Submitted in part fulfilment of the requirements for the degree of Doctor of Philosophy

A Method For Creating Digital Signature Policies

By

Nikolaos Papas

School of Management

UNIVERSITY OF
SURREY

October 2010

Abstract

Increased political pressures towards a more efficient public sector have resulted in the increased proliferation of electronic documents and associated technologies such as Digital Signatures. Whilst Digital Signatures provide electronic document security functions, they do not confer legal *meaning* of a signature which captures the conditions under which a signature can be deemed to be legally valid. Whiist in the paper-world this information is often communicated implicitly, verbally or through notes within the document itself, in the electronic world a technological tool is required to communicate this *meaning*; one such technological aid is the Digital Signature Policy.

In a transaction where the legality of a signature must be established, a Digital Signature Policy can confer the necessary contextual information that is required to make such a judgment. The Digital Signature Policy captures information such as the terms to which a signatory wishes to bind himself, the actual legal clauses and acts being invoked by the process of signing, the conditions under which a signatory's signature is deemed legally valid and other such information.

As this is a relatively new technology, little literature exists on this topic. This research was conducted in an Action Research collaboration with a Spanish Public Sector organisation that sought to introduce Digital Signature Policy technology; their specific research problem was that the production of Digital Signature Policies was time consuming, resource intensive, arduous and suffered from lack of quality. The research therefore sought to develop a new and improved method for creating Digital Signature Policies.

The researcher collaborated with the problem owner, as is typical of Participative Action Research. The research resulted in the development of a number of Information Systems artefacts, the development of a method for creating Digital Signature Policies and finally led to a stage where the problem owner could successfully develop the research further without the researcher's further input.

Statement of Originality

"This thesis and the work to which it refers are the results of my own efforts. Any ideas, data, images or text resulting from the work of others (whether published or unpublished) are fully identified as such within the work and attributed to their originator in the text, bibliography or in footnotes. This thesis has not been submitted in whole or in part for any other academic degree or professional qualification. I agree that the University has the right to submit my work to the plagiarism detection service TurnitinUK for originality checks. Whether or not drafts have been so-assessed, the University reserves the right to require an electronic version of the final document (as submitted) for assessment as above."

Some of the material contained herein has been presented in the form of the following publications:

Refereed Conference Papers Published/Accepted
Alamillo, I., Martinez, D., Seltsikas, P. and Papas, N. (2007). "Designing a Modelling Methodology for Legal Workflows." Jurix 2007: The Twentieth Annual Conference, Leiden, Netherlands, IOS Press.

Refereed Journal Papers Under Review
Papas, N., O'Keefe, R. and Seltsikas, P. (2010). "Legal Workflows and Digital Signatures in eGovernment: Action Research or Design Science?" European Journal of Information Systems, Under Review.

....

Nikolaos Papas

28 October 2010

Acknowledgments

I owe my thanks to Dr Philip Seltsikas for introducing me to the wonderful world of academia and for seeing the dim light of potential in me to suggest I could embark on the long and arduous journey which you are reading the end result of.

I would also like to thank Professor Bob O'Keefe for providing me with continuous and insightful guidance and supervision, without which I could not possibly have refined the work to its current state.

I acknowledge the case study company and their staff, for their time, assistance and support to ensure the completion of this thesis.

On a more fundamental note, I would like to extend my deepest thanks to my dear mother who instilled into me a thirst and respect for knowledge from an early age and whose lessons have not faded over time.

Finally, I would like to express my most fundamental feelings of gratitude to my wonderful wife Harshita, who gave me self belief and continuous encouragement and for making the unachievable seem achievable. Without her continuous support, constant advice and positive nature and attitude, I could not have gotten to where I am today.

Table of Contents

Index of Figures

Index of Tables

List of Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
AR	Action Research
B2B/B2C	Business To Business / Business To Citizen
BPM	Business Process Modelling
BPMN	Business Process Modelling Notation
CA	Certification Authority
CATCert	Catalan Certification Authority
CEO	Chief Executive Officer
DSP	Digital Signature Policy
DS	Design Science
DSS	Digital Signature Service
DR	Design Research
ETSI	European Telecommunications Standards Institute
EPC	Event-driven Process Chain
EJIS	European Journal of Information Systems
IS	Information System
ISO	International Standards Organisation
IT	Information Technology
MIS	Management Information Systems
NIST	National Institute of Standards and Technology
OASIS	Organisation for the Advancement of Structured Information Standards
PADS	Process Acts Documents Signatures
PKI	Private Key Infrastructure
RFC	Request For Comments
RST	Rhetorical Structure Theory
UML	Unified Modelling Language
XML	eXtensible Markup Language

1 Introduction

In recent years, increased political drivers (e.g. EC, 2005; EC, 2006) have pushed administrations towards implementing electronic Government Information Systems in order to reduce administrative burden and increase service to citizens and businesses (ibid.). One of the many phenomena observed by this push is the increased proliferation of electronic document exchanges and increased research into solving specific issues relating to electronic document exchange; specifically, there are a number of issues that appear only when trying to convert paper-based concepts to electronic documents and making Information Systems (IS) capable of dealing with such issues. The research within this dissertation concerns itself with one such issue.

The research topic of this dissertation is in the general area of digital document security and is therefore concerned with technology similar to Digital Signatures (e.g. Wilson, 1999) and Digital Certificates (e.g. Hazari, 2002). However, the technology in question – Digital Signature Policies (Hernandez-Ardieta et. al., 2008) – differs in many points from both Digital Signatures and Digital Certificates in that it has different aims and usages. Whereas Digital Signatures are concerned with document security and are a technology stemming from cryptography (e.g. Rivest et. al., 1978), and Digital Certificates are concerned with identity and non-repudiation (Hazari, 2002; Broderick et. al., 2001), Digital Signature Policies (DSPs) are actually concerned with issues of legality concerning the actual document and the legal *meaning* of the Digital Signature applied on it (ETSI, 2003). Therefore, instead of providing physical document security, this technology carries legal information encoded in a formal language such that an Information System can interpret this information and make decisions on it. One of the main intended uses of this technology is for the Digital Signature Policy (DSP) to inform a validating Information System about whether an attached Digital

Signature and Digital Certificate are valid within a specific legal context (ETSI TS 101 733).

In order to illustrate this concept, consider the following: Mikle (2004) describes a model where a Digital Signature and a Digital Certificate are used in combination in order to protect a contractual document from being altered in transit (and subsequently highlights flaws in their current implementations by demonstrating a successful attack). The Digital Signature uses cryptographic means to ensure the contract's content has not been altered, whilst the Digital Certificate gives assurance to the receiver that the contractual document was signed by the same person that claimed signed it. However, what is not known (in spite of the presence of both Digital Signature and Digital Certificate), is whether the person that signed the document is actually authorised to endorse the contents of that contract, whether the signing person even intended to endorse the contents of that contract, whether the contract was signed in the correct locality, and whether the correct procedure of contract endorsement was followed. These and other issues relating to the *meaning* of a signature on a particular document are, in the paper-world, typically known through either contextual, implicit or *a priori* knowledge but rarely stated explicitly (e.g. Garner, 2001; Kratovil, 1946). DSPs were developed in order to electronically capture this kind of contextual and legal information that relates to the legality of signatures and documents and the rules governing both. The DSP can then be used by the validating Information System to correctly assess the validity of the Digital Signature and Digital Certificate against a given piece of legislation.

Research into Digital Signatures and Digital Certificates has matured these technologies to the point where they can be used to protect other types of documents, such as E-mail (Deng et. al., 1996), and this progress has resulted in applications being able to automatically determine the validity of the used Digital Signature and Digital Certificate (ibid.). However, regarding DSPs, very little –if any- discussion exists regarding its technological

implementation, suggested methods by which such DSPs can be drafted, ways of validating the content of DSPs and other such discussions relating to the use and application of DSPs. In other words, barring the official documentation issued by Standards bodies (e.g. ETSI, 2002) which describe and formalize the concept and technology, little discussion exists on how to use, apply, validate, and create this technology in a real organisational setting. The one peer-reviewed article that does exist on the technology discusses a potential and theoretical application in network exchange protocols, beyond the area of use originally intended by the standards bodies (Hernandez-Ardieta et. al., 2008).

It can therefore be said that there is a research gap covering DSPs and how they can be used, created, edited, and otherwise handled by IS. As there is limited information on this technology, the researcher investigated the issue of whether it is possible to impart legal knowledge on an Information System at all by studying material on Legal Arguments (e.g. Dung, 1995; Prakken and Sartor, 1997; Bench-Capon, 2002), the analysis and autonomous manufacture of Legal Contracts (e.g. Daskalopulu, 1998; Bons et. al., 1995) and different methods of representing legal information (e.g. Knackstedt et. al., 2006; Sijanski and Münch, 2006). Examining these sources revealed that imparting legal knowledge on an Information System is a possibility and provided the researcher with an array of different methods that could be used for the research.

The research focused on a specific governmental organisation, called CATCert, experiencing the above research gap. CATCert is the Catalan Certification Authority and is an autonomous organisation of the Catalan regional government in Spain, tasked with providing the necessary tools and expertise to ensure electronic transactions between the administration and businesses and citizens are secure and legal (more information on the problem owner is provided in Chapter 4). As a result of the research gap described in the earlier paragraph, the ability to impart legal facts onto a new

Information System being developed was undermined due to the lack of literature and knowledge on this problem. This new Information System was required to achieve legally compliant document and signature exchanges between government, business and citizens and therefore required digital security technology. The organisation, having chosen DSPs as a tool to carry this legal information, struggled with the aforementioned research gap to develop a way to be able to use this technology efficiently; the specific issue was the ability to create DSPs (an XML file) out of legislation written in natural language text. A prototype method called "PADS" (Processes-Acts-Documents-Signatures) was developed without much success and it is at this stage that the researcher started intervening.

The research, on the basis of the aforementioned research gap and the organisational problem, was thus centred on solving the following research question:

"How can the current method of creating Digital Signature Policies be improved such that Digital Signature Policies in ETSI TR 102 038 format are created in a reproducible and more formalised manner that allows users without legal training to use it?"

Interpreting that statement, a number of implications are revealed:

- A method for creating DSPs does exist, but is inadequate
- There is a need for a new method to be more formal and reproducible
- The use of a particular DSP standard is mandated
- The research outcome must specify a solution that can conform to the needs and requirements of the problem owner, specifically the users not needing legal training to use the method

The above research question and associated implications can therefore be expanded into the following research aims:

- To develop a method enabling individuals to convert natural language legal acts and convert those to process models
- To develop tools and methods to convert the process models into a codified form
- To produce standards-compliant signature, evidence and archival policies (adhering to ETSI TR 102 038)
- The developed method should allow transformations in a structured and repeatable manner

In order to find a satisfactory answer to the research question that satisfies the above implications, the researcher adopted a Research methodology known as Participatory Action Research (e.g. Baskervilie, 1999; Kemmis and McTaggart, 2008), a special form of Action Research (e.g. Baskerville and Wood-Harper, 1996; Elliot, 1997; Kemmis and McTaggart, 1992) that is aimed at structuring research undertaken with a collaborator who is elevated to co-researcher status (Baskervilie, 1999). This particular Research Methodology was chosen due to its adeptness to the research question, which seeks to find an improved practice of creating DSPs. Furthermore, as the research seems to be focused on the imparting of legal data to an IS artefact and since improvement was defined as 'reproducible' and 'formalised', it concerns the input of legal data (which is natural language text). This means that the research subscribes to a qualitative research design (e.g. Gray, 2009) because the research deals exclusively with textual data and the requirements can not be expressed numerically. Therefore, as a result of the requirement for the solution to adhere to the 'truth' constructed by the organisation (i.e. it must fit the organisation's specific requirements), the epistemological position used is Constructivism (e.g. Crotty, 1998; Golinski, 1998; Landesman, 1997); Constructivism posits that knowledge is created through the interaction of the subject and the world (Gray, 2004). The author *verified* that Action Research can be undertaken as part of a qualitative research design with a constructivist epistemological position (e.g. Gray, 2009) in order to ensure a consistent research design.

The standards document referenced in the above research question is called ETSI TR 102 038 and is a technical standard published by the European Telecommunications Standards Institute (ETSI) that specifies DSPs and how they are to be implemented using XML. ETSI is an organisation similar to ANSI or NIST in the US and have published many standards for Digital Signatures, Digital Signature Policies and other communications standards. The document mentioned above, ETSI TR 102 038, is a technical specification that captures the various data fields a DSP needs to contain, it directs the data type and field lengths for each data element within a DSP and describes specific conditions that need to be satisfied by certain fields depending on the usage of the policy. It is one of only two such technical specifications on the make-up of a DSP (the other being ETSI TR 102 272, which describes a Signature Policy in ANSI.1 format) and is therefore a credible source to base the research on, by virtue of being the only technical specification; ETSI TR 102 272 is not being considered because XML is a newer technology and recent research has focused on developing ASN.1 to XML translators in order to allow 'legacy' applications using ASN.1 to communicate with more modern XML-based applications (Imamura and Maruyama, 2001). Furthermore, XML is considered to be more readable by humans than ASN.1 and therefore requires less technical knowledge to use (Imamura and Maruyama, 2001; Chadwick and Mundy, 2003), which addresses the need for users to not require specialist training, as stated in the research question.

The conducted research resulted in the yield of several distinct artefacts, which are:

- A Questionnaire aimed at eliciting relevant legal information from legislation
- A Process Modelling Notation that captures the procedural aspect of law, captures relevant legal information in its metamodel and graphically illustrates the use of Digital Signatures (and thus DSPs)

- A Transformation tool that transforms the modelling tool's XML output into an ETSI TR 102 038 compliant DSP
- A method that uses the above artefacts in order to produce DSPs out of legislation

Expanding on the final bullet point, the method consists of the following four-stage process:
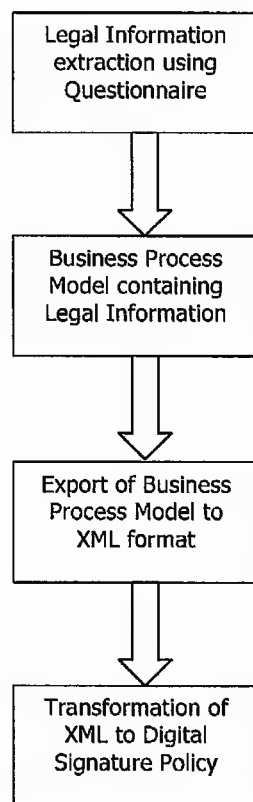
Figure 1-1: The complete process from natural language law to Digital Signature Policy

As can be seen from figure 1-1, the legal information is extracted from legislation using the questionnaire. The information in the questionnaire is then translated into a Business Process Model that represents the legal process in question and captures the legal requirements of the signing occurring as part of the process. Once completed, the process model is

exported to XML using the process modelling tool's export facilities. As the modelling tool's facilities can't create customised XML output, the produced XML file must be passed through the transformation tool in order to be converted to an ETSI TR 102 038 compliant DSP. Thus, a DSP in ETSI TR 102 038 format has been created out of legislation written in natural language text. The above paragraph also demonstrated the use of the artefacts created as part of the research intervention.

During the investigation, the researcher realised that many elements of the work undertaken could be compared to Design Science (e.g. Hevner et. al., 2004; Peffers et. al., 2008). Further research into this research methodology revealed that it shares many different features with Action Research (e.g. Järvinen, 2005) and can therefore be considered as similar (ibid.) or perhaps even equivalent (e.g. Cole et. al., 2005) research methodologies. Careful post-hoc analysis of literature on the similarities and differences between these two research methodologies and a re-evaluation of the collected data suggest that, whilst similar in many (but not all) of the employed methods and in the epistemological orientation, there are a number of differences that set Action Research and Design Science sufficiently apart from each other to the point where this research can be regarded as Action Research and not Design Science. The differences are in the formality of evaluation, which in Action Research can be informal as it is an inherent activity of the research process and not a formal activity following the research (e.g. Gray, 2009; McNiff, 1988) and in the importance of the produced artefact. In Action Research, the produced artefact is of minor importance (Henfridsson, 2005) as the main purpose of Action Research is to improve practice, whereas in Design Science the aim is to improve practice through the design and build of an artefact (e.g. March and Smith, 2005). It is these subtle differences that set Action Research apart from Design Science and thus explain why this research is Action Research and not Design Science – the importance of the research (as seen through the research question) was in the improvement of a practice, not the production of artefacts.

To summarise, the research contributed to knowledge in a variety of ways:

- It produced a formal method that can be used to create DSPs in ETSI TR 102 038 format
- It produced artefacts that can support the above method in creating DSPs in ETSI TR 102 038 format
- Whilst the above method and artefacts were designed such that they satisfy the problem owner's own requirements, the method and artefacts can be modified to be used in different organisational settings as well
- The research contributed to current methodological debate on Action Research and Design Science and applied practical findings to a, so far, mainly theoretical discussion
- It raised the profile of DSPs in peer-reviewed literature, where it is rather under-reported
- It imparted learning on both researcher and collaborators, who were shown capable of turning learning into actionable knowledge

This shows that there were a number of contributions that this research made and this is highlighted by the fact that the research resulted in one confirmed publication of the results and one publication in review, with further publications planned.

The following pages shall now outline the details of the research. Chapter 2 discusses related literature and gives a background on the difference between Digital Signatures, Digital Certificates and DSPs. It also discusses various methods that can be used to impart legal knowledge onto an Information System.

Chapter 3 then introduces, explains and discusses the Research Design of the research and discusses elements such as the guiding Epistemology, the

employed Research Methodologies, justification for choosing those and finally describes the detailed Research Methods employed in the study.

This is followed by the presentation of the results in Chapter 4, which describes the various artefacts and the method guiding their use. Note that a lot of in-depth technical detail can also be found in Appendices D and E, where further descriptions of the results are provided.

In Chapter 5, the results of the research that were presented in Chapter 4 are analysed and discussed. This section assesses the validity of the results when compared against the research question, the chosen research methodology and against the unique issues in conducting collaborative research with the particular problem owner. It also addresses questions regarding the validity of the research intervention as a whole and shows why it is Action Research and not Design Science.

Chapter 6 concludes the document by highlighting the achievements of the research and assessing the contributions to the existing body of knowledge. It also highlights new questions raised by this research and identifies what forms this future research could take. It finishes off by discussing some of the weaknesses of the intervention.

2 Literature Review

In order to better understand the research question and why it is causing problems to a specific organisation, it is necessary to gain an understanding of the problem domain. This section will investigate the problem domain and highlight how the research question causes problems to an organisation.

2.1 Digital Signature Policies and other Electronic Document Security technologies

DSPs are related to Digital Signatures and Digital Certificates; however, they are separate entities to either of those and in order to understand the difference better, a short technical and functional description will be provided of both Digital Signatures and Digital Certificates before describing DSPs in detail.

2.1.1 Digital Signatures

Digital Signatures are a legally recognised tool which can be used to prove the authenticity of a document and verify the person that signed it (Wilson, 1999). Important aspects of Digital Signatures are that they can be used to uphold the principle of non-repudiation for legally binding documents (Alsaid and Mitchell, 2005) if used in combination with Digital Certificates (see below), as Digital Certificates provide a statement on who digitally signed the document (Hazari, 2002). Also, Digital Signatures prove that the document received by the receiving party is the same document that was sent by the sending party (Broderick et. al., 2001). In other words, Digital Signatures are valid and useful tools in order to prove the authenticity of documents and assert their validity.

The basic functionality that provides the above features was developed mathematically in 1978 by Rivest et. al. (1978), only the second ever work to deal with the concept of Digital Signatures. In their groundbreaking work, Rivest et. al. (1978) describe both a PKI infrastructure, as well as the specific

mechanisms that create and secure signatures and the documents they sign. According to Rivest et. al. (1978), the document is first encoded into a hexadecimal number through a hashing algorithm. The resulting hash is then encrypted using a cryptographic algorithm. Thus, the encrypted hash represents the Digital Signature.

To verify whether the document was modified in transit, the process is reversed – first, the hash is decrypted, then the document is hashed using the same hashing algorithm and the two hashes are compared – a change in the document will automatically result in a different hash due to its mathematical properties (Rivest et. al., 1978).

Thus, with the two hashes being the same it can be asserted that the document is the document the signer signed and therefore the signer can not contest the content of the document (Rivest et. al., 1978).

For the above model to work, however, a method must exist by which the document receiver can be notified of the correct key to use to decrypt the document hash and also by which the received document can be hashed so that the validity can be verified by the receiver; finally, the Digital Signature must be tied to the identity of the signing person. These issues are resolved by the use of Digital Certificates, which are introduced in the next section.

Blythe (2005) describes the various legislative provisions made for Digital Signature in a number of different legislative environments, such as the UN, EU, USA and the UK. Blythe (2005) observes that whilst "many countries have now adopted some form of digital signature law", these laws can be of differing degrees of stringency and take a "minimalist", "hybrid" or "prescriptive" form (ibid.). In other words, digital signatures are generally recognised as a legally valid tool in most jurisdictions. Kisswani and Al-Bakri (2010) augment this view with their observation and analysis of digital signature law in Australia and China. Both authors recognise that the design

and implementation of various signature laws were not fully satisfactory, however, and that most implementations have some drawbacks; both authors are calling for a renewed look at legislation which in some cases is over 10 years old and has since been rendered partially obsolete by newer technological developments in the digital signature field.

It should be noted that there are different types of Digital Signatures in circulation, which differ from each other through the type of data they record and thus the sophistication of protection they can offer to documents in particular settings. Details of these Digital Signatures have been recorded in Appendix B.

2.1.2 Digital Certificates

Digital Certificates, in combination with Digital Signatures, provide useful tools in establishing the four basic security services (e.g. Wilson (1997), Hazari (2002)) of *authentication, integrity, non-repudiation* and *confidentiality.*

First of all, the Digital Certificate contains the name of the entity (e.g. a person authorised to use the signature) to whom it was issued, thus providing authentication services. Furthermore, the Digital Certificate also contains the Public Key that can be used to decrypt the Digital Signature; due to the mathematical properties of Public Key cryptography, the Public Key contained in a Digital Certificate can decrypt a message that was encrypted by only one single Private Key (Rivest et. al., 1978) – therefore, it can be concluded that if the Public Key can indeed be used to decrypt and verify the Digital Signature, then this serves as further proof that the original signer is indeed the entity he/she claims to be due to the match of the mathematically unique private-public key pair (Wilson, 1997).

The current *de facto* standard for Digital Certificates is the X509 v.3 standard, also known as RFC 3280 (Robiette, 2001). According to this standard, the contents of the Certificate not only include the aforementioned information on

Public Key and Name, but there are further data fields for items such as validity period, certificate extensions, Certification Authority identifier information, information on the Certificate Authority chain and unique identifiers (Housley et. al., 2002).

From the above information it becomes clear that even though Digital Signatures and Digital Certificates are capable of providing solid statements on whether what was signed is what was received and that the documents were signed by the person claiming so, in a business context these assertions are not enough in order to make digitally signed documents fully legal in the eyes of the law. The missing 'link' is provided by DSPs, described in the section after the next one.

2.1.3 Threats to PKI?

The security provided by Digital Signatures and Digital Certificates within the PKI architecture is dependent on two key factors:

1. A hash function will create a unique hash value of a document such that it is not possible to have a different document yielding the same hash value
2. There exists only 1 public key that can decrypt a message encrypted by only 1 private key, such that no other public key can decrypt a message from the same private key

Recent research in the scientific literature suggests that key factor 1 is currently under contention and a survey of research in this area suggests that the assumption (namely, that a hash value can not be reproduced) might be invalid after all, poising security risks to a network implementing PKI security. This research is presented here in condensed form.

The CRYPTO 2004 conference rocked the cryptographic world when research teams published their results of breaking common hash functions (Randall and Szydlo, 2004). Of particular interest were the results of Wang et. al. (2004), who published their work on breaking the hash functions MD4, MD5, HAVAL-128 and RIPEMD (Wang et. al., 2004) – according to Randall and Szydlo (2004), they went as far as demonstrating an MD4 collision "by hand". These were significant results since MD5 is a "popular hash function" (Randall and Szydlo, 2004) which is still in use for "fingerprinting" software (ibid.). These findings were then expanded on in a later paper by two of the original four authors and published at EuroCrypt 2005 (Wang and Yu, 2005); in that expanded paper, Wang and Yu make the assertion that their method was capable of colliding MD5 "in about 15 minutes to an hour computation time" (ibid.) and that their method "is also able to break efficiently other hash functions, such as HAVAL-128, MD4, RIPEMD, and SHA-0" (ibid.).

Another blow to the concept of hashing came at the RSA 2005 Conference, when Wang et. al. (2005) presented their research on breaking SHA-1 (Wang et. al., 2005), showing how it could be broken with 2^{69} iterations (in Chan and Dworking (2005), they reduced the complexity of this attack to 2^{63} iterations). This was "bad news" for the cryptographic community and applications depending on hash functions, since according to Wang and Yu (2005), SHA-1 is a "widely used hash function".

The reaction to these potentially fundamental threats varied amongst experts. For example, a position paper by the European Commission-funded ECRYPT project (IST-2002-507932) analysed the various collision attacks and identified the implication that "hash functions using a simple message schedule such as those derived from the MD4 type construction are at risk for use in real-life implementations. These include MD4, MD5, RIPEMD, HAVAL and SHA" (ECRYPT-Project, 2005). The paper also identified that "Collision attacks are thus a real concern in the context of digital signatures" and ECRYPT also issued a recommendation that hash functions for which collisions

had been demonstrated ought to be discontinued in applications requiring collision-resistance (ibid.). In particular, ECRYPT recommended to discontinue using "MD5 in signature applications with medium to high security requirements" and also recommended "to be cautious with new deployments of SHA-1" (ibid.).

On the other hand, William Burr, manager of the security technology group at the 'National Institute of Standards and Technology' (NIST) is quoted as saying "There's no real emergency here" in an article on FCW.com (Olsen, 2005). A similar reaction was issued by RSA Laboratories, who concluded in their news report on CRYPTO 2004 that "There is no need to panic, since it will likely be some time before the weak hash functions can be turned into practical exploits" (Randall and Szydlo, 2004).

However, within quick succession of the publication of the above results, three papers appeared, all demonstrating *practical* exploits of the MD5 collision attack originally published by Wang et. al. (2004). The first of these papers is by Mikie (2004), who demonstrates in his paper how this attack can be used to create two different PDF documents, both featuring the same hash value. He also demonstrates how the same attack can be used to create the same digital signature for two different files, thus giving real-world examples of a theoretical attack (Mikle, 2004). In practical terms, this demonstrates the ability to alter a digitally signed contract document post-signature and thus introduce altered terms to a transaction.

In similar vein, Kaminsky (2004) published results on how the same MD5 attack can be used to perform collision attacks on the distribution of software and thus mask a malicious program with the MD5 checksum value of the original, harmless program. He also shows how the same attack can be used to compromise Digital Signatures and Digital Rights Management systems (Kaminsky, 2004).

Finally, Lenstra and de Weger (2005) published research at ACISP 2005, demonstrating how the same MD5 attack can be utilised to create two different "X.509 certificates with identical signatures" (Lenstra and de Weger, 2005). The result of the identical signature is that a Certification Authority will be able to validate both certificates, as they have the same signature. This is a significant result, since one of the key principles underlying PKI is "that a CA guarantees the binding between an identity and a public key" (Lenstra and de Weger, 2005). The paper also shows how the principle of non-repudiation is violated. Lenstra and de Weger have developed increasingly sophisticated attacks on the X.509 certificate since then (Sotirov et. al., 2008).

