal pressures to implement electronic Passports, which include smartcard and biometric technologies, following specifications mandated by International Civil Aviation Organisation (ICAO) Document 9303.
- The passing in 1999 of the European Directive on Electronic Signatures [4] has lead to various initiatives both at a pan-European and national level to enable the realisation of this directive.
- Multiple national initiatives to define and deploy advanced identity cards, including the ability to support functionality for the above two points.

While the topic of e-ID cards is a topical one, an academic paper illustrating the challenges and basic functions of an e-ID card goes back to over twenty years ago. Amos Fiat and Adi Shamir highlighted at CRYPTO '86 [5] the limitations brought about with not using e-ID technology:

- Passports can be photocopied by hostile governments
- Credit card numbers can be copied
- Computer passwords are vulnerable to hackers and wire-tappers
- Military Command & Control terminals may fall into enemy hands

Fiat and Shamir illustrated [6] three levels of protection which could be applied using e-ID cards.

Scheme	Description
Identification	A can prove to B that he is A, but someone else can not prove to B that he is A
Authentication	A can prove to B that he is A, but B can not prove to someone else that he is A
Signature	A can prove to B that he is A, but B can not prove to himself that he is A

Table 1: Three Levels of Protection [6]

These three schemes, which are also referred to as I-A-S (Identification, Authentication & Signature), remain key pillars in defining the primary capabilities of today's e-ID Cards.

When reviewing e-ID related literature for this project, it became apparent that there are two schools of thought that are studying and attempting to define the necessary steps for wide-scale adoption of e-ID cards. The one school attempts to use I-A-S features and representation of an identity in electronic form (e-ID) to meet the national legislation that fulfils the requirements of the European Directive on Electronic Signatures [4]. A second school tends to look more at extending existing ID card schemes to make them more secure. Adding a smartcard chip to

an identity card can make it harder to forge or offer additional functions to be added to the card, above and beyond being presented by the holder to identify themselves. In some cases these two schools overlap, such as when the former school looks to represent their e-ID token on a national identity card. Likewise, existing national identity card issuers look to add new features, such as supporting it for electronically signing documents or providing sophisticated e-Government services. Both schools use the same term, *e-ID card*, to mean in many cases two different things. In addition, the initiatives to launch ePassports, has caused further confusion, because some of the base technology, such as smartcards, are the same. However, the challenges and primary functions are from the onset different. Passports are seen as a border control document. National e-ID cards will focus on "everything else", though some countries are looking to integrate e-Passport functionality into their e-ID cards.

Needless to say, the confusion caused by using the same terminology for different things, has lead the necessity to define the scope of e-ID Cards for purposes of this project.

2.1 Scope & Objectives

2.1.1 Scope relating to e-ID Cards

The e-ID cards which will be studied in this document will be those which generally fulfil the following requirements:

- Serve as a national identity card and are issued by a government body to a uniquely defined citizen or resident
- Performs I-A-S functionality, or a subset thereof
- Is not a legally accepted passport, though it may support ePassport functions or standards

2.1.2 Project Objectives

Prior to starting this project it was agreed upon to accomplish the following objectives:

- Review and analysis of existing and future e-ID standards and technologies
- Review and analysis of national e-ID card schemes (in Europe), including their objectives and the policy drivers (motivation).
- A review of the applications that e-ID cards enable, both for public policy purposes and commercial usage (planned & actual).
- Lessons learned from existing e-ID card schemes (successes and failures) and determine whether new international schemes/standards will address past short-comings or not.

2.1.3 Out of Scope

e-ID cards in themselves are only as good at the systems and processes that support their issuance and usage. It is important to keep in mind that processes around enrolment of identities, implementing secure card delivery and ensuring usage, loss and re-issuance (card life-cycle management), as well as managing the application environment around the cards is critical to their success. Despite

their importance, these topics will remain out of scope for this project. Additionally, other systems that support the e-ID cards, including readers, public key infrastructure, back-end systems, as well as necessary organisational aspects related to the e-ID card, though on occasion mentioned, will be out of scope for this project.

Beyond the technical and process/operational aspects of an e-ID card system, a successful deployment is also dependent on a healthy user-adoption rate. In some cases, especially recent debate in the UK has shown [3], the aspects of violations to citizen's privacy has illustrated signs of possible resistance. Likewise, the size of e-ID cards requires significant financial investment. Both the privacy and financial aspects of e-ID card deployment, while very important, will not be addressed in this study.

To conclude, we will focus primarily on the components and information security aspects that are necessary to represent the e-ID on a card. We will thus only briefly mention, but not go into any detail, the other aspects of the e-ID card, such as additional physical security features, materials used or content printed/engraved onto the card.

2.2 Motivation for e-ID Card Implementations

In December 2004 at a European Committee for Standardisation / Information Society Standardization System (CEN/ISSS) workshop on eAuthentication [7], it was concluded that some of the primary drivers for supporting a national e-ID are as follows:

- Need to support national e-Government services
- Address common and global Identity Fraud (primarily an issue in the in financial/card-payments area)
- Address national and pan-European anti-terrorism measures
- Build a more "inclusive" European society, hence creating a "European Identity"
- Stimulate emergence of new "intra-European" services in order to reduce costs of infrastructure (efficiency gains …)

In addition to the above driving factors, various legislative drivers also exist. Examples include:

- Ensuring National Security, such as through the European Directive on Money Laundering [8] requiring stronger identification mechanisms to be used by financial institutions.
- Enabling use of the European Directive on Electronic Signatures - not only for purposes of serving as a tool to signing electronically, but also serving as a form of entity authentication [9].
- In some countries, particularity the UK, that don't have an existing national identity card, put legal acts [10] in place to require national identity cards to be issued, including supporting some e-ID card functions.

2.2.1 e-Government Services

In this study we will focus primarily of the first driver identified by CEN/ISSS. This seems to be the focus of many e-ID card implementations, at least in terms of illustrating benefits to citizens. The focus on public, rather than private services, could be due to the fact that it is government institutions that are primarily driving the issuance of e-ID cards, rather than the private sector.

The European Commission's benchmarking study [11] on electronic public services in Europe has shown a general increase in both the quantity of public services and their level of sophistication.

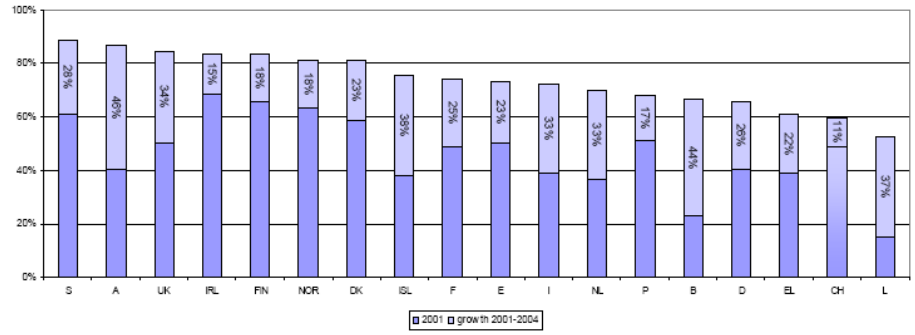

Figure 1: Growth Rates in Online Sophistication 2001-2004

Without going into detail, the method for defining online sophistication is split into four major stages, where it is only at the third stage onwards, that the need to use some authentication mechanism together with an intake of an official electronic document is required. It can be considered that at this more advanced stage of e-Government service do e-ID cards play a significant role. The above table illustrates a general increase across Europe of government services becoming more and more sophisticated.

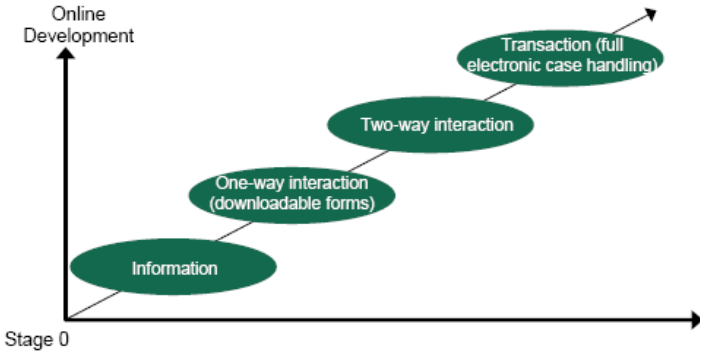

Figure 2: Stages of Online Sophistication [11]

An example of "sophistication" includes strong client authentication. E-ID cards are good vehicles in performing such functions. Hence, motivation for e-ID cards can be seen as enablers to perform more sophisticated e-Government applications.

2.3 Information Security & e-ID Cards

The three pillars of information security (confidentiality, integrity and availability) are just as relevant to e-ID cards as they are in any other information-centric system. We will briefly address these three pillars here, as the elements associated with them will occur throughout this project in various forms to ensure e-ID cards can be considered secure.

Confidentiality:
Whether using symmetric or asymmetric cryptography, the identity of which keys and related material is divulged to is critical.

Integrity:

Using often the same cryptographic mechanisms as with supporting confidentiality, proving non-repudiation, or other aspects of integrity, relies significantly on being able to prove/ensure who has the ability to make legitimate changes.

Availability:
If your e-ID card is unavailable (e.g. problem with chip, network or loss of card), then the card becomes unable to operate as designed. It is critical to ensure that an e-ID card is designed in a robust manner. Prevention due to technical failure, intentional or otherwise, can lead to denial of services, for which availability is hence critical to maintain.

For all three pillars, risks exist due to threats and vulnerabilities associated with the design and motivations of others. Aspects associated with failure of the above pillars will be addressed in the Risk Assessment chapter (Chapter 9).

Given the focus on supporting e-Government services, one should note that Leithold et al [12] defined the key security requirements of an e-Government application as the ability to support the following attributes:

- Entity Authentication – ensuring that the source of data supplied is only from the single individual as claimed
- Data Origin Authentication – ensuring that the data supplied is indeed from the source being claimed
- Confidentiality – ensuring that data supplied is not revealed to unauthorised parties
- Non-repudiation – Ensuring that a false denial of having performed a transaction can proven

In addition to these security requirements, Leithold et al pointed out [12] that, unlike in more commercial deployments, e-government applications are often mandated to illustrate aspects of being non-discriminatory towards their citizens in terms of accessibility and selection of technologies and standards. When e-government applications are deployed to incorporate private parties or corporations (sometimes also referred to as public-private-partnerships), then e-government applications are also required to publish standardised (sometimes also referred to as open) interfaces.

In a more traditional non-e-government scenario, [12] points out that these requirements are accomplished using special stationary, envelopes, hand-written signatures, stamps, public notaries, as well as face-to-face encounters and use of registered postal mail.

3. INTRODUCING IDENTITY

3.1 Identity

Identity has a meaning in a variety of disciplines, including:

- Philosophy
- Mathematics
- Social Science & Psychology
- Business
- Computer Science

For purposes of this study, we will focus on the applicability of identity in the social sciences, mainly to identify individual persons, but also take a closer look at the use of identity from a computer science perspective, which attempts to represent the identity in an electronic form (though not necessarily confined to human beings).

In Clarke's 1994 paper on human identity [13], he attempts to define *human identity*, mainly as they pertain to information systems. His definition, after considerable discourse, is as follows:

"human identification is the association of data with a particular human being."

This definition may seem quite obvious, but Clarke makes a point that information systems literature has actually not done a comprehensive job of defining how humans are identified in an electronic context.

Clark provides [13] the following list as an illustration of means by which an individual can be identified:

Means of Identification	**Clarke's Definition**	**Examples**
Appearance	How the person looks	Use of photographs on identity documents, facial biometrics
Social behaviour	How the person interacts with others	Education records, mobile phone records, credit card statements, video surveillance data
Names	What the person is called by other people	Name listed in national registry, on passports, birth certificates etc.
Codes	What the person is called by an organisation	ID card numbers, social security numbers
Knowledge	What the person knows	Passwords, PINs
Tokens	What the person has	Smartcards, Secure ID cards
Bio-dynamics	What the person does	Signature biometrics
Natural physiography	What the person is	Most forms of biometrics: fingerprint, iris, retina, etc.
Imposed physical characteristics	What the person is now	Height, weight

Table 2: Means of Identification [13]

The national identity card is a tangible device which attempts to represent the above forms of identification. Specifically, the e-ID card attempts to use electronic data processing techniques (e.g. leveraging biometrics, public key infrastructures, secure storage mechanisms on smartcards etc), to perform a more accurate representation of a specific identity than more traditional paper or plastic card identity documents.

3.2 Allegiance, Citizenship & Nationality

As this study has a focus specifically on national identity cards. It is important to explore various aspects of what is understood by nationality, especially in the context of this term being used for e-ID cards. It might be helpful to look at the origin of nationality, as a concept, as this helps explains some of the motivation for deploying national identity cards.

Allegiance

Since ancient times, allegiance as a concept has existed "you had a king, you owed allegiance to him. It was as simple as that" [14]. English law started making references to the concept of allegiance starting as early as the thirteenth century. [14].

Citizenship

In Roman times, law defined the terms of citizenship, which ultimately defined to whom you paid your taxes to. Citizenship could be obtained by enemy aliens through defection and collaboration. With the rights to citizenship, also came certain duties beyond paying taxes, most notably military service. A refusal to partake in the service would mean a revocation of the citizenship. Likewise, Romans would automatically lose their citizenship if the became prisoners of war [15] being referenced in [14]. Today, e-ID's can be revoked as well (e.g. though published Certificate Revocation Lists) [16], though their motivation tends to be to due a change in the status of the card or contents as opposed to a revocation of citizenship!

Nationality:

Unlike citizenship, the concept of nationality is a more modern one. In fact it is not until the early nineteenth century that one seems to find initial references to nationality in the English language. According to Lloyd [14], it seems likely that the English borrowed the term from the French *principe des nationalités.* This term had its origins in revolutionary theory that "persons having a common language and culture form a nation and, as such, ought to be entitled to self-government as a state." While this definition may seem to make sense, it caused confusion especially in Britain where holders of passports did not necessarily imply holders of British citizenship. In fact Lloyd illustrates how even until the end of the twentieth century, British passport holders could have one of the following descriptions to define their "nationality", which did not necessarily equate to citizenship.

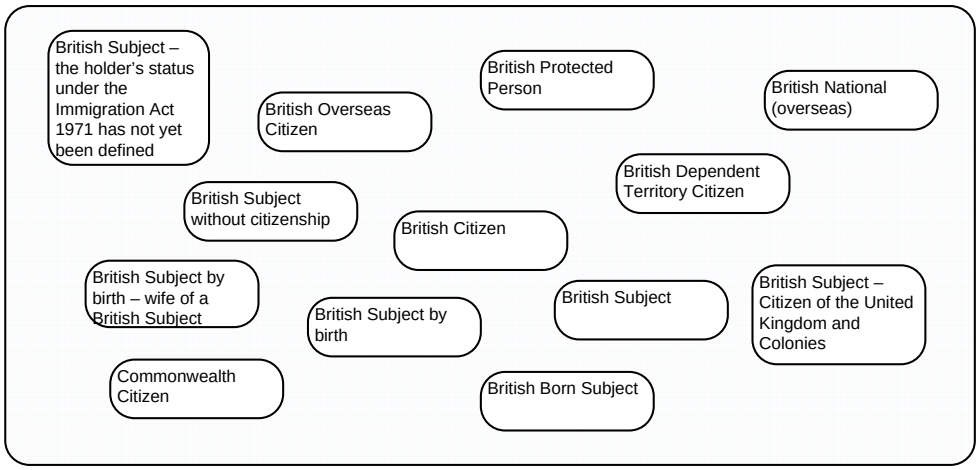

Figure 3: British Nationality Types [14]

Needless to say, such classification schema can cause quite some confusion, and does not make it any easier to then define the use of what types of persons, citizens or otherwise, should be eligible or required to hold a national identity card. The requirements for who is eligible (or in the case of certain countries, where mandatory), required to hold an identity card, tends to lie within national laws. In chapter 10 we will take a closer look at the legal environment associated with e-ID cards.

Lloyd has pointed out [14] that "the passage of time has somehow fused and confused the ideas of allegiance, nationality and citizenship." This fusion and confusion is increased further when incorporating the concepts of e-ID and e-ID cards, especially when pertaining to national e-ID cards, which imply nationality, but not necessarily citizenship.

3.3 Identity documents

While the focus of this project is on the electronic identity (e-ID) card and some of its related infrastructure, it helps to review the e-ID in a historical context. The concept of using a document to prove a credential for identification purposes has been known to go back as far as 1500 BC when "common people in Egypt were required to register themselves with the magistrates." [14] This form of registration required not only names, but also other particulars to be registered. Interestingly, the same registration procedure was not only used for individuals, but also ships, that wished to leave a given port. This technique from the ancient Egyptians can thus also be seen as one of the earliest forms of a passport [17] attributed by [14].

3.3.1 The Passport

The forerunner to the passport concerned such concepts as identity, nationality and allegiance, and were not only used for safe passage of individuals, but also in sixteenth century England for the safe passage of ships [14]. This use of identity documents to not only accredit persons, but also objects, brings up an interesting use of identity, something which today we are once again "re-discovering" as applied in the digital world. As an example, federated identity management systems are sometimes applied to services, rather than mere individuals. Also, we see certain e-IDs being used to represent business entities rather than mere individuals.

According to Lloyd [14], today's passport serves primarily two functions: establish the identity and the nationality of the holder. The e-ID card, which is a focus of this study, is primarily used to serve the primary function, and in addition to serve other functions, such as authentication and signing capabilities. However, as e-ID cards are issued by sovereign nations, and issued as national identity cards, they also represent the nationality of the issuer, though not necessarily of the holder.

Today a number of standards associated with passports are defined by the International Civil Aviation Organisation (ICAO). These standards include, the specifications necessary for machine-readable travel documents (MRTD) [18], which most recently has included biometrics and other identity attributes stored on a smart card embedded into the passport. To this extent, the ICAO MRTD specifications are similar to e-ID card implementations. We sometimes see confusion between passports with biometrics (also referred to as ePassports) and e-ID card specifications. For example, during the definition of the UK ID Card, we have seen reference to the Identity Card and the ePassport as being practically the same thing: "when we record and store fingerprint biometrics (all 10 fingerprints for each person), we store a complete set in the National Identity Register (NIR) and a subset of these will be *recorded on the card or the passport*, *in line with ICAO recommendations.*" [19]

What is clear though is that a passport, with the exception of Russia (and the former Soviet Union) which issues an "internal passport", all passports are issued with the primary motivation to identify a person to enter and exit across international borders. Any other use of the passport is secondary. On the other hand, e-ID cards, or identity cards in general, have always had multiple primary purposes, depending on when and by whom they have been issued.

3.3.2 Seed Identity Documents

An identity document, when issued, is based on some form of verification that is performed. Usually a procedure is put in place and multiple attributes about an individual are put together to create a profile, as well as ensure that along the way nothing suspicious or contradictory is presented.

A human identity can be said to be "created" when a person is born. At this stage, it is often the case that the birth is registered in a national birth and death registry, though the method mandated differs based on local legislation. The registration of the birth within a registry enables the creation of a birth certificate. This document is often considered a "seed identity document". In other words, with this document one can "prove" one's existence and hence enable subsequent identity documents to be issued (e.g. drivers licenses or public library cards). Needless to say, this method of proof is subject to considerable vulnerabilities. As a result, often multiple "proofs" of identity are collected to generate a profile. Collectively, assuming no inconsistencies, these records suffice to create a single seed document, such as a passport. Examples include school, employment and medical records, as well as other forms of identification, which may have been created with- or without a seed document (for example a drivers license).

3.4 The Electronic Identity (e-ID)

While in subsequent chapters we will take a closer look at how e-IDs are implemented at a national level, Myhr [9] illustrated some of the key attributes necessary for a successful e-ID, taking into account a desire to define one for pan-European acceptance. Note that the focus here is not so much on an e-ID card as on the definition of an electronic identity (e-ID) as it pertains to citizens.

Attribute	Definition
Universality of coverage	Every e-ID holder requires some identifier
Uniqueness	Every e-ID holder must have only a single identifier No two persons can have the same identifier
Permanence	The identifier should neither change, nor be changeable
Exclusivity	Using an identifier, will require no further form of identification to be presented
Precision	It should be sufficiently easy to detect differences

Attribute	Definition
	between two similar identifiers in order to avoid errors

Table 3: e-ID Attributes [9]

This table does not actually mention anything that is unique to an electronic representation of identity. This is a critical aspect to keep in mind, as it is fundamental to how e-IDs are used, namely to fulfil the same requirements as using a physical identity. A classic example is the use of e-IDs for electronic signatures. Here the European Directive on Electronic Signatures [4] assures that EU citizens can use an e-ID (though that term is not used but rather the term "signatory" that carries a Secure Signature Creation Device, SSCD), to perform a signing of a document with same legal acceptance as a handwritten signature. For that to be the case, the above definition needs to be as closely aligned with the physical world, in terms of attribute applicability.

An e-ID system is defined by the European Standards body CEN/ISSS as having [2]:

> "the aim to guarantee the identity of a person (or a legal entity, e.g. a company) during the access to e-services and in order to provide the trust to the parties involved in the electronic transaction."

The e-ID card, as we study it in this paper, is generally seen as a tangible representation of the e-ID to support this e-ID system.

It should be noted that efforts have been made to define electronic identities for more commercial or closed user group systems. These forms of e-ID are out of scope for this project, though some of their best practices, such as PKI implementation techniques, relevant technologies and standards are sometimes adopted for national e-ID card schemes (see Chapter 10).

3.5 The National e-ID Card

As this study is about analysing the implementation of e-ID Cards across Europe, it becomes necessary to define the e-ID Card itself. In the above sections we have taken a closer look at the various definitions and forms of identity, as well as electronic representation of identity (e-ID) and the systems that support this e-ID. The concept of electronic identity, however, is much more recent than identity documents. As a result, when references to e-ID Cards are made, there tend to be two schools. One school of thought looks at the e-ID Card as a token representing an electronic identity (e-ID). Another school sees the e-ID Card as more of an extension of a traditional identity card that supports a chip, which may or may not contain an e-ID.

Setting these two schools aside, we will provide the following simplified definition of a national e-ID card, in order to understand the scope of this study:

> A national electronic identity (e-ID) card is a physical representation of a human or corporate identity, which is able to serve one or more of the following three functions: Identification, Authentication and Signing (I-A-S). While these functions may be possible through physical presentation of the card and the use of visual checks, what makes the card electronic, is the ability to perform I-A-S functionality electronically, often simultaneously striving to increase the security and integrity of the function.

Using today's technology, the e-ID card generally is a piece of plastic or polycarbonate containing a contact- or contactless smartcard chip. For purposes of this study, we will assume that the core computational engine on the card will be a smartcard. One should keep in mind, however, that European legislation as it is

defined today [4], speaks of a more generic Secure Signature Creation Devices, rated than explicitly requiring a smartcard to be used.

3.5.1 Secure Signature Creation Devices (SSCD)

The European Directive on electronic signatures [4], which is a key driver for issuing e-IDs in many European countries, defines the requirements for “Secure Signature Creation Devices” (SSCD). In today’s technology, the SSCD tends to be some form of smart card. The form factor for e-IDs tend to be defined by ISO standards for identity cards, but in some jurisdictions, such as Austria, the form factor is not seen as critical, such that mobile phone SIM cards and USB fobs are also seen as legally valid carriers of e-ID.

4. E-ID CARD APPLICATIONS

4.1 Application Users

Depending on the type of application where an e-ID Card comes to use, different users interact with the card. At a high level, the following are the key users of e-ID cards:

User	Role
Identity Provider & Issuer	Generally a government agency (or trusted third party) that verifies and collects the necessary credentials in order to issue an e-ID card. In addition to issuing the card, the identify provider generally also carries some form of accountability/liability/assurance with regards the authenticity/validity of the identity.
Civil Servant	Government personnel / public officials that handle the e-ID card for various purposes
Private Citizens	The primary holder, user of the e-ID card. The e-ID card is generally issued in their name.
Business Representatives	Identities that are not private citizens, but that represent legal entities, such as corporations.
Other identities	Identities not covered in the above categories

Table 4: e-ID Users

4.2 Base Functionality

As mentioned in the Introduction (Chapter 2), and is initially identified by Fiat and Shamir [5], the primary purpose of an e-ID card are to perform variations of three key functions: Identification, Authentication and Signature (I-A-S).

The applications illustrated in this chapter related to applications that perform these functions.

4.3 Government Applications

The 2005 CapGemini benchmarking study, conducted on behalf of the European Commission, of public services online [11], illustrated most public services as fitting into the following twenty categories, of which 60% are focussed on use by citizens, and the rest by businesses.

Citizens	Businesses
Income Tax	Social Contribution for Employees
Job Search	Corporate Tax
Social Security Benefits (unemployment benefits, child allowances, medical costs & student grants)	VAT
Personal Documents (passports, drivers licenses)	Registration of a New Company
Vehicle Registration	Submission of Data to the Statistical Office
Building Permits Application	Customs Declarations
Declaration to Police	Environmental-related Permits
Public Libraries	Public Procurements
Birth & Marriage Certificates	
Enrolment in Higher Education	
Announcement of Moving	

Citizens	Businesses
Health-related Services	

Table 5: Public Services [11]

The study [11] took a closer look at the level of online sophistication for each category, and which ones were more likely to incorporate the use of e-IDs (i.e. requiring stage 3 or above). Some of the key findings from this study were as follows:

- Online sophistication of public services is much higher (72%) for the original EU countries, as opposed to those who joined in 2004 (53%)
- Public services for businesses are generally (77%) more sophisticated than those for citizens (57%)

The CapGemini study also identified a trend when clustering online services, by the type of impact the service would have. The four clusters were identified as:

Service Cluster	Definition
Income-generating	Generates income for government, usually in the form of taxes and social contributions (e.g. income tax, VAT, corporate taxes etc.)
Registration	Services related to submission of data for completion of administrative obligations (e.g. car registrations, submissions to statistics bureau, company registrations
Returns	The provision of services in return for taxes and public contributions (e.g. public procurements, social security benefits, health related services etc.)
Permits & Licenses	Provision of documents provided by government bodies (e.g. enrolment in schools, environment-related permits, building permissions etc.)

Table 6: Online Services Clusters

Overall, the income generating cluster had the highest levels of online sophistication (88%), while all other categories were around 50-60%. This clear gap between levels shows in a way that "services go where the money is."

4.3.1 Deployed e-Government Applications

The following is a listing of e-Government applications that are presently deployed across Europe where e-ID cards can be used. This table is not meant to be an exhaustive listing, but rather provide a representative sampling of the diversity with regards to the types of applications that are today e-ID card enabled.

Application	Description	Location
Age Verification	Age verification for cigarette vending machines	Italy
Checking Personal (Registered) Data	Check that data in National Registry is accurate and ability to request changes	Finland, Estonia, Belgium
Child Alimony	File application	Austria
Child Pornography	Registration of case	Austria
City of Vantaa Online Services	Online services, such as Social assistance, day-care and rental apartment applications with Vantaa municipal authorities	Finland
Criminal offence registration	Reporting offences (civil and penal) to police	Italy

Application	Description	Location
Disability Insurance	Application of insured widowers upon death of spouse	Austria
e-grandparents	Electronic meeting place where children can communicate with “e-grandparents”	Finland
Electronic Birth Registration	Maternity hospitals register newborns online on day of birth	Finland
Employment Office's vocational adult education	Apply online for vocational education	Finland
e-Tickets	Purchase tickets for public transport	Estonia
Internet Voting	Voting in elections online	Estonia
Municipal tax	Filing of municipal tax forms	Austria
Notification of move	Notify Post Office and Population Information System of change in address	Finland
Online service for general housing allowance	Housing allowance applicant can check whether housing allowance application has been processed, the amount of allowance and from when the allowance has been granted	Finland
Online service for parental allowances	Parents who have applied for maternal, special maternal, paternal or parental allowances may use service for tracking their own allowance data	Finland
Online Tax filing	Authenticate and digitally sign online tax submissions	Estonia, Belgium
Post Office's NetPosti service	Receive electronic bills and letters, change own online service contact information, send an ePostcard	Finland
Request administrative documents	For example request issuance of a birth certificate	Belgium
Residence Change	Notification of change in address	Italy
Retirement pension calculation	Calculate and estimate of retirement pension and predated retirement pension based on employment history	Finland
Retirement, including early retirements	Registration with municipality of status change	Austria
Secure email	Send authenticated and encrypted emails – email address is assigned for life and associated with e-ID card (stored in certificate)	Estonia
Social Insurance Institution of Finland's online service	Sickness allowance or a special care allowance customer can check whether their application has been processed, the amount of allowance and from when the allowance has been granted	Finland
Telephone Bill	Check telephone bill online	Estonia

Table 7: Deployed Application Landscape [20], [21], [22]

Today most governments promote the number of e-ID cards (Chapter 5) they have issued, or the number of applications that are e-ID card “enabled” (see table above). However, there is practically no statistics, and certainly no overview study, that provided a measurement of success based on usage. It is unclear, for example whether popular or high-use functions such as tax submission, are seeing an increase in submissions with e-ID cards, not to speak of an analysis regarding the reasoning (such as convenience or other added benefits unavailable offline).

The Mondis Study on Identity Management in eGovernment [21] is one of the more comprehensive pan-European overviews. However, it only mentions quantitative usage of e-ID cards in passing. One figure which is worth mentioning, however, is that in Estonia, which has a very high e-ID card penetration rate, 65% of persons declared their taxes online. However, they did so using their online banking applications rather than their e-ID cards. This is due to the fact that banks issued e-Banking authentication mechanisms before the e-ID card launched, which has lead to the e-ID card not bringing added value to a population already accustomed to online authentication using their banks (including to access government portals).

4.3.2 Non-Governmental and Other Applications

While until today the actual success in terms to user acceptance and uptake of e-IDs has been limited, especially in what is referred to as the A2C (administration to citizen) domain, one should not disregard the secondary usage effects of e-IDs.

In some cases, for example in Estonia, the e-ID has laid the foundation for an advanced (e-)ID card. This card, while not necessarily having considerable daily usage by citizens for electronic signing purposes, as primarily designed, it has become a trusted citizen ID card for more conventional purposes, such as name and age verification – not to speak of acting as an accepted machine-readable document replacing the need for a passport at certain foreign borders.

It seems that at present, the only use of e-ID cards in non-Government sector comes in two flavours:

- Use of e-ID card as an SSCD to digitally and electronically sign documents with legal validity
- Collaboration with financial institutions to share authentication infrastructure (e.g. PKI). This seems popular in some Nordic countries.

Probably the only notable exception is Austria, while not having a single e-ID card, allows a nationally valid e-ID card to be issued on banking/ATM cards (Chapter 5).

The focus of this study is on Europe, were we can conclude that there really are no good examples of non-Government applications for e-ID cards, beyond secondary use as a physical identifier. As will be illustrated in the next chapter with a review of the Malaysian e-ID card, MyKad, there are examples of the e-ID card serving a more multi-purpose function, including non-Government applications. In fact it was shown there to be of importance to get private-sector participation to increase the adoption rates. Sadly, this approach does not seem to be taken in Europe, which might explain the limited success of e-ID cards used for electronic transactions.

4.4 Possible Future/other Applications

As mentioned above, the focus of e-ID cards today is almost exclusively of their use in operating e-Government applications. Their ability to securely authenticate citizens in the private sector could be significant, though until now there has been no active definition of such scenarios. One exception is banking, which due to the banks driving e-Banking applications in the early 1990's put their own strong authentication mechanisms in place before e-ID initiatives were launched. In general though, their systems have been of a proprietary mechanism. In the future, though, authentication using a national e-ID card for banking could be possible.

In addition to incorporating existing stand-alone e-ID cards, such as heath cards, it is the secondary use of e-ID cards that shows the potentially unlimited examples of e-ID application use.

A few examples of innovative future applications being adopted, include:

- Access to Public Wireless LANS / Metronets [23]
- Use e-ID for e-Voting (trials already performed in Estonia)
- Encryption – while the use of smartcards for encryption is an easy extension, we have not seen this use of e-ID cards for a number of reasons:
  - Requires an additional (encryption) certificate – this is an additional (certificate) management task required
  - No mandating legislation seems to be in place
  - The demand does not seem to exist – conventional alternatives are already present.
  - While privacy is being dealt with, mainly from a data retention perspective, the encryption of communications does not seem to crop up in existing e-ID Card literature.
- Access for Gambling and conducing other activities that require age-verification

It should also be mentioned that the EU Directive on electronic signatures [4] defines the validity of digital signature with pseudonyms, however e-ID cards today do not seem to support this type of functions.

4.4.1 Identity Mixer

Today's "traditional" certificates and signatures used for e-ID cards generally require card holders to hand over all attributes contained within a certificate. For example, X.509v3 certificates in Belgium [16] divulge name and the certificate serial number. As will be illustrated with the Austrian interoperability demo in the following chapter, this can be a practical piece of information to uniquely identify a citizen. Specifically, looking at a scenario where a citizen wishes to provide strongly authenticated attributes, such as eligible age to conduct a business transaction, but does not need to divulge any personally identifying data, such as those found in the X.509v3 certificates, present technology reaches a limitation. Today, such a scenario can not be implemented using available e-ID cards, despite European privacy legislation encouraging some form of "data minimisation", since the e-ID application is unable to be discretionary (i.e. minimising) in which content from within the certificate to divulge.

IBM Research has developed the Identity Mixer [24] [25], also known as Idemix, which is an anonymous credential system. The Idemix is based on anonymous credentials instead of X.509v3 certificates for certifying attributes. A credential is a list of attributes signed with a specific signature scheme. The signature scheme allows a holder of a credential to reveal a subset of the attribute information of the credential within a transaction. For example, the birth date attribute of a credential can be used to established qualified age categories without actually revealing the value of the birth date, which in a small population sample could reveal the actual identity. As another key property, multiple transactions conducted with the same credential are unlinkable to each other unless the revealed attribute information allows for linking of the transactions. This approach reduces the amount of released data to a minimum, thus making the solution more privacy friendly, especially if one compares to how X.509v3 certificates would be used today. In addition, this approach, as we will see in the following chapter, is completely different with regards to addressing unlinkability by the Austrian scheme.

5. NATIONAL E-ID CARD IMPLEMENTATIONS

In this study, rather than conducting a comprehensive review of all e-ID card schemes in Europe, we have decided to select a few illustrative examples that show the diversity of e-ID card implementations.

5.1 Austrian Bürgerkarte

Austria has a population of around 8 million inhabitants. Since passing of the e-Government act in March 2004, over 10 million e-IDs have been issued. This number may sound deceptive, as the Austrian concept of an e-ID does not necessarily equate to an e-ID Card. In fact every ATM card issued since March 2005 [21] in Austria has a built-in Secure Signature Creation Device (SSCD), as defined by the European Directive on electronic signatures [4], and is capable of being activated as a citizen card.

The Austrian e-ID, unlike many other initiatives around Europe, is not so much focussed on being a single card. Of all implementations studied for this project, the Austrians seem to strive towards having the most technology/vendor agnostic implementation. The e-ID scheme in Austria is supported by multiple physical tokens: *Bürgerkarte* (translated as Citizens Card), which is not only issued as a national e-ID card called *e-Card* but also bank cards that are issued by local banks, A1's telecom infrastructure, leveraging the smart-card functionality embedded into A1-issued SIM cards, and finally tokens are also issued as a USB dongle [2], [26]. Actually, the government, while having very stringent regulations on who can issue an e-ID identifier, provides significant freedom with regards to who can issue the card itself.

Since the activation service of certificates started in November 2005, about 3,200 *e-Card* certificates have been activated. The volume of A1 and the A-Trust (private sector certificate authority) certificates activated is not public knowledge. By the end of 2006, e-Card wanted to reach a target of 50,000 activated certificates. If one includes the 8 million target cards to be issued (one per citizen), the number of bank cards with e-ID functionality, and other forms of e-ID to be issued, the total number of e-IDs expected to be in circulation by the end of 2007 is expected to reach 15 million [27].

The primary motivation of the *Bürgerkarte* has been to increase the adoption of e-Government services by providing a framework to enable electronic signing and identification. It should be kept in mind that the Austrian interpretation of the European Directive on electronic signatures [4] does not assume a unique identity associated with an electronic signature. As a result, the supporting of electronic signatures and identification are treated as two separate functions. This strict separation is especially helpful when dealing with interoperability towards supporting other countries, as "foreign" identities can be just as easily accepted within Austria to conduct electronic signing functions.