All these developments and results were of significant enough impact that the National Institute of Standards and Technology saw it fit to organise and host two 'Cryptographic Hash Workshops' in order to examine the attacks, examine the security of current and future hashes and discuss strategies on dealing with these recent attacks. The summaries of these workshops are presented in Chang and Dworkin (2005) and Nechvatal and Chang (2006). To summarise the findings of these two workshops, NIST concluded that:

- Currently unsafe hash functions (where collisions had been demonstrated) should be phased out and not be included in new security software
- The use of state-of-the-art algorithms (SHA-2) ought to be encouraged for the time being
- It should be expected that SHA-2 itself will be broken within 5-10 years
- It would be wise to have a competition for new hash functions that are, by design, collision-free and will be ready for publication in 2012

(Adapted from Chang & Dworkin (2005) and Nechvatal & Chang (2006))

In summary, recent developments have shown that PKI technology is at risk, especially in environments where hash functions are used that are now considered broken due to the demonstrated collision attacks. These attacks

were considered significant enough by one of the world's most important standards bodies to initiate a complete redesign of the underlying hash functions of this security model in order to avoid such attacks in the future. However, it should be born in mind that these attacks did not occur by malicious elements; instead, they were engineered and designed by some of the world's finest researchers over a period of many years. It is reasonable to assume that elements outside of the scientific community will require time to understand and implement attacks based on the methods presented earlier. Not only is the theory behind these attacks quite involved, but the computing power required to perform these attacks is also substantial – Wang et. al. (2004) showed how it can take up to 1 year to collide an MD5 hash, and computed that a SHA-1 collision requires up to 2^{63} hash iterations before a collision can be found. Therefore, whilst practical attacks have been proven to be possible and have been performed by scientists, it remains to be seen when and how elements outside the scientific community will be able to perform these attacks themselves. Nevertheless, the simple fact that successful attacks have been performed should be signal enough that there needs to be a rethink about security in a PKI network and how current hash technology compromises it.

As for the relevance to DSPs – they govern the use and legal validity of Digital Signatures. If, however, Digital Signatures become obsolete as a technology due to the above attacks eroding their value as a security tool, then there is no need for DSPs either. In other words, threats to the nature of Digital Signatures affect DSPs directly. It will be necessary for stakeholders of DSPs to keep a close eye on the above developments affecting the cryptographic community and essential elements of Digital Signatures.

2.1.4 Digital Signature Policies

It is frustrating to note that there is very little discussion on DSPs within the scientific literature. Searches using scientific indexing services, such as

Science Direct, EBSCO, Emerald and Elsevier, revealed just one paper (apart from the author's own conference publication) that deals with DSPs directly. Even within the practitioner community, the use of the phrase 'Digital Signature Policy' or 'Electronic Signature Policy' tends to be widely ambiguous and can have several meanings, none of which may refer to the use and meaning of DSPs in the spirit of this research. For example, Microsoft uses the term 'Digital Signature Policy' as a reference to something they refer to as 'Software Restriction Policy' which is aimed at users being prevented from running unsafe files on their operating system and therefore this concept has no documentary relevance at all[1]. Other uses can relate to qualitative usage rules and conditions under which E-mail messages must be digitally signed without specifying or referencing the technical meaning of a 'Digital Signature Policy' in the ETSI-term, but rather the use here is a number of guidelines issued to members of staff, advising them under which circumstances Digital Signatures must be applied to their E-mail communication; in other words, a DSP is considered to advise the protection of E-mail communication using Digital Signature technology and does not indicate the crucial legal importance with regards to electronically capturing the legality of a signature under a piece of writing that is hinted upon earlier[2].

Additionally, Shao and Cao (2006) talk about 'signing policies' as a cryptographic protocol in a threshold signature scheme featuring multiple signers, but this work is within the cryptographic domain and not relevant to the meaning of the term DSP as used in the context of this research.

Despite the best efforts of the researcher, only six documents in the practitioner community that describe DSPs as a concept complementing Digital Signatures and Digital Certificates could be found. As it happens, the

---

[1] See http://support.microsoft.com/kb/973825 Accessed on 31/08/2009.

[2] The researcher has provided two examples for this type of use (there are many more):
   1) Oregon State University. http://oregonstate.edu/fa/businessaffairs/sites/default/files/OSU_E-Sign_Policy_Fina2l.doc. Accessed on 31/08/2009.
   2) Albuquerque City Council.
      http://mesa.cabq.gov/polisy.nsf/WebApprovedX/4D4D4667D0A7953A87256E7B004F6720?OpenDocument. Accessed on 31/08/2009.

majority of these are the official standards on this technology and these documents are:

- ETSI TR 102 038: The structure of a DSP is defined using XML in this document. It is the technical supplement to ETSI TS 101 733 (see below) and, as far as the researcher can ascertain, one of only two *technical* specifications of a DSP.
- ETSI TR 102 272: This document is equivalent to ETSI TR 102 038, but uses ASN.1 (a formal notation, different to XML) to formally describe the structure of a DSP.
- ETSI TS 101 733: This document primarily defines different types of Digital Signatures (from a functional, non-technical perspective), but extends several Digital Signature types to allow for the use of DSPs.
- ETSI TR 102 045: This document provides background research and an extended business model for DSPs. It mainly focuses on the meaning of DSPs and their electronic equivalent to various legal contexts of the 'signature' process.
- ETSI TR 102 041: This is a report aimed at practitioners about the possible organisational impact of DSPs if they were implemented as a technology in an organisation. In other words, potential implementations of DSPs along with their pitfalls are examined.
- RFC 3125: This document represents another standard for DSPs. The scope covers both functional and technical aspects and in its own words bases itself on ETSI TR 102 038 and ETSI TR 101 733.

A further mention of DSPs is made in the eXtended Signature Services (XSS) Profile of the Organisation for the Advancement of Structured Information Standards (OASIS - publishers of many open standards on web and other IS technologies) Digital Signature Service (DSS) specification (OASIS, 2005); this is an extending profile to the OASIS Digital Signature Service (DSS) standard (OASIS, 2007) in order to allow a Digital Signature built in accordance with the OASIS DSS standard to carry a reference to DSPs and thus enable DSS to

include DSPs. However, the profile makes no mention of the detailed make-up of the DSP, other than defining the DSP fields that must be present within a DSS Digital Signature. In other words, this extension enables applications utilising DSS-compatible Digital Signatures to also peruse DSPs.

Of the referenced documents, only ETSI TR 102 045 goes into some depth explaining the legal meaning of a DSP, why it ought to accompany a Digital Signature and suggestions on necessary infrastructure to support the concept. Whilst the document does feature a bibliography and a summary of information sources, it is extremely limited and the document fails to use a scientifically acceptable referencing system. Therefore, assertions quoted or paraphrased from this document ought to be treated with caution since their origin can not be determined. On the other hand, considering that this document was issued by a credible standards body (the European Telecommunications Standards Institute, which is ISO 9001:2000 certified), its significance ought to be recognised and its accuracy accepted with only slight reservations.

Standard ETSI TR 102 045 is referenced as a primary source in the only peer-reviewed article that the researcher was able to unearth, namely Hernandez-Ardieta et. al. (2008), who also acknowledge DSPs as "a document that collects a set of rules to create and validate electronic signatures, under which an electronic signature can be determined to be valid in a particular transaction context" (Hernandez-Ardieta et. al., 2008), thus complementing the researcher's conclusions on the use of DSPs that were based on studying the ETSI documentation. Hernandez-Ardieta et. al. (2008) state that a DSP can be authored using natural language (requiring the clear identification of the usage rules) or one of the formal notations specified by ETSI (i.e. either ASN.1 or XML, as identified above). They further state that natural language policies require human intervention for inspection and judgment on validity, whilst the assessment and evaluation of Signature Policies authored according to a formal notation can be fully automated. However, the focus of

Hernandez-Ardieta et. al. (2008) is on a theoretical B2B & B2C application, where transactions between buyers and sellers follow their suggested protocol that would present the buyer a DSP that captures the rules of the transaction and would thus enable the buyer to examine the transaction rules before deciding whether to continue the transaction or not. In other words, their theoretical research piece describes a potential area of use outside the realm of document security and in the area of network protocols. They see the technology of DSPs as a meta-document carrying information regarding rules and norms that can have a number of applications; it can carry legal rules in the context of document security (as is the case in the research described by the author) or it can carry transactional rules in a type of network protocol, as demonstrated by Hernandez-Ardieta et. al. (2008). It shows that the technology can be used in more than one application domain and in scenarios other than those involving documents and document security. Furthermore, due to the limited amount of research published on this technology, there is scope for domains and uses other than those described herein to be explored as potential application areas of the technology of DSPs. However, these usages remain outside the scope of the research problem being discussed and the focus on DSPs is for their application in the document security domain that they were originally designed for by the ETSI Institute. It can be said with certainty that the original intended use was in document security and related to document signature, due to the fact that the published standards documentation all refers to signature-related issues, such as ETSI TR 102 045, which is explored in greater detail below.

Two other references on DSPs are made neither in a practitioner context nor in a peer-reviewed article context. Fernandes (2006) published an evaluation and extension to the ETSI DSP model in his Master's dissertation, but since only the abstract is in English and the main body in Portuguese, and since his dissertation was not published online until 2010, details of the work were not studied by the researcher. On the other hand, Pasquier and Devoret (2006)

submitted an extension to the ETSI DSP standard to the European Patent Office, aimed at securing the unsigned properties field (see Appendix C on technical description of the DSP standard) against an attack that could see unsigned properties being replaced with malicious code. As this is a current patent application, no details of their work are accessible apart from a summary page. Comparing the body of literature on DSPs to the body of literature on Digital Signatures reveals that there is a wide gulf in the number of publications dealing with DSPs (very few) and number of publications dealing with Digital Signatures (many).

With reference to the research aims, these identified sources are therefore of key interest to the researcher. One of the research aims clearly states that the aim of the research is to "produce standards-compliant signature, evidence and archival policies (adhering to ETSI TR 102 038)"; therefore, the official standards will be key in guiding the technical work towards achieving compliance. However, two other research aims (convert natural legal acts to process models; develop tools and methods to convert process models into codified form) will also greatly benefit from these standards documents because these standards documents contain relevant information with regards to data and data relationships, which will need to be represented and exploited by the tools and methods being developed. In other words, analysing and perusing these documents is very important to achieve the research aims of this research.

The following sections are based on ETSI TR 102 045 and paraphrase large parts of that document. The approach taken is to firstly outline signature issues in the paper world and study their impact on electronic signatures. Secondly, paper equivalents of signature policies are introduced before, finally, signature policies and their implications are introduced and studied. At this stage, the other documents outlined above will contribute information on the nature of Signature Policies. Where possible, sources other than ETSI TR

102 045 will be utilised in order to strengthen the conclusions of the ETSI document and to further exhibit the legal issues.

2.1.4.1 Signature Issues in the Paper World

Paper-based signatures are a very common part of modern every-day life; so common, that there are very few legal definitions of signatures in EC countries, the exceptions being France (who define signatures in the Code Civil) and the UK (where legal validity of non-manuscript signatures is equivalent to legal validity of handwritten signatures, based on case law).

In the paper-based world, signatures are not restricted to merely representing the name of the signer. There are also a wide variety of commitments that are being agreed to; to further complicate manners, signatures are not the only method by which a party can agree to a commitment. Courts in different countries acknowledge items such as engraved stamps, rubber stamps, seals and even ticks or crosses as valid forms of expressing a commitment and thus equivalent to a signature. Garner (2001) mentions how "some jurisdictions - esp. U.S. states on the eastern seaboard-require deeds to be sealed. A few even require leases to be under seal" (Garner, 2001; p. 785), thus showing that seals have a place in law even today, which creates a real problem for introducing electronic infrastructure aimed at supporting or supplanting such legal processes.

As an example of commitments that can be entered and agreed to, one can consider a bank clerk signing or stamping the back of a cheque to indicate receipt of the cheque, a signature under an application form confirming the signers truthfulness of the data supplied within the application form or the signature of two chief executives agreeing to the terms of a trade deal between their two organisations. All of these scenarios utilise signatures, but each have very different legal meanings which are badly (or not at all) documented and would need to be represented electronically for the corresponding electronic scenarios.

From these examples it becomes evident that one needs to consider signatures, whether they be electronic or paper-based, from a variety of viewpoints in order to understand their legal meaning. These viewpoints are treated individually in the sections below.

Transactional Context

As shown in the above examples, the meaning and role of the signature varies depending on the context it is used in. Going back to the trade example, such a contract does not contain any explanatory text on the meaning of the signature, as it is general knowledge that the position of the signatures at the end of the contract communicates the meaning of the signers agreeing to the terms contained within that contract. On the other hand, signatures on a similar contract that is labelled 'Draft' or 'Proposal' do not indicate acceptance of the contained terms and thus an agreement to a specific commitment. Another such example is a defendant in court, who needs to make his plead in court official through the submission of, amongst other things, his signature; the plead is therefore not valid if the signature is not present (Garner, 2001; p. 668).

The interpretation of the meaning of the signature is very much based in people's everyday understanding of what a signature is, resulting in lesser appreciation in the subtleties that separate the meanings of different signatures. These subtle differences are, however, crucial to be included in an electronic environment as an automated processing system will not have the same intuitive understanding of signatures. These subtleties will therefore need to be highlighted and organised so that they become accessible to a computer system.

Formality of Signing and the Intention to Sign

When documents are being signed, there is often a different ceremony surrounding the signing of the document. As an example, one could consider a supply manager who signs several purchase orders every day without

ceremony, as it would be inhibitive in his high workload. On the other hand, a significant transaction between two major industrial companies may be signed in a big ceremony with formal signing and exchanging of documents.

In both examples, the documents being signed are of major significance, yet in one case the signing is a routine activity whilst the other is a big ceremony. In order to avoid subjective attachments to the degrees of importance when signing a document, many jurisdictions insist on certain mechanisms that communicate the importance of the commitment to the signer, e.g. by pre-printing the words "I........declare that the information above is true".

Identity of Signer

As a signature is literally worthless if it can not be attributed to an individual signer, it is necessary to ensure attribution of the signature to the individual. A commonly used method is to have the signer's name printed underneath the signature. However, in certain situations it may be sufficient that "it is presumed that the signature...is in that person's handwriting" (Garner, 2001) when an explicit attribution through the printed name is not present or required.

Furthermore, in certain business scenarios the identity alone is not sufficient, as the role and/or attributes of the signer are just as important as his identity. For example, a secretary or a warehouse operative would never be allowed to sign off a high-value deal between two major international corporations. Finally, the purpose of a signature, especially in a business scenario, is not to identify the signer but to inform the signer of the significance he is about to undertake.

Roles and Attributes of Signer

Across business scenarios, the concept of 'apparent authority' of the signer is sufficient to assume that the signer acts on behalf of his organisation. In most cases, the status and authority of the signing individual is not verified and this is established in the laws of most jurisdictions. Some exceptions do apply

however, such as transactions for land sale, company financial returns and other high value transactions. In such transactions, the signature must come from a designated company representative and thus there must be a way of establishing the signer's authority to agree to such commitments.

In Real Estate Law in the United States, however, "It is sufficient if the testator states to the witnesses that the signature is his signature. This is known as acknowledgment of the signature" (Kratovil, 1946) and shows that in certain situations 'apparent authority' can be self-conferred where individuals and not organisations are concerned.

Signature Commitment Types
A commitment represents the precise nature of the responsibility assumed by signing, and in the paper world this responsibility has to be inferred from the circumstances surrounding the act of signing. Examples for commitment types are:

- Signing a draft to identify the status/integrity of the draft, but no intention to be bound by its contents
- Signing a contract (an intention to be legally bound)
- An acknowledgement of receipt
- Giving mandate to a Transfer/Appointment

The last item is an example of a signature representing someone in power, who appoints a person to a certain position through the use of a signature, rather than declaring so in person, such as "the Governor's signature evidencing my appointment as Attorney at Law and Solicitor in Chancery" (Safire, 1984); in other words, here the signature acts as a 'mouthpiece' and thus negates the need of the signer to be present in person to conduct the appointment.

A signature can also be used in order to *exit* an agreement; for example, a person may add a stipulation to one's signature in a bill of exchange which

repudiates his liability to the holder (Garner, 2001; p. 937). This creates a particularly complex issue, in that the liability that the signer is repudiating himself from must (in an Information System) be identified and marked or linked such that this liability repudiation can be recorded accurately.

Timing and Sequence

The sequence of applying signatures has significance. For instance, to authorise a piece of work, the authorising person must sign it after it was signed by the original author in order to represent the fact that the authorising person agrees with the findings of the original author. Other examples include signatures of witnesses, who must be physically present to witness the signing they are supposed to witness (thus, not only time, but also location becomes important). Also, one has to consider complicated business scenarios where multiple documents are part of a single transaction; in such a circumstance, the validity of the acceptance of an agreement may be contingent on certain approvals having taken place before the signing of the final contract, i.e. the documents must have been signed in a specific order.

Timing is also of significance, especially since certain events (e.g. safety equipment inspections) have to occur within a certain time frame to be legally conformant. Other examples can be drawn upon from Italian life insurance, where a medical report must be recent in order to be considered relevant.

Location

It was mentioned above how location can become important when a witness has to sign a document in the previous section. Further, other areas where signatures and location must be tied are in banking, specifically in cheques. In the French, German and Italian jurisdictions, a cheque must not only be signed by the account holder, but the account holder must also include his

geographic location of where the cheque was signed. It is merely a claimed fact, but it serves to bind the signer to his assertion.

In federal countries, location information can also determine the legislation under which a dispute would be handled.

Longevity

A provided signature must be available for inspection and verification after the signing event. In the case of a will, this may be decades after the original will was written and signed. Due to the durability of ink and paper, the facility of being able to verify a signature long after it was produced is taken for granted.

Security Considerations

In order to increase trust and confidence that a signature belongs to the signer and therefore a valid agreement is entered, certain transactions have security requirements imposed on them, especially in the banking sector. Some examples are listed below:

- Requiring a printed signature
- Requiring a cheque card, with a specimen signature
- Maintaining a specimen signature on a database
- Requiring identification (e.g. passport)

Multiple Signatures

Within a business context there exist documents that require more than 1 signature to become effective and binding, as shown above. For example, in a two-party agreement (say buyer and seller) a contract must contain signatures from both parties to become binding, otherwise the absence of signature from one party will not bind that party to the contract as no proof of the party's commitment to the contract exists. Furthermore, there are three special cases of multiple signatures that have to be considered:

countersignatures, witness signatures, notarial signatures. Of countersignatures, Garner (2001) defines them to mean "a second signature attesting to the authenticity of the instrument on which it appears" and identifies that this term originated as a legal term in 1807 (Garner, 2001; p. 230 ff.).

With regards to witness signatures, Atkinson (1953) states that "An appropriate testimonium or concluding clause is 'In witness whereof I have subscribed my name this _ day of 19_', although 'Witness my signature this _ day of 19_' will do just as well" (Atkinson, 1953; p. 820), thus showing two legally valid methods for producing a signature to evidence someone standing witness to a certain procedure.

In order to address the above signature issues for the electronic world, several solutions have been found. In most cases, however, the concept of a signature policy guiding the use of signatures does not exist explicitly in written legislation; as explained earlier, understanding on the use of signatures has developed over time and is highly contextualised. Understanding the legal implications of what legal weight a signature carries for a given context is therefore going to be key to help answer the research question and meet the research aims.

Specifically, the research aim of developing a method to convert natural language legal text will benefit from this legal information by receiving guidance on what information, and how much, to take from legislation. The research aim to convert the process models to codified form will benefit from this legal information by highlighting mandatory and voluntary information and guiding the form that this information can take. Finally, the research aim calling for a structured and repeatable method will benefit from this legal information in terms of highlighting the relevant legal information that the method must be capable of capturing through the questionnaire and the process modelling notation.

This completes the summarisation of the different issues affecting DSPs and the legal circumstances that need to be taken into account when developing Signature Policies. All these issues were used by ETSI to author the content of DSPs and the two standards that describe the two formal notations that must be followed when authoring a DSP (ETSI TR 102 272; ETSI TR 102 038) were written in such a way that accounted for the type of legal information discussed above. Appendix C describes in detail one of these standards and introduces the various elements of data found in a DSP. The following section shall describe *how* the various elements forming a DSP (described in Appendix C) are utilised in order to provide a mechanism for capturing the crucial legal information described in this section and therefore shows that DSPs are a valid medium for carrying this information.

2.1.4.2 Signature Issues and Digital Signature Policies

In the previous section it was discussed how there are a range of signature issues affecting paper documents that need to be catered for in an electronic document environment in order to satisfy regulatory constraints surrounding the application of signatures and their purpose in providing legal meaning to specific transactions. This section will therefore discuss how the various data elements in ETSI TR 102 038 provide a mechanism to solve most of these signature issues and how this is therefore a valid technology for the stated purpose.

Signature Commitment Type

This relates to the information regarding the purpose of the signature, e.g. acknowledging a draft, entering a contract or giving purchase authorisation. The applicable data field in the DSP is the `RecognizedCommitmentType` element, which specifies a commitment type ID and a 'Field of Application' field to explicitly identify what the Digital Signature is to be used for.

Legal Meaning

The legal meaning provides context to the commitment type and could be considered as, for example, the governing legislation for a particular commitment type. Information on this type of contextual legal information is provided with the `RecognizedCommitmentType` element, which contains a `Semantics` field, which is defined to hold contextual defining information regarding the 'Field of Application' and the overall commitment the signature is being used for.

Transactional Context

The Transactional Context, therefore, is catered for by the use of the `RecognizedCommitmentType` element, which provides information on the Legal Meaning, the Commitment being entered into, and thus some information on the Transactional Context. In the example on Transactional Context earlier, it was mentioned that this goes beyond what the signature is for and includes information required to conclude a certain transaction - the stated example was of a defendant having to sign his plea. This kind of procedural information is not catered for by DSPs and will therefore need to be embedded in a suitable manner compliant with the relevant legislation.

Formality of Signing/Intention to Sign

These signature issues are also not catered for in the DSP as it is difficult to capture electronically whether the signer was truly aware of the formality of the signing and what the signing entailed, since there was no formal signing procedure to inform the signer of the formality and significance of the signing procedure. Therefore, this signature issue needs to be addressed through a suitable artefact.

Identity of Signer

This signature issue does not require the use of DSPs. As explained in the earlier section on Digital Certificates, a Digital Certificate contains sufficient information to provide a statement on identity. However, the DSP data fields

provide the `MandatedCertificateInfo` field that allows the Certificate used in the signing process to be provided, thus creating a link between the DSP and the Digital Certificate used to create the Digital Signature.

Roles and Attributes of Signer

The restrictions on roles and the associated required attributes against a role of a particular signer for a particular use of a Digital Signature are captured by the `RoleTrustCondition` element, which provides several data fields that include and exclude certain roles and attributes of a signer for a signature to be valid. Therefore, the signature issue of role and attribute of a signer has been catered for by the ETSI standard.

Timing and Sequence

This kind of signature issue, typically encountered in tendering, is provided for via the `TimeStampTrustCondition` element, which contains fields on time delays, can include sequences and even fields on reference to special Timestamp certificates for more formal timing/sequence requirements.

Location

This signature issue is not explicitly captured in the DSP standards. It could be included in the `Semantics` field, for example, but validating that particular field would pose a processing problem as it would then require the `Semantics` field to hold data in a format that can be processed by a machine. Therefore, this signature issue needs to be resolved through other means.

Longevity

The signature issue that relates to the length of validity of a particular signature is catered for through several means. A Digital Certificate contains information on the Certificate's validity period (i.e. how long it may be used for), thus ensuring that at signing time the Digital Signature was valid. For ensuring the validity post-signing and post-Certificate expiration, however,

the longevity is established through the use of an 'ES-A' type Digital Signature, which contains the relevant information on how long the Signature is to be archived for and how the archival is qualified (i.e. the use of a reference to an Archival Certificate). Therefore, this issue does not need to be catered for in a DSP.

Security Considerations

The `AlgorithmConstraintSet` element and the `SignerRevReq` element provide a set of fields that allow the DSP to specify what type of security is to be applied to the Digital Signature. For example, a high-value transaction may only permit one particular type of hashing function and one particular type of Digital Certificate validation mechanism in order to comply with relevant legislation. This element provides the necessary fields to capture this type of information.

Multiple Signatures

The issue of witness, notary and other cases of multiple signatures are also catered for by the DSP standard through the use of `CommonRules` and `CommitmentRules` elements. The ETSI TR 102 038 standard states that `CommonRules` are applied to all Signatures, whereas `CommitmentRules` is an element that can have one or more occurrences, with each element specifying the unique identifier of the Digital Signature it refers to. Through these elements it is therefore possible to use one DSP to provide contextual and legally binding information to multiple Digital Signatures.

2.1.5 Summary

This section has introduced the specific technical domain which the research is concerned with. Using a number of documentation issued by the relevant standards bodies as well as relevant peer-reviewed scientific articles, it was explained what Digital Signatures, Digital Certificates and DSPs are and what they may be utilised for. The discussion was rounded off by mentioning a

threat to the use of this technology through a range of papers that were aimed at breaking some of the fundamental assumptions of Digital Signatures and Digital Certificates.

With regards to meeting the Research Aims and answering the Research Question, this information will help guide the research because it informs the researcher of the rules and interrelationships between documents, legal acts and signatures within legislation. It also informs the researcher of the standards documentation that the research results must adhere to. In other words, the author has gained important information that will help guide the research towards a solution that can satisfy technical requirements set by the mandated standards and satisfy legal requirements set by legislation.

In order to further explain why DSPs are necessary, a range of Signature Issues that affect paper-based processes were illustrated, whilst the previous section described and explained how these paper-based signature issues are resolved through the use of DSPs.

2.2 Making Legal Concepts accessible to Information Systems

Ever since advances in the areas of Artificial Intelligence and Natural Language Processing allowed Computer Scientists to develop computer systems that were able to make decisions and process natural language text, the academic discipline of Law became interested in harnessing computers' vast processing powers (Rissland et. al., 2003).

Since Computer Science and the nature of IS offer a wide array of technologies and techniques that would allow their use in the area of Law, questions arose on how to best utilise these abilities in the context of Law and legal applications. In order to be able to address this question, it was realised that it was necessary to understand the nature of Law better in the first

instance, and only with this extended understanding in place would it be possible to understand how to utilise and use IS within a legal capacity.

Therefore, most contemporary research has a two-tier focus: the first tier focuses on *representing* and *analysing* the specific area of Law earmarked to become IS enabled or IS assisted, whilst the second tier focuses on the *implementation* of IS into that specific area of Law. This is evident in the works of Bench-Capon, Daskalopulu and other contemporary Law and Computer Science researchers, who structure their research in this manner.

There are several areas of Law that receive a special research focus in order to enable the use of IS within different areas of Law. Firstly, there is the area of Legal Arguments, which is the area that Trevor Bench-Capon focuses on most. This area comprises legal arguments of a defeasible context (Bench-Capon, 2002) as they are conducted in a courtroom (e.g. New Mexico vs. Morton, 1975 (Bench-Capon, 2002)) and involves the representation and abstract analysis of the arguments brought forward by both prosecution and defence in such a case. The techniques and methods used by Bench-Capon and other researchers in this area will be introduced below.

The next area of research is Contracts. The main driver of this research area is Aspassia Daskalopulu, who focuses on contract assembly (Daskalopulu & Sergot, 1995), contract representation and analysis (Daskalopulu, 2000) and other related research efforts in the (aspirational) automated handling of legal contracts. Other research efforts include the analysis of legal contracts using Petri Nets (Bons et. al., 1995) and the representation of contractual agreements using RuleML (Governatori & Rotolo, 2004). Again, more details shall be provided later on in this section.

Another, more recent area of research, is focused entirely on the representation and analysis of law using Modelling Languages. The difference to the above two methods is that the representation and analysis of legal

matters is performed using well known Process Modelling Languages. For example, Sijanski and Münch used the Process Modelling Language "UML" in their work for the European-funded eJustice project (Sijanski and Münch, 2006), whilst Knackstedt et. al. researched and used an extended version of eW3DT to represent legal requirements in system design (Knackstedt et. al., 2006). The details of this research are outlined below.

Another important area of research is decision making. Research in this area has focused on utilising findings from Artificial Intelligence research by utilising traditional AI concepts in a legal environment. Two of the major Artificial Intelligence decision mechanisms (Neural Networks, Knowledge-Based Systems) were studied by a variety of researchers and some interesting findings were reported by Borges et. al. when they applied a Neural Network to legal disputes that they had studied (Borges et. al., 2003). On the other hand, in the area of Knowledge-Based Systems, Graca and Quaresma researched a method for keeping a knowledge base up to date with frequent changes in the legislative environment (Graca & Quaresma, 2003). The details of their studies are reported below.