5.1.1 The Austrian Citizen Card Concept

5.1.1.1 Requirements

The Austrian Citizen Card concept was defined as a framework to fulfil two key requirements for the Austrian e-ID [26]:

- A mechanism to make electronic signatures in Austria legally accepted and compliant to the European Directive on Electronic Signatures [4]

- In order to fulfil the first requirement, where a unique identity is not required, the Austrian Citizen Concept was defined to also support a unique identification procedure, while still adhering to data protection legislation

From the initial design of the Citizen Card Concept, ensuring a lack of linkability for data protection/privacy reasons was seen as critical. While there is no legal definition of linkability, [28] references the ISO 15408 (Evaluation criteria for IT Security) technical definition, providing some insight into this concept:

"[Unlinkability] ensures that a user may make multiple uses of resources or services without others being able to link these uses together. [...] Unlinkability requires that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system."

Performing a level of unlinkability is provided to a certain extent by the Austrian Citizen Card Concept, through the use of source and sector specific PINs, which are described below.

The definition of identity in an Austrian card requires a closer review, as this is specific to the Austrian context, as well as being a key enabler for interoperability of foreign-issued e-ID cards. The Austrian e-Government Act of March 2004 defined two types of identity: Unique Identity and Recurring Identity.

Identity Type	Definition
Unique Identity	Designation of a specific person (or data subject) using features that can enable the person can be unmistakably distinguished from all other possible persons.
Recurring Identity	Designation of a specific person (or data subject), which enables the person to be uniquely identified if presenting themselves again in the future. There is no guarantee, or use of techniques, to ensure this person is unique amongst all possible persons.

Table 8: Austrian Identity Types [29]

What the above definitions of identity mean in practical terms is that e-IDs, regardless of whether being a Unique or Recurring form of identity, both can be considered valid for generating legally compliant digital signatures, and thus being a representative identity for an Austrian e-ID.

5.1.1.2 National Registers

All entities represented by a *Bürgerkarte* are stored in one of the following national registers:

National Register	Function
Central Residents Register (CRR)	Central register for all Austrian citizens (Identifier/PIN publicly available)
Commercial Register (CR)	Register of all commercial entities in Austria
Register of Associations (RA)	Register of all non-commercial associations in Austria
Supplemental Registers (supR)	Contains citizens not enrolled in CRR, such as expats, foreigners, “others”

Table 9: National Registers in Austria [29], [30]

5.1.1.3 The Source PIN (sPIN)

Each entity in the above registers is given a unique identifier, which we will call a Personally Identifiable Number (PIN). This PIN, however, is not used as an

identifier by identity processors, despite it being public knowledge. Rather, a Source PIN (sPIN) is generated, using the PIN as an input variable. The sPIN can only be generated by a central government source PIN Registration Authority, and under the protectorate of the Data Protection Commissioner [29]. The sPIN is generated by converting the PIN to binary, adding a secret seed value, applying a 3DES encryption and BASE-64 encoding the value.

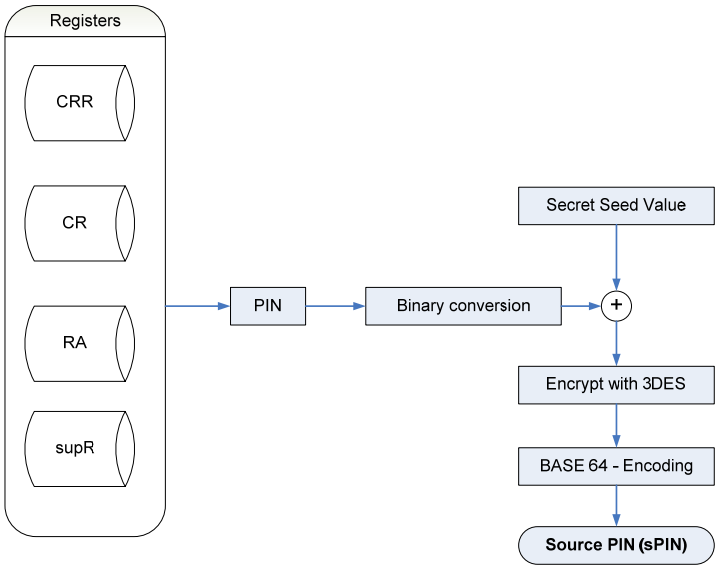

Figure 4: Generating the Source PIN (sPIN) [30]

Only the entity owner, to whom the sPIN is issued, maintains a copy of this identifier (e.g. on their *Bürgerkarte*). For data protection purposes, not even the sPIN Registration Authority maintains a copy of the sPIN. A new sPIN can only be re-calculated again under the supervision on the Austrian Data Protection Commissioner.

In parallel, a SAML-based XML data structure is stored in the *Bürgerkarte*, known as the Identity Link. The Identity Link is actually a certificate signed by the sPIN's Registration Authority. This certificate acts to bind a citizen's public key to the sPIN. Specifically, the certificate contains the citizen's name, date of birth, the sPIN and the public keys [29]. One can thus say that the sPIN acts primarily to identify a citizen, while the Identity Link acts to authenticate the citizen [30].

5.1.1.4 The Sector Specific PIN (ssPIN)

The use of the sPIN as an identifier, however, still poses a risk associated with regards to linkability. Were an individual to use their sPIN as an identifier to each identity processor, it would be possible to link the same sPIN across processors. For this reason, the sPIN is further processed to create a Sector Specific PIN (ssPIN). Each ssPIN that is generated, is used for only a single identity processor, such as a single government administration [30]. The ssPIN is generated by applying a one-way hash function (based on SHA-1) to the sPIN and a sector specific identifier (e.g. tax authorities or social security department). This technique serves two purposes. First, a government department (or any other identity processor) is unable to determine the sPIN of the entity. Second, since the department uses the ssPIN as the unique identifier solely for their administrative department, they would be unable to perform a cross-search with other departments that would be relying on a different ssPIN [29].

:

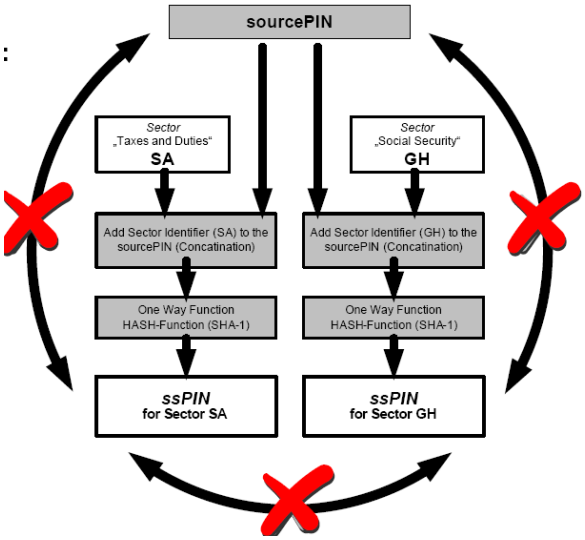

Figure 5: Generating the Sector Specific PIN (ssPIN) [30]

5.1.1.5 Interoperability

With regards to interoperability, the integration of Belgian, Estonian, Finnish and Italian cards into the Austrian Citizen Card has been proven possible [27].

While presently only at a prototype stage, the Austrian government has demonstrated that both existing Finnish and Italian e-ID cards can be used in an interoperable manner in an Austrian context. Specifically what this means is that foreign e-ID cards that contain a Secure Signature Creation Device (SSCD), as defined in Annex III of the European Directive on Electronic Signatures [4], as well as support the PKCS #11 interface (a Public Key Cryptography Standard related to generic interfaces to hardware tokens such as smartcards), are able to be accepted in the same way that an Austrian e-ID SSCD is accepted.

In the case of the Italian e-ID, the tax identifier which is unique to each citizen and accessible though the card is used to identify the citizen. This unique identifier is hashed and encoded to create a Substitute Source PIN, also known as a Subsource PIN. This new PIN is legally accepted in the same manner as the sPIN of a genuine Austrian e-ID.

The Finnish e-ID does not supply access to a unique identifier in the way that the Italian e-ID does. To get around this limitation of uniquely identifying the Finnish cardholder, the serial number on the electronic signature certificate of the Finnish e-ID card is used.

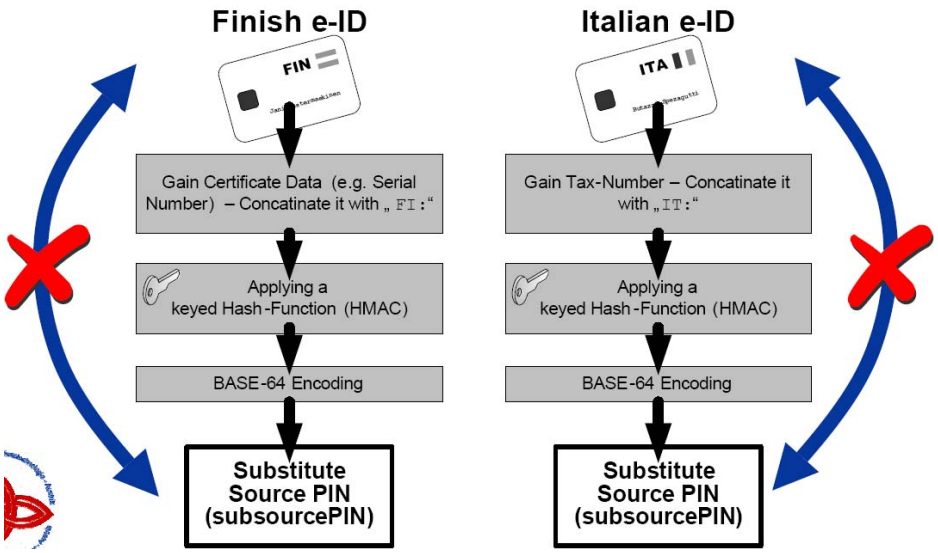

Figure 6: Generation of sPINs from foreign e-IDs [30]

There are primarily two factors which make supporting foreign e-IDs a unique proposition of the Austrian implementation:

- The Austrian definition of identity, specifically Recurring Identity, which by the Austrian e-Government Act of March 2004 makes use of a non-unique identity, such as Italian tax ID or Finnish certificate serial number as legally acceptable to generate source PINs [29]
- The lack of a single identity issuer, means that in the same way that an Austrian ATM card equipped with an SSCD is legally accepted for representing an e-ID, so is one that is issued by foreign countries

To conclude, the Austrian e-ID is in a league of it's own in that there is no true concept of a single card, yet it is set-up in such a way that it performs many of the functions of an e-ID card, particularly related to digital and electronic signing purposes. The Austrians have also promoted their card as being privacy friendly from the outset, the focus has however been of lack of linkability rather than addressing specific privacy legislation (e.g. Data Protection Directive). Last, but not least, the Austrians, albeit only an initial attempt, have been the only ones so far in Europe to demonstrate some form of interoperability with regards to foreign e-ID cards.

5.2 Belgian Personal Identity Card (BELPIC)

Belgium has a population of approximately 10.5 million inhabitants. As of May 1, 2006, 2,712,825 e-ID cards were delivered. As each chip is designed to hold two certificates, the number of activated certificates is around double the number of issued cards at 4,137,314. By the end of 2007, the Belgian authorities plan to have issued 5 million cards – i.e. to roughly half the population. [27]

The Belgian e-ID, also known as the Belgian Personal Identity Card (BELPIC), is issued to all citizens of Belgium. A foreigner's card also exists, but as of now does not have the functionality of an e-ID card. Work is underway to make changes to government systems to support non-Belgian nationals in the future [21]. For children below the age of 6 a "Kids card" is issued without any certificates. For children below the age of 18 a Kids card only with an authentication certificate is issued. From the age of 12, the e-IDs are distributed together with a card reader so that children, a form of early adopters to information technology, can use the e-IDs

to perform simple transactions, such as authenticating clients to websites and for access control purposes, such as public libraries. Once children reach the adult age of 18, a complete e-ID card is issued containing both the authentication and non-repudiation (signature) certificates. [16]

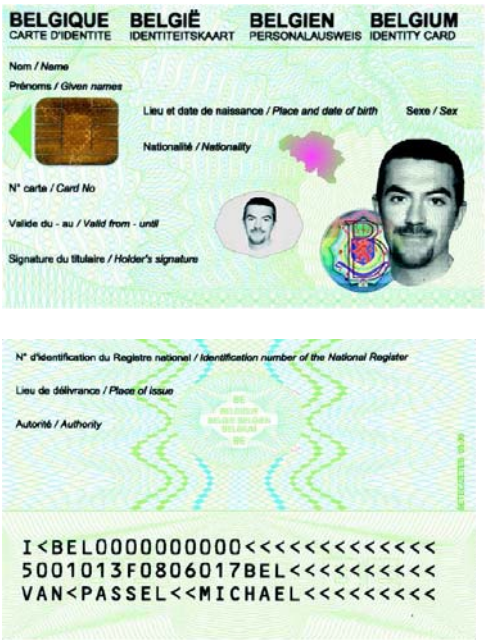

Figure 7: Belgian e-ID Front and Back [31]

The Belgian e-ID card conforms to ISO specifications regarding card sizes (ID-1). The card is manufactured using polycarbonate, which explains the use of a black & white image. There are other physical security features, such as changeable laser image (CLI), Optical Variable Ink (OVI) and other forms of laser engraving which are hard and/or expensive to tamper with or forge. In addition, the card's backside bottom has a machine-readable text zone that is compliant to ICAO specifications. As a result the e-ID card can also be used in certain countries that accept MRTD ID cards for border control purposes. [16]

The contents of the chip were designed prior to completion of ePassport specifications. As a result the chip does not contain any ICAO MRTD functionality. The BELPIC contains two key pairs for each adult citizen. The key pairs are activated during the initialisation process of the card.

As discussed in Chapter 8, an e-ID PKI can serve multiple functions. In the case of the BELPIC, there are three primary purposes for which key pairs are generated:

- Authenticating the Citizen – this is represented through an X.509v3 authentication certificate
- Digitally Signing – Advanced electronic signatures, complying to the European Directive, are represented through a second X.509v3 qualified signature certificate
- Card Authentication – A third key pair is generated to ensure the authenticity of the card. In this case no certificate is generated, rather the public key is known to the National Registry (RRN)

The mentioned certificates above comprise part of the Identity File, which is about 160 bytes in total size and stored in the chip's EEPROM. The chip has a unique identifier. In addition, certain citizen specific identifiers are stored on the chip, such as names, date and location of birth, gender, nationality and card specific information, such as the card identifier number, validity dates and a SHA-1 hash of the citizen's photograph. This data is subsequently signed using a digital signature

issued by the RRN. In addition to the Identity File, a few other components are stored in the card:

- The citizen's Address File (approx. 120 bytes). In order to save on the administrative effort of issuing a new card each time someone changes address, the address information is only stored in electronic format on the card's chip
- A JPEG image of the citizen (approx. 3 Kb)
- Digital signatures of the Identity File and the citizen's Address File

The smartcard contained within the BELPIC runs on a JavaCard operating platform, which enables a high level of security to be incorporated, as well as running multiple applications on the same chip (see Chapter 7 for details on JavaCard). Mainly from a card management perspective, this enables only the National Registry (i.e. appointed government authority) to make any authorised changes to card contents.

The following table illustrates a breakdown of hardware components on the BELPIC chip:

Component	Specification
Card Type	Infineon issued CryptoFlex SLE66CX322P (32K) JavaCard
CPU	16-bit microcontroller
Crypto co-processor	1100-bit crypto engine, based on RSA 112-bit crypto-accelerator, based on DES
ROM (for OS)	136kB, including Java Virtual Machine
EEPROM (for applications and data)	32 KB
RAM	5 KB

Table 10: BELPIC Chip components [16]

Though somewhat different in their approach, the Belgian card carries similarities with the Finnish and Estonian e-ID card in that all three national solutions rely on the use of X.509v3 certificates [32]. The use of the X.509 standard defines the structure of a digital certificate. Together with the issuing of certificates is also the ability (and necessity) to operate Certificate Revocation Lists (CRLs). The Belgian CRL's are public records published on the internet. Naturally, the entire system can be compromised in the event that a Certificate Authority (CA) is compromised. For this reason, Authority Revocation Lists (ARLs) are also published, though as of 2006 [31] this list has never been used.

It should also be noted that the use of the electronic signing features that come with the e-ID card are not mandatory. Hence, while it is mandatory to have a card, citizens can opt-in/out depending on whether they wish to use this e-ID functionality of the card. This has an additional impact on whether a compromised card is published on the CRL or not (non-activation of the card means it will never be published on the CRL). In the event that a card is reported lost or stolen, it is temporarily put in a suspend status for up to seven days. After this period the card is either reported found, in which case it regains an active status, or it is considered permanently revoked, thus requiring a new card to be issued.

It should noted that the usual challenges faced with digital signatures and their validity also exists in the Belgian context. In order to assure long-term validity of a digital signature generated using the e-ID card, despite it being revoked or expired in the future, a Belgian digital signature is considered valid "forever." The conditions for a permanently valid digital signature are as follows:

- Data is digitally signed

- Digital signature is part of the data
- The signers certificate is stored (maintained)
- Validity of the signer's certificate (at time of signing) exists
- The signature has a valid verification time stamp

If the above criteria are met, then the digital signature is still considered valid and hence non-repudiation and authenticity can be assured. [16]

Unlike the Austrian e-ID, which from the onset has attempted to be privacy-friendly through use of unlinkability schemes, the Belgian e-ID card has not addressed privacy. No privacy enhancing technologies (PETs) have been implemented, through there is discussion of including them in future enhancements of the card [31].

Also unlike the Austrian model described above, interoperability is still an issue not completely addressed by the BELPIC. Present focus is on interoperability of e-IDs across different administrative units within Belgium (federal, regional, community and municipality). There has not been any work on interoperability activities with regards to foreign e-ID cards [21].

5.3 United Kingdom

The United Kingdom is one of few countries without a national ID card, though they have existed twice in past. The motivation for issuing an e-ID card is also very different from the above two examples. Rather than focus on representing an e-ID in order to electronically sign or authenticate, the focus revolves around a number of topics which shifts, depending on the political climate from reducing crime, fraud (identity), fighting terrorism, and entitlement. This politicisation of the UK Identity card has lead to significant public debate. The UK Identity Card scheme though is more than just a card, it is actually the role of the National Identity Register (NIR) which is more critical, and in some cases deemed controversial.

The following is a high-level summary [3] of the order of events that have lead to the existing UK Identity Card scheme:

1. 2002 UK government undertakes a public consultation regarding "Entitlement Cards" – see *Entitlement Cards and Identity Fraud: A Consultation Paper [33]*
2. 29 Nov 2004 – Government issues *Identity Cards Bill*, which after being debated in both houses, is suspended, pending 2005 elections.
3. March 2005: London School of Economics (LSE) issues *Interim Report*
4. June 2005: LSE issues *Main Report*
5. Following the elections, a slightly revised form of the bill was presented to House of Commons on 25 May 2005
6. November 9 2005: Home Office releases 60% of cost model based on KPMG review. Also, the minister responsible for the bill makes clarifications regarding the government's cost estimates as only including those affecting the Home Office operationally (i.e. set-up costs and those affecting other government departments were excluded).
7. January and March 2006: LSE publishes additional reports
8. Bill becomes law on 30 March 2006

Without going into the details of the debate, the above sequence of events illustrates the more complex implementation sequence that has taken the UK to lead to the set-up of an ID Card– all of these without the use of the card for any form of electronic or digital signing purposes. The focus is clearly on authentication, and that too for persons in front of a verification terminal, as opposed to online in a possibly remote location.

UK Scheme in Brief:

- Available to all residents in UK above age of 16
- Includes multiple documents: biometrics visas & documents for foreigners, enhanced passports, ID cards for British citizens
- Income will be generated from charging for certain services (income generator)
- From 2009 Identity and Passport Service (IPS) will issue ID cards for British citizens

Core component of the UK scheme is the National Identity Register (NIR). This is covered in more detail in Chapter 6. The key service of the UK e-ID card is to authenticate a cardholder. This can be done through various schemes, depending on how strong an authentication is required:

Authentication Service	**Description**
Visual check	Only a manual check of the content printed on the identity card (no electronic communication)
Card chip authentication	Verification of authenticity of chip (using card reader)
PIN-check	Require cardholder to enter a (secret) PIN to authenticate cardholder
Online/Telephone verification	Verification using online / telephone mechanisms
Biometric check	Require cardholder to verify their fingerprint biometric for comparison to the enrolled biometric. It is not clear whether this verification is done using a mach-on-card (MOC) verification or whether a check with the NIR is performed
Information Provision	Provisioning of personal details to third parties, for example to cascade a change in address to other government departments

Table 11: UK e-ID Card Authentication Services [19]

The services listed above are really only serving Identification and Authentication purposes. The S part of the I-A-S model is clearly missing from the UK scheme. This can possibly be explained because the UK (along with Ireland) does not have an existing national identity card, which would serve some of this basic functionality already. From the considerable debate revolving around the UK ID Card scheme, the fact that it is difficult for public authorities to know who their citizens are, illustrates that in the UK there is a drive to first “solve” this problem. The passing of the UK Identity Cards Act [10] in 2006 was the first step. Interestingly enough, despite considerable debate and activities around the use of e-ID cards to act as an SSCD, this discussion has not been conducted in the Strategic Action Plan for the National Identity Scheme, which is the officially mandated road-map for the UK e-ID card.

There are however two observations that are unique to the UK scheme, which should be noted:

- The role of PKI is emphasised as a form to ensure card and back-end security. This infrastructure, however, is not seen as an enabler to digitally sign electronic documents as other e-ID card schemes across Europe
- There is mention of the cards being EMV compatible, i.e. that the UK ID Cards can be read from a conventional payment card reader. This, while technically possible poses some interesting questions regarding the use of the EMV technology for an unintended purpose.

As this scheme is still under development, it is important to keep a close eye on further developments.

5.4 Malaysian MyKad

In 2006 it was estimated [34] that Malaysia had a population size of 26.64 million inhabitants. A government status update in 2006 claimed [35] that by the end of 2005 a complete migration from paper based ID to the September 2001 launched electronic ID had taken place.

Figure 8: Malaysian MyKad e-ID Card (front) [36]

Unlike other national e-ID cards, such as those European ones reviewed earlier in this section, the Malaysian e-ID card, often referred to as the *MyKad*, has taken a somewhat different approach. It is also one of the earliest forms of e-ID launched worldwide, and that too at a significantly larger scale than in some European countries. Specifically, the MyKad is a truly multi-purpose card, containing on the 64K chip not only the standard personal identification, but also driving licence details, passport information, health information and an electronic purse cash balance [37]. More recently, the card has been expanded to offer digital certificates for signing purposes, as well as a frequent traveller card. Specifically the electronic purse illustrates that role that non-government institutions have played in the delivery of services. In other countries across Europe private institutions play a role in delivering certain infrastructure components, however, the use of the e-ID cards are still primarily to perform I-A-S functions for e-Government applications.

Besides the waiving of an application fee, the MyKad has generally been well accepted by the population. This can be attributed to the fact that even since before Malaysia's independence in 1965, Malaysians from the age of 12 have had to carry a national identity card [37]. There is thus a cultural acceptance to carrying a national identity card, which while also the case in some European countries, has proven to be a barrier towards acceptance in the United Kingdom.

The primary driver for MyKad has been the "Vision 2020" scheme setup by the government to lead Malaysia into a developed country status by the year 2020. In order to accelerate achieving these objectives, seven Flagship applications were identified [38], one of which was the MyKad, also referred to as the Multipurpose Card (MPC).

Unlike many European e-ID cards which evolved from a drive to deliver a token to fulfil requirements associated with the European Directive on electronic signatures, the key objectives of the MPC were to

> "develop a single and common platform for a Multipurpose Card (MPC) that will enable the government and private application providers to implement smart card solutions without duplications of effort and investment." [39]

In other words, seeking synergies across government departments and streamlining services for citizens was more of an objective than mere compliance to a digital signature acts, though a PKI deployment was designed as one of the initial applications. Simultaneously, the role of MyKad functioning as a payment

card meant that the card delivered value to both private sector banks and citizens for usage outside their transactions with government.

Launching a MyKad with EMV (standard from payment card industry) compliant banking applications served the following purposes:

- Encouraged use of the card for more purposes
- Banks, including foreign owned Citibank, played a financial role in delivery of the solution, leading to the MyKad to be a showcase Public-Private-Partnership (PPP) deployment
- Encouraged cashless, including electronic wallet, payment transactions
- Shift from magnetic strip ATM cards to use of more secure chip cards [38]

In his 2004 paper [37] Mathews Thomas went into considerable depth analysing the legal aspects of protecting privacy in a Malaysian context, especially related to operation of the MyKad. Thomas concluded that while considerable effort was made to secure the card, little was done to protect the privacy of the card holder's data. Most notably, interpretations of the Malaysian constitution would imply privacy of card holders should be better protected, however, there was an urgent need to clarify and enforce matters through passing additional legislation.

6. NATIONAL REGISTRIES & BACK-END DATABASES

The focus of this project is the e-ID card. However, the role that national registries and back-end databases play is very closely coupled to the e-ID card in terms of set-up, management functionality provided and how the security and privacy aspects are addressed. This chapter will briefly review a few examples of national registries and back-end systems to illustrate their set-up, functionality and relevance to e-ID cards.

A national registry is often seen as a repository of national identities. The base components that a national registry or other database consists of are:

Technology	Description
Databases	Generally in the form of Relational Database Management Systems (RDBMS), National Registry databases may contain biometrics or other unique identifiers
Networks	Provide the communications/connectivity to the databases
Security	Mechanisms to ensure all security aspects of the database system (confidentiality, integrity & availability) are maintained. Examples: access control mechanisms, audit logs, …

Table 12: Database Key Components

The different architectural set-up of such systems is out of scope, but in the following section we will illustrate, by way of example, a few systems that illustrate their diversity in terms of set-up and functionality.

6.1 National Databases

Population registries and in general databases of a national – or even international significance, can either be designed in a centralised or decentralised manner. Benefits and challenges lie in both models. For example a centralised database offers more control in terms of securing the data in a single repository. However it is more likely to be a target, as it simultaneously operates as a single point of failure. A decentralised system can be considered more privacy friendly, however, this is not always the case, and really depends on how the system is setup – in other words, a decentralised system with poor access control mechanisms is just as likely to be privacy unfriendly as a centralised one is implied to be.

The following countries are examples where agreement has been reached to operate a centralised national databases [2]:

- UK
- The Netherlands
- Sweden (storage planned at the police)
- Italy

While in Italy and Germany it has been explicitly defined that data related to biometrics identity be stored in a decentralised database (with the municipalities), France is still in the process of defining their e-ID system, as a result the form of database deployed will depend on the system

- INES (proposed by ministry of interior) – centralised database for all citizens
- Strategic e-government plan – decentralised storage of biometric data

6.1.1 The UK National Identity Register (NIR)

The British National Identity register (NIR) has been defined in the Strategic Action Plan for the National Identity Scheme [19]. The NIR is still in the process of being

defined and developed. However, early indications of the purpose and set-up have been published [19]. Some of the key elements, known so far, about the NIR are as follows:

- Biometrics, such as fingerprints, will be recorded and linked to a single, confirmed biographical record
- A Biographical record is seen as an individual's name, address, etc and will also contain a link to administrative records, such as details related to the issued e-ID card associated with the individual, incl. relevant PKI certificate details
- The Identity Cards Act [10] defines which information can be recorded and accessed in the NIR
- Integration of existing biometric database systems, such as for asylum seekers
- Integration of biographical information from the Department of Work & Pensions (DWP) Customer Information System (CIS), which contains records for all holders of British National Insurance Number

As with the UK Identity Card scheme as a whole, there is still some public opposition to the NIR set-up, use and financial viability. However, it should be noted that at present the dialogue is, as of writing, still in progress. Hence no final decisions have been made (at least not publicly) regarding the final set-up of NIR and how it will address the privacy (including data protection) and financial viability concerns of the public.

6.2 Pan-European Central Databases

As mentioned above, while some e-ID card schemes are relying on a de-centralised database system, most rely on some form of centralised national identity database. There in fact already exist pan-European identity databases. Two examples include:

- EURODAC
- Visa Information System (VIS)

It is interesting to take a look at these database systems, how they have been set-up, and what measures have been put in place to operate and protect them. In a number of areas, national e-ID card database systems face similar issues, such as legal compliance, use of biometrics for identification and verification purposes and placing protection measures to ensure the database system is not misused.

While both EURODAC and VIS contain centralised identity databases, including biometrics, it is also interesting to note that neither systems rely on an identity document, per say. EURODAC is simply used to check whether an applicant presenting themselves (no document) has presented themselves before. In the case of VIS, a Visa may be issued into a passport, usually only represented in the form of a sticker pasted onto a passport page. [2]

6.2.1 EURODAC

The EURODAC system [40] is a good example of a single-purpose application which serves a particular function that often is used to justify an e-ID card system with centralised databases.

EURODAC was setup in 2003, based on the European Council Regulation (EC) No 343/2003 of 18 February 2003, which looked to facilitate to objectives of the Dublin II Regulation, to ensure member states take accountability for asylum seekers. Simply put, a person can only seek asylum in a single member country. If he or she seeks asylum in another country, then EURODAC will identify which country the first application was put in at, so that the first country can take accountability for the applicant. Or in other words, if no match is found, then one can safely assume that

the applicant had not sought refuge in another EURODAC-member country (EU, plus a few other countries such as Norway, Iceland and Switzerland).

The system requires all fingerprints from all fingers be captured of any asylum seeker over the age of 14. The database does not include any personal details about the individual, such as name. It only lets the user of the system know if the applicant has already been registered in the database or not.

The set-up of EURODAC has ensured compliance to European Convention of Human Rights and UN Convention on the Rights of the Child. There has also been no problem associated with violation to any data protection acts. As an example, a data retention period of ten years ensures that after that time the fingerprint records are removed from the central system.

The EURODAC Central System is considered to be the "first common Automated Identification Fingerprint System (AFIS) within the European Union." [40]

6.2.2 European Visa Information System (VIS)

As with EURODAC, the Visa Information System (VIS) [2] is a centralised database driven by multiple EU policies (Dublin accords, Schengen agreement etc.) to ensure the free movement of persons, provide a common asylum policy and removing of border-checks.

Citizens of 134 countries are required to apply for a visa to enter the European Union. Until the creation of VIS, each country could issue and/or deny an applicant. This lead to the concept of "visa shopping", which meant if, for example, a German embassy were to deny you a visa, you could go to the French embassy and if granted a Visa, could enter into Germany due to a French issued (Schengen) Visa.

In addition to national database systems (referred to as NI-VIS), the VIS also has a centralised database, run by the Commission (referred to as CS-VIS). This database contains all applicant data, including biometrics of applicants. In many ways, this system is similar to a national registry used for issuing national e-ID cards, but for visa applicants.

As with EURODAC, data retention is clearly defined at 5 years, after which the records are deleted from the system. By 5 years this means records – 5 years from the expiry of the last valid visa issued or when a record was created.

In terms of access control, as VIS serves multiple purposes, including ensuring national security – above and beyond prevention of "visa shopping" and ensuring visas are issued using a centralised system. As a result, various intelligence and security agencies have access to VIS. With this regard, while data of a very sensitive nature is stored, the access provided is also to a much larger pool of users across all member states.

7. KEY COMPONENTS OF E-ID CARDS

This chapter will introduce the key components that go into the manufacturing of an e-ID card: card, chip as well as some other components used to represented the identity on the card. Focus will be on the key components representing the e-ID, rather than the other features of a more traditional identity card, such as details that tend to be printed, laminated or laser-engraved into the card.

The following example below illustrates some of the key components on an e-ID card:

Figure 9: Some Key Components of an e-ID Card [41]

7.1 Card Lifecycle

A card's lifespan depends on a number of variables

- Material used
- Communications type
- Chip & security mechanism used

Taking a closer look at these 3 variables:

Variable	Impact
Material used	Plastics/PVC – 3-5 years [42] Polycarbonate (PC) Others, such as paper
Communications type	Contact – 10 years using PC, though max 5 yrs for Plastics/PVC [42] Contactless – 5 - 10 years [42] Dual-interface – minimum 5 years [42] Hybrid – 5 – 10 years, depending on whom you ask. More than 4 years hard to prove. [42]
Chip & security mechanism used	Chips with more memory, storage or custom crypto co-processors define the lifecycle. • Ability to use longer key lengths means content signed and/or encrypted can last longer • Depending on the form of encryption used, the lifecycle is also impacted

Table 13: Variables affecting card lifecycle

7.2 Card Materials

In general e-ID cards either consist of Polycarbonate or Polyvinly chrolide (PVC). There are other materials as well, but these two are the most common. A card material is critical to ensure not only extensive wear and tear, but above and beyond the physical security features built-in, is the ability to securely embed a contact- or contactless smartcard which contains the e-ID.

Cards can consist of different materials [43] [42]:

Material	Advantages	Disadvantages
PVC – Polyvinly chrolide	Low material price Optimised for use as ID card ISO standards have been defined for this material Recyclable	Highly inflammable due to chlorine content Surface wear & tear due to scratching, wearing away of printing & delamination means a lifecycle is limited to 3-5 years. Limited thermal stability
PC – Polycarbonate	High Temperature stability High mechanical strength Recyclable	High cost of materials Low scratch resistance High heat consumption when laminating, difficult handling Brittleness can affect automatic handling of finished cards

Table 14: Common materials for e-ID cards

The material and manufacturing process are critical in ensuring that the chip remains well integrated into the card. Failure to do so can lead to malfunctioning of the card. A protection against a lack of availability is critical to a successful implementation.

7.3 Smartcards

Though not explicitly mentioned by name, the smartcard chip is a prime example of a Secure Signature Creation Device (SSCD), as defined in Annex III of the European Directive 1999/93/EC on electronic signatures [4].

A smartcard is in many ways nothing more than a small conventional computer. The key components being a central processing unit (CPU), various forms of memory, generally ROM, EEEPROM and RAM, in addition to custom hardware components, such as cryptographic co-processors.

Moore's law is just as applicable to smartcards as it is to more conventional semiconductor products (PCs and servers), leading to estimates that EEPROM capacity is able to double every 18 months [44]. That said, the implementation of smartcards tends to be driven by volumes and extremely low costs. As a result, despite newer technologies causing more powerful processors to be manufactured, the pressure on cost has caused a greater popularity (in terms of volumes sold over time) with less powerful chips.

In the sections below, we will focus on conventional smartcard hardware capabilities as they are being implemented in e-ID cards across Europe (as well as for that matter with many ePassport implementations). One should note, however, that recently a number of vendors have issued a new breed of smartcards, which are capable of increasing memory 1000+ fold and increasing communications

interfaces 100 fold. This new breed of smartcards is known as High Density Smart Card (HDSC). The use of such high-density smartcards is still being studied [44], but one can imagine that with more memory available, new applications and/or techniques could be applied to e-IDs. Examples could include other forms of biometrics (such as voice or DNA), incorporating an on-card audit trail, supporting applications for persons with disabilities (e.g. video clips), as well as storing additional personal data, such as higher-resolution images. At present, the cost of HDSC cards are at par with conventional flash memory. Given the high volume at which e-ID cards are issued, and the pressure to keep costs low, the use of these cards still remains only a possibility for the future. However, if these cards are to be adopted by mobile phone vendors for next generation SIM cards (USIMs, in 3G/UMTS networks), we might see a significant drop in prices, leading to a future adoption of these cards. For the moment though, such ideas are not being circulated widely among the e-ID research community and until standardisation bodies adopt HDSC more specifically, we might not, as is the case with LaserCard's Optical storage, see a large-scale commercial adoption of this technology for e-ID cards [44]. For this reason, the focus for now will be on conventional smartcards only.