Finally, a parallel research stream is Semantics that could be used by automated systems in the legal area. It is a parallel research stream as its outcomes offers solutions for other types of research that may be in need of an established set of semantics. Work in this field was performed by Jouve et. al. (2003), who propose a framework for the semantic modelling of documents and include a hierarchical order of different types of legal documents (Jouve et. al., 2003). A slightly different direction was taken by McCarty, who instead went ahead and proposed a knowledge representation language for law and provided the rules of this language (McCarty, 1989).

The details of the research in these research streams are outlined in the following sections.

2.2.1 Legal Arguments

As mentioned above in the previous section, an authority in this area is Trevor Bench-Capon, who as early as 1997 identified the need and necessity to analyse and abstract the reasoning applied in court cases. Early on, he attempted to set apart his research into the make-up of arguments from other, more traditional approaches, such as case retrieval of matching cases and the application of *stare decisis*, which he regarded as "a gross simplification" and concluded that "Such systems are better regarded...as case retrieval systems" (Bench-Capon, 1997). He links his work to similar research performed by Prakken and Sartor in 1997, who focused on a rule-based framework for the representation of case arguments (Bench-Capon, 1997). Bench-Capon focuses on arguments by stating that "because we are interested in producing an argument, the cases we wish to find and deploy are not determined by their similarity alone" (Bench-Capon, 1997), thus hinting that case retrieval by similarity is not suitable enough in order to investigate and analyse arguments. He continues that case based reasoning "requires:

1. A position to argue for
2. A structure for a case based argument, determining a variety of argument moves
3. Consideration of cases with reference to the argument moves they support"

Adapted from: Bench-Capon (1997)

Thus, Bench-Capon sets the scene for a new approach towards court case analysis by focusing on the analysis of arguments, dissecting the nature of arguments and by representing them accordingly. His early work attempted to represent arguments using two languages developed for the earlier shunned purpose of case retrieval, namely a language called "HYPO", described in Prakken and Sartor (1997), as well a language called "CATO" (Aleven & Ashley, 1997). In his work, he combines the two languages by "follow[ing]

the argument structure of HYPO, but use CATO's argument moves" (Bench-Capon, 1997). This fusion results in two important algorithms, which are reproduced below. It is assumed that the system argues for the plaintiff:

```
Argument Algorithm (AA)
AA1 Find all citeable favourable cases
AA2 Until no response possible or no more citeable cases:
Construct 3-Ply argument for citeable case
Next Citeable case
AA3 End
```
Taken from: Bench-Capon (1997)

The interesting variable here is the 3-Ply argument, which is presented as follows:

```
3-Ply algorithm (TP)
TP1 State point
TP2 Respond
TP3 Make rebuttal
```
Taken from: Bench-Capon (1997)

With these two algorithms, Bench-Capon sets his work apart from other research that he dubbed as "case retrieval systems" through the inclusion of the 3-Ply algorithm into his argument algorithm. This allows the system to construct a case similarly to how a Plaintiff would do so in a real court room, because the system is prompted to not only state an argument, but to also find both supporting and counter arguments. By introducing these algorithms, Bench-Capon thus also introduces the need to identify cases individually, as well as the need to identify arguments used in each case as variables that need to be recorded and taken into account. This, in turn, requires more analysis and the classification of arguments and past cases, which is performed awkwardly in his early 1997 work due to the nature of the two languages he chose to represent his point of view. However, his work in 1997

nevertheless managed to establish that case retrieval and arguing with cases are two separate approaches and therefore must be treated separately. In his view, case based reasoning serves as a tool that "involves important rhetorical aspects as well as logical aspects" (Bench-Capon, 1997), which means that case based reasoning provides not only arguments for a particular point of view (i.e. for either the plaintiff's point of view, or for the defendant's), but it also provides integrity for arguments, as the inclusion of the TP3 algorithm implies.

This issue of integrity of arguments is an important point to keep in mind, which (along with the entire idea of case-based reasoning) is expanded by Bench-Capon's later work when adopting some of Prakken and Sartor's (1997) ideas to develop the so-called 'Argumentation Frameworks' (originally developed by Dung (1995)) further, with the above summarised research results complementing Prakken and Sartor's (1997) ideas. Thus, Bench-Capon manages to contribute to a major paradigm in this area of Legal Arguments and case-based reasoning – Argumentation Frameworks.

Bench-Capon was instrumental in showing that Argumentation Frameworks were more than just theoretical mind-games on abstract concepts. The aim of Argumentation Frameworks is to "represent arguments as abstract entities, whose role is determined solely by their relation to other arguments. No attention is paid to the internal structure of arguments" (Bench-Capon, 2002). Furthermore, the arguments can interact with each other through the 'attack' function, which is in essence a statement that Argument A invalidates Argument B. In other words, the basic aim of an Argumentation Framework, as applied to a court case, is to analyse the arguments presented during a court case and to investigate which arguments counter or invalidate which other arguments; the outcome then shows whether the plaintiff (plaintiff's arguments were not attacked successfully) or defendant (plaintiff's arguments were attacked successfully) won the case. The central question, therefore, is which argument can successfully attack which other argument? As Bench-

Capon explains, "The key question to ask about an [Argumentation Framework] is 'which arguments should I accept?'" (Bench-Capon, 2002). This is the central issue in Argumentation Frameworks and this prompted Bench-Capon to perform more research into this area. The reason this is an important issue is because arguments do not always cancel each other out in a 'scissors-paper-stone' fashion. Sometimes, arguments can be equally valid and the question that arises in such a case is how can a winning argument be chosen between two arguments with equal validity?

Bench-Capon's continued research into Argumentation Frameworks resulted in an extension of the constructs of Argumentation Frameworks; the research resulted in the development of so-called Value Based Argumentation Frameworks (VAF) (Dunne and Bench-Capon, 2004). As mentioned in the previous paragraphs, an argument does not become a winning argument simply through its validity, but for an argument to be considered 'more valid' depends on "the opinions, values and, perhaps, even the prejudices of the audience" (Dunne and Bench-Capon, 2004). Thus, Dunne and Bench-Capon establish that an argument's persuasiveness does not only depend on its ability to withstand attack from other arguments and to successfully attack other arguments; it is also necessary for this argument to appeal to certain values and opinions of the party that is to be persuaded. They propose that Value Based Argumentation Frameworks should take into account a measure for an audience's values, which can be used to measure its effects on a decision.

The following example is used by Dunne and Bench-Capon to firstly demonstrate how arguments may not defeat each other successfully and secondly how the values of the party to be persuaded can affect the outcome.

Example:

Hal, a diabetic, loses his insulin and can save his life only by breaking into the house of another diabetic, Carla, and using her insulin. We may consider the following arguments:

A. Hal should not take Carla's insulin as he may be endangering her life
B. Hal can take the insulin as otherwise he will die, whereas there is only a potential threat to Carla
C. Hal cannot take Carla's insulin because it is Carla's property
D. Hal can replace Carla's insulin once the emergency is over

Now B attacks A, C attacks B and D attacks C. Moreover...A attacks D, since if even if[sic] Hal were unable to replace the insulin he would still be correct to act so as to save his life...it seems we have no coherent position, which is why it is seen and discussed as an ethical dilemma. If, however, we consider it as a VAF, we can see that arguments A and B rely on the importance of preserving life, whereas C and D depend on respect for property. We will now have two preferred extensions, depending on whether life or property is preferred. If we prefer life, we will accept {B,C}; whilst we respect Carla's property rights, we regard Hal's need as paramount. In contrast if we prefer property to life, the preferred extension is {B,D}; the property claim can be discharged if restitution is made. Thus B is objectively acceptable, C and D are subjectively acceptable and A is indefensible. This...shows how...explicit value preferences [can be used] to cut through what would otherwise be an irresolvable dilemma."
Dunne and Bench-Capon (2004), discussing an ethical dilemma originally discussed in Christie (2000)

This example shows how Argumentation Frameworks were extended to include the highly subjective concept of 'values'. In other words, what Dunne and Bench-Capon (2004) managed to achieve with this example was to show that a logical construct like an Argumentation Framework can be extended to include a subjective property, like values, and with this example they have therefore shown that a machine could thus take subjective properties into account when it comes to making or assessing decisions in this area. To put it differently, values were added to Argumentation Frameworks as another variable to be considered by a machine, thus allowing an entity with no grasp of subjective concepts to quantify and use this otherwise inaccessible concept. In recent years, Bench-Capon has worked towards consolidating this research and studying implications and extensions to argumentation

frameworks. For example, in one paper the importance of audience and their value systems is expanded upon in greater and more refined detail (Bench-Capon et. al., 2007), whilst the aforementioned example of a moral and logical dilemma in arguments is revisited and solutions offered to address moral issues through reasoning (Bench-Capon et. al., 2006) and Bench-Capon also forays into expanding Argumentation Frameworks to being able to detect and generate intentions through argumentation, an expansion of the concept of taking audience values into account (Bench-Capon et. al., 2005).

Bench-Capon's research into Argumentation Frameworks, both into its roots and into its extensions, has resulted in some very interesting and important findings. This research shows that representation of case law was necessary in order to make it accessible to IS. Once a valid representation method is found, it can be used to provide input to an Information System so that a computer can then use this representation method to reason on new or unresolved cases by using the methods explained above. Since court cases involve humans, with all their subjective traits, the representation method of Argumentation Frameworks was extended to include the concept of 'values', in order to be able to quantify a subjective concept and thus allow an IS to grasp it and include it in its reasoning. In other words, this research has highlighted the need to model, dissect and analyse law and court cases to such an extent that it can become quantifiable. Once quantification has been performed, an Information System can then be programmed to assist in these areas, as demonstrated by Bench-Capon and his use of HYPO and CATO. What this means is that Bench-Capon and other researchers in this field have shown that it is possible to communicate the meaning and mechanics of law to a machine and then allow the machine to perform computation against the information provided, which is a key finding for the research undertaken in this paper - in order to automate the process of creating an item to carry legal meaning, the automation process must be capable of possessing some knowledge and understanding of the legal information itself. The work discussed above shows that it is possible for a machine to possess that

knowledge and use it in some way, whether this is by arguing a legal case or by creating a DSP.

As important as this work is, it has one serious shortfall. This word does not address how a machine could take a court proceeding and identify and classify the arguments contained in the court proceeding. Here, the work of a human is required to perform this work such that the machine can be 'fed' with 'processable' information. Therefore, in order to make greater use of an Information System's abilities, the next step would be to develop technologies that would allow a machine to perform this abstract representation of arguments as an Argumentation Framework autonomously.

2.2.2 Legal Contracts

Contracts are the heart and soul of business relationships, since they describe, explain, define and regulate the nature of a business relationship, conditions for payment, requirements for product delivery and other important aspects of a business relationship between two entities. They are a regulatory tool that can become an 'insurance policy' should the business relationship deteriorate due to a perceived breach of contract by one party. Therefore, it is pertinent for both parties to ensure that they both agree on what has actually been captured in the contract such that definition and interpretation problems will not occur at a later time. In other words, the content and the nature of the contract must be captured by the participating parties and in many cases this is very difficult to do. Daskalopulu (1998) frequently mentions contracts in the area of Natural Gas Exploitation as an example, where contracts in this field frequently reach sizes of several thousands of pages. Managing such large volumes of very important text is therefore extremely difficult and thus the enormous processing powers of computers can be extremely helpful in order to keep such a large volume of text manageable. For computers to be able to manage contracts, a lot of research is necessary in order to be able to represent contracts in a machine-readable form. Abstraction, modelling, semantic research and analysis are

therefore some important aspects that must be covered in order to enable computers to understand and eventually manage contracts. Thus, this is of particular interest to the general area of eCommerce also.

Contracts are similar to legal arguments that were discussed in the previous section, a complex arrangement of natural language text requiring abstraction in order to become computable to a machine. One possible abstraction mechanism is the construct of a Petri Net (Petri, 1962). The first known use of Petri Nets for contractual purposes was in 1995, when Bons et. al. (1995) realised that the nature of contracts, contractual disputes and contractual trade procedures in the electronic world required the "definition of a common, publicly available language for the specification of trade procedures, which is formal, computable and executable" (Bons et. al., 1995). Based on this need, Bons et. al. (1995) proposed the use of Documentary Petri Nets as a representation technology for modelling trade contracts (Bons et. al., 1995).

In order to achieve their aim, Bons et. al. (1995) analysed the requirements that needed to be met in order to accurately represent trade procedures. Firstly, they went about to identify modelling entities and found that the following entities required representation:

- The trade procedure in itself, incl. the business transactions to be performed, the business participants and their approved behaviour and the required information requiring exchange
- Roles of the involved parties
- Information Parcels, specifying the semantics exchanged between roles
- Scenario attributes, specifying other important information, such as document and information standards to be employed, registration information and other such requirements (adapted from Bons et. al. (1995))

In addition to these entities, Bons et. al. (1995) identified that a range of other requirements needed to be met in order to permit the accurate representation of trade procedures. These extended requirements extend to include formal requirements such as concurrency, decision points, deontics (deontic logic), dynamic properties and the representation of absolute and relative time, notational requirements (graphical representation and hierarchical decomposition) and verification requirements (automated verification, performance evaluation) (Bons et. al., 1995). In other words, Bons et. al. (1995) required the content of a contract to be represented electronically, following a strict structure and agreed set of semantics.

Their strict requirements made Bons et. al. (1995) come to the conclusion that a very appropriate representation format would be in the form of Petri Nets. Petri Nets were developed in 1962 in C.A. Petri's PhD thesis "Kommunikation mit Automaten." Since their invention, they were applied to a wide-ranging array of uses, such as logistics, system modelling and systems design and analysis. In other words, Petri Nets were widely adopted as a valid and helpful tool for graphical representation of complex systems and mechanisms.

Bons et. al. (1995) state that their specific reasons for choosing to use Petri Nets as a representative notation of trade procedures were based on the fact that "in addition to its capability to graphically model both concurrency and choice, is that it offers various kinds of both formal and informal analysis methods, which make Petri Nets especially suitable" (Bons et. al., 1995). However, the statement also implies that whilst Petri Nets have a high degree of matching the stated requirements, there does appear to be a lack of support for some other requirements not mentioned in the above statement. Bons et. al. (1995) determined which requirements were not being met by Petri Nets and therefore they developed the Petri Net formalism further and developed an extension that caters for their need to use Petri Nets for the representation and analysis of legal contracts.

The extension to the Petri Net formalism is as follows:

- Transitions are labelled in order to identify the role causing the transition
- Absolute time is modelled through the specification of timers and implementation of an extra constraint on firing rules, where the timer condition needs to be satisfied in addition to the other firing rules
- Colours and predicates are used to specify different tokens, such as information parcel types, goods, funds, and deontic states
- Roles are modelled as separate Documentary Petri Nets, thus allowing full view of a particular role's tasks and involvement

Adapted from Bons et. al. (1995)

Furthermore, these extensions result in Documentary Petri Nets being able to use "a top-down and a bottom-up approach for the modelling of trade procedures" (Bons et. al., 1995). Thus, Bons et. al. (1995) managed to establish Petri Nets as a viable tool for representing legal contracts and trade procedures.

Daskalopulu (2000) took up the concept of Petri Nets for her research aims into verifying the validity of a contractual agreement and identification of potential loopholes or contradictions. Her approach was to investigate the use of both traditional and Documentary Petri Nets as a tool to perform verification checks on contracts and thus managed to develop a method that uses Petri Nets as an aid to perform the necessary verifications. Her method comprises the following basic steps:

1. Create a Petri Net/Documentary Petri Net model of the contract to be verified
2. Create a State Diagram out of the created Petri Net/Documentary Petri Net model

3. Test the truth of conditions in the State Diagram by using Propositional Temporal Logic (e.g. Computation Tree Logic)

Adapted from Daskalopulu (2000)

Using temporal conditions, this method therefore aids to identify inconsistencies, contradictions and cases where the contract might not function as intended.

Daskalopulu's research revealed some shortcomings, however. A contract containing many decision paths might be computationally very expensive to resolve. To address this, Daskalopulu suggests creating a Binary Decision Diagram out of the created State Diagram (i.e. after step 2 in her method described above), which would help limit the number of decisions, and thus speed up the logical analysis. However, this extra step does not aid in cases where the contract itself is extremely complicated (e.g. contracts governing the exploitation of Natural Gas) and the creation of the Petri Nets themselves creates conceptual problems due to the extensive and sometimes fragmented knowledge contained in such huge contracts.

Another weakness in her method is the fact that "Obligatory, permissible or prohibited actions that parties may perform during the transaction are interpreted and incorporated in the model implicitly" (Daskalopulu, 2000), which means that using Daskalopulu's method will not provide a complete understanding and overview over a contract's nature. This is an important shortcoming that one needs to be aware of when applying Daskalopulu's method to contract verification.

These are two examples of research in the area of Petri Nets used in the contractually governed business environment. Whilst Bons et. al. (1998) developed an extension to Petri Nets, called Documentary Petri Nets, with the aim to represent a contract accurately, Daskalopulu instead focused on using such a representation to allow for automated verification of the rules

contained within the contract. Both of these works are important for the area, as they allow machine processing of complicated natural language contracts. Similar to research performed in the area of Legal Arguments, however, this research stream also ignores the need and technologies surrounding the creation of the necessary constituents out of the natural language texts in question (in this case, the creation of the Petri Nets) and therefore leaves it open to other academic disciplines (e.g. Computer Science) to research how a machine could be able to create a Petri Net out of a natural language text autonomously.

Research into the electronic handling and representation and analysis of legal contracts is not restricted to Petri Nets. There are other research streams that aim to gain a more complete picture over how contracts are being treated, investigated, analysed and represented. Reed and Daskalopulu (1998) performed a lot of research in this area, and one of their approaches was to treat contracts as arguments and thus perform a similar analysis of contracts as Bench-Capon did on legal arguments. Reed and Daskalopulu (1998) used a different tool for their analysis, however, preferring to look into the use of Rhetorical Structure Theory (RST), a method that was developed by Mann & Thompson (1987) for the area of discourse analysis (Reed & Daskalopulu, 1998).

Initially, Reed and Daskalopulu (1998) agreed with Mann & Thompson (1987) who stated that "although RST can be successfully applied to a wide range of texts from diverse domains, it fails to characterise some types of text, most notably legal contracts" (Mann & Thompson (1987), quoted in Reed & Daskalopulu (1998)). In other words, Reed and Daskalopulu were aware that RST was actually unfit for their specific needs. This unorthodox approach allows Reed and Daskalopulu to identify RST's specific failings in their own subject domain and thus enabled them to modify and extend RST in such a way that it suited their needs perfectly.

Their investigation into RST revealed a number of shortcomings when considering the requirements of abstracting a contractual agreement. Reed and Daskalopulu quote research by Moore and Pollack (1992), whereby RST is incapable of dealing with communications failure (e.g. the speaker mispronouncing, the listener misunderstanding), nor is it capable of dealing with follow-up questions (Moore & Pollack (1992), as paraphrased by Reed & Daskalopulu (1998)).

Furthermore, a much more serious issue identified by Reed and Daskalopulu (1998) is the fact that "RST seems to be unable to adequately represent the high level abstract structure of argument" (Reed & Daskalopulu, 1998) – in other words, the basic need of Reed's and Daskalopulu's research is not met by RST. They provide more detail on this issue, which identifies the main problem lying in the fact that many arguments use complicated sentence structures that hide the true meaning of a large piece of text (Reed & Daskalopulu, 1998). It should be noted that Argumentation Frameworks also had issues in dealing with multi-nodal arguments.

Another failing of RST in the area of arguments is the fact that there is "no way of dealing with the idea of argumentative support" (Reed & Daskalopulu, 1998), yet another key issue which makes RST seem unsuitable for the intended use, namely as an abstraction tool to deconstruct legal contracts as a set of arguments. Tied in with this major issue is the fact that "it is impossible to identify an argumentative relation on the basis of RST alone" (Reed & Daskalopulu, 1998). The failings identified in RST seem, when considered together, to point towards RST's inability to support Reed's and Daskalopulu's aim of modelling an argument structure in contractual text (Reed & Daskalopulu, 1998).

These fundamental problems with RST may seem like a big barrier to adopting it for use in a contractual context, but Reed and Daskalopulu (1998) developed an important extension to RST which addresses the fundamental

flaws of RST and thus enables its use in a contractual context. This extension is the subsuming of RST with a layer that explicitly represents argumentative constructs. In this layer, a reification of support relations between propositions is performed, in order to define structure of arguments. Furthermore, operators are developed to help encapsulate various argument forms (Reed & Daskalopulu, 1998).

This addition of an extra layer thus manages to solve all major problems with RST in a contractual context. This layer allows the abstraction of argumentative relationships at an abstract layer, thus allowing the characterisation and analysis of argument structures. Furthermore, this allows the capture of mononuclear arguments and structures, thus solving the issue of complicated sentence structures not being deconstructed properly by RST (Reed & Daskalopulu, 1998). In Reed's and Daskalopulu's words, the extension thus "offers a fully functional account by distinguishing the intentional and informational components of text structure…[and enables] argumentative relations between textual units to be handled explicitly" (Reed & Daskalopulu, 1998).

With this extension, Reed and Daskalopulu managed to add the ability of understanding the structure of arguments by allowing the abstraction and visualisation of the constituents of an argument, thus providing a mechanism by which arguments can be deconstructed, understood and acted upon. Through enabling RST to understand and dissect arguments, it was thus also enabled to dissect and understand contracts, since there is an "isomorphic relationship between the structure of persuasive discourse [arguments] and that of deliberative discourse [contracts]" (Reed & Daskalopulu, 1998). Thus, methods developed for one type of discourse can therefore be applied to a different type of discourse if there is an isomorphic relationship. This conclusion therefore means that it should be possible to use Argumentation Frameworks to dissect and analyse contracts.

The ability to dissect contractual agreements into a set of arguments and counter arguments should help an Information System to answer 4 important questions in contracts, namely the "who-questions", the "when-question", the "how-question" and the "what-if question" (Reed & Daskalopulu, 1998). The answer to these questions is dependent on an understanding of the argumentative structure of the contract, which is provided by the earlier stated abstraction layer allowing an RST-based system to identify the mononuclear constituents that help answer these important questions. Therefore, with this aid an RST-system is capable of solving a large number of disputes that are typically centred on answering these four basic questions.

There are other alternatives to approaching the issue of making a contract manageable by an Information System through abstraction of a legal contract; one such method was investigated by Governatori and Rotolo (2004), who looked into applying RuleML (Grosof & Labrou, 2000) in order to make contracts electronically and autonomously manageable in an eCommerce environment (Governatori & Rotolo, 2004). The use of RuleML allows the automatic management of contracts by computers since RuleML is an executable language which allows the expression of business rules as nuclear, stand-alone units (Governatori & Rotolo, 2004). RuleML has the ability to identify and solve conflicting clauses in a contract through the 'priority' facility; this is a property that determines how much priority a given rule has. Thus, through this quantitative property RuleML can determine which rule takes priority over which other rule, thus resolving conflicting rules.

Governatori and Rotolo (2004) started their work by being aware that RuleML had some noteworthy limitations for its intended use. The limitations they identified are the fact that RuleML "does not support explicit reasoning on deontic concepts and is unable to identify the behaviour of roles in the contract and contract violations" (Governatori & Rotolo, 2004). Therefore, Governatori and Rotolo realised that RuleML can not handle the concept of obligations and permissions, nor is it capable of understanding the concept of

'role', all of which are key concepts (Which party is responsible for delivering the goods? What data does that party have access to? Which are the parties?) in a contractual environment and therefore must be grasped by an Information System if it is expected to support the execution and management of contracts.

Another limitation identified by Governatori and Rotolo (2004) is the absence of facilities aimed at dealing with contract violations. RuleML has no provisions on how to respond to an event that causes a breach of contract. Since the usage aim of RuleML is to be the autonomous management of contracts, such facilities must be implemented in order to deal with such a situation.

Governatori and Rotolo overcame these limitations by proposing to add two new elements to RuleML, namely `<Obligation>` and `<Permission>`, which thus add representation of the deontic notions of obligation and permission (Governatori & Rotolo, 2004). In other words, Governatori and Rotolo managed to extent RuleML such that it can represent the necessary deontic concepts that are a key element of any business contract. This will allow the extended RuleML language to deal with contracts more accurately, as it will be able to determine what obligations and permissions exist in a contract.

In terms of the limitations identified in facilities dealing with contract violations, Governatori and Rotolo recommend to replace the `<head>` element with a `<Behaviour>` element, which contains a range of `<Obligation>` and `<Permission>` elements in order to be able to pin down the accuracy of the contract and thus be able to explicitly express a rule violation, which gets triggered through the omission of an obligation (Governatori & Rotolo, 2004). Through this extension, RuleML thus has the ability to identify rule violations and thus the ability to act on identified rule

violations. These extensions make RuleML usable in the environment of autonomous, automatic contract management.

Governatori and Rotolo (2004) realised that with these extensions, the methodology for using RuleML for contract management was slightly changed. They proposed a new way of reasoning about contracts and using RuleML for this purpose, which can be summarised in the following steps:

1. Transform a natural language contract into its logical representation
    a. Extract facts, definitions, normative rules
2. Apply Introduction Rule until no further rules can be derived
    a. Might produce redundant rules
3. Discard redundant rules
4. Feed result into RuleML engine to execute or monitor contract performance

Adapted from: Governatori and Rotolo (2004)

Thus Governatori and Rotolo (2004) provided a methodology that can be used to apply the extended RuleML to autonomous contract management by IS. One drawback in the described method is the potentially computational extra cost of step 3 – further research in this area might result in a more advanced method for step 2 which could automatically detect redundancy and remove redundant rules as they are encountered, thus negating the need for a separate step dedicated to redundancy.

This section introduced some of the current research in the area of legal contracts, abstractions of legal contracts and the subsequent use of the analysed material obtained through the abstractions performed. Different methods were introduced, such as executable languages and Rhetorical Structure Theory. The work of prominent researchers in this field was presented and thus it was shown how legal contracts can be abstracted and modelled for better understanding. It should be noted that there is a lot more research going on in this area, however, the work presented in this section is

some of the most prominent and significant one due to the closeness to this research.

2.2.3 Process Modelling Approaches

The area described as 'Modelling' (sometimes spelt as 'modeling') describes a different research approach to the ones described above. This research approach looks at using or extending an existing Business Process Modelling Language in order to include and describe legal concepts. Whilst in the previously described sections the abstraction of legal concepts was merely the first step in gaining an understanding of the legal concepts, the abstraction is the main research focus of this approach. That is, research in this area attempts to *maximise* understanding through the abstraction, rather than trying to get sufficient understanding for a secondary purpose other than mere understanding, such as engaging in legal arguments.

One noteworthy research strand is the one pursued by Knackstedt et. al. (2006), who researched how to take into account legal requirements when designing eBusiness web applications. Their case was built around the fact that if the legal requirements are not taken into account sufficiently in eShops, the re-engineering of these applications might be very costly. Therefore, they argue, it would be much more efficient and beneficial to the client and the developer to take into account the legal requirements as the eShop is being developed in order to avoid costly re-engineering in a later phase of the project (Knackstedt et. al., 2006). One of their key propositions is to force the developers to take into account the legal requirements and legal position of their customers as well – this requires the capture of legal requirements during the planning phase of a project, rather than receiving legal advice after a prototype version is finished, which is the current business practice (Knackstedt et. al., 2006). In order to allow the capture of these requirements, Knackstedt et. al. recommend the addition of a process view

for both developer and client for the three major development phases –
analysis, design, and post-design (Knackstedt et. al., 2006).

This additional process view, according to Knackstedt et. al. (2006), allows a
developer to take into account all necessary legal requirements that occur at
the various stages of the project, such as privacy and data protection laws
during the analysis phase, copyright laws, the inclusion of a contact page
during design, and final checks through lawyers of the documentation and the
completed application. Knackstedt et. al. (2006) use examples of German
eCommerce legislation to point out what needs to be taken into account when
developing a web application, but their views are still very valid as most
countries have similar legislation that needs to be taken into account when
developing such web applications. Minor issues, such as should a radio button
or check box be active when a page is loaded (known as the difference
between 'opt-in' and 'opt-out'), must also be addressed at one stage during
the development process. Their overall requirements for a process modelling
notation for legal requirements capture can be summarised as follows:

- Must provide both internal and external points of view
- Must provide information on data views and data operations
- Must provide information on actuality of content
- Must provide information on whether external links require special
  annotations[3]
- Must provide information on activity fields (e.g. should a radio button
  be marked when the page is loaded?)

Adapted from: Knackstedt et. al. (2006)

This legal requirements capture, in order to be performed by developers,
requires a special modelling notation in order to assist a developer with the
capture of necessary legal information. To this end, Knackstedt et. al. (2006)

---

[3] In German law, the content of external websites becomes liable to a website owner, unless
a clear statement is provided that states the website owner is not responsible for the content
of external links

developed an extension to the eW3DT construct, developed by Arno Scharl (1998), since eW3DT was the only description methodology that met the requirements Knackstedt et. al. (2006) had set (other methodologies considered were Araneus, WebML and OO-H) for the capture of legal elements. However, even though eW3DT met many of the requirements set by Knackstedt et. al., it still required some extensions in order to capture all legal aspects that might affect a web application. Knackstedt et. al. (2006) therefore developed the following extensions:

- Internal View: eW3DT was integrated with the process modelling technique (e)EPK in order to connect content, data, maintenance and data use functions
- Data view and Data operations: integration of data structure views in eW3DT and Enterprise Resource Planning notation in order to gain a greater understanding of data views.
- Actuality: addition of information on maintenance intensity, specifying the maximum age content can take
- Input fields: mechanisms for input are represented by the information object "interaction" within eW3DT. This was extended to include information on the selection status (e.g. "active")

Adapted from: Knackstedt et. al. (2006)

According to Knackstedt et. al. (2006), these extensions make eW3DT compliant with the requirements they had set in their research. One requirement that has apparently not been addressed is the requirement of having to make special annotations to external links – an extension is not required, since eW3DT already has such facilities in its original specifications. The same can be said of the requirement of having to have an external view. Regarding data actuality, it should be noted that eW3DT provides primitive facilities to represent this requirement, which do not meet the requirements' needs fully. eW3DT provides information on maintenance intervals, but does not explicitly state how up-to-date data has to be.

With these extensions, Knackstedt et. al. (2006) managed to provide a development based framework to capture legal requirements in (web) systems design. The modifications of eW3DT means that web developers can use the methodology to not only develop a robust web application, but a web application that is also in line with legal requirements posed on it. The adaptation and extension of eW3DT is key to this ability, as in its original form it is not capable to provide this information. This is therefore a good example of research which has modified a process modelling notation for the purpose of the modelling of legal requirements.

Similar research with a similar aim is Sijanski and Münch (2006) focusing on the question on whether Business Process Modelling (BPM) was actually suitable at all for modelling legal procedures. As part of the EC funded IST-IP project (IST-2002-001567) "eJustice", they firstly looked at what possible benefits might be given by BPM to the legal sector in general. The two key benefits identified were the "opportunity to optimise legal procedures" (Sijanski & Münch, 2006) and the opportunity to arrive at a better understanding of legal workflows through their visualisation (Sijanski & Münch, 2006).

These benefits were investigated and Sijanski and Münch found that as far as process optimisation goes, "legal proceedings must always take second place to protecting rights" (Sijanski & Münch, 2006). That is, whilst process re-engineering in the commercial sector aims to reduce usage of resources and maximise value, process re-engineering in the judicial sector has to take into account that the process, as laid out by the law, may not be modified. Furthermore, legal workflows are not aimed at efficiency or profit maximisation – they are aimed at protecting a citizen's rights. Therefore, the requirements of the law and the rights of the citizen must always supersede the possibility of efficiency gain through process re-engineering and subsequent legal or rights violations.

Regarding the other benefit of increased understanding of legal workflows, Sljanski and Münch found that increased transparency offered several benefits. Firstly, they looked at cross-border implementations of BPM representations of law in other European research and realised that because of the differences that exist in the areas of "language, legal culture and legal systems" (Sijanski & Münch, 2006), which are further amplified in a cross-border environment, the graphical and "descriptive quality of a [business process] model" provides a language-independent overview over a legal process and might thus greatly enhance the understanding of legal processes, especially in the cross-border domain (Sijanski & Münch, 2006). Another advantage that comes with increased transparency is the fact that transparent legal procedures will "[increase] citizens' confidence in the legal system" (Sijanski & Münch, 2006), as it allows the citizen to see for himself in a clear, concise and visual manner how a legal process ought to function.

With these advantages identified, Sijanski and Münch (2006) went about defining some requirements that a BPM notation in the legal environment ought to meet. Their defined requirements are summarised in the following list:

1. Modelling of starting and finishing points through statute description, without relying on the statute description alone to define a process
    a. Since statutes provide only a rough description of processes, it must be understood that courts themselves will have their own, individual way of organising the statutes
2. Organisational model of a particular judicial authority
    a. Including actors, roles and their attributes
    b. Including how which actor becomes involved at which stage
3. Modelling of non-statutory events, e.g. document flow
4. Other contextual information, including temporal aspects, that are not captured in words

Adapted from: Sijanski & Münch (2006)

Through these requirements, Sijanski and Münch (2006) realised that a model of a judicial workflow will be extremely complex and their research focus then shifted to hiding some of this complexity, without simplifying the process description too much so that the abstraction would become useless. Their approach resulted in the implementation of hierarchies, which "differentiate the degree of detail of a function through using different abstraction levels" (Sijanski & Münch, 2006). This is a well-established method in business process modelling known as sub-processes. Sijanski and Münch (2006) recommend that "the number of the abstraction levels should not exceed ten" (Sijanski & Münch, 2006). The use of hierarchies will therefore allow a very general birds-eye overview of a legal procedure, whilst at the same time provide facilities to focus on a particular detail of a process. This aids the benefit of increased transparency stated earlier.

Sijanski and Münch (2006), in order to further facilitate understanding of legal procedures, recommend the use of modules. This concept borrows the computer science concept of reusability in object-oriented programming, where little units of activity that are repeated often can be re-used in larger, more complex operations (Lethbridge & Laganiére, 2001). Examples from the legal environment can be "the sending of a document" (Sijanski & Münch, 2006) or "examination of witnesses" (Sijanski & Münch, 2006). Thus, through re-use a lot of model creation work is saved since many legal procedures include similar operations. Thus, the use of modules will greatly increase the speed at which models of legal workflows can be created.

Sijanski and Münch (2006) thus put these recommendations into practise and implemented several judicial workflows in ARIS. A prototype application, called Lexecute, was created and demonstrates a process in UML describing a legal process within the ARIS suite. This prototype is on the web and can be found at http://rechtsinformatik.jura.uni-sb.de/ejustice/lexecute (accessed on

10/01/2007). The prototype shows how Sijanski and Münch (2006) implemented their recommendations and how a BPM representation of a legal process looks like in ARIS.

A similar approach was taken by Mercatali et. al. (2005), who used UML to decompose regulatory text, created UML class models to accurately model the relationship between the various statutes and sub-statutes, and then used the model to 'recompile' the regulatory text into meaningful legal text using their developed prototype. Thus they were able to demonstrate that it is possible to have an Information System 'recognise' legislative text and, conversely, to support the validation and verification of legislative text, as a model would quickly indicate potential missing links and similar defects. This shows that it is possible to 'consume' legislative text using established graphical process modelling notations.

Further research into this area was conducted by Giblin et. al. (2005), who developed a notation loosely based on UML called 'REALM' (Regulations Expressed as Logical Models) as a response to increasing regulatory pressure on processes and procedures. Giblin et. al. (2005) used UML as a basis to create REALM models that capture legal restrictions, provisions and similar regulations such that permissive and prohibitive regulatory enforcement can be applied autonomously. To achieve this, the REALM models can be used to control and program high-level policies (e.g. Data Retention Policy, Privacy Policy, Access Control List) which in turn regulate the operation of Data Stores; other uses are for the REALM models to be included in Process Execution Engines and make decisions in a process, and they can even be used to govern Correlation Rules in a Correlation Engine. In other words, graphical REALM models are used as a computational tool used to govern an organisation's IT infrastructure to enforce regulatory compliance on a variety of levels.

The above research streams have demonstrated how it is possible to represent judicial workflows and knowledge with business process modelling languages. In order to adapt a BPM notation to this specific area, slight modifications were necessary, which did not detract from the conclusion that BPM notations can indeed be applied to the legal environment. Especially the applications of ARIS and UML are an important piece of research to consider, since ARIS (and UML even more so) are a popular modelling methodology that were applied to an area that they was not originally intended for. This shows that it is possible to apply modelling methodologies to the area of modelling legal workflows and that further work ought to be undertaken in this area, since the judicial area can only benefit from these visualisations and increases in process transparency.

The above sections provided an overview over some very relevant research being conducted in the area of legal workflows and their enabling for automated and autonomous use. A major outcome of all of this research is that a greater understanding of law itself is required before attempting to enable it for computer use, therefore a lot of effort is aimed at making legal concepts accessible to computers.

2.2.4 Other Approaches

For example, Borges et. al. (2003) attempted to use Artificial Neural Networks in order to arrive at a system that is capable of performing legal analysis and make a legal decision autonomously. Their research was remarkably successful, since it revealed that their neural network not only arrived at the same outcomes as legal experts, but that even individual neurons categorised legal sub-areas in similar manners as legal experts had done. This remarkable research shows that it is possible to implement automated decision systems in the legal environment and future research ought to be aimed at refining this approach, since initial results seem very promising indeed.

On the other hand, Graca & Quaresma (2003) attempted to deal with a different problem, namely how can a computer keep up with continuous changes in legislation? In their paper, Graca and Quaresma (2003) apply dynamic logic programming in order to dynamically update a knowledge base of legal rules, implemented in an Expert System. Their results show promise that this is possible, however, if Borges et. al. (2003) research into Neural Networks continues to show such remarkable results, it is doubtful that Expert Systems will become widespread in their use. This is because Neural Networks offer much greater flexibility by being capable of learning.

Other noteworthy research is the research conducted in Jouve et. al. (2003), where it is attempted to arrive at a semantic model for creating hierarchies and descriptions of legal documents.

2.3 Summary

The above sections provided an overview of some very relevant research being conducted in the area of legal workflows and their appropriateness for automated and autonomous use.

In summary, the following table shows the key authors, their key research and the relevance to the research discussed in this document.

Names	Research Area	Relevance to Digital Signature Policies
Bench-Capon (2002)	Legal Arguments, Analysis of courtroom argumentation	Gaining an understanding of the legal area and translating it for Information Systems
Daskalopulu (2000) Bons, Lee, et. al. (1995) Governatori and Rotolo (2004)	Contracts	Representation of paper documents in a digital environment Application of contractual bindings in a digital environment Visual representation of documents
Sijanski and Münch (2006) Knackstedt et. al.	Process Modelling Languages in Law	Applying Business Process Modelling Notations to represent Legal Facts electronically

(2006) Giblin et. al. (2005) Mercatali et. al. (2005)		Representation of Legal Acts in a sequential manner Using Business Process Modelling Notations to enforce regulatory compliance. Using Business Process Modelling Notations to decompose, construct and analyse regulatory text.
Borges et. al. (2003) Graca and Quaresma (2003)	Neural Networks and Legal Disputes	Digital systems being aware of Legal Facts and acting on these facts' basis
Jouve et. al. (2003) McCarty (1989)	Semantic Modelling of Legal Documents	Understanding legal documents and their semantics; Legal knowledge representation language

Table 2-1: Relevant Research strands

A major outcome of all this prior research is that a greater understanding of law itself is required before attempting to develop computer supporting tools. This has direct relevance for this research, as it shows that it required this research to undertake analysis in understanding the legal issues surrounding DSPs, something that was demonstrated in the previous chapters. Furthermore, it was demonstrated that it is feasible to employ Business Process Modelling techniques to the legal domain and that *understanding* of legal documents and legal understanding of the *meaning* of the documents can also be mapped using various IS tools.

Furthermore, it has been noted that there is a distinct lack of literature on the subject of DSPs, including literature on authoring DSPs out of existing legislation and automating this process. Clearly, in an environment where DSPs are an important technology, their creation is a significant aspect and the literature review has revealed that there has been limited research into this area where DSPs are concerned. Therefore, the most significant outcome of this literature review is the understanding gained of how legal knowledge can be imparted on Information Systems.

The importance of the presented results by other researchers is highlighted by the research aims of this research:

- To develop a method enabling individuals to convert natural language legal acts and convert those to process models
- Tools and methods to convert the process models into a codified form
- Produce standards-compliant signature, evidence and archival policies (adhering to ETSI TR 102 038)
- The developed method should allow transformations in a structured and repeatable manner

This section has introduced a number of tools, techniques and methods that tackle various aspects of the above research aims. Bench-Capon's research describes tools and methods that 'teach' an IS about legal information and provides sufficient information to the IS to allow it to make judgments on the basis of legal facts. Daskalopulu has introduced techniques and tools that allow an IS to 'understand' a contractual document and the legal information encoded within it. Bons, Mercatali, Giblin and Sijanski have all demonstrated tools and methods to represent legal information graphically and permit an IS to peruse this information. In other words, the researcher has assessed a number of different tools, techniques and methods that could be used to help achieve the above research aims.

3 Research Design

According to Gray (2009), Research Design is "is the overarching plan for the collection, measurement and analysis of data" (Gray, 2009; p.131) and thus describes the techniques of collecting and analysing data. In other words, it describes the theory that is behind the methods chosen for the research, which techniques were applied and how these methods and techniques were applied in order to find a solution to the research question stated in the Introduction of this document.

3.1 Epistemology

When performing a research project, it is pertinent to be aware of the researcher's understanding of knowledge and truth. Any researcher has to pose what Curd and Cover (1998) call "philosophical questions about science", which provide both the researcher and the reader of research with an understanding on how the researcher posits himself amongst the various philosophical views and thus how the researcher's understanding of knowledge is formed. Through this understanding, it is possible to follow the researcher's approach to performing the research and interpreting results, and it is through this understanding that one can make a judgment with regards to the validity of the conclusions and their consistency within the researcher's *weltanschauung* (Lincoln & Guba, 1985), which literally translated means "View of the world" and, according to Lincoln and Guba (1985) represents the researcher's philosophical position and understanding of knowledge. Gray (2004) established that a research project consists of six elements that are hierarchically related from top to bottom as follows: Epistemology, Theoretical Perspective, Research Approach, Research Methodology, Timeframe and Data Collection Methods. Gray (2004) stipulates that the choices at the upper levels of the hierarchy inform the choices at the lower end of the hierarchy, meaning that a particular choice of Epistemology will determine the type of Research Methodology and Data Collection Method

a research project may use if it aims to produce meaningful and consistent results (Gray, 2004). This chapter will explore the themes of Epistemology and Theoretical Perspective of this project.

3.1.1 Background on Epistemology

3.1.1.1 Hierarchical View

Before one can investigate the meanings of Epistemology and the effects it has on a research project and the analysis of its results, one must first be aware of certain terminology and the precise meanings of common terminology employed in Philosophy. A key word is ontology, which Gray (2004) defines as "the study of being...the nature of existence...ontology embodies understanding *what is*" (Gray 2004, p.16, emphasis in original) and he proceeds to identify two opposing positions that go back to Ancient Greece. In the 5th century BC, philosophers Heraclitus and Parmenides argued about the nature of reality and the former regarded reality as "a changing and emergent world" whilst the latter regarded reality as "a permanent and unchanging reality" (Gray 2004, p.16). These are known as *becoming* and *being* ontologies (ibid.; emphasis in original). These ontologies determine a variety of epistemologies and their meanings. Gray quotes Crotty (1998) when grouping Objectivism, Constructivism and Subjectivism as three different Epistemologies which follow the two ontologies introduced above (Crotty, 1998).

Gray (2004) defines Objectivism to mean that "reality exists independently of consciousness – in other words, there is an objective reality 'out there'" (Gray 2004, p.17) and places it within the *being* ontology, whilst Constructivism is defined to mean "Truth and meaning do not exist...but are created by the subject's interactions with the world" (ibid.) and is also placed within a *being* ontology, whilst in Subjectivism "meaning...is imposed on the object by the subject" (ibid.) and this is placed in the *becoming* ontology.

Gray (2004) then states that a Theoretical Perspective follows from an Epistemological perspective and that there is a link between what Theoretical Perspective can be placed within a certain Epistemological perspective; he states that a Positivistic perspective is most logical for someone adopting an Objectivistic epistemology, whilst Interpretivism is a likely choice of perspective for someone following the Constructivist epistemological position.

Thus, Gray creates a definition and classification of different philosophical positions that can not only be grouped, but which also contain a top-bottom hierarchy, with the Epistemological view dictating the choice of Theoretical Perspective, and thus choice of Methodology and Research Methods. This view is supported by Kumar (2005), who shows that different research approaches all have "their own values, terminology, methods and techniques" and that researchers therefore ought to "adhere to [the paradigms'] values" since "the application of these values to the process of information gathering, analysis and interpretation" all constitute vital parts of the "research process" (Kumar, 2005). Out of this follows that depending on the philosophical position chosen, distinct avenues of research are opened and others closed. Other noteworthy authors stating ideas similar to the above are McNeill (1985), who states that "A ... theoretical perspective will guide the...research method adopted", showing how resolving one's theoretical and philosophical stance will directly influence the research methods (and thus the data to be collected and mechanisms to evaluate it) adopted later when the research is conducted. The view that looking into philosophical issues and taking a philosophical stance is augmented by Easterby-Smith et. ai. (1991), who states the three benefits of resolving one's research philosophy are:

1) It can help to clarify research designs
2) It can help identify limitations and advantages of research designs
3) It can help the researcher identify, and perhaps even create, designs that the researcher has not personally encountered before

(adapted from p. 27 in Easterby-Smith et. al., 1991)

This view is rounded off by Golinski (1998), who paraphrases Rouse (1987) when he explains Kuhn's (1962/1970) underlying philosophical principles that "science is governed by a logical structure of theory, a worldview or Weltanschauung", thus furthering the argument that the idea that the choice of philosophy influences the choice of research method, research tools, analysis techniques and other elements of research is widespread amongst researchers and that these interconnections between the various research elements are supported by a "logical structure" (Golinski, 1998).

Such a grouping and hierarchy of perspectives risks introducing intellectual barriers that allows for absolute statements, such as "If you are an Objectivist, you can't possibly be conducting Constructivist or Interpretivist research." Such statements can be restrictive when it comes to choosing appropriate research methodologies and are also in violation of philosophic principles – a key property of Philosophy is that ideas and views are debated and reasoned about (e.g. Plato's "Dialogues", such as Gorgias, Crito or Meno), but absolute statements such as the above restrict the possibility for such debate. Indeed, McNeill (1985) quotes from Halsey et. al. (1980) and their position that "the choice of [research] topic must be influenced by values...but that such value-commitment should not stretch to the methods used" (Halsey et. al., 1980, quoted by McNeill, 1985), showing that whilst the above concepts may be widely accepted, they are by no means a universal view of science, research and truth.

3.1.1.2 Temporal View

A different approach to classifying views and theories on truth and knowing is chosen by Lincoln and Guba (1985), who chose the term *paradigm* to describe a set of beliefs and views. They define paradigm as "a distillation of what we *think* about the world" (Lincoln and Guba, p. 15, emphasis in original) and choose to group paradigms in a temporal fashion; consequently,

they identify three major periods in which inquiry and beliefs were conducted and held in distinct ways: prepositivist, positivist, and postpositivist (Lincoln and Guba, 1985; p. 15).

According to Lincoln and Guba, the prepositivist view was established by Aristotle and continued on up until the 17th century AD. The prepositivist view "took the stance of 'passive observer'" (Lincoln and Guba, 1985; p. 18) and this would remain the dominating view up until the 17th century, when people like Newton pushed science into the "active observer" (Lincoln and Guba, 1985; p.19) and thus into the positivist era.

Positivism, according to both Potter and Lincoln & Guba, "advocate[s] the use of the empirical physical science methods" (Potter 1996, p. 28) and was thought to initiate paradigm revolutions in areas as diverse as "ethics, religion and politics" (Lincoln and Guba 1985, p.19). In essence, positivism meant that "If something cannot be verified, it is non-sense by definition" (Potter 1996, p.29). Additionally, Gray (2004) states that in positivism, "the social world exists externally to the researcher, and that its properties can be measured directly through observation" (Gray 2004, p. 18), a view that is supported by de Santillana and Zilsel (1970). Furthermore, de Santillana and Zilsel (1970) talk about Comte's ideas on positivism (indeed, they state he coined the term; Santillana and Zilsel, 1970; p. 86) and that, in addition to the aforementioned properties of positivism, "*to know* meant *to foresee*" (emphasis in original; de Santillana and Zilsel, 1970, p.85), thus showing that prediction is another key element of positivism and thus also empiricism (de Santillana and Zilsel, 1970).

On the topic of verifying observations, Popper (1991) quotes Hume when stating that "even after the observation of the frequent or constant conjunction of objects, we have no reason to draw any inference concerning any object beyond those of which we have had experience" (Hume, quoted by Popper (1991), p. 42); Popper (1991) takes this statement as evidence

against inferring theories and knowledge "from observation statements, or rationally justified by them" (ibid.). Popper (1991) argues that observations depend on context and circumstance and that it is not possible to build a valid theory on the basis of repeated observations, especially if the context and circumstance do not change. Rather, Popper argues that theory *precedes* observation and that "the scientist consciously and cautiously tries to uncover in order to refute his theories with searching arguments" (ibid., p. 52); in other words, Popper (1991) states that meaning is only obtained if a theory is falsified through a single observation, since it is not possible to make sufficient observations that test a theory under all circumstances and thus doubt about the theories truthfulness will always remain. On the other hand, a single falsification-observation yields tangible meaning, in that it shows that the theory is not sufficient. Thus, Popper (1991) advocates the use of observation in order to not verify a theory, but in order to verify its falseness. Such criticism exhibits that certain philosophers and scientists were not satisfied with the positivistic stance and led to the formation of other philosophical approaches towards truth.

It is interesting to note that, despite the added 'requirement' of verifiability through empirical study, positivism is still based on a key concept of prepositivism – observation. One can thus see the evolution of the paradigms and the interconnection of these different eras.

This interconnection between these different eras of paradigms becomes even more evident in postpositivism, which Lincoln and Guba (1985) define as the "reverse" (ibid., p.29) of positivism. Lincoln and Guba (1985) quote Rom Harre (1981) in identifying the exact points in which postpositivism is the reverse of positivism, putting their point across as follows:

> "Where positivism is concerned with surface events or appearances, the new paradigm takes
> a deeper look. Where positivism is atomistic, the new paradigm is structural. Where
> positivism establishes meaning operationally, the new paradigm establishes meaning
> inferentially. Where positivism sees its central purpose to be prediction, the new paradigm is
> concerned with understanding. Finally, where positivism is deterministic and bent on

certainty, the new paradigm is probabilistic and speculative." (Lincoln and Guba 1985, p.30;
originally by Rom Harre, 1981)

From the above quote, one can make conclusions about what postpositivism entails:

- Postpositivism takes a holistic picture and does not simplify systems to the sum of their parts
- Postpositivism draws conclusions and meaning from observing and from analysing existing facts, rather than relying on formulae
- Postpositivism does not attempt to generalise and does not attempt to create 'Laws' that hold true at all times

Therefore, one can see postpositivism as a departure from believing in scientific laws that govern all systems and their interactions by a set of infallible laws, as well as a departure from the view that there is one single truth 'out there', waiting to be discovered. In fact, postpositivism seems to accept that humans are fallible, thus human 'discovery' of the world is fallible and therefore probability seems to be a more appropriate measure for understanding the outside world than absolute statements.

This is a view shared by Denzin and Lincoln (1998), who describe postpositivism as being associated with "much greater ambiguity" (ibid., p. xii) and state that features of postpositivistic approaches include the absence of "well-formulated hypotheses, tightly defined sampling frames...and pre-determined research strategies and methods and forms of analysis" (ibid.). Again, we see the attempt to decouple the rigidity of the scientific method and attempts to introduce the idea that not everything can be deconstructed to a set of laws and smallest constituents. It is recognition of the fact that the world might be too complex to be able to understood in piecemeal fashion and that a holistic view might be more appropriate. This is in line with Popper's (1991) earlier stated rejection of induction through observation, as this statement gives credence to Popper's (1991) views that because an

observation is true in one particular case, it is not plausible for this observation to be true in a different set of circumstances.

Gray (2004) has similar views when he paraphrases Crotty (1998) by stating that positivistic research will present its outcomes "as objective facts and established truths" (Gray 2004, p.18). He goes on to state that, as a result of social science challenging the stalwart nature of positivism, "we now inhabit a post-positivist world in which a number of alternative perspectives (for example, anti-positivist, post-positivist and naturalistic) have emerged" (Gray 2004, p. 20). He thus agrees with Lincoln and Guba, namely that postpositivism is the 'natural' successor of positivism and takes a more realistic approach to science by looking at systems holistically and not attempting to abstract and generalise on the same level as positivists would attempt to do. However, Gray (2004) notes that some aspects of positivism have been adopted and remain in use, especially where empirical inquiry is necessary. One such example is Graziano and Raulin's (1989) work, who outline a number of assumptions that are supposedly shared amongst scientists and try to use this as the basis for their book of empirical research methods in Psychology:

- A true, physical universe does exist
- The universe is primarily an orderly system
- This universe is knowable through human intelligence
- All knowledge is tentative

(Taken and adapted from Graziano and Raulin, 1989)

One can immediately see how these assumptions follow the positivistic framework, such as the reference to an external world that can be dissected by human knowledge.

3.1.2 Justifying Epistemological Choices

Whether one chooses to follow Lincoln and Guba's temporal approach to classifying paradigms of knowledge, or Gray's hierarchical approach to grouping paradigms hierarchically, it becomes evident that a researcher has to choose between a Prepositivist view based on Ancient Greek philosophical views, a Positivistic view or a Post-Positivist view; indeed, if adopting Gray's approach, one will then have to choose from a number of post-positivist approaches to research. Note that the emphasis here is on 'has to choose', since identifying and adopting a philosophical stance has wide-reaching implications for one's research, as identified earlier.

Adopting a Prepositivist view can hardly be justified, seeing how Positivism was thought of as a 'successor' to this view. The basic premises of Prepositivism of passive observation without interference are not likely to be helpful at all to this research study. There is no dedicated research team that will work on solving the research question in isolation and permit the researcher to observe their processes, methods and procedures. Neither is there any mechanism by which a method can create or improve itself and let itself be observed by the researcher. Therefore, the only real choice lies between adopting a Positivist or Postpositivist view.

Some key concepts of Positivism were introduced earlier and it is those concepts that render Positivism as not applicable to this IS research project. It was stated earlier that Positivism thrives on abstraction, by attempting to reduce complexity to smaller constituents. In this particular research project, however, the system is deeply interconnected with all of its parts to the extent where meaningful abstraction is not possible. Abstraction can be a useful tool in areas such as natural science, where 'building blocks' can be researched through the increased complexity of the research tools, but in this project one must take a holistic view of the system since an Information System, such as the one being studied in this project, does not consist of

identifiable basic building blocks and therefore abstraction will yield no useful results.

Furthermore, it was stated that Positivism attempts to generalise by creating laws that hold up in different areas; for example, Newton's Laws of Motion can describe both a tennis ball trajectory as well as the path of an iceberg. Such a generalisation is not applicable to this research as no generalisation is planned on being derived from this project – it is an investigation into a closed system with specific purpose, a feature that is generic to qualitative research in general (Gray, 2009). The research is going to be adapted to fit closely to the organisation's specific needs and to the specific needs of creating a Digital Signature Policy. It is not expected to be applicable to another organisation; there may be a small amount of generalisation possible, but only within the confines of a similar organisation facing similar issues in a similar setting.