The following diagram illustrates a high-level overview of components in a smartcard chip:

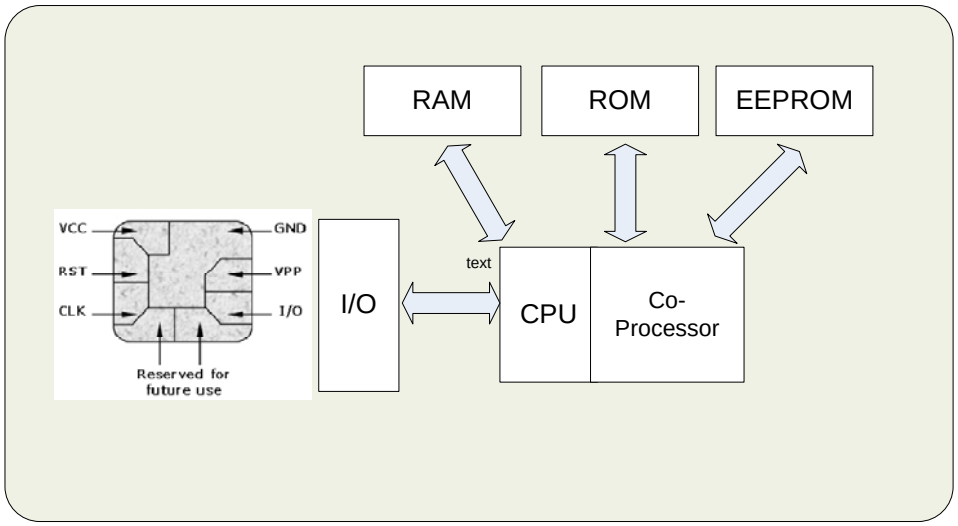

Figure 10: Smartcard components (without antenna) [45] [46]

7.3.1 Central Processing Unit (CPU)

As with a personal computer, the "brains" of the smartcard is the CPU. Generally speaking, the CPU is based on an 8- or 16-bit architecture. More advanced chips, such as those based on a 32-bit architecture are also available, though are generally not applicable for e-ID implementations due to their higher costs.

Especially for secure e-ID applications that perform cryptographic functions, the use of a built-in crypto co-processor is also important. Depending on the supplier, the co-processor can handle different key-lengths and standard algorithms such as DES, 3DES and AES.

7.3.2 Memory

Depending on the vendor and chip packaging process, the distribution of ROM, EEPROM and RAM vary, but could be, for example, distributed along the ratios of 1:4:16 [47].

ROM – Read Only Memory

Generally used to store the operating system and specific applications which are not subject to change after that card has been issued.

EEPROM – Electronically Erasable Programmable Memory
Contents of the EEPROM can be changed at any time, and is therefore more flexible. The constraint put on it is generally the size (of available memory)
In general, smartcards today can support 64-128 EEPROM [44].

RAM – Random Access Memory
Challenge: limits the run-time capabilities of the chip, and is often seen as a constraint on the performance of applications running on the chip [47].

FERAM (requires less power, which is important for contactless cards).

7.3.3 Multi Application Card Operating Systems (MACOS)

The selection of a smart card's operating system (COS) is a critical design decision. Based on which COS is selected, the entire card and application management are impacted. As with personal computers, here too there have been attempts to control the OS of a smart card. This effort has generally been driven by specific smart card suppliers that would gain from a "lock-in" to a specific COS. Some vendors, such as Microsoft, launched a COS, Windows for Smart Cards, but ultimately withdrew it from the market due to limited acceptance. This too illustrates another example of where even when selecting an OS from a major IT vendor can cause investments in a "failed" technology to take place.

It is safe to say that today there are two key COS platforms that are relevant to e-ID cards: MULTOS and JavaCard. Rather than going into detail comparing the two, we will focus on their key similarities, which illustrate their popularity as opposed to more closed/proprietary card operating systems.

Both MULTOS and JavaCard are known as being a Multi-Application COS (MACOS). This means that they are able to support multiple applications on a single card. Originally, smartcards were only able to handle single applications or in more primitive cases simply support a file system. The MACOS, due to their architecture design, not only can handle multiple applications running from a single chip, but also ensure that from a security perspective, the applications are clearly segregated.

In addition to the security aspects, one of the key features of JavaCard and MULTOS is the ability to manage the applications on the card after the cards have been issued. This post-issuance management of card applications is critical to ensure not only new applications can be loaded to the cards, but also that critical security updates can be made, if necessary.

Other key functionality of a COS are as follows [48]:

- Ability for the card to communicate with the rest of the word using standard protocols (usually via a card reader)
- File and data management within the various parts of the chip (e.g. memory)
- Managing the access control to various parts of the card to enable CRUD (Create, Read, Update & Delete) functionality
- Managing all security aspects associated with the card and algorithms associated with the crypto co-processor
- Ensuring chip operates as designed and in a stable manner (reliability, integrity)

- Managing the card throughout its life cycle from chip fabrication, personalisation both pre- and post issuance, active use and end-of-lifecycle. The management of the entire lifecycle is critical, given the security aspects that the chip manages (such as those related to private keys).

The above review of Multi-Application Card Operating System similarities generally ends at around this stage. When going into the details between JavaCard and MULTOS, a clearer divergence regarding implementation approach emerges. It is outside the scope of this project to review these. A good comparison, however, is illustrated in a report published by the Open Smart Card Infrastructure for Europe (OSCIE) v2 report [49].

At present both MULTOS and JavaCard are considered serious card operating systems for e-ID cards. For example the Belgian e-ID card is based on JavaCard, while Hong Kong is considered to be one of the first ever e-ID implementations and is based on MULTOS. Also, depending on the supplier, different security certifications have also been awarded to JavaCard and MULTOS, such as ITSEC level 6 (for MULTOS) and Common Criteria level 4 and FIPS 140-2 level 3 (for JavaCard).

7.3.4 Card Communication: Contact vs. Contactless

The UK Identity and Passport Service (IPS) commissioned a survey [42] from leading vendors, which included comparing the various forms of cards. While results from respondents varied regarding the time required to develop and accredit multi-application software for various cards, based on communication type (17% claimed 6 or 12 months for contactless cards, 25% claimed 6 months for dual-interface cards), it was clear that two thirds of respondents felt the development time was independent of interface type.

According to the survey [42], one vendor stated that issuing of contact cards is considered more efficient, as one can more easily personalise cards in parallel. Processing a contactless card creates additional electro-magnetic interference, making high-volume manufacturing slower.

The time it takes to create, and ultimately issue (or re-issue) a card can have an overall impact of the quality of service delivered for e-ID cards.

What is clear, however, is that development of applications clearly depends on the type of communication. Changing this attribute once a card has been deployed, can cause significant confusion and delays.

7.3.4.1 Contact card communication

As shown in the above figure of smartcard components, a smartcard generally has 6 or 8 contacts (also referred to as pins). The exact dimensions and locations of contacts are defined by the ISO 7816-2 standard.

Examples for the pin usage include the standard chip features, such as providing for power-supply, ground, clock, reset, input/output as well as some more application-specific or vendor defined usage.

Using a contact, as opposed to contactless chip, requires that the pins physically touch (hence their name, contact card) sensors inside a card reader. This procedure can be seen as an additional security enhancement when operating the card, as it requires the card holder to “do something” – namely insert the card into the reader. While this can be seen as an added activity, hence inconvenience to users, it can be seen as a means to prevent unauthorised reading of the card due

to the proximity of the holder's card to an attacker "skimming" the card with a contactless reader.

Another weakness of contact cards is their exposure, especially their readers, to natural environments. In some harsh environments, particles such as water or dust can cause the readers to more easily malfunction.

7.3.4.2 Contactless card communication

While the implementation of ePassports is outside of the scope of this project, it is worth taking note at the International Civil Aviation Organisation (ICAO) specifications for Machine-readable Travel Documents (MTRDs) with respect to contactless technologies are defined. Implementations of contactless cards for ePassports is leading to de facto standards to support various e-ID card implementations.

ICAO has defined MRTDs to support an operating frequency of 13.56 MHz, which lies within the RF Frequency range. This is the same range used by conventional RFID tags, and comes under the ISM band, which is generally available for use across the world. This frequency is also suitable for efficient power transfer. The read/write range is defined to support ranges of up to 10 cm, which is more than close-coupling systems (0-1 cm) and certainly significantly less than long-range systems capable to of being detected from more than 1 meters distance. [2]

From all forms of smartcard, the contactless card is considered by industry experts [42] to have the highest form of physical durability. Nonetheless, how durable a contactless card is, depends on the method that the antenna is inlaid into the card, as well as the strength of the antenna connection to the chip. Due to the manufacturing technique, contactless cards are thus vulnerable to failure, if put under physical strain, such as flexing [42].

Generally, durability of contactless cards is considered higher than contact cards, as the physical contact with the reader is eliminated.

7.3.4.3 Hybrid Cards

A hybrid card contains 2 chips: A contactless chip and a contact chip.

According to [42], the risk of failure doubles with two chips, as the potential for needing two connections between the two chips is required.

Hybrid cards have been deployed in the US as the Common Access Card (CAC), which is the de facto standard for US Government issued employee ID cards [42].

7.3.4.4 Dual-Interface Smartcards

Unlike the hybrid card that has two chips on a single card, a dual-interface smartcard is a single chip that can operate both as a contact- and contactless mode.

There are a number of advantages that a dual-interface card brings [42], especially in a multi-application context:

- Use of contactless mode for lower-value applications (more convenience), and contact for higher-value applications (added verification)
- Use contact interface where transaction time is more critical
- Contact interface can force user to interact for a longer time (as card is inserted into reader). This can be useful in certain applications which require users to present something (e.g. a PIN or biometric)

- As only a single chip exists, the personalisation of cards is more efficient

Though no examples could be found of national e-ID cards in Europe using dual-interface technology, it is already widely used as an identity card. For example in Japan over 100 million cards have been issued as driving licenses using dual interface technology, and in Hong Kong the Octopus public transport card has been issued to 8-10 million inhabitants [42].

7.4 Other Card Options

7.4.1 Magnetic Strips

The use of magnetic strips to store data on cards has been in use for many years, especially in the banking sector. In the case of magnetic strips being standardised for use as identity cards, there only seems to be examples of this being done for some US drivers licenses that use the standard specified by the American Association of Motor Vehicle Administrators (AAMVA). ISO specifications pertaining to magnetic strips only define their physical properties. [50]

Magnetic strips are prevalent due to their low production and personalisation costs. Most cards carry three tracks for storing data elements associated with the card, such as name, account number, expiration date and check-sums. [50]

While in the banking world there has been a transition of using the magnetic strip to the smart card, in terms of functionality the two technologies differ significantly – most notably in terms of the smart card being able to handle numerous security functions, as described above.

Despite their limitations, according to [2] magnetic stripe card technology will co-exist for “at least another decade”, due to the investment already made into existing infrastructure.

7.4.2 2-D Barcodes

While the focus on e-ID cards has been on the usage of smartcards, there is in addition to the magnetic strip another technology which has recently been both standardised and deployed to support secure data storage and identification capabilities using an inexpensive technology: the 2-D Barcode.

The International Labour Organisation (ILO) has worked to define standards for ISO standardisation that can support representing a biometric template and other personal details on a printable 2D barcode. These standards are to be applied to the ILO seafarers’ identity document. It should be made clear that this document is to be issued by nation states as a form of verifying the identity of seafarers. It is not supposed to be used as a travel document (passport replacement), for which the ILO is seeking to adopt ICAO specifications. [51]

The 2-D barcode technology for the ILO card is defined to store up to 686 bytes of data and 64 data symbols to support error correction functionality. This is sufficient space to store the biometric templates for two fingers and other details regarding the user and issuer which are also printed on the card, such as the issuing authority name, unique identifier numbers, expiration dates and the holder’s personal details such as name, date of birth, nationality etc. [51]

As the Liberian card implementation has shown [52], additional features can be implemented when using the 2-D barcode, such as data compression enabling facial images to also be stored on the barcode, as well as the ability to perform encryption on the content printed.

7.4.3 Optical Storage

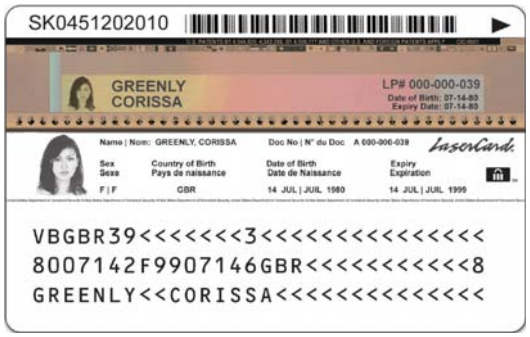

Figure 11: Optical Storage Card [53]

Optical Storage is a technology that despite being defined by ISO/IEC standards 11693 and 11694 has so far only seen adoption in the Italian Carta d'Identità Elettronica (CIE). [54]

In the case of the CIE, it is not seen as a replacement to the smartcard, but rather as a complement. Currently models with a chip can store up to 1.1 MB of data (without a chip, up to 2.8 MB). This is a significantly higher volume of data than on a smartcard (excluding new HDSC cards). [53]

Probably more than for the ability to store high volumes of data, the optical storage on the CIE cards are used as a physical attribute on the card, as images can be engraved on the card, which are difficult to forge.

While ISO standards for the technology exist, Italy seems to be the only country that has deployed the technology. It also seems that the technology is dominated by a single vendor, LaserCard. Lastly, the reading of the data requires specific card-readers, which are expensive and not widely deployed, hence reducing their adoption outside Italy even further.

8. CARD SECURITY MECHANISMS

This chapter will discuss three key mechanisms used to enhance the security of e-ID cards:

- Biometrics
- PKI Integration
- Physical Protection Mechanisms

It should be kept in mind that the need to secure the care is multi-dimensional. The card in itself is used to perform transactions that need to be conducted in a secure manner (e.g. using PKI to sign documents). On the other hand, conducing secure electronic transactions can only be performed, if the implementation tools (such as the e-ID card) are not put at risk. Hence, we will see here technologies that are put in place on e-ID cards hat address both of these dimensions.

8.1 Biometrics

8.1.1 Overview

The ancient Egyptians were not only one of the first to issue identity documents in the form of passports, they also were one of the first to use fingerprint biometrics. Not exactly for identity documents, but rather by potters to mark their wares [55].

Taking a look at the use of biometrics in a travel/border control context, one has to primarily focus on the considerable activity that is taking place at ICAO. Specifically, ICAO is working to standardise the integration of biometrics as identifiers into ePassports. As mentioned in the introduction, we will focus on the e-ID card for non-travel purposes. In most cases, the use of the e-ID for travel purposes is simply fulfilled by adopting ICAO MRTD standards into the national e-ID specifications.

We will for purposes of this study focus, from an e-ID Card perspective, on the application of biometrics for the purposes of non-repudiation and identifying an individual to digitally sign a document. In order to do this in a European context requires compliance to local legislation, which is subsequently compliant with the EU Directive on Electronic signatures [4].

There is another application domain, which is to use a biometric for identifying a cardholder when presenting themselves. A scenario where this could be applied is when providing an entitlement (e.g. social services). While this use of biometrics is often discussed, beyond use of biometrics at the border, there are very limited activities to use biometric verification elsewhere. In fact while conducting this study, the reference to biometrics in an e-ID context kept appearing. It therefore merited further investigation and coverage in as an e-ID card security feature. What has become apparent, however, is that with the exception of the UK, whose system is still very much “in progress”, there does not seem to be any active use of biometrics in European e-ID cards, neither to protect the integrity of the card, nor to perform transactions, such as digital signing more securely. There is one exception, which is the Italian e-ID card, that is already deployed and is capturing both fingerprints and facial images for non-travel purposes. However, although the biometric identities are captured and stored within the optical storage component of the card, there does not seem to be any documented evidence available describing any actual use of this data.

Furthermore, it does not seem, as of present, that any existing legislation exists in Europe that clearly defines the use of biometrics for digital signature purposes. As a result, the focus of biometrics in an e-ID context is generally replicating the efforts

of the ePassport domain. In fact the British use of biometrics is being driven by compliance to ICAO standards for ePassports which are to be issued by the same agency [19].

There are many forms of biometrics, and the focus here will be on the two most commonly ones used for e-IDs and other identity documents, such as ePassports: Fingerprints and Facial Images.

Capturing and analysing biometrics can either be performed in an overt or covert form [55]. Examples of covert biometrics are video surveillance mechanisms to conduct facial recognition, or the use of biometrics in forensic activities. For the purposes of e-ID Cards, however, we will focus purely on overt biometrics.

Biometrics can also be viewed as being used to perform either positive or negative identification. Positive identification is one where reliance on the given biometric is not mandatory. Instead, one can fall back on relying on an alternative form of identification. An example of this would be if a smartcard-based biometric verification does not work, a manual verification of a facial image printed on the card suffices to perform the identification. A negative identification using biometrics requires a mandatory biometric operation to be conducted; an example of this would be the mandatory use of a biometric to be presented in order to digitally sign a document. [55]

8.1.2 Biometric System Model

The topic of using biometrics is an entire project subject in itself. We will focus here on using the generic Biometric System Model [55] to illustrate five subsystems which describe the various functions performed for biometric identification purposes. The five sub-systems which we shall take a closer look at are Data Collection, Transmission, Signal Processing, Data Storage and Decision.

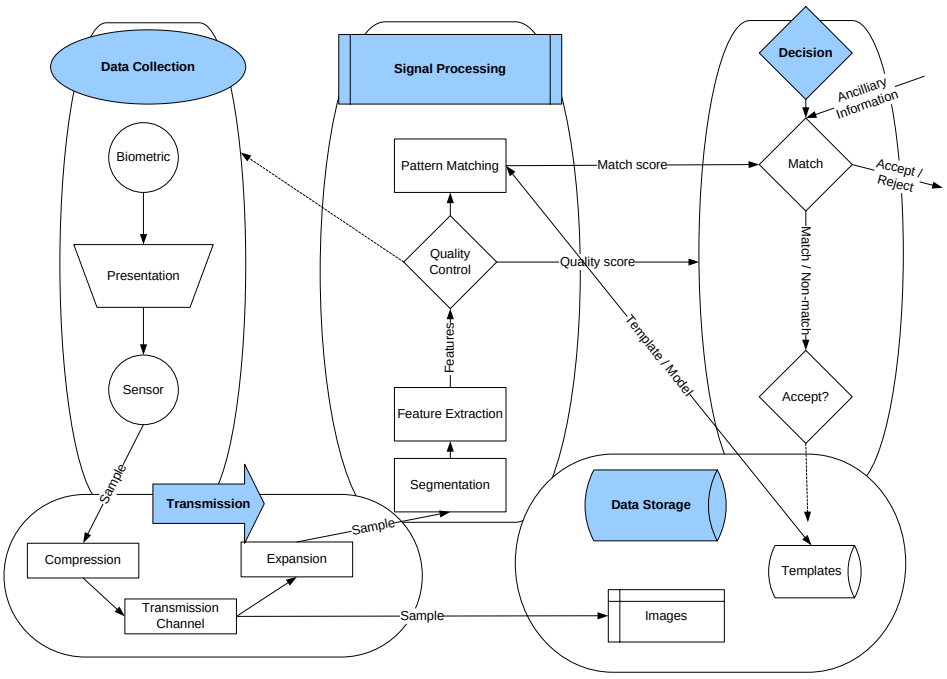

Figure 12: Biometric System Model [55]

Data Collection:
The data collection of a biometric generally falls into two stages of use: enrolment and subsequent presentation stages. During enrolment stage, the biometric is captured through the use of a sensor (e.g. a fingerprint reader or camera) for the first time or whenever the biometric credential needs to go through the enrolment

process. The method of collection should be the same regardless of whether for enrolment or future purposes to collect the biometric data.

Transmission:
The transmission stage is a form of data transfer from the sensor to another component where the biometric is further processed – this could be either storage on the ID card, such as the smartcard (see data storage phase), another part of the card reader or biometric sensor (for signal processing), or a back-end system, where any of the remaining stages may take place (storage, signal processing or decision making). The biometrics might at the transmission stage be compressed using various techniques. For example, a common technique for fingerprint image compression is to use Wavelet Scalar Quantisation (WSQ), while for facial images, many standards, such as those defined by ICAO specify JPEG or JPEG-2000 formats. [2]

Signal Processing:
A key component of signal processing is the feature extraction procedure. This can be seen as a form of non-reversible compression. For example, once fingerprints are processed to be represented in a template form, while less data is needed for storage (as opposed to a raw image), and also the templates can be compared for verification and identification purposes, the ability to obtain the original image is not possible. Another important aspect of the signal processing stage is the quality control procedure. A poorly enrolled biometric means that subsequent verification against the original becomes difficult. The poor quality may be obtained due to poor equipment, enrolment conditions (e.g. dusty sensors), or poorly placed biometrics – the inability to adequately enrol is often referred to as the Failure-to-Enrol-Rate (FTER). For e-ID purposes, the signal processing stage is critical in ensuring – or at least being in a position to measure – the quality level, often by comparing the ability to compare (or lack thereof) the presented sample with the one in the data storage.

Data Storage:
The storage of biometric data may consist of different forms (depending on how it has been processed) as well as being placed in different locations. The placement location where biometric data is stored depends a lot on the design of the system, which is ultimately driven by the functional requirements that are defined for a given solution. For example, for the purposes of conducting a 1:1 verification in a privacy-friendly manner, a biometric template can be stored in a secure manner together with a verification engine on the smartcard itself, ensuring that the enrolled template never leaves the smartcard. This concept is sometimes referred to as match-on-card (MOC) functionality – i.e. combining the decision stage (also defined in ISO/IEC 24781) in the same physical location as that of the data storage. In cases where a primary motivation lies more towards identification as opposed to verification, such as with EURODAC and VIS systems (see chapter 6), a more centralised data storage system tends to be more prevalent. The larger a centralised biometric database, the greater the impact one can expect on speed and accuracy (more errors) of the system. Considerable research is still being conducted with regards to processing of large-scale biometrics database systems. It should also be kept in mind that due to the pre-processing of biometric templates in previous stages, the ability to re-construct the original biometric data in the data storage stage tends to be difficult. Depending on the design of the system, this can have an impact when an e-ID card needs to be re-issued.

Decision Stage:
At the decision stage, the presented biometric is compared (matched) to the stored template. Based on pre-defined policies regarding acceptance thresholds associated with multiple variables, such as quality levels, a decision is made as to whether to “accept” or “reject” the candidate biometric being presented. The techniques applied depend significantly on the algorithms used for matching purposes, as well as handling the variables defined in the accept/reject policy. One

must also consider the longevity of the algorithm being applied. This is particularly important, as e-ID cards (as well as ePassports) are being defined to carry a lifecycle period of up to ten years. [56]

8.1.3 Measuring Biometric Accuracy

There are many criteria that can be used for measuring the accuracy of a biometric technology. Some of the more common ones are listed in the following table.

Measurement	Description
False Match Rate (FMR)	The probability that an identity is incorrectly matched.
False Non-Match Rate (FNMR)	The probability that a valid identity is incorrectly not matched.
Failure to Enrol Rate (FTER)	The rate at which a biometric identity is unable to enrol sufficiently to be used later for identification/verification purposes.
Equal Error Rate (EER)	Used to generally describe accuracy levels of biometric systems. EER is error rate when FMR = FNMR

Table 15: Biometric Accuracy Measurement Criteria [56] [57]

It should be noted that the FMR and FNMR are inversely related and so while one may wish to reduce both variables, this is impossible. As a result, one needs to find a balance between the level of convenience one wishes to provide, versus the risk one is willing to take. These decisions depend significantly on the type of application being deployed, impacting the overall accuracy of the system, which can be seen as another form of trust associated with the technology to do the job as designed. The “balanced” rate, if agreed upon, is often referred to as the Equal Error Rate (EER).

8.1.4 Fingerprint Biometrics

The use of fingerprinting to identify individuals has also been a legal form of identification for over a century. Yet its use in European e-ID cards is only now being seen as a viable or required attribute. It can to some extent be seen as viable because of the ability to do something with the fingerprint biometric (e.g. perform an identification or verification). Both these types of services require either a sophisticated chip (i.e. smartcard) embedded into the card or the availability of an IT network infrastructure (to conduct a back-end system check: either identification or verification), though alternatives to a smartcard have been illustrated by the use of 2-D barcodes.

There are many technologies which can be used to capture fingerprints. Leading technologies, as those selected feasible for the BioFinger project [56] include:

- Pressure
- Capacitive
- Optical
- Thermal

There are other sensor technologies, but as was done in [56], for purposes of this study we will focus only on those technologies which are well accepted today, and for which vendors are supplying products with substantial support and assurance levels.

It should be noted that beyond the dilemma of accuracy levels, the number of open issues with regards to use of biometrics from a remote, unattended, location are

greater than would be desired. While various innovations exist, to ensure liveness (i.e. fake or dead fingers are not used), the main prevention for the use of fingerprint biometrics in e-ID cards is their lack of industry standards.

8.1.5 Facial Biometrics

The earliest forms of identity documents naturally did not have a photograph. In fact it took abound a hundred years after the modern form of photography had existed, until photographs started appearing in identity documents [14]. In 1914, Charles Inglis (an alias for a German spy carrying a fake US passport) had a passport consisting of a single sheet, valid for two years and bearing no photograph. Five weeks after the execution of the apparent Inglis, on December 21 1914, the US Secretary of State, William Jennings Bryan required photographs to be issued with passports. [14]

One of the key reasons why it took over a century for photographs to be used together with identity documents has initially to do with the cost to develop photographs (both equipment and material) but also due to the complexity with which to take the photographs. The first form of portrait photography in 1839 required the subject to remain motionless for half an hour facing sunlight! [14] This challenge with cost (time and money) associated with using a secure form of biometrics is once again being discovered with DNA, which is being ruled out for secure identification due to the complexity, not its accuracy.

The first use of colour photographs for passports appeared in the US passport in February 1958 [14]. The first use of digital images for passports appeared in the Japanese passport in November 1992 [14]. While digitisation of facial images can be seen as an improvement, Lloyd expresses his doubts, when stating that pixilation “reduces definition and accuracy” [14]. In fact, Lloyd illustrates an example of a Czechoslovakian passport photograph taken in a 1931 studio as an example of image quality that would put “present-day photographs to shame” [14].

It should be noted that even the use of facial biometrics today is primarily focussed on image presentation rather than conducting a sophisticated matching or verification procedure. Thus the use of the facial biometric is considerably different for an application use than a fingerprint.

As an example, today’s use of facial biometric in the Belgian e-ID card only store the image electronically, and then digitally signs it for integrity purposes [16]. There does not seem to exist any e-ID system in Europe today that uses (or has near plans) to use facial biometrics for electronic matching via verification or identification techniques, as described. This, despite significant research on facial matching research being conducted in the context of secure identity documents.

8.1.6 Hybrid – Multimode Biometrics

While accuracy levels with the use of single forms of biometrics are limited by the technology available today, studies have proven [58] that combining multiple forms of biometrics, for example facial and fingerprint recognition, increases the overall accuracy of the ability to verify an identity. Use of multimode biometrics may be one of the answers to overcome limitations of single-use biometrics today.

8.1.7 Other forms of Biometrics

In addition to fingerprint and facial images, there is considerable research, as well as many commercial vendors, that illustrate other forms of biometric that can be used to uniquely identify individuals. As these forms of biometric are presently not seeing their way into present e-ID standards, we will only mention them here to illustrate the breadth of the field, as well as the lack of a single dominant biometric standard for e-ID cards moving forward.

- Iris Scan
- Dynamic Signature
- Retina
- DNA
- Speaker identification / voice verification
- Hand geometry

8.2 PKI Integration

The Directive on Electronic Signatures (Article 3.2) states [4] that an advanced electronic signature is defined as:

"an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."

According to Myhr [9], today only PKI-based technology is able to fulfil these requirements. Therefore, for those e-ID cards which wish to support being used to implement (advanced) electronic signatures, the use of PKI is critical.

8.2.1 PKI Interoperability

As mentioned, the use of PKI is fundamental to e-ID deployments. However, as pointed out in [2], there exists no pan-European Root-CA. This leads to a key challenge facing e-IDs today, namely a lack of interoperability.

The use of a pan-European PKI is beyond the scope of this project. It is however a key inhibitor related to enabling interoperability across national e-ID cards. The use of PKI is also a subject in e-ID cards, where the use of the technology is deployed in order to protect and trust the contents from being viewed or tampered. Once again, in parallel, ICAO is studying aspects of PKI, but purely from the perspective of supporting an ePassport.

A general agreement in the research community seems to be that the use of federated identity management (FIM) is the key to addressing interoperability. The use of federation, however is only now been addressed in an e-ID context, primarily following an initial EU-funded project called GUIDE, which attempted to use of federated network identity management to address the interoperability challenges from a technical perspective, specifically in an e-ID card context.

8.2.2 Functions of PKI for e-ID Cards

The use of a PKI to support basic e-ID card functionality is critical. In general, there are five areas where PKI plays an important role:

- Proving integrity/authenticity of card
- Proving integrity/authenticity of data stored on card
- Authentication of the card holder or other contents on the card
- Digitally and electronically signing electronic documents
- Encryption using key material stored on the card

Naturally the above are not the only usage areas of PKI in an e-ID card context. For example, a lot of the critical infrastructure that supports the deployment of e-ID cards (readers, back-end databases) will also leverage PKI to ensure integrity, secure communication links and protect access to critical data. These application domains however are out of scope for this project.

8.3 Physical Protection Mechanisms

The following section will briefly illustrate various forms of physical security mechanisms that have been incorporated into e-ID cards. These protection mechanisms provide benefits associated with preventing forgeries – either clones or tampering with genuine cards. The objective of these technologies is in many cases to at least making it more difficult and expensive to reproduce the technique applied.

Some of the mechanisms can be verified using visual or tactile checks. Others require special equipment to verify authenticity. All technologies, with the exception of DNA gene coding, are already being used today on e-ID cards across Europe. There is a natural trade-off with these protection mechanisms, namely their high costs, which while increasing the barrier for forgers, likewise governments are put under pressure to produce a card that is inexpensive to procure.

Mechanism	Description and Benefits
Laser engraving	Use of laser engraving as opposed to other forms of printing causes permanent changes to the card (generally polycarbonate). Can be used to create tactile dots or engraved dots (leaving surface untouched). Requires expensive equipment to generate engraving. Engraving can take place at same time as chip personalisation.
Holograms	No standards exist for holograms, enabling customised holograms to be produced for optical checks of 3D image visible to naked eye.
Multiple Laser Images (MLI)	Functions similar to a laser image with regards to multiple images being displayed for visual checks. Unlike holograms, however, laser engraving techniques are used to create the images. As a result, they are more deeply integrated into the card, thus making it harder to forge.
UV Colours	Special inks which change the way they look when put under a ultra-violet (UV) light.
Micro-printing	Printing technique used on the card with a font size so small that it nearly impossible to read with the naked eye. As a result, making a photocopy or use of more conventional printing (forging scenario) makes it difficult to reproduce.
Thermal transfer printing	Works similar to a heated needle for printing purposes. Allows high resolution images such as logos and photos to be printed on the card for visual checks.
Thermal sublimination printing	A process of heat-sensitive inks transferred to a permanent dye-substrate with polymer-coated surfaces. Due to the sublimination process, images printed on card are highly scratch-resistant.
Optical Variable Ink (OVI)	Special inks that change colour/appearance when changing the viewing angle. These inks are proprietary and difficult/expensive to procure.
Nano Code	Using nano-sized dye films of different colours

Mechanism	Description and Benefits
	are layered and ground creating a special powder. The pigments of this powder can be analysed using a special technique verifying the authenticity of printing.
Gene Code	Use of hereditary DNA dissolved in solutions and imprinted for authentication purposes. Still under research.

Table 16: Physical Protection Mechanisms [43]

9. RISK ASSESMENT

The focus of this chapter is to take a critical look at the risks associated with the present-day and future e-ID card implementations. It should not be seen as a formal risk assessment of e-ID cards, but rather a risk assessment of the topics covered in this project, which have been scoped out in Chapter 2.

As a guideline, the principles of The British Standard Information Security Management Systems – Part 3: Guidelines for Information Security Risk Management, BS 7799-3:2006 [59], have been used. Using this model of conducting risk assessment, the topics addressed include reviewing relevant assets, sources of requirements, identification of significant threats and vulnerabilities, as well as their valuations, and last but not least, an identification of any relevant controls or countermeasures that could be put in place.

9.1 Sources of Requirements (Legal & Business)

As discussed in the introductory chapters, the drivers for e-ID cards differ from country to country, however there is a general theme within Europe for government to put the necessary frameworks and infrastructure in place to enable electronic signatures to be used, for e-Government services to be more widely adopted. These are all initiatives that can be seen as organisational or business objectives that drive the launching of e-ID cards. In addition to these drivers, which exist both at a European and national level, there are supporting legal and regulatory requirements. These are covered in the following table, with specific detail to the legal landscape in the next chapter.

Drivers	Legislation
National Security	Often the e-ID cards are issued by government departments closely related to protection of national security, such as Ministry of Interior. The assets that come under their domain, such as national database registries that contain e-ID data, are considered critical national infrastructure. Each country has measures, such as dedicated agencies in place to protect this infrastructure.
e-Government	European Electronic Signatures Directive and national legislation enforcing directive European Data Protection Directive and national legislations enforcing directive European Directive on Privacy and Electronic Communications and national legislations enforcing directive
Identity Theft / Data Protection	National ID Card Legislations European Data Protection Directive

Table 17: e-ID Card Drivers

9.2 Assets Requiring Protection

In a formal BS7799 evaluation, the first stage to conduct is a comprehensive review of existing assets. This review is just as relevant to an e-ID card system as any more conventional system. However, the scope of this project is focussed on the e-ID card, and hence many additional relevant assets will not be reviewed within this assessment.

Asset Type	Asset	Description
Identity Information (in chip)	Identity Attributes	Data, stored electronically on the chip that by itself, or in combination, uniquely identifies the identity. Examples: Name, Date of Birth, National Registry number, Address, but also non-text information such as biometric identifiers
	Cryptographic/PKI relevant material	Non-identity attributes that are relevant to ensuring the security (integrity, secrecy) of the contents on the card are handled as intended. Examples include public and private keys, certificates and digital signatures, key generation material.
Software (in chip)	Card Operating System (COS)	Smartcard operating system, such as JavaCard or MULTOS. Includes card-management and certain crypto-applications.
	Cryptographic / Key management applications	Applications associated with managing the keys. These include access to key though PIN entry, generation of keys, use of keys etc.
	Core e-ID card applications	Applications loaded onto smartcard to perform standard e-ID card applications such as identification, verification, digital signing, authentication
	Other applications	Other applications that are added onto the card that are beyond the standard I-A-S types. May be government issued/related, such as for supporting e-Health, MRTD/ICAO specifications or driver licenses. Or may be applications from private sector, such as use by banks for authentication or payment purposes.
Physical Assets (on card)	Plastic / Polycarbonate card	Physical card on which e-ID is represented, embeds chip and antenna (if contactless). May contain physical protection mechanisms, such as holograms.
	Smartcard Chip	Smartcard chip (silicon) that manages and contains e-ID. May also have an antenna for contactless access.
	Other forms of storage	Optical storage, 2-D barcodes, magnetic stripes…
People	Private citizens (cardholder)	The primary holder, user of the e-ID card. The e-ID card is generally issued in their name.
Organisational Assets	Reputation / Image	Reputation / image of issuing agency or other organisations/institutions associated with the image of the e-ID card.
	Trust (in national infrastructure / government)	The trust put in by the citizens who use the card, as well as other institutions using the e-ID card to perform I-A-S applications with the card.

Table 18: Relevant Assets for e-ID cards

Other relevant assets, such as card readers, back-end systems, PKI, other persons involved in the enrolment and production process are critical, but will remain outside the scope of this evaluation. Their significance, however, should not be underestimated.

9.3 Valuation of Assets

When assessing the above assets, it is important to understand their value. When an asset is somehow compromised, then only if their value is deemed high enough, that one can put the necessary controls in place at a level pertinent to their value.

Asset Valuation Scale

Scale Level	Impact
High	Impact is so great that trust in using e-ID card is lost. Impact of damaged caused by a compromised system leads to significant risk exposure.
Medium	Compromising/losing the asset will cause an inconvenience but not disrupt the entire e-ID system. Will require some or significant administrative effort to address any disruption caused.
Low	Compromising/losing the asset will cause minor inconvenience.

Table 19: Asset Valuation Scale

In our scenario, the physical assets can in general be replaced if damaged or otherwise compromised. Hence, the on-card assets are in general of medium value. If, however, vulnerabilities in these assets are found to impact an entire population, then the value of the impact is significantly greater. We will not conduct a formal valuation at this stage, but rather present in the table above the types of valuation levels that need to be considered when conducting a more formal assessment.

Probably the most critical value, more than the identity attributes, are the cryptographic applications and their relevant material. Should these be compromised, on an individual or mass-scale level, then probably not only damage is done to the true identity (person), but also if made public, to a general trust, and hence reputation of the entire system. An example where this caused some issues was in Singapore where authorities did not trust the system sufficiently enough to accept it as a valid replacement for a passport [60]. On the other hand, it was a matter of overall trust, which is a human assessment, since Brunei assumed the card sufficiently trustworthy to accept it.