Finally, Positivism stipulates that the researcher is an independent entity outside of the system to be studied. However, this project requires the researcher to use and modify the system being studied and to interact with the most important constituent of this system, namely the users; thus the independence is not given and instead researcher and system become interconnected. For the above reasons, it is therefore not feasible to adopt a positivist outlook for the current study.

The above paragraphs should not be taken to mean that Positivism as a whole should be disregarded as useful in any kind of IS research. The paragraphs merely aim to show that for the proposed study in the specific domain and for an inquiry under the specific restrictions placed upon the researcher, a Positivistic outlook is not viable. Other IS research may well benefit from a Positivistic inquiry and there are plenty of examples in literature where this is the case.

3.1.2.1 Constructivism

The previous section established that a Postpositivist paradigm would be appropriate, given the nature of the study in this project. One of the first perspectives discussed by Gray (2004) is Constructivism.

According to Golinski (1998), Constructivism became a "movement" (Golinski, 1998) that was incepted by Thomas Kuhn's "The Structure of Scientific Revolutions (1962/1970)", "much against its author's wishes" (Golinski, 1998) claims Golinski. The basic premise of Constructivism is that "The external world is a mental construction" (Landesman, 1997; p. 61) and therefore this represents a view that the senses can be deceiving and that what we see is not what 'is'. This view of the world was first formed by Descartes in his work "Meditations on First Philosophy" by saying "the senses occasionally deceive us with respect to objects which are very small or in the distance" (Descartes, 1984: p.12). Descartes goes on to state that the senses are unreliable altogether by saying "there is absolutely nothing in the world" (Descartes, 1984: p.16). Landesman (1997) interprets this to mean that Descartes "provided a reason for doubting the existence of the external world" (Landesman, 1997; p. 47). This approach would later be coined Skepticism (Landesman, 1997; p. 46, ff.).

The impatient reader prone to quick conclusions might therefore deduct that choosing a Constructivist point of view automatically results in the rejection of the existence of the universe, a rejection in the meaning of science, religion and a rejection of meaning itself since, apparently, it is all a figment of our imagination caused by unreliable sensory input from our senses. This deduction has been done before and it represents the school of Solipsism (Pfeiffer, 1966; Landesman, 1997).

Solipsism is a possible deduction of Descarte's Skepticism (as shown in Landesman, 1997; p. 50), but early ideas of Solipsism were actually formed in the 5th century BC by the Greek philosopher Gorgias, who stated that

"Nothing exists, Even if something exists, nothing can be known about it; and even if something could be known about it, knowledge about it can't be communicated to others" (Empiricus, 1961). This statement was arrived at by proving that elementary concepts, such as time, proof and mathematics do not exist.

However, this is a very extreme deduction which misunderstands what Descartes and other Skepticists were trying to say. The fact that our senses are not capable of giving us an accurate representation of the outside world does by no means exclude the existence of the outside world – in other words, there is in all possibility an outside world, but what Descartes and other Skepticists were trying to say is that we don't really know what this outside world is, due to our limited senses giving us false perceptions of this world. This is an unsatisfactory position that Kant called "a scandal to philosophy and to human reason" (Kant, p. 34), but Berkeley (1993) - according to Landesman (1997) - "did not deny the existence of matter...[but] the claim...that material objects exist independently of mind" (Landesman, 1997: p. 59, paraphrasing Berkeley (1993)). In other words, Berkeley (1993) saw a link between the existence of matter and the existence of matter within the mind, whilst at the same time applying "common sense" (Landesman 1997, p. 54) to sensory perceptions (and thus refuting Descartes (1984)). This view of the interaction between mind and matter is supported by Duffy and Jonasson (2004), who state that "Constructivism...holds that there is a real world that we experience. However...meaning is imposed on the world by us" (Duffy and Jonasson, 1992). Thus, Constructivism acknowledges both the existence of *a* reality, which is interpreted differently in people's minds as compared to how it actually exists.

An absurd side of Solipsism is that it can not be adopted by someone unless he reads about it somewhere, since humans need to obtain knowledge from some source; obviously, if no sources to gain knowledge from exist, a human can not have any 'useable' knowledge. However, by reading about Solipsism

one immediately acknowledges the existence of whoever wrote about Solipsism and thus invalidates one of the key aspects of Solipsism, namely that such an author providing such knowledge can not exist. Of course, a Solipsist might then retort that infancy and growing up and being educated were all imagination, but from a realistic point of view this is a *non sequitur* that is in no way helpful in viewing the world from a practical perspective. It is, however, an interesting logical problem to reason about Solipsism within the confines it sets – however, this is beyond the purpose and scope of this text.

Returning to Descartes and Constructivism, it is extremely ironic to note that natural science, long regarded as the stalwart of Positivistic world views (see Potter 1996, p.29 for example), the sole entity that was capable of describing the world 'as-is', provides us with data and information that supports the earlier mentioned view – namely, that the existing outside world functions and looks quite differently to how we perceive it.

Two concepts, which relate directly to our senses, show that our senses are not capable of understanding and describing the world as it is. Physics, for instance, tells us that the light and colours that we see are in fact non-observable waves of energy whose wavelength determines whether we see the colours blue, red and orange, or whether this 'light' actually has wavelengths that are so large that it crosses the air as radio waves and carries music, or that it has wavelengths so short that it is in fact harmful UV radiation that burns our skin (Adams & Allday, 2000). So from a Physics point of view, colours, UV radiation and radio waves are all the same phenomenon, yet our eyes are only capable of seeing colours and our eyes definitely do not see any waves 'carrying' the colour or representing the colour. Therefore, our senses fail to see that three apparently unrelated phenomena are actually the exact same one and they also fail to register the mechanism by which these phenomena manifest themselves – we are only capable of registering the effects by seeing colours, or by being burnt or by listening to the radio

without actually understanding where it all comes from, at least where visual sensory input is concerned.

Similarly, our ears also fail to pick up the 'sound' of ultrasound and infrasound noise. By definition, ultrasonic sounds are sounds which are beyond the upper boundary of our hearing range, whilst infrasonic sounds are sounds which are below the lower boundary of our hearing range (Adams & Allday, 2000). Whilst these sounds occur in nature, it is not possible for our ear to pick them up and therefore, they essentially do not exist to us. In order to make them exist for us, we need to develop theories which may or may not be accurate in order to explain the phenomenon of unheard sounds to ourselves – we construct meaning.

Taking this into account, one must also consider that different people have differing eyesight and hearing abilities. Some people even suffer from colour blindness and can not perceive colours in the same way as non-colour blind people can. It can therefore be said that due to their affected senses, they perceive the world differently than someone without colour blindness, or someone with better/worse hearing. In other words, the way the world is perceived is different for different people, in many cases this is down to their senses.

Apart from sensory input providing us with a 'distorted' view of the real world, we also need to take into account what Chia calls "unconscious metaphysics" (Chia, 2002). Chia develops an idea originally stated by Whitehead (1933), who stated that a person's cultural and social background determine a person's world view, and thus view of knowledge (Whitehead, 1933). Chia builds on this by saying that "Certain forms of knowledge are, hence, privileged over others in each historical epoch and cultural tradition" (Chia, 2002), thus indicating that there is a bias on a person's view born out of both cultural background and tradition, but also out of historical epoch and thus socially accepted world views. The logical conclusion, therefore, is that every

person is inherently biased, a view which is also shared by Chia, who states "Selective abstraction and interpretation are, thus, inevitable facts of the process of knowledge-creation" (Chia, 2002).

The above statement by Chia is even more evident when considering the following thought experiment: a normal person is walking down the road when he sees a green car pass by. The person, with limited knowledge of cars, will recognise it as a green car with two doors, a boot, and four rather large wheels. Further down the road, a car mechanic with a great deal of technical knowledge on cars is also walking down the road and sees the same car. However, due to his knowledge and experience, he will not see a green car with doors and large wheels – he will recognise the model and make, he will be able to tell what engine size and what fuel type is consumed by that car, he will know the specific sizes of the car's tyres, he will be aware of mechanical trouble spots, he will know technical performance data and he will know how much these cars cost. What this thought experiment shows is an extension of Chia's statement, namely that knowledge creation is dependent on selective abstraction and interpretation. Both the person and the mechanic saw a car, but they perceived it differently, they attached different meaning to their observations, even though the basic nature of the car was unchanged between the two of them.

Another point to consider is that bias and ambiguity are not just a result of sensory distortion. Meaning can also be agreed upon culturally. That is, a culture can arrive at a convention on how to use or regard a certain object, irrespective of the object's *nature* or physical properties. For example, it has been culturally been agreed that a plate is to hold food for one's consumption. The food, after having been cooked, is placed on it temporarily until it is consumed. However, this may well be the established cultural convention on how to use a plate, but it is not the only possible use for a plate. The nature of the plate allows the food to be cooked on a plate, or we may choose to use a plate to drink water out of, or we may choose to plant a

plant in the plate, or we may choose to employ plates as Frisbee toys, or we may employ plates as weapons or use them as covering up material for holes in walls. Any of these functions can be performed by a plate, but very few if any people employ plates in that fashion because cultural meaning was constructed that governs a plate's use as temporary food holder, to be eaten from. Thus, we have a case of cultural construction of meaning, which employs the plate in a specific manner, even though the nature of the plate permits other usages also (Seltsikas, 2007).

From a Constructivist point of view, therefore, traditional empirical research that is based on non-participatory observation can not yield valid research outcomes due to the inherent cultural and personal bias of a person and the unavoidable sensory distortion by the senses. This is a logical conclusion due to two simple facts: if the senses distort the view of the world, how can they be relied upon to deliver bias-free observation of an event – can we even trust the sensory input to deliver an accurate representation of how the event unfolded in reality? It has been shown how we can not trust our sensory input...and even if we could get a distortion free picture, our cultural and social and individual backgrounds will then distort this picture due to different ways of deducing and interpreting meaning from it. Therefore, the positivist form of research is not acceptable to a Constructivist thinker.

A Constructivist thinker will also discount Positivism from the angle of scientific validity. Scientific validity is a positivistic measurement and is linked to the positivist trait of generalisation, as hinted upon earlier. In other words, through validity a positivist researcher will measure how much can be generalised from his research work in order to arrive at a wide-sweeping law defining the behaviour of the research subject. However, in order to be able to achieve this, two requirements must be met: firstly, *a priori* knowledge must exist about the problem at hand, and secondly, the problem must be abstractable (Seltsikas, 2007). It has been mentioned several times that there is no suitable method to create DSPs, therefore *a priori* knowledge about this

problem is very limited. Also, the research will not attempt to abstract the problem to such a stage as to be able to determine external validity and therefore positivism is not a viable option from this point of view.

One final viewpoint to take into account is the one of axiology (Lincoln & Guba, 1985). Axiology describes the value system of a Theoretical Perspective and an axiological point relating to positivism raised earlier states that in positivism the researcher is considered to be independent of the system being researched; this, from the positivist point of view will result in the elimination of bias. However, as mentioned above, bias can not possibly be eliminated, so axiological reasons also result in positivism not being a viable option.

The adoption of Constructivism is further supported by various factors that exist within this research project. Firstly, the research is going to be conducted in the environment of CATCert. Chapter 4 will introduce more details about the research collaborators, but one distinctive feature of this organisation is the fact that the organisation has been involved in many initiatives that sought the definition of new Digital Signature standards. Therefore, the organisation has a high degree of competence in this field and this means that their views on Digital Signature Policies are going to be highly applicable to the researcher and will thus help the researcher to 'construct' an understanding of Digital Signature Policies and help construct a solution. Also, the research will need to consider the specific requirements of the organisation that have been stated. This means that the research will be conducted within the influence of a constructed social reality as it applies to CATCert, further evidence that Constructivism is applicable in this setting. Finally, Chia's concept of a 'distorted' view is also a factor that will apply in this research project due to the aforementioned high degree of competence in the client organisation on the topic of digital document security. In summary, plenty of reasons exist to suggest that Constructivism is a valid concept for this research.

Constructivism, in recognising all of the above restrictions on human understanding and knowledge, permits the use of research methods that work to overcome these restrictions. For example, it was stated above that in positivism the researcher and the system to be researched are separate entities. In Constructivism, they are interacting in order to allow the researcher to view the system from different angles, thus overcoming the restrictions placed on him by his senses and cultural and individual bias and thus providing the researcher with a clearer and more insightful picture than a positivist researcher. Thus, since positivism has already been discounted as an appropriate viewpoint for this research project, and since Constructivism allows for a holistic interpretation from many view angles, it can be regarded as appropriate for this research project.

3.2 Research Methodology

Research includes both practical and theoretical perspectives. At some stage during a research project, be it at the start, during or after the project, one needs to reflect on the theoretical aspects and perspectives of the project. Gray states that "Sometimes this will occur before undertaking the research (the deductive approach) and at other times after it (inductive)" (Gray, 2004). In the case of this research project, reflection on the theoretical perspective occurred once the research had gotten underway. Since this approach allowed reflection on a range of possible theoretical perspectives, the most appropriate one was chosen – therefore, the engagement with the theoretical perspective is thus in the realm of the inductive research approach.

3.2.1 Background and analysis of Research Methodologies

3.2.1.1 Quantitative vs. Qualitative Research

Though it has been established that this research is of an inductive nature, it does not necessarily determine the methodology to be used in the project. A methodology, according to Denzin and Lincoln (1998), "comprises the skills,

assumptions, and practices used by the researcher...when moving from a paradigm and a research design to the collection of empirical materials...[a methodology] connects researchers to specific approaches and methods for collecting and analyzing empirical materials" (Denzin and Lincoln, 1998, p. xv). Potter also states that "Methodologies are based on assumptions that researchers must hold..." (Potter 1996, p. 23) As can be seen, this implies that the research has to be performed in an organised manner that corresponds with the researchers' views on epistemology. In other words, the methods employed must match the methodology chosen, all of which must match the theoretical outlook and epistemology views that the researcher has. However, before being able to choose a methodology, the type of research must be established. There are two major paradigms in science: qualitative and quantitative research. There are different methodologies for both types of research, therefore before choosing a methodology, the type of research must be determined.

Creswell defines qualitative research as follows:

"Qualitative research is an inquiry process of understanding based on distinct methodological traditions of inquiry that explore a social or human problem. The researcher builds a complex, holistic picture, analyzes words, reports detailed views of informants, and conducts the study in a natural setting." (Creswell, 1998)

As can be seen, Creswell states the importance of the use of methodologies to perform an inquiry into a problem. More importantly, there is an emphasis on analysing words, thus hinting on the type of data to be encountered in qualitative research. Also, the fact that a "holistic picture" is mentioned, points towards a view that the research ought to examine the problem in its entirety, that is the research should not only focus on causal relationships, but also on the effects of the problem on other entities, the problem should be placed within a wider picture of events, effects and interactions. Finally, Creswell mentions that the research is conducted "in a natural setting", which indicates that laboratory experiments with theoretical and practical confines are not satisfactory settings for a qualitative study. It instead indicates that

the study must be performed within full influence of the environment in which the problem exists.

On the other hand, quantitative research was described by Kerlinger as "hypothesis-testing research" (Kerlinger, 1986) and this is substantiated by Newman and Benz (1998), who state that in quantitative research one begins with a theory statement around which a research hypothesis is formed. They then state that experiments are designed to test a sample for the hypothesis and the resultant data is then analysed using statistical methods (Newman and Benz, 1998). According to them, quantitative research is "deductive in nature, contributing to the scientific knowledge base by theory testing" (Newman and Benz, 1998). Thus, they agree with Kerlinger's view.

3.2.1.2 Justifying the Qualitative Research Approach

Based on the above definitions, it can therefore be said that the project is of a qualitative nature for a variety of reasons. Firstly, it was stated earlier that the theoretical engagement is being performed inductively. This precludes the possibility of the research being deductive in nature; Furthermore, there is no specific hypothesis that is to be tested for its validity. The project aims to not find out whether there is a methodology by which legal processes can be turned into executable code; instead, it is assumed that there is indeed a methodology by which this can be achieved and the onus of the project is therefore to develop this methodology. The fact that this process already exists, albeit in an awkward and non-systematic manner, hints towards the research aims being possible to achieve. In other words, there is no hypothesis requiring to undergo validity testing. Also, if one looks at Creswell's definition of qualitative research again, one finds the requirement for the study to be performed in a natural setting. This study is going to be conducted in as close a natural setting as permissible. The research will analyse existing tools and methods, stakeholder feedback will be elicited and analysed against the stakeholders' current working processes and the expected new methods to be developed are going to be adapted to fit within

the stakeholders' environment, honed towards handling DSPs. The stakeholders will be involved in evaluating the end results. In other words, this research is being conducted in a natural setting. Creswell also states that a qualitative study paints a holistic picture and analyses words; again, this is evident to occur in the project through the fact that the holistic picture is the entire system between extracting information from legal texts and the creation of the associated DSP. The research will aim to create methodologies that cover this entire flow of information, therefore a holistic picture of the Digital Signature Policy creation process is indeed being painted here. Also, due to the nature of law the analysis is focused on words and their meaning and how this meaning can be conveyed through computer code. Finally, it was stated earlier that Gray (2004) presents a hierarchy where certain data collection methods are dependent on specific choices in Research Methodology and Epistemology. The previous chapter stated that this research is being conducted from the Constructivist viewpoint. Therefore, referring back to Gray's (2004) hierarchy, Constructivism excludes Research Methodologies and data collection mechanisms which are positivistic in nature. In conclusion, there is plenty of evidence to suggest that this is indeed a qualitative research project.

3.2.1.3 Qualitative Research Methodologies

Having established that the research is qualitative in nature, the next step is to identify which research methodology would be best suited to this project. Creswell identifies five qualitative methodologies that represent a "representative picture of approaches in the disciplines" (Creswell, 1998) and because they "have been discussed recently in qualitative books" (Creswell, 1998). Creswell also states that he does not wish to exclude other worthy approaches; his approach makes sense since there is indeed a multitude of approaches out in the field and summarising and describing them all would be a mammoth task which would fill several books. His attempt is therefore to not paint a representation of all available methodologies but to highlight

methodologies that are quite different from each other to the extent that a particular research project would have clear preferences over choosing one of these methodologies over another.

Creswell chose to present and demonstrate the following methodologies: Biography, Phenomenology, Grounded Theory, Ethnography and Case Studies.

According to Creswell, Biography is rooted in History and Sociology and it focuses on a single individual. Biographical studies perform their data collection through conversations, observations and through story telling. Typically, the study will focus on a special event in an individual's life and the study will attempt to interpret the meaning of that special event. It is typical of a Biographical study to then attempt to relate that meaning to existing literature on similar themes and the study is usually concluded with a section on lessons learned. Creswell defines the methodology with the words "the study of an individual" (Creswell, 1998; p. 39).

Creswell opines on Phenomenology that it has a base in the disciplines of Psychology and Philosophy. Creswell identified that the typical approach in a Phenomenological study is for the researcher to first identify a central issue and then to propose a causal investigation of that issue. Typically, the Phenomenological researcher will perform a literature review on the philosophical perspectives of his phenomenological approach before focusing on the actual study of the phenomenon. Throughout the duration of the study, the researcher will attempt to not let his preconceptions affect his study. There is a variety of specific Phenomenological data analysis steps that are to be performed in such a study and once this is complete, the researcher will reflect and interpret the results of the data analysis within the confines of the philosophical base established earlier in the study. According to Creswell, Phenomenology is "the examination of the meaning of experiences toward a phenomenon" (Creswell 1998, p. 39).

Creswell describes Grounded Theory as having originated from Sociology and that it contains a very systematic and rigorous approach. Typically, Grounded Theory studies contain a visual model, a coding diagram and a conditional matrix in order to describe the study better. These studies are very construct and category oriented and Grounded Theory research usually involves the search for both corroborative and disconfirming evidence. Creswell sums it up quite simply by saying Grounded Theory deals with "the generation of a theory" (Creswell 1998, p. 39).

Ethnography is identified to have originated from Anthropology and Creswell states that this type of study is typically very descriptive and contains a high level of detail in both analysis and interpretation. Furthermore, one of the key aspects of an Ethnography is that there is always an exploration of some kind of cultural theme (Creswell mentions role and behaviour as examples) and that the study usually concludes with a new and reflective research question. Creswell interprets Ethnography to be about "the description and interpretation of a culture-sharing group" (Creswell 1998, p. 39).

Finally, Creswell lists Case Studies as being prominent in the human and social sciences, and evaluation research in particular. Creswell quotes Lincoln and Guba (1985) when describing that the structure of a Case Study contains the statement of the problem, the context of the problem, the issues to be examined and finally the lessons learned. Creswell also notes that in a Case Study, the data collection utilises multiple sources. In other words, Creswell concludes that a Case Study is an "in-depth study of a single case" (Creswell 1998, p. 39).

These are Creswell's five methodologies that he examined and proposed different criteria for choosing amongst them. Creswell himself notes that this is by no means a comprehensive overview, therefore in order to get a greater understanding of qualitative research methodologies, some methodologies

identified by Potter (1996) will also be introduced. Potter (1996) attempted to achieve something similar to Creswell, namely to provide an overview over how qualitative research can be conducted, what methodologies one can choose to employ and how to handle the choice between the different methodologies. Potter chose to introduce seven different methodologies and the ones he chose to introduce and present are: Ethnography, Ethnomethodology, Reception Studies, Ecological Psychology, Symbolic Interactionism, Cultural Studies and Textual Analysis. Unlike Creswell, however, Potter makes a very strong statement with regards to the methodologies chosen by saying that "these seven are currently the dominant ones – the ones you will see time and again when you read the work of theoreticians as well as the qualitative research itself" (Potter, 1996). In other words, he does not attempt to paint a representative picture and provide an overview of methodologies that span multiple disciplines. Instead, he chooses the dominant methodologies that are in popular and common use. As a result, Potter's list comes across as quite subject specific as opposed to Creswell's list, and an examination of the methodologies will reveal that this is indeed the case. The majority of Potter's methodologies are much more deeply rooted into their 'parent' sciences. In order to stress this difference, only two of Potter's seven methodologies will be introduced – Ecological Psychology and Textual Analysis.

Potter writes about Ecological Psychology that it is an approach which stems from Psychology, as the name suggests. In short, Potter states that unlike Psychology which is concerned with the effect of individual variables on human behaviour, Ecological Psychology focuses on "the pattern of influences [on human beings] in naturally occurring settings" (Potter, 1996). 'Naturally occurring settings' refers to social settings which one the one hand are natural to the subjects (e.g. an individual's living room) and on the other hand how different factors within that setting affect the subject. Potter states that "human behavior is affected by elements...such as physical properties...human elements...and programmatic elements" (Potter, 1996: p.

57). Traits of this methodology include data collection through observation, specimen records and surveys of behaviour. The data collection is inherently subjective (Potter, 1996).

On Textual Analysis, Potter states that does not focus on people as the creators of culture, but instead it focuses on the premise that texts (i.e. the written word) have an effect on cultural development. Lately, Textual Analysis has expanded to study television and the internet as a different manifestation of 'text' (Potter, 1996). According to Potter, this methodology evolved out of literary criticism and structuralist linguistics. According to Potter, the main data are the texts which, and he quotes Jensen (1991), "the analysis is performed primarily from a literary point of view (Jensen, 1991; quoted by Potter 1996, p. 63) using the analysis of discourse, narrative, genre and auter [sic] among others" (Potter, 1996).

3.2.1.4 Choosing the appropriate Research Methodology

Seven qualitative research methodologies have been presented. The author faced the difficult choice of identifying which one would be best suited to the research project. Each methodology introduced shall be examined axiologically and a decision will then be made on whether the methodology is suitable or not when mapped against the research.

Starting with Biography, it was stated earlier that Biographies are studies of individuals who have experienced a special event that requires interpretation. This methodology is therefore inappropriate for this research project since the project does not focus on individuals and their experience of a specific phenomenon – the project is about the development of a methodology for turning legal texts into executable code, and the research investigates how the existing method of creating Digital Signature Policies can be improved, taking into account organisational restrictions. Therefore, Biography can not be considered as a viable methodology for the project as the emphasis of the study is not on individuals and their experiences of specific events.

Phenomenology was another methodology considered. Due to Phenomenology's base in Psychology and Philosophy, and due to Creswell's definition of "the examination of the meaning of experiences towards a phenomenon" (Creswell, 1998), this methodology must also be discarded as an alternative since it is concerned with in-depth study of a phenomena. There is some merit in looking at the issue of Digital Signature Policy creation as a phenomenon that warrants further in-depth study, but the aim of the research is not to fully study and understand the complete Digital Signature Policy creation process. Instead, the study aims to improve the process without necessarily studying it in-depth in its environment. As a result, the aims of the research and the aims of Phenomenology are not quite compatible and thus Phenomenology is not quite appropriate within this research setting.

Next, Grounded Theory was considered and there are some qualities of Grounded Theory that may make it suitable for use in this project. It was stated earlier that Grounded Theory is systematic and rigorous in its approach and that Grounded Theories are usually complemented by visual models. These are traits that are also present in this research project – the research is systematic and rigorous, as is evident from the split into three complementary work packages. Also, a visual model is utilised through the development of the graphical component of the methodology to be developed. However, this project does not employ a construct or category oriented approach, nor is there going to be a search for disconfirming evidence. Finally, Creswell defined Grounded Theory as "the generation of a theory" (Creswell, 1998). Stephen Hawking writes about the concept of theory that "any physical theory is always provisional, in the sense that it is only a hypothesis..." (Hawking, 1996). Therefore, if according to Stephen Hawking a theory is a hypothesis, then due to the earlier establishment of the fact that there is no hypothesis to be to be tested for validity in this project, there is also no theory to be established or tested within this project – therefore, the suitability of

Grounded Theory as a methodology for this project can not be established (as it is explicitly stated that Grounded Theory generates theories) and therefore Grounded Theory has to be discarded as a candidate methodology for this particular research.

Next up is Ethnography as a methodology to be considered. It was stated earlier that Ethnography deals with the exploration of cultural themes and that Ethnography is "the description and interpretation of a culture-sharing group" (Creswell, 1998). The fact that there is a mention of culture and groups hints towards the fact that this methodology is also concerned with individuals and the way they combine to form a group and a culture. This is a useful methodology for research involving the interaction between culture and IS, and in particular on how certain cultures adopt IS use in comparison with other cultures. However, a group or culture are not the subjects of this study, nor is their specific interaction with the Digital Signature Policy process. Instead, the research concerns itself with the process itself; considering organisational restrictions undoubtedly requires the consideration of people's views and expertise too, but in an Ethnographic study the research concerns itself primarily with the people, not with what they use. As this research is focused on the creation of Digital Signature Policies, this methodology can therefore not be considered as suitable for this particular research.

Another methodology considered was Case Studies. Creswell defines it as an "in-depth study of a single case" (Creswell, 1998); for a Case Study, it must be absolutely clear on what the case is. Applying the stated definition to this research, the question is then: is it the organisation that the Case Study is based on, or is it the Digital Signature Policy creation process? The research does not consider either view. The research will not examine in detail all of CATCert's activities relating to DSP's and other technologies. Nor will the research attempt to study DSP's in detail in order to make the technology more accessible. The research will simply look at an existing process and attempt to improve it under certain organisational restrictions. It becomes

apparent that this methodology is unsuitable for this project as the research will not produce an in-depth study of a case and will not collect the rich data set normally associated with Case Studies. Therefore, there is no specific case *per se*, therefore Case Studies can not be considered as an alternative for suitable methodologies within this research project.

Ecological Psychology is another qualitative methodology that was described earlier as being considered as a methodology for the project. However, similar to Ethnography and Biography, Ecological Psychology is a methodology which deals with effects and influences on individuals and cultures in natural settings. However, this research has a reverse focus, in that it focuses itself on an effect and may consider some influence of individuals of the organisation on that effect (= the DSP creation process) but this is not the main focus of the study and therefore this methodology is not quite applicable to this research context.

This leaves Textual Analysis as a methodology to be considered for this research project. It was stated above that Textual Analysis has the premise of texts being influential on cultural development. Whilst the project does deal with texts (legal texts), it does not consider these texts as any kind of influence, other than the provision of test data for later in the project. That is, legal texts will be used to test the developed methodologies, but these texts will not be considered and analysed as to how they possibly shape culture. Also, culture was previously defined to be not relevant to this project, therefore Textual Analysis has to be discarded as well as a possible research methodology.

As has been shown, a number of qualitative research methodologies could not be aligned axiologically with the research being undertaken. Many methodologies are designed to deal with a people or cultural aspect and this is a hindrance in the search for a suitable methodology that can be applied to a piece of research that has a strong technical aspect.

3.2.1.5 Finalising the choice of Research Methodology

Having performed some research into qualitative and quantitative research methods, it occurred to the author that it is difficult to choose an appropriate research methodology in this research project. One of the key data of this project will be the created XML code of the DSP. Due to its nature, computer code can be looked upon as a quantitative entity since it is unambiguous and (if deconstructed to the lowest level) is basically just a collection of the numbers 0 and 1. Incidentally, this reminds one of Kerlinger's famous quotes, which states "There's no such thing as qualitative data. Everything is either 1 or 0" (Kerlinger, 1986). Since Kerlinger states so eloquently that computer code is quantitative, the question arises on how to treat code as data in an IS research project which is otherwise qualitative in its nature. The problem is that existing statistical calculations can not be performed on this data, as one would do with traditional quantitative data. It can not be analysed qualitatively due to its quantitative nature. The author feels that, especially where computer code forms part of the data to be examined, it is not a straightforward choice between either quantitative, qualitative or mixed research methods.

These concerns were also made and identified by Baskerville (1999), who wrote several articles regarding the specific nature of IS requiring an approach that is different from the positivistic, empirical natural science approach typically associated with IS. Baskerville identified Action Research as a possible candidate for IS, e.g. in Baskerville and Wood-Harper (1996) and Baskerville (1999).

Baskerville and Wood-Harper (1996) paraphrase Banville and Landry (1989) when they identify the nature of IS as being a "highly applied field, almost vocational in nature" (Banville and Landry, 1989). It is this applied nature of IS that associated it originally with positivistic natural science methods and out of which the conflict with regards to the suitability of research methods in

IS is caused in the first place and led to Baskerville advocating the use of qualitative research methods in IS to improve the study of IS (Baskerville, 1999).

3.2.2 Action Research

3.2.2.1 General Background on Action Research

What is Action Research? Through its name it seems to suggest that there is some kind of progressive activity involved, and some definitions of Action Research do indeed hint upon the requirement of progression occurring. For example, Elliot (1997) states that "The fundamental aim of Action Research is to improve practice rather than to produce knowledge" (Elliot, 1997: p. 49). This shows that Elliot regards Action Research as research that is not quantitative in nature (that is, it does not intend to create knowledge through the validation of a hypothesis), nor does he regard Action Research as an activity that purely aims to create knowledge out of its activity. Instead, his quote hints that the research will result in a change of practice, where the change is of a positive nature. In other words, an existing problem will be tackled differently once it has been researched under the Action Research paradigm.

A similar view is taken by Kemmis and McTaggart (1992), who define Action Research as "a form of collective self-reflective enquiry undertaken by participants...in order to improve...their practices..." (Kemmis and McTaggart 1992, p.5). Just like Elliot, there is a stress on the fact that the use of Action Research will lead to an improvement of practice. Furthermore, Kemmis and McTaggart seem to hint that Action Research ought to be collaborative in nature, due to the presence of the words 'collective' and 'participants'. Finally, the collaboration is to be reflective in its nature, which hints that intermediate results are to be reflected upon and that the research itself is thus steered and driven by intermediate results. Therefore, whilst it might be clear from the onset on what the goal of the research is meant to be, the journey

towards achieving that goal is by no means clear-cut. This requires a flexible approach and a plan that ought to take into account eventualities that might derail a plan.

A slightly different view is taken by McNiff et. al. (1997), who state that "Action research is a form of practitioner research that can be used to help you improve your professional practices in many different types of workplaces." (McNiff, et. al., 1997: p.7). Whilst McNiff et. al. (1997) still recognise that Action Research will result in an improvement of practice, they also indicate that the research activity does not have to be in academia; they state that it is 'practitioner' research, thus leaving it open to both practitioners and researchers to perform Action Research, but also allowing the possibility for a researcher to act as a practitioner. Also, McNiff et. Al. show that it is a flexible methodology since they state it can improve "practices in many different types of workplaces" (McNiff, et. al., 1997). Thus, McNiff et. al. (1997) establish a strong link between the research and its practical applications, certainly stronger than Elliot and Kemmis do.

To round a range of views up, here is another definition of Action Research by Gray (2004): "...Action Research...symbolizes much of what modern research is about – analysing the world but also trying to change it" (Gray 2004, p. 373). Gray thus shows that Action Research is about change, something that the previous definitions coined as "improving practice." In other words, all definitions brought forward emphasise a few key points:

- Action Research is about improving practice and inducing change
- It is reflective and collaborative in nature
- It can be applied in a variety of settings

The above definitions have given a quick overview about the general characteristics of Action Research. However, such a view is too vague and

high-level to be of much use, therefore the following pages will see a more detailed analysis of more features of Action Research

Another feature of Action Research, according to Elliot (1997), is that one needs to appreciate "the importance of empirical data as a basis for reflectively improving practices" (Elliot, 1997: p.51). This is an implicit property of Action Research because since the methodology requires one to improve existing practices, one needs to have some proof or results to initiate change in practices. However, since Elliot also believes that the stress of Action Research lies on improving practice rather than generate new knowledge (Elliot, 1997), it becomes clear that he would condone such a view because implementing a practice change based on empirical data will prove to be quicker and more accurate than the implementation of changed practice on the basis of purely theoretical data. Furthermore, theoretical (and thus peer-reviewed) data can be seen as data that is to be accepted by the scientific community but, if one recalls Elliot's statement, the generation of knowledge is only a secondary purpose of Action Research.

Elliot states further that in Action Research the focus is on practically significant aspects of the study (Elliot, 1997) and this mirrors his views with regards to Action Research being primarily about inducing change in practices. In terms of practically significant aspects, the project will focus solely on developing a holistic method that turns legislation from natural text into executable code. No hypothesis or generalisations will be made about the applicability of these methodologies to other types of text or code. Therefore, it means that the research is entirely practical based as it deals with the problem at hand only. With regards to the aspirated 'holistic method', Elliot also mentions that a "holistic appreciation of the situation as a whole" is another key aspect of Action Research which takes precedence over analytical or theoretical understanding (Elliot, 1997).

Finally, Elliot says about Action Research that "'theories' are not validated independently and then applied to practice. They are validated *through practice* (Elliot 1997, p. 69; emphasis added)." In other words, the practical aspect of Action Research gets stressed yet again and 'traditional' theory and hypothesis testing is rejected. In practical terms, this means that one hypothesises as to how a practice could be improved and then goes about proving this hypothesis through applying it and measuring the outcome. This is a view that is similar to the definition of Action Research by Kemmis and McTaggart, who state that Action Research must be self-reflective, and thus cyclical (Kemmis and McTaggart, 1992).

Kemmis and McTaggart (1992) have similar views to Elliot, but there are some slight differences, which shall be examined in the following passages. The similarities in their views will also be pointed out. In line with the earlier mentioned definition of Action Research by Kemmis and McTaggart (1992), they add that Action Research "is only Action Research when it is collaborative, though it is important to realise that the Action Research of the group is achieved through the critically examined action of individual group members" (Kemmis and McTaggart 1992, p. 5). So not only is collaboration an important ingredient of Action Research, as stated above, but instead they try to make the point that collaboration is actually a key ingredient (and thus a defining one) of Action Research. Such a statement makes sense if one looks at the way Action Research is applied – practice is meant to be improved through reflective consideration of data (e.g. Elliot, 1997), and it is important that one's reflections are reviewed and validated by another knowledgeable person in order to ensure that no major mistakes or misinterpretations are made. Thus, Kemmis and McTaggart (1992) hint towards the need for collaboration as a means of ensuring that no mistakes are made during the Action Research process. McNiff et. al. (1997) identify a similar need when they state that Action Research ought to include a 'validation group' that validates intermediate results. However, Kemmis and McTaggart (1992) understand the term 'collaboration' as far more wide

reaching than simply as a means of peer review; they indicate that all affected parties in the research project ought to work together. For example, they state that in Action Research, "those affected by planned changes have the primary responsibility for deciding on courses of critically informed action...and for evaluating the results of strategies tried out in practice" (Kemmis and McTaggart, 1992, p. 6). Therefore, Action Research is an integrated effort where all parties (researchers, practitioners, sponsors, validators, etc.) work together to arrive at improved practices that are useful and to gain important scientific outcomes.

In terms of the research process within the methodology, Kemmis and McTaggart (1992) quote ideas of Lewin (1946), which state that Action Research is "a spiral of steps, each of which is composed of planning, action and the evaluation of the result of the action" (Kemmis and McTaggart 1992, p. 8). This shows how reflection is an important part of Action Research and how it is implemented into the general Action Research methodology, as pointed out earlier by Elliot (1997).

Finally, Kemmis and McTaggart (1992) state that an Action Research has a very typical kind of research question: "The general form of the question an Action Research group has at the beginning of an Action Research cycle is thus: 'We intend to do X with a view of improving Y'" (Kemmis and McTaggart 1992, p. 19). The wording of the research question thus shows how the emphasis lies on improving practice, which is an important point to bear in mind.

It was stated earlier that Kemmis and McTaggart (1992) have similar views to Elliot (1997). This is evident through the insistence of both parties that Action Research is aiming to improve practice (Elliot, 1997), is meant to be practiced in collaboration (Kemmis and McTaggart, 1992) and that data is validated through applying it and reflecting on the application (see both Kemmis and McTaggart (1992) and Elliot (1997)). Finally, the closeness between the views

of Kemmis and McTaggart (1992) on the one hand, and the views of Elliot on the other hand, is evident through the fact that Kemmis and McTaggart quoted no less than 4 different publications of Elliot's work on Action Research in the 1970's.

Whilst these views are all heavily based on the teaching profession and on how the teaching profession as a whole can improve its personal and collective teaching practice, it is widely acknowledged that Action Research has valid applicability to the Management Science (and indeed Management Information Systems) field, as acknowledged by Eden and Huxham (1996), by Coghlan and Brannick (2009) and Reason and Bradbury (2008), who all describe various applications of Action Research in Management Science. Action Research and its applicability to Information Systems is described in a separate section below.

McNiff et. al. (1997) see Action Research as a more individualistic activity than Kemmis and McTaggart do. They state that "...the research is done by individuals themselves into their own practices" (McNiff et. al., 1997). However, this is not a direct contradiction with Kemmis and McTaggart (1997), since they also state that Action Research requires the presence of a 'validating group' that can validate and approve performed research and implemented practice (McNiff et. al., 1997). Instead, McNiff et. al. were attempting to stress that Action Research is as much a development and improvement of practice as much as development and improvement of the primary researcher involved. They point this out by saying that "an important principle of Action Research is for the research to be educational in the sense of self-developing" (McNiff, et. al., 1997). Such a view is to be expected from them since they advocate and prescribe the use of Action Research in a teaching environment and see the improvement of one's teaching methods through self-applied Action Research as an important tool in facing modern teaching challenges (McNiff et. al., 1997). It is the researcher's view that regardless of the project's content and methodology, the researcher will gain

and develop from any research project since it is an important mile stone in the researcher's professional career. The researcher therefore does not agree with McNiff et. al. (1997) that self-development is a trait limited to Action Research. In direct contrast, Eden and Huxham (1996) see Action Research as a form of research that should be collaborative, but must not necessarily be so. In other words, Eden and Huxham (1996) see a much broader applicability of Action Research to the improvement of broader practices than just personal practice and that a researcher should not work in isolation. However, Eden and Huxham (1996) do not go as far as to state outrightly that individuals can not conduct Action Research on themselves, thus not completely contradicting McNiff et. al. (1997).

However, McNiff et. al. (1997) also state that "...Action Researchers are intent on describing, interpreting and explaining events while they seek to change them for the better" (McNiff et al., 1997: p.12). This statement is in broad agreement with the reflective approach described by both Kemmis and Elliot.

Finally, McNiff et. al. (1997) state that the research question of an Action Research project is of the type "How can I Improve..." (McNiff et. al., 1997). Whilst the wording is different from the one used by Kemmis and McTaggart (1992), the general idea behind the wording is still the same – an Action Research project is focused on improving practice, as stated by Elliot (1997).

Elliot was quoted above, saying Action Research takes a holistic approach (Elliot, 1997). This is reiterated by Gray, who states that "Action research...sees issues as only being understood not through the study of a single variable, but within a holistic, complex social system" (Gray, 2004). Thus, two prominent experts agree that Action Research must be carried out in a holistic manner. Gray (2004) also states on Action Research that it is focused on action through the researcher acting as a "change agent", whilst research is also being performed in a "participative manner" simultaneously. Furthermore, Gray explains the role of the "change agent" by saying that "the

researcher is a catalyst for achieving change by stimulating people to review their practices and to accept the need for change" (Gray 2004, p. 383).

3.2.2.2 Action Research and its suitability to Information Systems

It was mentioned earlier that Baskerville regards Action Research as very suitable to IS research in general. It is not only Baskerville who holds that opinion, however; important research within the IS domain was conducted by Checkland through the development of the Soft Systems Methodology (Checkland & Scholes, 1990), a methodology linking Action Research and Systems Development and thus providing a link between Action Research and IS in general. According to Baskerville and Wood-Harper (1996), this is regarded as a "landmark for the [Action Research] technique in IS research" (Baskerville & Wood-Harper, 1996).

Baskerville and Wood-Harper (1996) consider the epistemological nature of Action Research to be another indication for its suitability to IS. They describe Action Research as "...empirical, yet interpretive...experimental yet multivariate...observational, yet interventionist" (Baskerville & Wood-Harper, 1996). This dichotomical nature of Action Research therefore makes it suitable to IS research since IS exhibits a similar dichotomy of being both qualitative and quantitative in nature, as described in an earlier section.

Furthermore, IS research is necessarily multivariate, since an IS system can not function if its complexion is reduced through abstraction. An IS system is an interconnected entity that must function without a reduction of its complexity. This point is also made by Baskerville and Wood-Harper (1996), when they stress the importance of Action Research maintaining relevance to the real world by avoiding abstraction. This is a point also identified by Galliers and Land (1987), who state that "The complex, multivariate settings of systems development methodologies inevitably opens a validity question for any method that assumes abstracted causality" (Galliers & Land, 1987). In

other words, abstraction is not desirable in IS research, therefore quantitative research methods are inappropriate for usage in such a context.

The author therefore agrees with Baskervilie and Harper (1996) when they state that "Action Research...is the most scientifically legitimate approach available" (Baskerville & Wood-Harper, 1996).

One final point that needs resolving is identifying the problem owner. According to O'Keefe (2007), the difference between Applied Research and Action Research is the nature of the problem, and the owner of the problem. A general problem with generic owners is a feature found commonly in Applied Research, whilst in Action Research the problem must be of a specific nature, owned by a specific entity. This is an important point to bear in mind, since Applied and Action Research employ different research methods, therefore this distinction must be clear.

For this research project, the problem is clearly defined, in that a specific organisation has a specific problem regarding the use of DSPs. The problem owners are clearly identified, and their research need, namely the previously identified lack of formal method for generating DSPs, has also been identified. Thus, the problem is domain specific and owned by specific entities; therefore, this is indeed Action Research and not Applied Research.

3.2.2.3 Participatory Action Research

According to Baskerville (1999), there are several different forms of Action Research that can be applied to IS projects, such as IS Prototyping, ETHICS, Action Science, Participant Observation and Participatory Action Research.

Baskerville says about Participatory Action Research that "An important change is the realignment of the roles of researcher and subject into more

collaborative and synergistic forms" (Baskerville, 1999). Baskerville goes on to clarify that the client participants are elevated to "co-researcher status" (Baskerville, 1999) and not mere research outcome consumers. In other words, the organisation that set the problem in the first place and asked for Action Research to be undertaken on a specific problem is now *participating* in the actual Action Research. Baskerville (1999) indeed states that the participating client will actively support the researcher with their years of experience, thus confirming that the collaborators' *a priori* knowledge is going to be contributing to the research.

A similar view on Participatory Action Research is provided by Gray (2004), who states that Participatory Action Research "means immersing people in the focus of the enquiry and the research method, and involving them in data collection and analysis" (Gray 2004, p. 374). Thus, Gray agrees with Baskerville that the researcher is working closely 'within' the research subject and is involved first-hand in the enquiry itself, in data collection methods, analysing the data and specifying and collecting results.

Kemmis and McTaggart (2008) consider Participatory Action Research to have seven features that extend the 'basic' features of Action Research (Plan-Act-Observe-Reflect) due to its collaborative nature that elevates the status of the research participant to collaborator. These seven features are:

1. *Participatory Action Research is a social process* which explores the *relationship between the realms of the individual and the social*
2. *Participatory Action Research is participatory* by engaging people in examining their *knowledge* and interpretive categories
3. *Participatory Action Research is practical and collaborative* as it engages people in examining the *social practices* that link them with others in social interaction

4. *Participatory Action Research is emancipatory,* as it aims to help people recover...themselves from...unproductive...and unsatisfying *social structures* that limit...[them]

5. *Participatory Action Research is critical* of...constraints embedded in the *social media* through which the [participants] interact

6. *Participatory Action Research is reflexive* through a spiral of cycles of critical and self-critical action and reflection

7. *Participatory Action Research aims to transform both theory and practice*

Taken and adapted from: Kemmis and McTaggart (2008), pp. 280 f.f. (Emphases in original)

The above features show that Participatory Action Research goes beyond mere collaboration; it empowers the participants by not only giving them co-researcher status, but by actually giving them the tools to change their social environment themselves. Interestingly, Kemmis and McTaggart (2008) admit that "Action Research is frequently a solitary process of self-reflection" and state that the collaborative aspect is a desirable (but not essential) element of both Action Research and Participatory Action Research (Kemmis and McTaggart, 2008; p. 277).

There is further, confirmatory, writing on Participatory Action Research by Reason and Bradbury (2008) who take a more Management Science-view of Participatory Action Research. In their handbook of Action Research, they confirm that Participatory Action Research must be applied in close collaboration with the beneficiary of the research and that a symbiotic relationship is entered, promoting learning in both researcher and client organisation (Reason and Bradbury, 2008). In other words, they confirm that in a Participatory Action Research setting, researcher and problem owner share an egalitarian power relationship which is symbiotic in nature and must therefore be of benefit to both. The emphasis on shared learning is interesting and this topic is revisted in Chapters 5 and 6.

3.2.2.4 Justifying the use of Action Research

From the above pointers it becomes evident that Action Research is indeed suitable for this research project. Going by the definitions of Action Research introduced above, several pointers to this suitability become clear.

Firstly, the ability to improve practice and induce change, as required by Elliot (1997), is very relevant since the research project aims to formalise informal approaches of turning legal text into executable code. In this case, the improved practice would be in an informal trial-and-error method being improved and changed towards a formal methodology that is traceable and yields valid results for a variety of legal situations. Thus, the anticipated change in practice would result in increased accuracy, increased validity and extra security.

Action Research is supposed to be reflective and collaborative, according to Kemmis & McTaggart (1992). For this research, reflection is a very important aspect which validates the developed methods and artefacts. It will enable the researcher to validate the obtained results and feed the reflections back into the original work on the methods and artefacts in order to improve results. This cycle will be repeated several times, until no further improvements will be acquirable by the developed methods and artefacts. Thus, a reflective activity will be part of the Research Methods employed in this research.

As for collaboration, the researcher has been provided with the current practice of turning legal texts into executable code and this information has proven to be a valuable starting point from which practice can be improved. Also, the researcher will utilise facilities developed by the problem owner in order to validate the improved practice and thus show the problem owner the success of the developed methods and artefacts; furthermore, the problem owner's experience has been pledged to assist the researcher in the quest for the new and improved methods. Apart from the collaborators' expert

knowledge on the technical subject, their knowledge of the organisation will be useful in ensuring that the artefacts and other solutions to be developed will be honed towards solving the organisation's specific issues in a manner that best fits the organisation. In other words, collaboration is going to be a key element throughout the life cycle of this research.

As for the aspect of multiple applicability of Action Research, it has been shown to be applicable to educational settings (e.g. McNiff & Whitehead (2002); Kemmis & McTaggart (1992); Elliot (1997)) whilst Baskerville claims that Action Research been used in the social and medical sciences (Baskerville, 1999) and, in the same article, Baskerville shows how Action Research could be used in IS. As can be seen, Action Research has been employed in a wide array of different disciplines and this research will provide further example of Action Research being employed and applied in IS.

With regards to the research aims, the application of Action Research will ensure that the four stated research aims will be achieved in order to answer the research question. The research aims were:

- Develop a method to enable individuals to convert natural language legal acts and convert these to process models
- Develop tools and methods to convert those process models into codified form
- Produce standards-compliant signature, evidence and archival policies (adhering to ETSI TR 102 038)
- The developed method should allow transformations in a structured and repeated manner

With this in mind, the AR method is anticipated to help meet these through the continuous and iterative verification with the problem owner that each of the aims has been met. In other words, continuous and iterative work on each aspect of the research will, eventually, result in the research aims being

met. The collaborative nature of this research method will ensure alignment between the research results and the problem owners' needs, which are encapsulated by the research aims.

3.3 Research Methods

Research Methods are the individual actions taken by a researcher to conduct research; whilst the Research Design is the overall plan of research, and the Research Methodology the more detailed description of how to do the research, the Research Methods are the individual activities undertaken that show how Research methodology and, ultimately, Research Design were implemented and followed.

3.3.1 Double-Iteration Research Loop

A high-level overview of the Research Design was provided in the previous sections. This section will give a detailed overview of how the research was conducted and what methods were employed.

Overall, the project will follow the cyclical development phases, as prescribed by Lewin (1946) and Elliot (1997) and it also features the collaborative aspects, as prescribed by Kemmis and McTaggart (1992). The following figure shows the research approach:
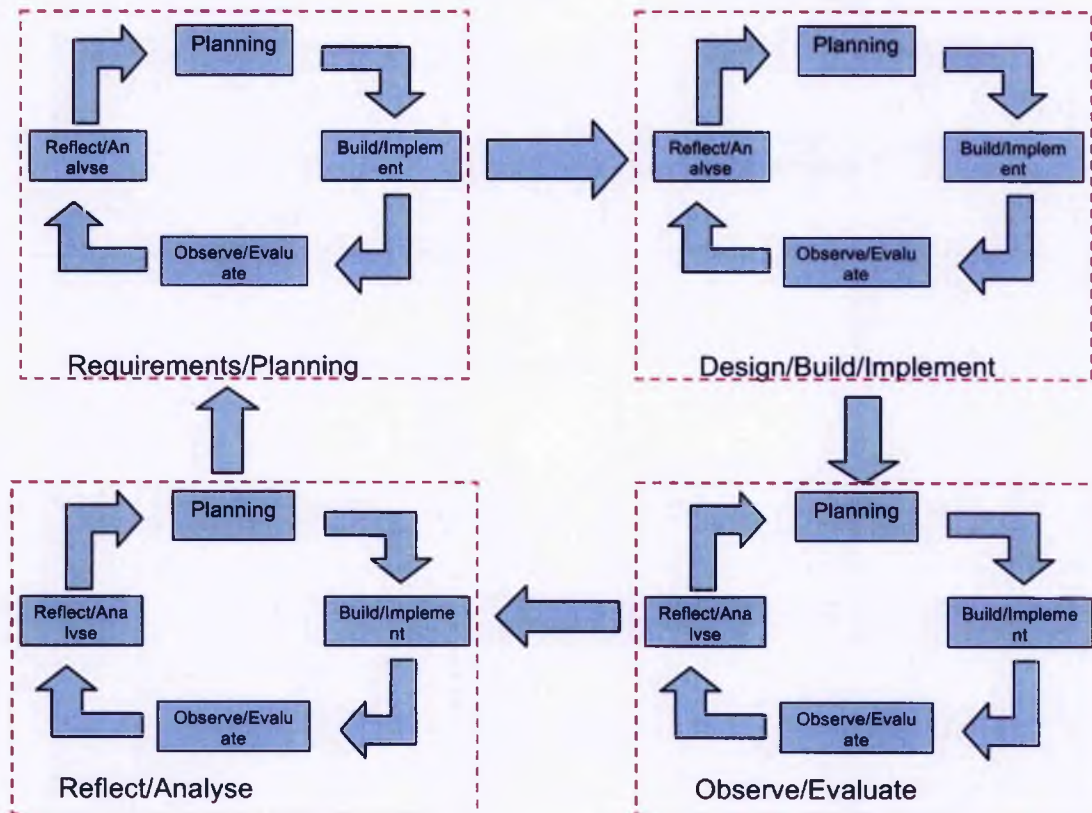
Figure 3-1: Action Research Methodology Approach

The above figure 3-1 is a general description of the research, showing how the research followed several iterative cycles. What is not shown in the figure is the collaborative aspect of Action Research; the collaboration occurred at several points in the research process (more detail below) and illustrating it graphically would obscure the figure and make it difficult to read, hence the collaborative aspect is going to be illustrated in writing only.

Figure 3-1 shows four red boxes, labelled "Requirements/Planning", "Design/Build/Implement", "Observe/Evaluate" and "Reflect/Analyse". Within each of these boxes, the activities "Planning", "Build/Implement", "Observe/Evaluate" and "Reflect/Analyse" are shown. At this point it should be noted that there are two aspects to the solution; one aspect directly refers to the research question and is concerned with the provision of a method to

create DSPs. The other aspect refers to the 'tools' developed in order to achieve this aim, which take the form of physical IS artefacts. The artefacts and the method are discussed in more detail in Chapter 4, where the research results are presented. The impact of having seemingly two solutions (and indeed, the question of which of the two aspects actually represent the solution - i.e., is the completed method the sought solution and the key research output? Or is it the developed artefacts?) is discussed in Chapter 5.2, where these methodological questions are addressed. Coming back to the figure, the use of the arrows connecting the red boxes, and the arrows connecting the blue boxes within the red boxes, are meant to show an apparent 'dual-research iteration loop', where both individual artefacts of the solution being designed underwent several iteration cycles of Plan - Action - Evaluate - Reflect, but also the complete method from conceptualisation to the results presented herein at least twice. The researcher therefore argues that the research was progressed very much in line with Action Research, as several iteration cycles of investigation were related to both specific aspects of the intervention and also the complete cycle from conceptualisation to results at least twice.

The following paragraphs will now show how the research was conducted in detail, i.e. the manifestation of the iterative activities will be described; it will be shown what each of the red boxes contributed to the overall research (i.e. what is the significance for the method being developed; the 'outer' iterative loop) and how that contribution was arrived at (i.e. what supporting activities, such as developing tools, had to be conducted; the 'inner' iterative loop). The format of this discussion will follow the red boxes, i.e. each red box is going to be discussed in turn (starting with "Requirements/Planning") and activities undertaken and then a final discussion on the 'outer' iterative loop and the meaning of the red boxes in unison.

Red Box 1: Requirements/Planning

Initially, the researcher had little to no knowledge of the nature of the problem and the requirements the problem owner wanted to be met; nor was the researcher aware of the problem owner's objectives of why they needed DSPs and method to create them with. Therefore, the researcher and the problem owners held a number of meetings, at which a number of techniques, such as mind maps and high level process diagrams (Winter et. al., 1995) were used in order to elicit requirements from a seemingly unstructured problem domain and to understand the objectives for which a method was required. For each meeting, the researcher would initially summarise the results of the previous meeting, highlight areas that were unclear or not well defined and point out areas where contradictions existed. These were sent to the problem owner prior to the meeting and discussion on the raised items was requested. This is therefore an example of the Reflect/Analyse activity leading towards Planning. At the actual meeting, the problem owners typically raised their own issues (mainly in response to the issues raised by the researcher) and the meeting was held in a manner such that both parties' issues were addressed in turn. Hence it can be seen that the problem owner also engaged in the Reflect and Planning activities.