9.4 Threats, Vulnerabilities & Controls

In this section, we will review the most relevant threats, vulnerabilities and applicable controls pertaining to the e-ID cards, as covered in this report.

9.4.1 Masquerading / False Accepts

An e-ID card may be falsely accepted. Either due to intentional or unintentional reasons.

Unintentional False Accept
Errors in technology, for example those inherent in biometrics, may cause incorrect identities to be falsely accepted.

A common countermeasure is to use an appropriate mix of identification techniques and technologies to increase accuracy. For example, combine two forms of biometrics to increase the precision levels.

Intentional through accessing key material
Various attack mechanisms exist (e.g. side-channel attacks) that can be used to divulge the key material for accessing the content. These tend to be physical attacks to the smartcard. Some common techniques used include:

- Power Analysis Attack [61] [62]
- Fault Analysis [63] [61]
- Timing Analysis [61] [64]
- Differential Power Analysis [61]
- Differential Fault Analysis [61]
- Optical Fault Induction Attack [65]

The above are methods also known as side-channel analysis, which enables, through an observation of communications on the chip to divulge the transactions, eventually leading to identification of relevant key material. These techniques of hardware (chip) attack are continuously being improved, while vendors likewise incorporate more sophisticated control measures to prevent various forms of attack.

This content (such as private keys) that are obtained from such attacks as the above mentioned, can be used to modify or create "clone" cards. The dangers that arise with e-ID that was less of an issue with non-electronic identities, is the ability to perform an e-ID transaction in a remote location where a malicious attack with the ID card is done without the supervision of a public official.

Intentional through skimming
In some cases, authentication is done in the form of a PIN entry. A common method of attack is to “skim” the PIN (i.e. overlook the genuine holder while they enter the PIN) after which someone steals the genuine card. While revocation mechanisms can be put in place to prevent a card reported lost or stolen, should a victim be unable (or unaware) of their card being vulnerable, can lead to such an attack being successful. Use of biometrics is an alternative form of countermeasure – assuming this is harder to skim.

Breaking and failing PKI
e-ID cards as they are designed today are dependent in more ways than one on the use of PKI technology.

PKI risks have been extensively documented [66] [2], to be vulnerable to attack, especially related to inability to protect private keys. Likewise, cryptographic lifetime of keys are also a limitation that can affect optimum use and trust of a system. Examples include electronically signed documents whose certificates have expired or encrypted documents that are due to lost keys unable to be retrieved (can also be seen as a form of denial of service, see next section).

9.4.2 Denial of Service / False Rejects / Lack of Acceptance & Availability

One of the three pillars of information security is availability. Lack of availability (e.g. of the e-ID card or material on it) can lead to a denial of service.

Acceptance of e-ID cards is also dependent on usability. There are multiple features of using an e-ID card which may be unfamiliar to the average user/citizen.

While the use of a magnetic stripe for swiping, as is the use of a PIN, are both considered conventional uses of bank/payment cards, their use in other application areas is less common. Especially when the chip is used to perform a function beyond simple authentication of user via PIN. The idea that the e-ID can be used to sign a document causes considerable confusion, if nothing else because the concept of electronic and digital signatures are not exactly the same as a human signature, let alone the perception of what an electronic/digital signature is to an average citizen.

Another usability challenge is being faced today by deployment of readers. According to [67] early deployments of smartcards in Europe faced challenges with the readers, so much so that in some cases around 50% of users required calling a hotline to get support with installing the necessary readers.

Intentional lack of availability
There is very little that can be done if a user intentionally wishes to deny access to a service. The card holder can easily dispose of a card and claim it was lost. More difficult is intentional tampering with the card to make it unusable. This is of course possible (nail polish on the chip can easily destroy the card from subsequent use), but countermeasures do exist, such as making the card contactless or use of stronger materials such as polycarbonate with more tamper-resistant laser-engraving. In general though, if someone doesn't want their card to be useable, there is very little to prevent them from doing so.

Intentional denial of service can also be initiated by impacting the systems that use the e-ID cards. Protection measures for such scenarios lies outside the scope of this project.

Inability to be Interoperable
Lack of interoperability, means "lack of market acceptance and market proliferation of electronic signatures" [68] referencing [5]

At present, most e-ID card solutions in Europe are being created as stand-alone or island solutions. Some attempts have been made in Austria to accept foreign-issued cards. However, such attempts are at a very early stage. There exists a general risk that adoption of e-ID cards for their intended purposes will be limited unless their acceptance across national borders can work, as is the case today with mobile phones and payment cards, not to speak of passports as a form if identification. As people in Europe are more likely to work or live in countries other than those of their citizenship (examples, Poles working in UK, Englanders retiring in Spain), this will be a more necessary requirement to fulfil.

There is no true "countermeasure" to address the above problem, other than put policies and standards in place that leads to e-ID cards being issued that are interoperable.

9.4.3 Human Error

As in many IT systems, e-ID cards are also prone to what can often be referred to as the weakest link: the human being.

Human error can take place at any stage where he/she is involved. For example, during the enrolment processing, data may be incorrectly entered leading to confusion once the identity card has been issued. This is especially true with seed documents whose validity is less questioned. Likewise, during enrolment, biometrics can be captured poorly leading to a higher level of false rejects.

10. STANDARDS & LEGISLATION

At present, interoperability across various national e-ID card systems is limited. This constraint could be alleviated if Europe decided on a common e-ID infrastructure, or at least common standards. While this is being attempted through various mechanisms, such as the Porvoo Group and the European Citizen Card (ECC) set of standards within European Standardisation body, CEN, the real restrictions lie with the legislative hurdles, most notably Art. 18 (3) of the European Commission Treaty, which will be discussed in more detail in this chapter.

10.1 Interoperability

One of the key drivers to define and adopt standards is to ensure interoperability across various implementations. While to the layman the term *interoperability* might seem quite obvious, taking a closer look at the theory behind the term illustrates some complexity behind the word.

The Future of Identity in the Information Society (FIDIS) Study on ID Documents [2] illustrated a modified Technical, Formal, Informal (TFI) model, influenced by Okusel's Open Systems Framework of Social Interaction [69], to show how supporting interoperability for e-IDs can be viewed from three different layers: Technological, Formal (Legal) and Informal (Socio-cultural).

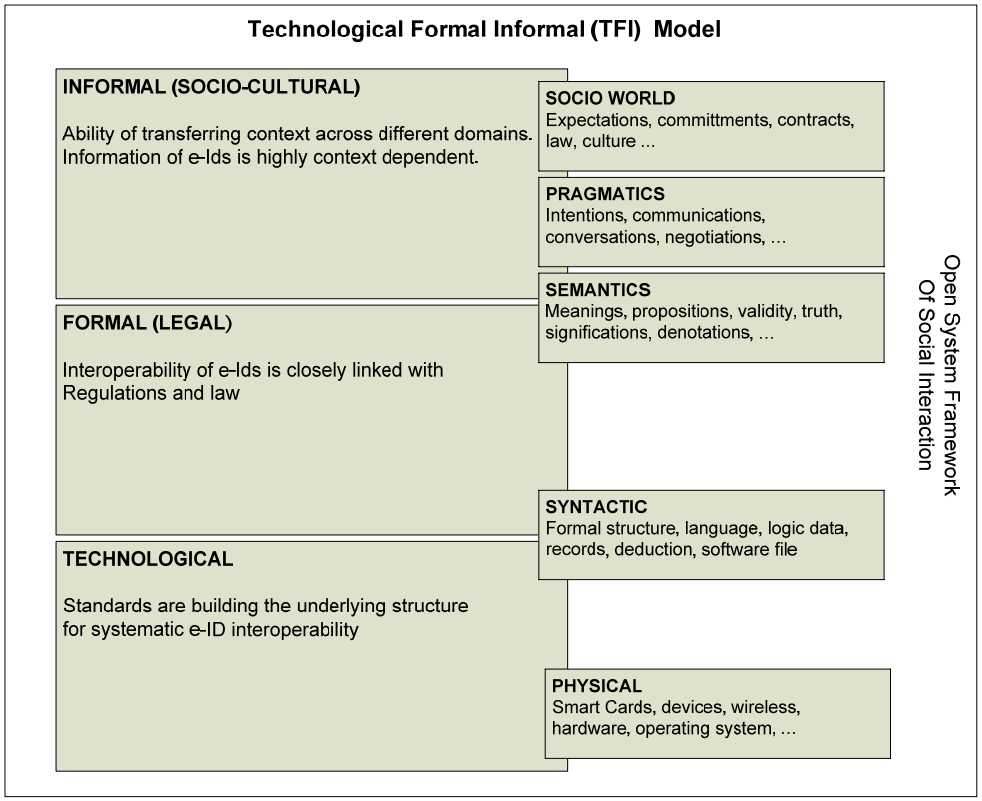

Figure 13: Modified TFI model, influenced by the Open Systems Framework of Social Interaction [2]

For purpose of this study, we will focus on the bottom two layers: Technological and Formal (Legal) drivers.

10.2 Technological Standards

10.2.1 International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IES)

The International Organisation for Standardisation / International Electrotechnical Commission (ISO/IEC) is one of the key institutions responsible for standardisation at an international level.

ISO and IEC have formed a joint technical committee focussed on Information Technology (JTC1). Within the "JTC" there is a subcommittee, SC17, that is focussed on standardisation of personal identification and cards. Many of the relevant standards that are applicable for European e-ID cards fall under the domain of SC17.

ISO Standard	Objective
ISO 7816	With 15 sub-sections, the ISO 7816 standards define many characteristics associated with electronic Identity cards, especially pertaining to aspects related to smartcards. Includes both definitions of physical attributes, as well as specific software related commands for card security and management.
ISO 7811	Defines the recording techniques for identification cards, primarily focused on those with magnetic strips [43].
ISO 7810	Defines 3 standard formats for Identity cards: ID-1, ID-2, and ID-3, each with different sizes. The ID-1 is the most common standard, which is often used for credit cards and all newly issued e-ID cards, as well as next generation drivers' licenses. The current (legacy) German Identity Card is defined by the slightly larger ID-2 specification.
ISO 24781	Consists of two parts. The first part defines a framework for the use of smartcards for applications where biometric matching takes place on the card itself, i.e. "Match-on-Card" (MOC). The second part defines process requirements related to interoperability.
ISO 19794	Biometric Data Interchange Format. Comes in 7 parts and includes among others, fingerprints, facial and iris biometrics.
ISO 14443	Defines the standards for "proximity" identity cards, also referred to as contactless cards. The standard comes in four parts, defining different communication protocols and coding schemes.

Table 20: ISO/IEC Standards

10.2.2 European Committee for Standardisation (CEN)

The CEN is the standardisation body at a European level. The CEN 224 committee is focussed on identification cards. Within CEN 224 there are a number of working groups (WG) that focus on various applications related to identification cards. Since 2003, WG 15 has been established to define standards for the European Citizen Card (ECC).

CEN Standard	Objective
CEN/TS 15480	European Citizen Card Standard split into 3 parts: Part 1: Physical, Electrical and Transport Protocol Part 2: Logical Data Structure and Security Services Part 3: Management of the card and services Part 4: Recommendations for ECC issuance, operation and use

Table 21: CEN ECC Standards

While within the e-ID card community across Europe there is frequent reference to the ECC standards and activities being performed by CEN to come up with a pan-European standard for e-ID cards, there is practically no publicly available documentation describing these standards, let alone any publication of the standards for public review. From what could be discovered through informal conversations only, is that the standards for the ECC are primarily being written by the card industry (vendors), who have a vested commercial interest in having a common card. This makes sense if one observes the success of standards in the payments (EMV) and communications (GSM SIM) sectors.

However, given that the ECC is a standard that would require adoption by national institutions, a lack of their active participation, and in some cases implementation of non-ECC standards (e.g. Belgium, Austria, Estonia, Finland, UK to name a few), illustrates that this standard is from the onset being developed primarily from a vendor's perspective and not from a "users" perspective. In this case the "user" being national governments that would issue the card.

10.2.3 International Civil Aviation Organization (ICAO)

The International Civil Aviation Organization (ICAO) is a United Nations (UN) body which defines numerous standards in the travel industry. For the purpose of this study, the most important ICAO specifications to pay attention to includes the one related to Machine Readable Travel Documents (MRTDs), often known as Document (Doc) 9303.

First published in 1980 as "A Passport with Machine Readable Capability", Doc 9303 is now published in three separate Parts.

ICAO Document 9393	Purpose
Part 1 - Machine Readable Passports	Initial specifications related to the Machine readable Passport (MRP), including the machine readable zone (MRZ), which is optical character recognition (OCR) readable text. A subset of standard is sometimes followed on e-ID cards that have an MRZ (see for example Figure 9). A second volume to Part 1 specifies the enhancements to MRP to include biometric identifiers, thus defining requirements for an "ePassport".
Part 2 - Machine Readable Visas	Defines standard format for machine-readable visas inserted into passports (similar to part 1 in terms of technology).
Part 3 - Size-1 and Size-2 Machine Readable Official Travel Documents	Specifies MRTDs to have dimensions including ISO 7810's ID-1 format. In 2007 a specification including adoption of ISO 14443 standards (i.e. use of contactless smartcards) will be published.

Table 22: Three parts to ICAO Doc 9303 [18]

e-ID card implementations across Europe are adopting various aspects of Doc 9303 to enable e-ID cards be used as an MRTD or as a passport replacement for certain countries (e.g. within Europe and North Africa). However, there is some "scope creep" with regards to use of the biometrics and authentication mechanisms for non-travel purposes. This poses a potential challenge as the requirements in ICAO were designed to serve a specific travel-related function, and poorly addresses use in non-travel scenarios. For example, the method of suspending or revoking an ePassport is very different from how it would be handled at a national level. Also, there are some legal challenges within Europe regarding the use of ICAO specification outside their adoption for ePassports.

10.2.4 Other Technological Standards

The above technological standards are only a glimpse into the most relevant ones today defining e-ID cards as a whole. There are of course far too many other standards that are relevant to e-ID card success. Some of them are already well established and used, such as RSA's Public Key Cryptography Standards (PKCS), most notably PKCS #11 and PKCS #15, which are specific to cryptographic tokens (i.e. smartcards).

Another example of an existing standard, which is finding wide use in e-ID cards, is the X.509v3 standard defining the structure of digital certificates. This standard was defined by the International Telecommunication Union (ITU). As this study has shown, X.509v3 certificates are, for example, used in both Belgian and Estonian e-IDs.

The above examples are only illustrative of other relevant standards. There are far too many to mention for this study, such as those defined by IEEE and Sun.

In addition to more established standards, many have yet to reach a level of maturity, such as ECC. Examples where standards are still in a more "emerging" stage include those related to interoperability and biometrics.

10.3 Formal (Legal) Standards

It should be noted that there is no European-wide legislation mandating or defining a National identity card, let alone an electronic one. The European Constitution, if it had been passed, would have set the path towards a European ID card. The ratification of a European Constitution, however, was stalled in 2004.

As the focus of this project is on European e-ID card schemes, we will emphasise the role that European legislation (i.e. mandated by the European Commission) has had on e-ID cards. We will conclude this chapter by also reviewing legislation at a national level, which at the end of the day defines the finer implementation details.

10.3.1 European Directive on Electronic Signatures – 1999/93/EC

This directive is critical in determining the future of e-ID cards. It is the principle directive behind legitimising (advanced) electronic signatures. The directive actually is primarily focussed on ensuring that electronic signatures carry the same legitimacy as hand-written signatures as opposed to defining the electronic signature's legal status and/or use.

Thomas Myhr's preliminary 2005 study on the regulatory framework supporting a pan-European e-ID [9] took a critical look at the directive, with an attempt to better understand whether the directive was purely focussed on digital signing or also addressing entity authentication. This is a fine, but critical point, which Myhr illustrated is in many cases subject to interpretation. Myhr concluded that while entity authentication can be said to be covered by the directive, it lacks many

critical aspects, and at best can be considered insufficient, mainly due to the fact that the directive does not explicitly distinguish, let alone address the differences between electronic signatures and entity authentication. That said, should it be assumed that entity authentication be covered by the directive, then one has to pose the question as to what mechanism can be used to represent an entity, which would need to be authenticated. This is where Myhr considers the e-ID (or equivalent) as something which is mandated by the directive. Even more so, given the universality of a directive to be supported by all member states, Myhr emphasises the need for the e-ID to be legitimate across all of Europe (i.e. function as a pan-European e-ID). Unfortunately, it remains unclear whether the directive does indeed cover entity and/or data authentication, in which case more legislation might be required. It is for this reason that Myhr goes on to illustrate the requirements necessary to draft a directive specific to defining authentication.

Before moving on to the importance of the Data Protection Directive, it is interesting to note Myhr's observation [9] that it is not only the Data Protection Directive, but also the Electronic Signature Directive itself which addresses privacy of e-IDs. Specifically, Article 8 makes it clear [4] that not only those providers of certificate issuance, but also the Certification Service Provider (CSP) is limited on "how he can collect data concerning the holder/signatory."

The directive [4] also defines in Annex III the key functions of a secure signature-creation device (SSCD), which is the technology that ensures an electronic signature can be generated. As has been mentioned in other parts of this study, in today's technology the SSCD is generally seen as being represented by a smartcard – at least for portable signing purposes. Naturally in a more static, e.g. server-side transaction, a signing device may also come in the form of a Hardware Security Module, often known simply as an HSM.

10.3.2 Data Protection and Privacy

In addition to the above legislation related to signatures, probably the second most referred European legislation of relevance to e-ID cards, is said to be the following two directives:

- European Data Protection Directive 95/46
- European Directive on Privacy and Electronic Communications Directive 2002/58/EC

As e-ID cards deal with individual citizens handling their own identity, the nature of each transaction they perform deals with sharing their identity credentials with third parties, be these governments or private organisations. Regardless of whom they share their credentials with, the very fact that a personally identifiable information (PII) is shared with a third party, requires this third party to comply with data protection and privacy legislation. Specifically, it requires that the information being processed is used only for it's intended purpose.

In addition to the e-ID credential stored on the card, as we saw in Chapter 6, the role of national registries and back-end database systems which are also subject to privacy and data protection legislation. These large, potentially massively complex and centralised systems have also caused considerable popular concern, but as we saw in Chapter 6, there have been promising signs, for example with EURODAC and VIS systems, that European legislation can be enforced to an agreeable manner.

10.3.3 European Commission Treaty Article 18

The EC Treaty Article 18 is probably the most important document pertaining to the inability to have a pan-European e-ID card which would solve many issued related to interoperability.

Specifically, Article 18 states the following:

"1. Every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in this Treaty and by the measures adopted to give it effect.

2. If action by the Community should prove necessary to attain this objective and this Treaty has not provided the necessary powers, the Council may adopt provisions with a view to facilitating the exercise of the rights referred to in paragraph 1. The Council shall act in accordance with the procedure referred to in Article 251.

3. Paragraph 2 shall not apply to provisions on passports, identity cards, residence permits or any other such document or to provisions on social security or social protection." [9]

The comments in paragraph 3 are the most critical. It suggests that identity cards can not be mandated at a pan-European level, even if they could fulfil other basic rights of Europeans, such as free movement (paragraph 1).

Despite Article 18 (3) of the EC Treaty, initiatives such as the Hague Programme in 2004 introduced the idea of defining common standards for identity cards amongst member states [2]. The ECC standard is an example where such attempts have been made, but not with any true political or legislative backing.

Likewise, one should not forget that, despite being turned down, had the European Constitution passed, we would have seen a reversal in policy, and set the stage for mandating a pan-European ID Card.

10.3.3.1 Council Regulation (EC) No 2252/2004 of 13 December 2004

Council Regulation (EC) No 2252/2004 of 13 December 2004 defines the "standards for security features and biometrics in passports and travel documents issued by Member States."

This regulation ensures European states offer interoperability of biometric technologies/implementations for passports and travel documents. As many e-ID cards are being defined to also act as travel documents, this regulation carries significant weight. [2]

It is of particular interest to note the reference in paragraph (3) of this regulation to ICAO's 9303 documentation. This reference has caused some contention as a report of the Parliament on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports concluded that "Document No 9303 should not be referred to in an EU regulation, since it is constantly being amended by a means which lacks transparency and democratic legitimacy" [2]

10.3.4 Other European Legislation

As with technological standards, likewise with European Legislation there is much more legal material that one can review. A few other pertinent legislation, as covered by Myhr [9], is referenced in the following table.

European Legislation	Purpose
Directive 2000/31/EC	… on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive

European Legislation	Purpose
	on electronic commerce')
Directive 2001/97/EC	… on prevention of the use of the financial system for the purpose of money laundering. Myhr points out [9] that this directive is a good example illustrating the need for an identity document that enables fulfilment of an European directive. The Money Laundry directive states: *"... institutions shall require identification of their customers by means of supporting evidence when entering into business relations."* [9] Depending on interpretation, the e-ID may serve as a qualified form of necessary identification.
Council Regulation (EC) No. 1030/2002 (proposed act)	proposal regarding a common format for residence permits for third-country national on the basis that it has proven technically impossible to incorporate biometrics onto a visa or residence permit in the form of a "sticker"
Commission Decision 2003/511/EC	… on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council
Directive 2004/18/EC	…on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts. Explicitly states that "one will need interoperability for advanced electronic signatures" [9] in order to develop the Internal Market.

Table 23: Other relevant European legislation

10.4 National Legislation

Generally national legislation for implementing e-IDs is driven by two primary types of acts: (a) Identity Document Act and (b) Digital Signature Act. In addition, various other forms of legislation play a supporting role that help shape of the card is issued and deployed. Example: Data protection acts.

Legislation Type	Purpose / Function	Examples
e-Government Acts	Provide a legal basis for the Identity Management Systems [29]	e-Government Act March 2004 (Austria)
Identity Cards Act	Provision for national scheme of registration of individuals and for the issue of cards identify registered individuals	UK Identity Cards Act (2006) [10] Identity Documents Law, (Estonia, January 1 2000)
Digital Signatures Act	Local legislation implementing European Directive on Electronic Signatures	Digital Signature Act (Estonia, 2000) [70] Administrative Signature Order (Austria) Digital Signature Act (Malaysia, 1997)

Legislation Type	Purpose / Function	Examples
Data Protection Act		Data Protection Act (UK, 1998)

Table 24: Legislation at National Level

11. CONCLUSION

The original objectives of this study were to gain a better understanding of the implementation landscape of e-ID cards across Europe. In order to accomplish this, various national schemes were studied, as well as the underlying technologies and legislative drivers. Conducting these activities were the primary objectives of the report. For the most part, these objectives were accomplished. The outcome of this survey, however, was somewhat unexpected, as described below.

First of all, while the focus of this paper was on e-ID Cards, during the course of the research, and while engaging in discussions with the e-ID card community, it become apparent that for many purposes a national e-ID was not important, but rather the e-ID in itself sufficed. The challenges faced in general with representing a (human) identity in electronic form, especially across different systems, is a far greater challenge than ensuring a citizen is represented uniquely. For this reason, considerable research today in the e-ID community is focussed on interoperability, sometimes from the perspective of federated identity management. In fact identity management systems, in general, are a “hot topic” within the e-ID domain. The review of identity management systems was not considered in scope for this project, but is certainly one area that could be researched further.

Another key finding that was somewhat unexpected, was regarding the focus on a single identity card, just as with a single e-ID, is not the only way forward. Specifically, the Austrian implementation of e-ID illustrated that it is not necessary to rely on a single card – or for that matter electronic identity. In fact designing a system that is from the onset flexible has shown benefits regarding solving such “issues” as supporting interoperability.

This brings up the topic of interoperability, as another key topic which took more importance than initially planned. Before starting the project, addressing this requirement was not defined (i.e. explicitly within the project objectives). It became apparent during the course of the research that this was a topic also meriting further study. In fact while working on this project, it was discovered that the topic of interoperability is a field of scientific research in itself, and it would be worth investigating further how lessons learned in the past and in other domains could be applied to e-ID card interoperability. At present, while there is discussion of e-ID card interoperability within the technical e-ID community, there are limited (Austria being the notable exception) illustrations of national e-ID card schemes addressing the issue of accepting foreign-issued e-ID cards. It seems like this is a short-coming of the current designs, which tend to be only looking within existing national borders. A reason for this could be the fact that the design of e-ID cards is taking place at a national, rather than pan-European level.

Another observation made during the course of this project is the focus on the e-ID card’s form factor. Today there is already a high usage of ISO compliant cards used for various aspects of identification (and authentication). Examples include existing national identity cards, banking payment cards, drivers’ licenses, health cards etc. While it may seem that an e-ID card’s form factor is not as critical as imagined to accomplish I-A-S functionality, the fact is that the use of mobile phone SIMs, USB dongles and in the future other form factors will be able to perform just as well the same functionality. Once again, Austria, despite their limitations (such as not using X.509v3 certificates as in other European schemes), have illustrated the constraint of reliance on a single card, let alone a single form factor. So far no other European e-ID card scheme seems to be following the path of the Austrians on this matter.

Another observation while conducting research for this report were the numerous inhibitors associated with successful implementations (setting aside the fact that

the definition of a successful e-ID card implementation remains to be defined). While smartcards have been around for a long time, and are widely accepted in fairly closed user-group environments, their use (a) together with biometrics and (b) compliant for use to generate legally binding electronic signatures are still fairly new. [7] This report also illustrated that in some cases, such as biometrics and the European Citizen Card (ECC) activities, standards are still being developed.

What also was very interesting, and was well documented in the e-ID card literature, was is the lack of any strong central leadership for a pan-European e-ID card. Also, a “not invented here” mentality has meant that there has often been a drive towards home-grown solutions. Some countries, such as Austria and Estonia have gone out of their way to showcase their solution, with a desire to make them a de-facto standard. Their desire to promote their standard, however, is not backed by any form of legislative drivers at a pan-European level. Hence, it is unclear what, if any, e-ID card standard will emerge in the near future.

Over and over again, reference was made in the e-ID card literature to the activities of ICAO. The activities of ICAO have lead, not only with regards to researching this report, but also by politicians, especially in the UK scheme, to interchange the ICAO guidelines or requirements for ePassports with requirements to be implemented in an e-ID card. ePassports and e-ID cards, while related at a certain level, should be treated as separate topics. Doing otherwise, has only caused unnecessary confusion, and may in the long run cause further poor design decisions to be made for e-ID card implementations.

Another interesting finding that came from writing this report that was not expected, was the true lack of third-party (i.e. non-Government) applications looking to use national e-ID cards. Banks have already implemented their own e-Banking authentication schemes, and hence see little value-add from adopting a different technology. Outside Europe, Malaysia is a good example illustrating a close public-private-partnership for e-ID card schemes. It seems however that in Europe the participation of private sector in defining e-ID card schemes is rather excluded. It merits possible further research in determining what secondary use of e-ID cards could be, and whether a tighter integration of third-party requirements could have a greater general acceptance of e-ID cards.

Finally, returning to the importance of interoperability issues requiring further investigation. As the need grows of claiming social services across borders, the need to address interoperability issues becomes more critical. As was mentioned in the report, Poles working in the UK claiming retirement pensions after returning to Poland or British pensioners claiming social benefits from a retirement home in Bulgaria are just a few sample scenarios where e-Government applications need to be reviewed to ensure the requirements of e-Government applications are met in a Europe that is more and more operating without national borders. Purely for such scenarios where people are far away from their local public administrations, an interoperable e-ID card would be valuable to both citizens and governments alike.

12. BIBLIOGRAPHY

[1] " ID in the News - http://www.no2id.net/news/newsblog/," NO2ID.

[2] WP3, "D3.6 Study on ID Documents," D3.6, 2006.

[3] E. A. Whitley, I. R. Hosein, I. O. Angell, and S. Davies, "Reflections on the academic policy analysis process and the UK Identity Cards Scheme," *The Information Society,* 2006.

[4] "Community framework for electronic signatures," The European Parliament and the Council of the European Union: Official Journal of the European Communities, 1999.

[5] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," in *Advances in Cryptology - CRYPTO '86*: Springer Berlin / Heidelberg, 1988.

[6] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," in *Advances in Cryptology - CRYPTO '86*: Springer Berlin / Heidelberg, 1998.

[7] "Towards an electronic ID for the European Citizen, a strategic vision " CEN/ISSS, Brussels December 31 2004.

[8] "Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing." vol. Directive 2005/60/EC, E. P. a. Council, Ed.: Official Journal of the European Union, 2005.

[9] T. Myhr, "Regulating a European eID," in *Porvoo 7 - Interoperable European Electronic Identities* Reykjavík, Iceland: Porvoo e-ID Group, 2005.

[10] "Identity Cards Act," 2006.

[11] "Online Availability of Public Services: How is Europe Progressing?," European Commission Directorate General for Information Society and Media 3 March 2005.

[12] H. Leithold, A. Hollosi, and R. Posch, "Security Architecture of the Austrian Citizen Card Concept," in *Proceedings 18th Annual Computer Security Applications Conference* Las Vegas, Nevada, 2000.

[13] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People,* vol. 7, pp. 6-37, December 1994.

[14] M. Lloyd, *The Passport*. Sparkford, England: Sutton Publishing, 2005.

[15] J. P. V. D. Balsdon, *Romans and Aliens*: Duckworth, 1979.

[16] D. D. Cock, "Belgian eID Card Technicalities," Heverlee, Belgium: Katholieke Universiteit Leuven, 2006.

[17] S. J. G. Wilkinson, *A Popular Account of the Ancient Egyptians*: John Murray, 1854.

[18] "Doc 9303, Machine Readable Travel Documents," ICAO, 2006

[19] "Strategic Action Plan for the National Identity Scheme Safeguarding your identity " UK Home Office Ref. No. 278283, December 2006.

[20] "Bürgerkarte - Anwendungen Bund." vol. 2007: HELP.gv.at, 2007.

[21] "The Status of Identity Management in European eGovernment Initiatives," DG Information Society and Media, European Commission 6 June 2006.

[22] "Services using an electronic ID card," Finnish Population Register Centre.

[23] P. Urien and M. Dandinou, "Designing Smartcards for Emerging Wireless Networks," in *7th Smart Card Research and Advanced Application IFIP Conference (CARDIS 2006)* Tarragona, Catalonia, Spain, 2006.

[24] J. Camenisch and A. Lysyanskaya, "Efficient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation," in *Eurocrypt 2001*, 2001, pp. 93-118.

[25] J. Camenisch, D. Sommer, and R. Zimmermann, "A General Certification Framework with Application to Privacy-Enhancing Certificate Infrastructures," in *SEC 2006*: Springer-Verlag, 2006.

[26] A. Hayat, H. Leitold, C. Rechberger, and T. Rössler, "Survey on EU's Electronic-ID Solutions," Secure Information Technology Center - Austria (A-SIT) 1.0, 10. August 2004.

[27] "Country Updates in Porvoo9 Slovenia 2006 ". vol. 2007: Porvoo Group, 2006, p. Country Updates.

[28] "Identity Management Systems (IMS): Identification and Comparison Study," Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG) 2003.

[29] H. Leitold, "The Austrian Citizen Card - Interoperability and Integration of Technologies," in *Online-Authentication and Identity Management* Bolzano, Italy, 2006.

[30] A. Hayat, R. Posch, and T. Rössler, "Giving an Interoperable Solution for Incorporating Foreign eIDs in Austrian E-Government," in *IDABC-Conference 2005: Cross-Border e-Government Services for Administrations, Businesses and Citizens* Brussels, Belgium, 2005.

[31] D. D. Cock, C. Wolf, and B. Preneel, "The Belgian Electronic Identity Card (Overview)," in *3rd Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik*: Bonner Köllen Verlag, 2006.

[32] "The Estonian ID Card and Digital Signature Concept: Principles and Solutions Whitepaper," 2003.

[33] "Entitlement Cards and Identity Fraud: A Consultation Paper," S. o. S. f. t. H. Department, Ed.: HMSO, 2002.

[34] "Key Statistics." vol. 2007: Department Of Statistics Malaysia, 2007.

[35] "Flagship Applications Progress Status (as of 30th September 2006)." vol. 2007: Multimedia Development Corporation, 2006.

[36] Wikimedia, MyKad.png, Ed.: Wikimedia, 2007.

[37] M. Thomas, "Is Malaysia's MyKad the "One Card to Rule Them All"? ," *Melbourne University Law Review,* vol. 28, August 2004.

[38] "The MSC Malaysia Flagship Applications." vol. 2007, p. Listing of MSC Malaysia Flagship Applications.

[39] "MSC Malaysia Flagship Applications: 2. Multipurpose Card." vol. 2007: Multimedia Development Corporation.

[40] "EURODAC guarantees effective management of the Common European Asylum System." vol. 2007: European Commission, 2005

[41] Wikipedia, Dnielectronico.png, Ed.: Wikipedia, 2007.

[42] "Smart Card Durability Study," Identity and Passport Service (Crown) 2006.

[43] Y. Haghiri and T. Tarantino, *Smart card manufacturing : a practical guide* John Wiley & Sons, 2002.

[44] "GlobalPlatform Card Specification Version 2.1," GlobalPlatform, 2001.

[45] Wikipedia, Mh_chipkarte_asynchron.png, Ed.: Wikipedia.

[46] contact.jpg, Ed.: CRYPTAS.

[47] K. E. Mayes and K. Markantonakis, "On the potential of high density smart cards," *Information Security Technical Report* vol. 11, pp. 147-153, 2006.

[48] "JavaCard and MULTOS smart card multi application operating systems and Windows for smartcards." vol. 2007: Jacquinot Consulting, Inc. , 2006.

[49] L. Gaston, M. Faher, A. Rhélimi, J. Pellicer, C. Wrathall, T. France-Massey, and A. Hovsto, "Basic Technologies for Multi-application Cards and Systems," March 2003.

[50] "Magnetic Stripe Card." vol. 2007: Wikipedia, 2007.

[51] "Seafarers' Identity Documents Convention (Revised), 2003 (No. 185)," International Labour Organization 2006.

[52] C. Lynch and S. Frey, "2D Barcodes & Biometrics: The Secure Combination on Seafarer ID Cards," in *Biometric Consortium Conference* Arlington, Virginia, USA, 2004.

[53] "Secure ID Document Card Features " www.lasercard.com: LaserCard Corporation, 2005.

[54] "Optical cards take hold for two Italian identity programs." vol. 2007: secureidnews.com, 2005.

[55] *Biometrics Systems - Technology, Design and Performance Evaluation*. London: Springer-Verlag, 2005.

[56] M. Arnold, C. Busch, and H. Ihmor, "Investigating Performance and Impacts on Fingerprint Recognition Systems," in *Workshop on Information Assurance and Security* United States Military Academy, West Point, NY: IEEE, 2005.

[57] K. A. Rhodes, "Challenges in Using Biometrics," U.S. General Accounting Office 2003.

[58] L. Hong, A. K. Jain, and S. Pankanti, "Can Multi-biometrics Improve Performance," in *IEEE Workshop on Automatic Identification Advanced Technologies (WAIAT-99)*, Morristown NJ, 1999 pp. pp. 59-64.

[59] "BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management," British Standard, 2006.

[60] M. N. Anis, "Singapore 'no' to MyKad." vol. 2007 Putrajaya, Malaysia: The Star Online, 2006.

[61] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cyptanalysis of Product Ciphers," *Journal of Computer Security,* pp. 141-158, 1995.

[62] T. S. Messerges and R. H. Sloan, "Investigations of Power Analysis Attacks on Smartcards," 1999, pp. 151-162.

[63] Noneh and e. al, "Checking Cryptographic Protocols for Faults," Konstanz, Germany, 1997.

[64] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Crypto '96*, 1996.

[65] B. S. Kaliski, Jr., "Optical Fault Induction Attacks," in *Cryptographic hardware and embedded systems : 4th international workshop* Redwood Shores, CA, 2002.

[66] J. Lopez, R. Oppliger, and G. Pernul, "Why have public key infrastructures failed so far?," *Internet Research,* vol. 15, pp. 544 - 556, 2005

[67] e. T. eGovernment, "eGovernment white paper on smart card applications and evolution: Analysis of developments," OSCIE Volume 1 Part 1-1, March 2003.

[68] A. Hayat, R. Posch, and H. Leitold, "Identifying Obstacles in moving towards an Interoperable Electronic Identity Management System," in *eGOV INTEROP'05, 1st International Conference on Interoperability of eGovernment Services* Geneva, Switzerland, 2005.

[69] A. Ouksel, "A Framework for Scaleable Agent Architecture for Cooperating Heterogeneous Knowledge Sources," 1999.

[70] "Digital Signatures Act " Estonia, 2000.