During these meetings, Soft Systems Methodology was then used in the Build/Implement cycle in order to elicit further requirements and obtain resolutions for the raised issues. Typically, this involved the researcher and the problem owners sitting together at the same desk and exchanging questions and ideas verbally, which the researcher would record. Thus, the Build/Implement activity led to the 'building' of requirements and introduced structure to the problem domain. It also infused learning about the problem in both researcher (who had no prior knowledge) and in the problem owner (who were 'forced' to structure their thoughts, with guidance from the researcher). In other words, what Rapaport (1970) calls 'Operational Research view of Action Research' and draws on Action Learning (Revans, 1983) to bring together technical approaches and organisational methods with a view of problem solution through shared learning, is starting to be

applied at this stage of the research and this shared Action Learning then continued throughout the remainder of the research. Section 5 explores the issues of learning and Action Research and the connection with the developed method and artefacts further.

At the end of these meetings, the researcher and the problem owner reflected on the arrived at requirements and information and assessed whether the requirements were reasonable, whether the researcher understood the provided information and whether the researcher was confident to work with what had been arrived at. Therefore, the researcher and the problem owner engaged in an activity of Observing and Evaluating the results of the meeting. As indicated earlier, researcher and problem owner then engaged in a period of Reflection and Analysis off-line from each other.

Red Box 2: Design/Build/Implement

Red Box 1 had, over several iterations, developed a set of requirements which enabled the researcher to start developing the tools for the intervention. Therefore, the initial iteration aimed to analyse the set of requirements, build and implement a suggested tools design with the problem owners, and then evaluate and reflect on whether the suggested design could meet those requirements. The problem owner provided some input through e-mail in the build/implement activity and in the analysis activity, but this was mainly to supplant some of the ideas the researcher developed, rather than actively engage *with* the researcher and the research material. A more active type of engagement going beyond limited supplanting of results and seeing the problem owner engaging with both research and research material actively, which is the more traditional type of collaboration in Participatory Action Research and (as shown above) leads to shared learning taking place, was started in subsequent research iterations that were concerned with the development of the actual physical artefacts. In other words, whilst the problem owner did not engage with the researcher in the initial research iteration phase, the problem owner took a more active role once the research

moved on to the actual physical artefacts, showing more interest in the functionality and success of the physical artefacts.

The main collaborative tool for exchanging ideas and working on problems together was E-mail, which was used by both problem owner and researcher to exchange questions, solutions and ideas and which therefore fostered shared learning. Complicated issues, which were not resolved via E-mail, were occasionally resolved through phone calls and once an unstructured interview had to take place in order for the researcher to understand a specific issue and explore potential solutions. The exchange of annotated and commented documents as well as the verbal feedback from the unstructured interview complemented the data collection. The 'inner' iteration loop, therefore, consisted of iterative development of the various physical artefacts, with the problem owner heavily involved in the 'Build/Implement' activity, whilst the researcher took a lead in the 'Evaluate' and 'Analysis' activities. Therefore, the researcher was mainly learning during the 'Build/Implement' activity, whilst the problem owner was learning during the 'Evaluate' and 'Analysis' activities, because the researcher could make use of the subject matter experience of the problem owner and because the problem owner could make use of the researcher's analytical and formal knowledge.

After several iterative cycles, the researcher and the problem owner agreed that the artefacts had been developed to a sufficient standard.

Red Box 3: Observe/Evaluate

In order to be able to develop a robust method of creating DSPs, the developed artefacts were required to undergo Evaluation, within their function of contributing to the development of DSPs; the artefacts had undergone cycles of evaluation as part of their Design/Build/Implement iteration loop, with the aim of completing and perfecting their manufacture. But the artefacts had not been evaluated as tools that contribute to a method for DSP creation.

Whilst there were multiple iterations in order to Observe/Evaluate, the actual iterative cycles had two distinct aims - the first set of iterative cycles was aimed at preparing the necessary data for the Evaluation to be able to take place. The necessity of this is explained by the fact that a DSP represents legal information in XML format. Therefore, the legal information would require preparing, which was done through this initial aim of the iteration. It could be argued that this preparation represents the 'Planning' activity alone (as it plans for evaluating the artefacts), but this would be inaccurate since researcher and problem owner collaborated in an Action Research-like, iterative fashion in order to construct the data necessary. Iteration was required as the necessary set-up was quite complex. Collaboration again mainly occurred through e-mail, but there was one presentation followed by an unstructured interview which yielded more data for the researcher and led to a further research loop.

On completing this first aim, the second aim was to use the created data and getting the developed artefacts to consume it; again, several iterative cycles were followed, since it had to be evaluated how the data was affected by the various artefacts. Also, the artefacts initially failed to act in a manner that satisfied the method being developed, and identifying and rectifying the issues required iteration loops to help researcher and problem owner to work together to inspect, identify and solve issues. It should be noted that the learning here extended into several different areas: both researcher and problem owner learned about the behaviour of the different artefacts; researcher and problem owner learned about the method being developed; researcher and problem owner learned about the legal information and how it would need to be consumed by the method being developed. Interestingly, all these activities of learning resulted in further iterations, aimed at perfecting the interaction between legal data, artefacts, and the method. Note that this investigation did not extend towards modifying the method because of either data or artefacts.

Red Box 4: Reflect/Analyse

It has been shown how learning took place when various parts of the research investigated the developed artefacts and the behaviour of the artefacts when presented with data. Whilst this investigation led to changes in the artefacts (as evidenced by the research loop iterations) until satisfactory behaviour was obtained, it did raise questions on how the artefacts could be purposefully deployed and used in a manner that would yield valid DSPs. Essentially, the learning output and results of all the previous iteration loops were reflected and analysed and the results shared with the problem owner. This caused a further iteration loop with the aim of planning the next step for the intervention; in other words, the 'planning' activity caused further collaboration that saw a plan built, evaluated and analysed. The outcome of this iteration loop was that the overall method of creating DSPs required adaptation, as did the developed artefacts.

The learning outcomes here were shared between problem owner and researcher, in that the nature of the method was realised to require a higher degree of formalism and that the amount of 'customisation' of the developed artefacts towards satisfying the requirements of the overall method had been underestimated.

The 'Outer' Iterative Loop

So far, it has been shown how there was one large iteration, the so-called 'outer' loop going around the red boxes. The outcome of this iteration (i.e. the conclusion following the final reflection) was that another iteration was required, i.e. another set of activities of Planning-Build-Evaluate-Analyse was required since the results so far were not satisfactory. This is therefore the outer part of the dual-research iteration loop that had been mentioned above and rather than focusing on an individual aspect of the intervention, was concerned with the overall method (i.e. the holistic aspect) being developed as part of the intervention. In other words, the focus of the research shifted

from the creation of artefacts towards achieving the goal that the artefacts were designed as aids for, which resulted in minor changes and modifications to the results arrived at so far. As stated earlier, the methodological implications for this are detailed in chapter 5.

An important item to note here is the fact that *minor* changes were required; the fact that these changes needed to be applied to both the overall method being developed and the artefacts designed to assist with the method does not mean that the validity of the overall method was questioned; rather, the developed requirements, the developed artefacts and the developed method had not been sufficiently integrated, resulting in initially disappointing results. Therefore, this corrective action is a case of single-loop learning (Sadler-Smith, 2006) and not double-loop learning (ibid.), since the overall assumptions and plans (i.e. the intended use of DSPs, the infrastructure they would be deployed in, the fact that the method requires the use of artefacts) or, in other words, the environment for which the research output was being prepared for, were neither questioned nor changed or abandoned. Therefore, this iteration represents single-loop learning by having taught researcher and problem owner that the various tools created for the intervention had not been aligned with the overall method.

Further aspects of the learning and an analysis of further findings are made in chapter 5.

From the above description of the research method, it becomes evident how this is an example of Participatory Action Research. The various research iteration loops were conducted by both researcher and problem owner in a collaborative way. The interactions resulted in learning outcomes being achieved in both and the final outcome was the creation of an intervention method, assisted by various artefacts. The results are listed in chapter 4 and discussed in chapter 5.

3.3.2 Data

As hinted upon in the previous section, all data was of a qualitative nature. The primary source of data were E-mails which discussed minor points, such as the symbols utilised for the graphical modelling notation, the data included in the new PADS questionnaire, and the syntax of the generated DSPs. This data was usually around two to three A4 pages sized and contained a wealth of mainly technical information, but did include on occasion more managerial-type of information (centring on visual presentation, as opposed to function), but this was rare. Similar to E-mails, phone calls were also conducted and yielded data that was very similar to the type of data yielded through E-mail, mainly focusing on in-depth discussions of more technical issues. E-mails were exchanged roughly every 3-5 days, except for when the collaborator was not available for response. Phone calls were limited to about once a month, sometimes rarer.

Another source of data was the exchange of formal documents (both authored by Standards bodies, e.g. ETSI and also authored by either researcher or collaborator on a specific issue) and the use of annotations and comments that highlighted areas of concern. These comments and annotations represent a type of data, as the problem owner identified issues and communicated these to the researcher in written format. These comments sometimes replaced e-mail communication, as such a facility made it easier to present ideas against specific parts of documents. Flick (2006) identifies documents as valid sources of data, provided they meet criteria of Authenticity, Credibility, Representativeness and Meaning (quoted in Flick (2006); originally by Scott (1990)), which must be met for the documents to be accepted as valid data sources. As official standards published by a standards body represent a commonly accepted authority, and since the collaborators can be considered as experts, it can be said that the documents investigated are indeed fit for extraction of data.

Further data was gained at more formal presentations and face to face meetings; the researcher was assisted in taking notes and the written minutes were approved by the problem owner. This type of information was usually less specific and technical and more aimed at the greater direction of the research, the discussion of general management issues and expectations of interim result reports. These more formal occasions therefore served less to validate conducted research and more to assess it in the light of the overall research objectives and to guide the researcher towards issues that may not have been recognised otherwise. The following table summarises the details of the six meetings that took place:

Date	Location	Details
14/09/06	Madrid	Initial meeting and superficial discussions on the problem and associated technology
27/10/06	Barcelona	Discussion about the problem, more details on the technology and how the problem affects the business. Discussed potential solutions and initial agreement to form a research project.
15/11/06	Brussels	Agreed content of project, aims and deliverables. More details on what was expected of the project.
05-06/02/07	Barcelona	Kick-Off meeting. Finalisation of scope, discussion and agreement on research aims. Responses to detailed technological questions.
25-26/06/07	Brussels	Presented progress update. Handover of in-progress technical material. Received encouragement and some changes/updates.
27/09/06	Barcelona	Presentation to CEO of CATCert. Research aims and conducted work received endorsement.

Table 3-1: Formal Meeting Details

The code written for the VB.NET transformation tool also serves as data, since it is possible for mal-formed and non-compliant XML code to have been

created through mistakes in the coding of the VB.NET transformation tool, which are not related to mistakes in the method. It was important to establish whether mistakes in the created signature policies were down to mistakes in the modelling notation or simple coding errors. A precise data mapping table, for example, helped with ensuring data consistency, and thus minimised source of errors in the modelling notation and the transformation tool.

The use of questionnaires to extract data from the problem owner was rejected since the researcher felt that it is not possible to receive precise technical answers to a big questionnaire with many questions – a 'piece meal' approach, whereby only a few questions would be asked in regular intervals, was felt to be much more appropriate. The researcher expected that large questionnaires would take a longer time to be completed, the answers might be less precise and the work load at the problem owner's organisation had to be considered (who were involved in many activities not related to the research presented herein) as another factor in receiving delayed responses. On the other hand, the piece meal approach (see above for use of E-mails and phone calls) allows for a few specific questions to be answered in greater detail and also allows for follow-up questions, since the other party would have to digest less written information in understanding the researcher's questions and collating an answer. Similarly, performing detailed qualitative analysis using an analysis package such as NVIVO would have caused even further delays through the necessary 'coding' of the responses. In other words, questionnaires were rejected because they would hinder progress through their containing large amounts of data and the associated processing times. The researcher felt that the 'piece meal' approach permitted the researcher to conduct the research in a more flexible and agile way, invoking the problem owners and seeking their input only when and as required, as opposed to a formal approach causing delays through the associated 'formalisms' of data preparation, data analysis, and waiting for the problem owner to provide long and detailed feedback.

A further advantage of the researcher's approach lies in the fact that the problem owners were communicating in a foreign language with some difficulty; the researcher felt that forcing the problem owners to engage with a formal questionnaire written in highly formalised English may have caused the problem owners to disengage, since not understanding the instructions correctly, or struggling with the content of the questions would have made the problem owners feel embarrassed and therefore the more personal piece meal approach allowed this language barrier to be overcome. The researcher feels vindicated in this choice through the fact that a number of E-mails and personal comments all included references to the problem owner's 'shame' of not being a fluent English speaker and that the problem owners saw this project as an opportunity to improve their command of English, a learning outcome that was quite separate to the research problem.

Expert Interviews of subject matter experts (Meuser and Nagel, 2002) were another data collection method that were used; however, their use was very sparing and they were mainly employed after or at meetings in order to obtain further information on particular issues than what was possible during the actual meeting itself. However, it could be argued that pointed, technical questions administered through e-mail could be a form of remote Expert Interview.

As technical descriptions of the PADS methodology and the ETSI TR 102 038 standard were available, as were examples of real DSPs, the researcher saw these documents as rich sources of content and information. In fact, a detailed analysis of existing material provided the researcher with much useful information that allowed the researcher to collaborate more effectively by gaining more understanding of the subject matter. The researcher is aware of the seemingly contradictory statement here, stating the published material was sufficiently available, and the statement in section 2.1.4 that there was frustratingly little literature on DSPs - the researcher feels there is no contradiction here, because whilst there is a very low quantity of information

available, the information that is available is extremely useful as it is essentially the main authority on this technology describing the technology, the syntax, the legal issues governing its use and even presenting future business models. In other words, the existing information on this topic is sufficient to be able to understand and apply the technology in question. However, it is abstract (as standards should be) and therefore no case-specific information is available.

With regards to obtaining information relevant to the specifics of the intervention, the use of Action Research gave the researcher access to the problem owners' knowledge through the collaborative nature of the research. Where the researcher encountered difficulties and uncertainty, the problem owner (who had greater knowledge of working practices within the organisation and had some experience in using DSPs) was able to transfer knowledge to the researcher; similarly, the researcher's analytical ability helped the problem owner realise that there were areas where problems were experienced.

3.3.3 How the Research Methods justify the choice of Action Research

It is necessary to investigate how specific features of Action Research relate to the project's Research Methods and the individual activities, in order to see the match between methodological requirements and research activities. This will emphasise that the research was methodologically compliant.

Elliot (1997) stresses several times that it is important to continue reflective activity of results, since results are context bound and therefore have to be continuously assessed within the context they were derived in (Elliot, 1997). This is evident in the research project through the inclusion of an Evaluation chapter (see Chapter 5.2.3), which will assess the general results of the whole project, whilst due to the nature of the software elements involved in this research, a prototype development methodology (Lethbridge &

Laganiére, 2001) will be applied to arrive at some of the artefacts. Prototype development methodologies are cyclical and reflective in nature (ibid.), thus mimicking the approach of Action Research. This similarity further condones the use of Action Research in this context.

Elliot (1997) states that acquiring empirical data during evaluation is required in order to be able to arrive at valid conclusions. This statement is relevant to this project, since this project will undertake a similar approach; in the initial stages of the research, once the analysis of the original PADS questionnaire has been completed, the data yielded by the original PADS questionnaire will be compared to the ETSI DSP standard and, progressively, a picture of present and missing information elicited by the original PADS questionnaire will be built up. These results will then be immediately implemented into both a new PADS questionnaire and an associated graphical component of it. Similarly, the research work will undertake several tests aimed at identifying whether the method and artefacts are capable of creating an ETSI-compatible DSP. A line-by-line evaluation will result in corrective action being undertaken immediately, whilst the problem owner will mirror these tests on their end in order to provide further feedback on the process and the quality of the results. Therefore, reflective action based on empirical data is a key ingredient for the rapid progression of the project and due to this agreement with Elliot's views on the subject of continuous evaluation, we also have further evidence that Action Research might be an appropriate research methodology to use.

Elliot (1997) also states that theories are validated through practice. As hinted upon in the chapter above, testing and evaluation are validation activities carried out as part of this research. However, the culminating evaluation to be carried out by the research is going to be the application of the developed methods and artefacts on a real-world or close to real scenario, in order to prove that the methods and artefacts not only work in artificial settings, but in natural settings as well. Therefore, this is evidence of more agreement with

Elliot (1997), which further strengthens the case that Action Research might be the appropriate methodology for this project.

The importance of the collaborative effort, as stressed by Kemmis and McTaggart (1992), is satisfied in the research project through several methods. Firstly, the recommended practice improvements by the researcher are validated against the views and opinions of both a validator and the research project's problem owners, those that will be affected by the change the most. Also, the research problem owners will put the developed practices to test within their production environments and provide feedback on improvements. Furthermore, the problem owners provide crucial information in technical areas where their experience will be extremely useful to the researcher. Thus, the researcher is capable of developing improved practice based on the requirements and experience of the problem owners. Through this close interaction between problem owner and researcher, the stringent collaboration requirements of Kemmis and McTaggart (1992) are met, thus this is yet another indicator that Action Research is a viable research methodology.

It was stated earlier that Kemmis and McTaggart emphasise the importance of the research question and how its emphasis must lie on improving practice (Kemmis & McTaggart, 1992). This is reflected in the research question, which was "How can the current method of creating Digital Signature Policies be improved such that Digital Signature Policies in ETSI TR 102 038 format are created in a reproducible and more formalised manner that allows users without legal training to use it?" In other words, there is a complete match between the requirements of an Action Research research question and the research question driving the problem.

Similarly, McNiff et. al. (1997) had stated that the research question of an Action Research ought to be aimed at improving a practice – almost a carbon copy of Kemmis and McTaggart's point.

On a different note, both Elliot (1997) and Gray (2004) state that Action Research must be carried out in a holistic manner, an approach that follows from the epistemoiogical requirements of Constructivism. Furthermore, Gray also states that the researcher in an Action Research project is a "change agent" (Gray, 2004) – in broad agreement with other authors on Action Research.

Therefore, the literature agrees that a change in practice is the primary purpose of Action Research, which at the same time is considered Action Research when there is a specific problem owner in a particular social setting. Also, the literature mentions that Action Research is of a collaborative nature and that the interaction occurs between the researcher and the people to be affected by the change in practice (in other words, the users) or, in the case of Participative Action Research, between the researcher and collaborators that are of a 'co-researcher' status. This bears resemblance with how the project is being planned and therefore serves as further evidence for the suitability of Action Research.

Finally, Gray (2004) identifies a minor issue with Action Research, namely that Action Research tends to be underreported in academic literature. This is not going to be an issue with this research project, since measures have been taken to advertise the project and its aims and achievements to the scientific community through the publication of a series of papers. Indeed, at the time of writing one article had been presented at a conference and another article had been submitted to a known journal for publication.

3.4 Design Science
As the researcher continued with the research intervention, the researcher considered whether the taken approach was more in line with 'Design Science' (e.g. Järvinen (2005); Cole et. al. (2005)). That is, the researcher designed artefacts for the problem owners to use and much of the effort was

concentrated on the design of these and associated process changes. The researcher undertook a post-hoc analysis of both Design Science and a methodological analysis to see whether the research can indeed be described as Design Science. The following sections will investigate and describe Design Science, whilst section 5.2 will present the methodological analysis of the research and investigate the suitability of Design Science.

3.4.1 Design Science in other Disciplines

Searching scientific literature for the term 'Design Science' revealed a number of alternative terms that all related to the same, or similar, topic; usually, this topic is a methodology or a more general approach to research design.

In the field of Engineering, the term 'Design Research' (Fulcher & Hills, 1996) is used to describe a methodology for Engineering design and also states an axiology that is indicative of the intended use of such a methodology. On the other hand, Eder (1998) understands the term 'Design Modelling' to be an activity framework for engineering projects, which captures a wide variety of activities that ought to be performed in an engineering project. He relates 'Design Modelling' to be originating from his own definition of 'Design Science', which he formulated in 1996 (Hubka & Eder, 1996). Eder (1996) defines 'Design Science' to be a taxonomy of engineering knowledge.

In Software Engineering, the term 'Design Theory' is used by McPhee (1996) and Preston & Mehandjiev (2004) to signify a 'theory' of design that determines how to influence the design of a Software Engineering artefact by taking into account influences on the artefact, such as knowledge representation schema, process models and an evaluation of whether an artefact's goals had been achieved (Preston & Mehandjiev, 2004) and providing a framework that shows how to integrate such influences into the design of the actual artefact (Preston & Mehandjiev, 2004).

It is very interesting to note that Preston & Mehandjiev attempt to include influences into their artefact design that do not solely stem from Software Engineering constructs, but also influences based on 'goal achievement' (Preston & Mehandjiev, 2004). This is interesting, because Lee (1999) defines an Information System as a system that consists of technology, social setting and the interactions and phenomena that between technology and the social setting (Lee, 1999). Attaching the concept of 'goal' to Software Engineering is the first step in recognising the influence of social setting on an artefact and this shows how the discipline of Software Engineering and IS converge on this point.

3.4.2 Design Science in Information Systems

The concept of Design Science has various names within the IS discipline. For example, Walls et. al. (1992) call it "Design Theory" and establish it as a methodology that guides the design of Executive Information Systems from requirements gathering to artefact evaluation (Walls, et. al., 1992). In 2004, Walls et. al. revised their earlier research and created a distinction between Design Science and Design Theory, whereby Design Science "selects from...theories and combines them with...existing artifacts and the goals of actors in the environment to create new Design Theories" (Walls et. al., 2004). In other words, Walls et. al. see Design Theory as a collection of theories from which Design Science selects elements of and uses those theories to combine them with an artefact and its social setting in order to achieve an actor's goal and to generate new Design Theories. Thus, Walls et. al. consider Design Theory to "prescriptively guide the design of...information system[s]" (Walls et. al., 2004), whilst Design Science is considered to be more applied and is using elements of Design Theory in combination with technology and social setting to arrive at new theory. In a long-winded way, Walls et. al. state that Design Science is actually a Research Methodology that is routed in a large body of knowledge which they call Design Theory.

Another word for such a methodology is Design Research. Authors such as Cole et. al. (2005) and Vaishnavi and Kuechler (2004) describe Design Research as an IS research methodology. Cole et. al. (2005) recognise that Design Science is also a widely used and interchangeable term for this methodology and, as later chapters will show, there is little difference between authors describing Design Research and Design Science; their description of the Design Science methodology differs only slightly in a few details and correspond largely, both from an axiological view as well as from the broad scope of methods employed by this methodology.

For the remainder of this document, the author shall adopt the term 'Design Science' as the label for this particular IS research methodology. The following section will now describe Design Science and highlight some key similarities and differences between the various authors on Design Science.

3.4.3 The Design Science Research Methodology

March and Smith (1995) trace Design Science back to Simon (1969), when they quote Simon to define Design Science as "concerned with 'devising artifacts to attain goals'" (March and Smith (1995), quoting Simon (1969)). Thus, March and Smith (1995) agree with Simon (1969) that the basic axiology of Design Science is to produce an artefact that will attain the goal of a group of people. March and Smith (1995) expand upon this point by declaring that Design Science "attempts to create things that serve human purposes" (March and Smith, 1995), thus furthering the idea that Design Science is a 'fit for purpose' approach, in that it is specifically aimed at serving human purposes through attaining their goals. Therefore, "its products are assessed against criteria of value or utility" (March and Smith, 1995), suggesting that Design Science's ultimate goal is to produce an artefact that serves human goals and that Design Science must evaluate the produced artefact as to whether it meets those goals or not. What March and Smith thereby hint upon is that Design Science really is a research activity consisting of two broad elements:

1) Design Science must produce an artefact that attains human goals
2) Design Science output must be evaluated to show it attains the stated human goals

March and Smith (1995) call these two elements the "build and evaluate" activity (March and Smith, 1995) and define the 'build' activity as "the process of constructing an artefact for a specific purpose" (March and Smith, 1995) and the 'evaluate' activity as "the process of determining how well the artefact performs" (March and Smith, 1995). Thus, March and Smith (1995) describe the broad axiology of Design Science, which closely follows Simon's statement of Design Science producing artefacts that are fit for a specific purpose. March and Smith (1995) expand the scientific element of such a statement by requiring the produced artefact to be shown to meet the specific purpose.

However, this is not sufficient, according to March and Smith; they postulate that, since they see a Natural Science influence on Design Science, it is also important to theorise on an artefact by assessing "why and how the artefact worked or did not work within its environment" (March and Smith, 1995). Furthermore, a justification must be provided for the theorisation activity; that is, once a researcher has established the 'why and how', the researcher must then test this theory by gathering evidence (March and Smith, 1995).

March and Smith (1995) identify four different types of artefacts: Constructs, Models, Methods and Implementations. They define constructs as the "language of concepts" (March and Smith, 1995), whilst models are defined as "higher order constructions" (March and Smith, 1995). Methods are defined as "ways of performing goal-directed activities" (March and Smith, 1995) whilst implementations are the "physical implementations" (March and Smith, 1995) of the above. Thus, March and Smith's concept of an artefact goes well beyond a computer system (the physical implementation) and

includes broad theoretical areas that describe the setting surrounding the computer system (e.g. language of concepts) and prescribe what problems the computer system is meant to be used for (e.g. ways of performing goal-directed activities).

March and Smith combine the above concepts to create a Research Framework for Information Technology Research, which makes a distinction between Research Outputs (=Design Science Artefacts) and Research Activities (=Build, Evaluate, Theorise, Justify). A conceptualisation of their Research Framework is provided below:

	Build	Evaluate	Theorize	Justify
Constructs				
Model				
Method				
Instantiation				

Table 3-2: March and Smith's Design Science Research Framework

Thus, regardless of the type of artefact produced by Design Science, they postulate that the artefact must be evaluated using Design Science methods of assessing fitness for purpose, and it must also be evaluated using Natural Science methods of assessing why it is fit for purpose and justifying this assessment. Their view that Design Science requires Natural Science justification goes back to Simon's (1969) idea that Design Science is a type of science. They thus attempt to find a method of justifying Design Science as a Science by stating that whilst "Natural science is descriptive and explanatory...Design Science offers prescriptions and creates artifacts that embody those prescriptions" (March and Smith, 1995). In other words, March and Smith view Design Science as the embodiment, the physical proof of a scientific theory. Hence the "Theorise" and "Justify" activities in the above framework; they represent the generation of scientific theory based out of the proof-of-concept. In other words, if something can be built that is fit for

purpose, then there must be a corresponding theory that explains why what was built is fit for purpose. This is a pragmatist view of the concept of truth (thus, March and Smith also establish the Epistemological position of Design Science as 'Pragmatism'), which is described as "what works in practice" (March and Smith, 1995, paraphrasing Rorty (1982)).

March and Smith (1995) round their paper up by providing examples of how the Evaluation of the different types of artefacts may be performed and also provides pointers on how to conduct the Theorise and Justify activities. The author finds it interesting that a paper on Design Science, published quite early in comparison with other Design Science papers in IS, attempted to seek a strong link with Natural Science. This mirrors Lee's (1999) view that "in the early days" of Management Information Systems, the MIS discipline was "in search of one or another better established field to provide guidance as its 'reference discipline'" (Lee, 1999), with Lee noting with a bit of irony that the 1998 International Conference on Information Systems had set out the task of establishing the "MIS field as a 'reference discipline' for other academic management fields" (Lee, 1999). Perhaps March and Smith's attempts to link Design Science so closely to Natural Science mirrors the attempt of the IS field as a whole to find itself justified as a scientific discipline in its own right. The fact that March and Smith chose Natural Science as their 'reference discipline' is explainable through the fact that they see themselves as "IT Researchers", with IT defined by themselves as "Information technology is technology used to acquire and process information in support of human purposes" (March and Smith, 1995), which stresses the importance of technology and thus they place themselves as closer to Software Engineering than IS, or indeed the Management Sciences.

March and Smith's attempts to explain Design Science as an approach closely linked to natural science is viewed by Hevner et. al. (2004) as an attempt to describe knowledge acquisition through a 'behavioral science' paradigm and they see this as a 'complementary but distinct paradigm' to Design Science

(Hevner et. al., 2004). Hevner et. al. acknowledge the behavioural science paradigm's roots in natural science research (as stressed by March and Smith, 1995) and state that the theories this paradigm tries to develop and justify, "...theories [that] ultimately inform researchers and practitioners of the interactions among people, technology, and organizations that must be managed if an information system is to achieve its stated purpose", (Hevner et. al., 2004) are "impacted by design decisions" (Hevner et. al., 2004). Thus, Hevner et. al. see Design Science as a complementary approach to conducting research as 'behavioral science', for which Bariff and Ginzberg (1982) proposed a framework for conducting behavioural science research in IS, and thus propose a different approach to conducting IS research; their proposal is that since "the goal of behavioural science research is truth" and "the goal of design-science research utility", and since Hevner et. al. position that "truth and utility are inseparable", it follows that Design Science and Behavioral Science approaches investigate the same problem from a different angle and that this suggests that these approaches can be considered to be complementary approaches, as opposed to exclusive approaches (Hevner et. al., 2004).

Following on, Hevner et. al. then agree with March and Smith's assertion that Design Science was 'invented' by Simon (1969) and explain Design Science as a "problem-solving paradigm" (Hevner et. al., 2004), which is focused on the design of innovations that will, on the one hand, define and help with the development of artefacts and, on the other hand, design innovations that will assist with the assessment of IS (Hevner et. al., 2004). By stating that "scientific research should be evaluated in light of its practical implications" (Hevner et. al., 2004), Hevner et. al. build on their earlier statement of Design Science being a 'problem-solving paradigm' and thus establish that Design Science Research must be aimed at addressing practical issues; this is very similar to March and Smith's axiological assessment of Design Science and regarding it as a 'fit for purpose' methodology, aimed at improving specific instances of an unsatisfactory state.

Hevner et. al. (2004) define the term 'artefact' in the IS domain in the same manner as March & Smith (1995), namely:

- Constructs (vocabulary and symbols)
- Models (abstractions and representations)
- Methods (algorithms and practices)
- Instantiations (implemented and prototype systems)

(Adapted *from Hevner et. al. (2004), p. 77)*

In other words, any one of these items represents an IS artefact and Hevner et. al. (2004) states that whichever form an IS artefact takes, it "must be evaluated with respect to the utility provided for the class of problems addressed" (Hevner et. al., 2004). This is due to Hevner et. al.'s view that "Design Science...creates and evaluates IT artifacts intended to solve identified organizational problems" (Hevner et. al., 2004), which means that an artefact is created for a specific purpose in a specific problem setting, and part of the research process is to prove that this artefact serves its prescribed purpose and achieved in solving or alleviating an organisational problem. Thus, evaluating performed research becomes a key activity in Design Science research.

In similar fashion to March & Smith (1995), Hevner et. al. (2004) then prescribe a "conceptual framework for understanding IS research and by developing a set of guidelines for conducting and evaluating good design-science research" (Hevner et. al., 2004). The framework they present has a lot more detail than March & Smith's attempt and provides more detail on the various elements of Design Science research and provides information on how to assess Design Science research. Hevner et. al. (2004) introduce seven 'guidelines', which represent the various elements of Design Science Research. These are:

Guideline	Description
Design as an Artefact	Design-science research must produce a purposeful artefact in form of a construct, a model, a method, or an instantiation.
Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Design Evaluation	The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods. The artefact must yield utility for the specified problem
Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.
Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact. The artefact must also be formally represented, coherent and internally consistent.
Design as a Search Process	The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment. This is an iterative process aimed at optimising a solution, described as the "Generate/Test Cycle" by Simon (1967).
Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

Table 3-3: Hevner et. al.'s (2004) Design Science Guidelines

Hevner et. al. (2004) argue that the above guidelines are going to "assist researchers, reviewers, editors, and readers to understand the requirements

for effective design-science research", meaning that applying these guidelines to a research project will allow a reader to understand whether the research fulfils the guidelines, and thus the requirements for Design Science research. However, one important gap is that Hevner et. al. (2004) do not specify any quality criteria or other measures for assessing to what extent the research complies with the prescribed guidelines; instead, they announce that "how well the research satisfies the intent of each of the guidelines is then a matter for the....readers" (Hevner et. al., 2004), thus leaving any assessment of the quality of Design Science and its adherence to the above guidelines firmly in the realm of interpretive analysis. This leaves a gap with regards to how strongly one of the above guideline needs to be implemented in Design Science in order .to be regarded as 'good' and adherent Design Science Research. The only restriction placed by Hevner et. al. (2004) is the statement that Design Science research ought to address all guidelines "in some manner" (Hevner et. al., 2004).

On the other hand, Peffers et. al. (2008) state that there is a "lack of a methodology...for DS research" and attempt to unite all previously published literature on Design Science by creating a new "Design Science Research Methodology (Peffers et. al., 2008)." Peffers et. al. agree with both Hevner et. al. and March & Smith in that IS is a discipline closely related to the social and natural sciences that form part of the wider Behavioral Sciences discipline (Peffers et. al., 2008). Peffers et. al. then agree with Hevner et. al. (2004) that Design Science deserves to be considered as a viable alternative to a Behavioral Science approach, since design, which Peffers et. al. define as the "act of creating an explicitly applicable solution to a problem" (Peffers et. al., 2008), features "in just a small minority of research papers" (Peffers et. al., 2008). Thus, Peffers et. al. have made three important statements:

1. They agree with Hevner et. al. (2004) that Design Science ought to be regarded as an alternative approach to IS that complements the Behavioral Science approach to IS

2. Design Science concerns itself with solving real-world problems through the creation of "applicable solutions to a problem" (Peffers et. al., 2008)

3. Design Science has yet to be broadly accepted by mainstream IS research

Statements 1 and 2 concern the earlier paragraphs in this chapter that aimed to pinpoint the origins of Design Science and to understand the principle aim of undertaking a Design Science approach in IS research. Three major authors of Design Science research have pinpointed Design Science as an alternative, yet complementary, approach to the Behavioral Science approach. The importance of this is grounded in the fact that Culnan and Swanson (1986) state that, actually, IS "represents the intersection of...computer science, behavioural science, decision science, organisation and management science..." (Culnan and Swanson, 1986; p. 289); this means that Design Science is seen as a methodology which widens the scope of one of IS' 'influencing' disciplines (namely Behavioural Science). This, in turn, widens the scope for IS research since it would give researchers a further set of tools with which to investigate the influences and effects of an Information System to a particular organisation.

Three major authors have also agreed that Design Science is all about problem solving within a real setting. Peffers et. al.'s final statement also shows their intent in producing their research paper – they see a lack of adoption of Design Science and realise that they consider a "lack of a methodology" (Peffers et. al., 2008) to be the prime reason for the limited amount of published Design Science research. Their justification for this conclusion is that due to the low exposure of Design Science in published work, they assert that "no such commonly understood mental model exists" and that "Without one, it may be difficult for researchers to evaluate it or even to distinguish it from practice activities" (Peffers et. al., 2008).

In other words, the lack of exposure through published research results in researchers being unfamiliar with the concept of Design Science, which then leads to researchers having a limited understanding of Design Science and thus their inability to properly assess and evaluate Design Science research output and leads to limited understanding about how Design Science research can be viewed upon as an activity different to practice activities. Peffers et. al. attempt to close this gap by developing a Design Science Research Methodology in order to "help with the recognition and legitimization of DS research and its objectives, processes, and outputs, and it should help researchers to present research with reference to a commonly understood framework" (Peffers et. al., 2008). Taking into account Peffers et. al.'s earlier assumption that the lack of methodology is a reason for the seemingly low adoption of Design Science, then the attempt to design a methodology seems like a prudent course of action in order to increase awareness and understanding of Design Science.

Peffers et. al.'s literature review does include March & Smith (1995) and Hevner et. al. (2004), but neither are regarded by Peffers et. al. (2008) as being capable of providing a complete methodology. Peffers et. al. (2008) define methodology as "a system of principles, practices, and procedures applied to a specific branch of knowledge" (Peffers et. al. (2008), quoting the DMReview Glossary (2007)). They thus consider March and Smith's (1995) research to contribute to a "conceptual and paradigmatic basis for DS research" (Peffers et. al., 2008), alongside with other research of the same time period (e.g. Walls et. al. (1992), Nunamaker et. al. (1990)), whilst Hevner et. al.'s research is considered to contribute "practice rules for conducting DS research" (Peffers et. al., 2008) through the provision of Hevner et. al.'s (2004) seven guidelines. Taking into account Peffers et. al.'s earlier definition of methodology (i.e. Principles, Practices and Procedures), Peffers et. al. thus see March and Smith's research to contribute to 'Principles', Hevner et. al.'s research to contribute to 'Practices' and they assert that 'Procedures', which "provides a generally accepted process for

carrying it out" (Peffers et. al., 2008), are the "missing part" (ibid.). Thus, Peffers et. al. (2008) wish to complete the gap in the theory of Design Science by providing a procedure for conducting DS research; through acknowledging the influence of other authors on the development of Design Science as a valid approach in IS, Peffers et. al. (2008) thus force themselves to "build upon prior literature about DS in IS" (Peffers et. al., 2008), meaning they are not going to change the nature of Design Science, but merely close a gap in it and thus provide a more complete picture of Design Science than was previously possible. This is therefore a slightly different approach to describing Design Science than any of the previously mentioned authors, in that Peffers et. al.'s research can be viewed upon as a consolidation of existing Design Science knowledge and offers to close an identified gap within the existing Design Science literature.

Peffers et. al. (2008) state that they closed their identified gap in the existing literature by building their findings "upon prior literature about DS in IS and reference disciplines" (Peffers et. al., 2008), thus stating that their findings are based upon previous research results and therefore their new material is building upon past material and can therefore be judged to be a continuation of earlier research. This is evident through Peffers et. al.'s continued references to ensuring the acceptance and adoption of past research, such as "we looked to influential prior research and current thought to determine the appropriate elements, seeking to build upon what researchers said in key prior literature about what DS researchers did or should do" (Peffers et. al., 2008), showing that Peffers et. al. placed great emphasis upon their results being compatible with prior research in this area. On this basis, Peffers et. al. developed a 'mental model' that defines their understanding of what constitutes a Design Science Research Methodology and the process required to conduct such research (Peffers et. al., 2008). Their model consists of 6 individual steps, all of which have groundings in past Design Science research. The steps are defined by Peffers et. al. (2008) as follows:

1. Activity 1: Problem identification and motivation. The specific research problem is defined and the value of the solution justified. This activity is to motivate a researcher to pursue a solution and help the audience of the research understand the researcher's understanding of the problem. Peffers et. al. (2008) state that this problem can not be directly translated into system objectives (also called 'metarequirements' by Walls et. al. (1992)).

2. Activity 2: Define the objectives for a solution. These are quality criteria that need to be met by the solution to the problem defined in Activity 1. It may be either quantitative ("terms in which a desirable solution would be better than current ones") or qualitative ("description of how...artefact is expected to support solutions"). As the objectives must be directly inferred from the problem specification, this activity will require knowledge of the problem, the current solutions (if existing) and the current efficacy of existing solutions.

3. Activity 3: Design and Development. This is artefact creation. It can be "any designed object in which a research contribution is embedded in the design" (Peffers et. al., 2008). This activity also covers the requirements gathering and planning activities necessary prior to constructing the actual artefact. According to Peffers et. al. (2008), "all of the researchers focus on the core of DS across disciplines – *design and development*" (emphasis in original; Peffers et. al. (2008).

4. Activity 4: Demonstration. Demonstration of the artefact's ability to solve instances of the earlier stated problem through "experimentation, simulation, case study, proof, or other appropriate activity" (Peffers et. al., 2008). In other words, this is initial proof that the artefact developed has the capability of addressing the problem stated in Activity 1.

5. Activity 5: Evaluation. Observe, measure and evaluate to what extent the artefact solves the problem stated in Activity 1. This Activity will apply the criteria identified in Activity 2, thus the evaluation can be either quantitative or qualitative, based on the quality criteria stated in

Activity 2. This activity has two possible outcomes: either research work iterates back to Activity 3 to refine the produced artefact, in case the evaluation reveals quality criteria were not met, or if the criteria were met, the research project will continue to Activity 6 (Peffers et. al. (2008)).

6. Activity 6: Communication. The dissemination of the knowledge gained in understanding and analysing the problem, the utility and novelty of the artefact, rigor of the artefact's design and the relevance to other practicing professionals. In particular, Peffers et. al. (2008) recommend applying the structure being explained here being applied in presenting Design Science research, such that the audience can follow the Activities in a structured manner.

Finally, Peffers et. al. (2008) state that Design Science would not necessarily need to follow the six activities in a sequential order; Peffers et. al. (2008) make an allowance for a Research Project to start between Activities 1 and 4, but state that a Design Science solution can only be achieved "if researchers work backward to apply rigor to the process retroactively" (Peffers et. al., 2008), meaning that whilst the starting point of the Design Science research process is fluid, the complete process must be followed through in order to constitute Design Science.

Design Science in Management Science

Design Science exists as a topic within the discipline of Management as well and, due to the inherent overlaps between the Information Systems and Management disciplines, it can be expected that there should be some overlap in the meaning of the term between these two disciplines. Indeed, published research in Management broadly agrees with the basic tenets of Design Science discussed above, such as the iterative development of a solution that must be of relevance to practice (e.g. Huff et. al., 2006; Van de Ven and Johnson, 2006; Van Aken, 2005). In particular, Huff et. al. (2006) mention that the 'end state' (i.e. the solution) of a Design Science

intervention in management must be "specifically designed", which is very similar to Peffers et. al.'s (2008) Activity 2 (see above); however, in Management Huff et. ai. (2006) warn against the research process taking too long and may thus produce outdated results that are no longer relevant to the overall context against which they were designed. Therefore Huff et. al. (2006) and also Van Aken (2005) stress that any Design Science in Management must always be fully cognisant of the contextual situation within which Design Science is being conducted. Most research in this area recognises that currently there is little codified design knowledge to link the type of intervention with the actual outcomes, an area of ongoing research (Huff et. al., 2006). Similar to the way Design Science is treated in Information Systems, it is expected that Design Science produces evidence that the results are relevant to practice, which furthers the view that Design Science is of a Pragmatist orientation. A key difference of Design Science between the two disciplines is in the nature of the artefact – whilst in IS an artefact can be one of Instantiation, Method, Model or Construct, in Management Science it is exclusively in form of a 'technology rule', a set of broad guidelines that make the research results applicable to a wider setting than that originally investigated (Huff et. al., 2006; Van de Ven and Johnson, 2006).

3.4.4 Design Science - Summary

The previous pages have provided a broad outline on what constitutes 'Design Science'; most authors indicated how they see Design Science as having evolved out of Simon's "Science of the Artificial" (Simon, 1969) and provided various methods and perspectives on what constitutes Design Science in IS, processes on how to do it, and methodological background on where Design Science fits in amongst other IS approaches.

Peffers et. al. (2008) identified 6 key activities that, in combination, provide a "mental model" that outlines a "Design Science Research Methodology" and

thus outlines a process that must be followed in order for research to be acknowledged as valid Design Science research (Peffers et. al., 2008). These activities are:

1. Problem identification and motivation
2. Define the objectives for a solution
3. Design and Development
4. Demonstration
5. Evaluation
6. Communication

As Peffers et. al.'s (2008) research is built upon previous research in the area of Design Science, it comes under no surprise that many of the elements identified by Peffers et. al. (2008) can also be found in Hevner et. al.'s (2004) results.

Hevner et. al. (2004) also investigated previous research on Design Science and identified a range of 'identifying features' which, when combined in a research project, are indicative of Design Science research having been carried out. Hevner et. al. (2004) identified the following features that constitute Design Science:

1. Design as an artefact
2. Problem Relevance
3. Design Evaluation
4. Research Contributions
5. Research Rigor
6. Design as a Search process
7. Communication of Research

Whilst a lot of Hevner et. al.'s features are very similar to Peffers et. al.'s activities, there is a significant difference between the two; Hevner et. al.

(2004) stated that the identified seven features must be present within a research project in order for it to be considered Design Science. In other words, this is the "what" of the research. On the other hand, Peffers et. al. (2008) specified a Design Science methodology; therefore, their activities must be performed and completed in order for research to be acknowledged as Design Science, meaning that Peffers et. al. (2008) identified the "how" of the research.

3.5 Conclusion

It has been shown how this research project can be identified as a qualitative study that utilises an Action Research methodology. It was shown how and why this is a qualitative study by presenting the aspects of a qualitative and quantitative study and relating them to the project. On establishing that it is indeed a qualitative study, a search was performed for finding the appropriate research methodology. Several traditional and well-known qualitative methodologies all had to be considered as inappropriate for the intervention in question before identifying Action Research as a candidate methodology, due to the nature and wording of the research question. Furthermore, it was established how Action Research can contribute towards achieving the wider research aims as well. Having reviewed several points of view on Action Research and having compared these views to the project, it was found that there is sufficient evidence to support the usability of Action Research as a methodology for this study. Baskerville (1999) hints that it is possible to use Action Research in an IS project and this project will add further evidence towards supporting the view that Action Research might generally be suitable to IS projects – it should be borne in mind that this would be a research by-product of little relevance to the research question, however. The primary focus of this study is the development of the transformation method that can provide a solution to the research question.

Also, these sections introduced the Research Methods that were employed in this project. An overview over the general approach to the project was given,

showing how the project follows the Action Research methodology by adopting a cyclical development approach, in close cooperation with the problem owner, as is required of Participatory Action Research. This 'feature' of this research methodology is important when considering the research aims, as the research aims do contain any obvious quantitative measures that could be measured at the end of the research. Instead, the research aims mention the provision of generic abilities and tools to convert legal acts to process models, to allow operation by staff not legally qualified and to allow operation in a structured and repeatable manner. These words are open to interpretation and therefore an iterative research methodology can allow the researcher and the collaborator to work closely together until both parties are satisfied with the research outcomes.

Finally, the previous section hinted upon the fact that the research may be adhering to the processes and procedures of an alternative research methodology, namely Design Science. A background on Design Science was provided and a full analysis between the activities of the research and the requirements of Design Science is going to be undertaken in Section 5.2.

4 Results

Having introduced an overview of the problem domain and illustrated what the motivation for the research is, and having illustrated and described the Research Methods and its influencing Research Methodology on how the research was undertaken, this section now introduces the results of the research and shows what was achieved.

4.1 Background and Initial Analysis

The problem owner referred to earlier is the Catalan Certification Authority, known as CATCert, who are based in Barcelona, Spain and were formed in 2002 as an autonomous organisation forming part of the eGovernment Administration of the region of Catalonia. Its mandate encompasses providing the necessary tools to conduct eGovernment transactions between the Administration and Businesses and Citizens in an easy and comfortable manner which at the same time adheres to the legal rules of Catalonia. As part of this mandate, CATCert has developed standards for Digital Certificates and Digital Signatures to be used in eGovernment transactions involving Catalonia's eGovernment infrastructure. CATCert is also involved in a number of research initiatives (e.g. project GUIDE, project STORK) and is involved in co-authoring Digital Signature standards for OASIS and thus demonstrates a high degree of competence and proficiency in Digital Signatures and related technologies. CATCert also organises an annual conference in Barcelona on Electronic Signatures (called "Jornades de signature electronic") which is used by CATCert as a platform to engage in discussions on Digital Signature standards for eGovernment in Spain.

Catalonia's regional government was in the planning stages for new eGovernment infrastructure, which included electronic document exchange between the government and citizens and businesses. Therefore, document security technology, especially DSPs, was of high interest to CATCert, who conducted initial research into this area and had developed a prototype

method for producing DSPs, called 'PADS'. CATCert suffered from the same issue that the researcher had, namely that there was a lack of information on how the technology could be utilised and, specifically, on how to turn natural language legal text into a formal XML DSP.

PADS stands for 'Processes, Acts, Documents, Signatures' and is a questionnaire developed by CATCert for capturing the necessary contextual information from legal process, document and signature flows in order to be able to create the necessary, legally valid DSP to accompany digitally signed official documents. Currently, this process is rather disjointed or ad-hoc, with no clear rules implemented to arrive at valid signature policies. The normal procedure is for an administrator to consult the appropriate legal texts with the PADS questionnaire and extract the appropriate legal information. The worker would then utilise his legal and technical knowledge and experience to place the information into a DSP by hand.

There are a number of drawbacks with this procedure; firstly, the administrator must be trained and well versed in both legal matters and have skills in programming in order to be able to create the XML-based DSP. Secondly, the legal procedures and statues relating to documents are process-driven within Catalan legislation, therefore there was a need to capture procedural aspects of the legislation, which the prototype method was capable of eliciting but not able to insert them in a DSP. Finally, completed questionnaires were usually discarded after use, which meant that the organisation lost any specific knowledge that could have been utilised in the future to re-create or update existing DSPs. One of the early requirements that emerged in an early meeting was the insistence that PADS form part of the 'new' solution as the organisation hoped to reduce the complexity of the transition between the 'old' and 'new' method, so that administrators could be trained quickly on the new method. Also, despite being made aware of recent automated legal information extraction research (e.g. Mercatali et. al., 2005),

they decided that a more conservative approach would present less of a risk when realising the technical complexity of the solutions involved.

The PADS questionnaire is divided into four major groups, Processes, Acts, Documents and Signatures. Each major group consists of a series of questions, aimed at extracting contextual information about a legal process, a document or a signature.

The first step taken by the researcher was to categorise the individual questions into groups of questions with similar content. For example, several questions aimed to extract contextual information on involved actors, or the involved legal provisions of a specific process. This aided in gaining a more concrete understanding of which type of information was important and needed to be captured in the method.

The second step was to examine the method from the point of view of how it could be implemented graphically. This was necessitated by the fact that Catalan law is process-driven and document and signature legality depend on the procedural nature of the law being followed; therefore, it was necessary to develop a graphical view of the process sequences that led to the application of a Digital Signature to a particular Document as part of a particular legal act, as graphical views through a Business Process Modelling notation are particularly adept at representing such sequences. The analysis of the questions required by the different views helped to bring shape to this step and aided the organisation of information. Additionally, the splitting of PADS into three distinct groups (Acts; Documents; Signatures) showed some clear boundaries between different types of data required for each of the different groups. On completing this analysis, the results were verified with CATCert and this reverse engineering was largely correct, with some details requiring several iterations to be corrected. Sample feedback from one of these iterative research cycles follows:

"The controls asking for question number 2. "Other accreditation"
panel must be only accessible if "Other" is selected as Personal
Condition. Controls about condition aren't needed in some cases,
and the "Signature Time" control is not needed, because we can't
know the exact moment of a concrete signature, and we can't
describe a Signature Policy for each document to be signed."

Further influences into the graphical element of the new PADS method being developed was the mandated need for regular office users to be able to quickly understand and be able to utilise effectively the graphical notation to be developed. As a result, many of the approaches identified in Chapter 2 were found to be ineffective due to their steep learning curves and the size of investment required to procure such an IS and IS specialists. An identified method that did work very well was the Business Process Modelling Notation developed by Seltsikas and Palkovits (2006), which was already familiar to the problem owners as a modelling notation used in cross-border eGovernment development. This provided a starting stone for the graphical notation and was agreed at the more formal kick-off meeting in Barcelona (see Table 3-1).

With the above influences having aided in understanding PADS itself on the one hand, and understanding the organisation of information within PADS on the other hand, it was possible to develop a range of graphical elements that capture the same information as PADS and to develop a scheme that allows the accurate 'transformation' of data from questionnaire to graphical workflow. Developing the graphical elements therefore completed the introduction of PADS into an electronic BPM toolkit. These graphical elements were initially created by hand, using pen and pencil, until the researcher was satisfied that PADS was adequately represented by the symbols. The researcher then utilised the help of an Adonis specialist to import these drawings into Adonis. Once in Adonis, the researcher created a short document that described each new symbol and how it related to PADS. This document was sent to CATCert and triggered several iterations of development as the researcher and CATCert refined the visual look of the graphical representation of PADS. After several iterations, the client

organisation and researcher were satisfied that the visual notation was suitable and well-adapted for CATCert's needs. Below follows a sample response, received after an early version of the graphical notation was sent to the problem owner:

> "I think that the adaptation you prepared of ADONIS is good, but there
> are some screens that perhaps need be changed"

The next step was then to look at the wording of the ETSI TR 102 038 v 1.1.1 standard and assess the type of information required by the standard in order to yield a valid DSP. This was necessitated by the fact that the 'updated' PADS had been deployed into an electronic BPM toolkit, but it hadn't been established whether the graphical PADS was capable of capturing sufficient data in order to satisfy the data requirements of the ETSI TR 102 038 DSP standard. Therefore, this analysis was used to assess how much of this information is yielded by PADS and its graphical equivalent. Discrepancies were recorded and improvements to both PADS and the graphical element implemented, in order to provide this information. These changes resulted in a slightly changed PADS questionnaire, as well as a changed graphical element of what was produced earlier. These steps were iterated several times and each iteration validated by the problem owners, resulting in a high degree of confidence in the results. Significantly, some of these exchanges between problem owner and researcher required the researcher to understand the content of some data fields. The explanation of these data fields by the problem owner revealed that these data fields needed to be completed with controlled data, which did not yet exist as such within the client organisation. Therefore, the researcher was not able to continue until the data had been controlled through the issuing of a data specification. This important point is discussed at lengths in Chapter 5.4. The following snippet from an email shows how the information provided by this document provided the researcher with an answer to a specific question:

> "Question 7: You can find CATCert's classification schema for
> authentication methods in the email attached. In ADONIS you have
> included selectors for identification and authentication. Perhaps
> only one of them is going to be needed. In any case, the
> authentication method control only has to be available when it's
> required (when question answer is yes)."

However, the aforementioned mapping document itself caused some further iterative research loops because the researcher lacked the intricate understanding of the subject matter that the problem owner possessed. Consider the following question asked by the researcher:

> "I also have a few questions from the mapping document:
>
> 3) Regarding the Qualifying Properties – you made a reference to TS
> 101 903, that document identifies 10 Properties (Signing Time,
> Signcing Certificate, etc etc), only one of which (Counter
> Signature) is unsigned. So I have several questions about this
> actually:
>   - there are therefore 9 signed properties (for signer), and
> the signer may have to provide 0 or more, correct?
>   - there is one unsigned property (for signer), which the
> signer may or may not have to provide, correct?
>   - What are the unsigned properties for Verifier? Is it also 0
> or more options?
>   - The standard mentions that the properties are all
> identified through URI – what are these URI's?"

The problem owner solved these questions through the use of examples; in this particular case, the problem owner sent some examples that showed the various conditions that the above property fields can take and appended those examples with the following:

> "3.- Take a look to signature policy attached. Commonly, the only Signed
> Property needed ever is the SigningCertificate, and the signature policy
> identifier in some cases. SigningTime is signed too, but it isn't
> required, because a timestamp is more secure. You can see, in the same
> example, how URI are introduced."

One can see that different methods were utilised to progress the research; sometimes explanatory comments were provided, at other times examples were provided, and the above exchange shows that a combination of explanation and example was used to progress learning in the researcher and the problem owner.

This analysis of the various data requirements quickly resulted in masses of information becoming unmanageable by the researcher and the client

organisation. In fact, as the work on the data elements was drawing to a close, the problem owner remarked that the complexity of the data had become too large and that they needed a guiding hand to understand the interrelationships better. As a result of this exchange, a UML technique known as 'metadata modeling' (Booch et. al., 1998) was applied in order to graphically visualise the relationships between the various elements of data, the data requirements of the individual 'concepts' (ibid.), and to provide a graphical aid in organising and understanding this complex data. The result of this modelling is presented in figure 4-1 and captures key information about the relationships between the various concepts.
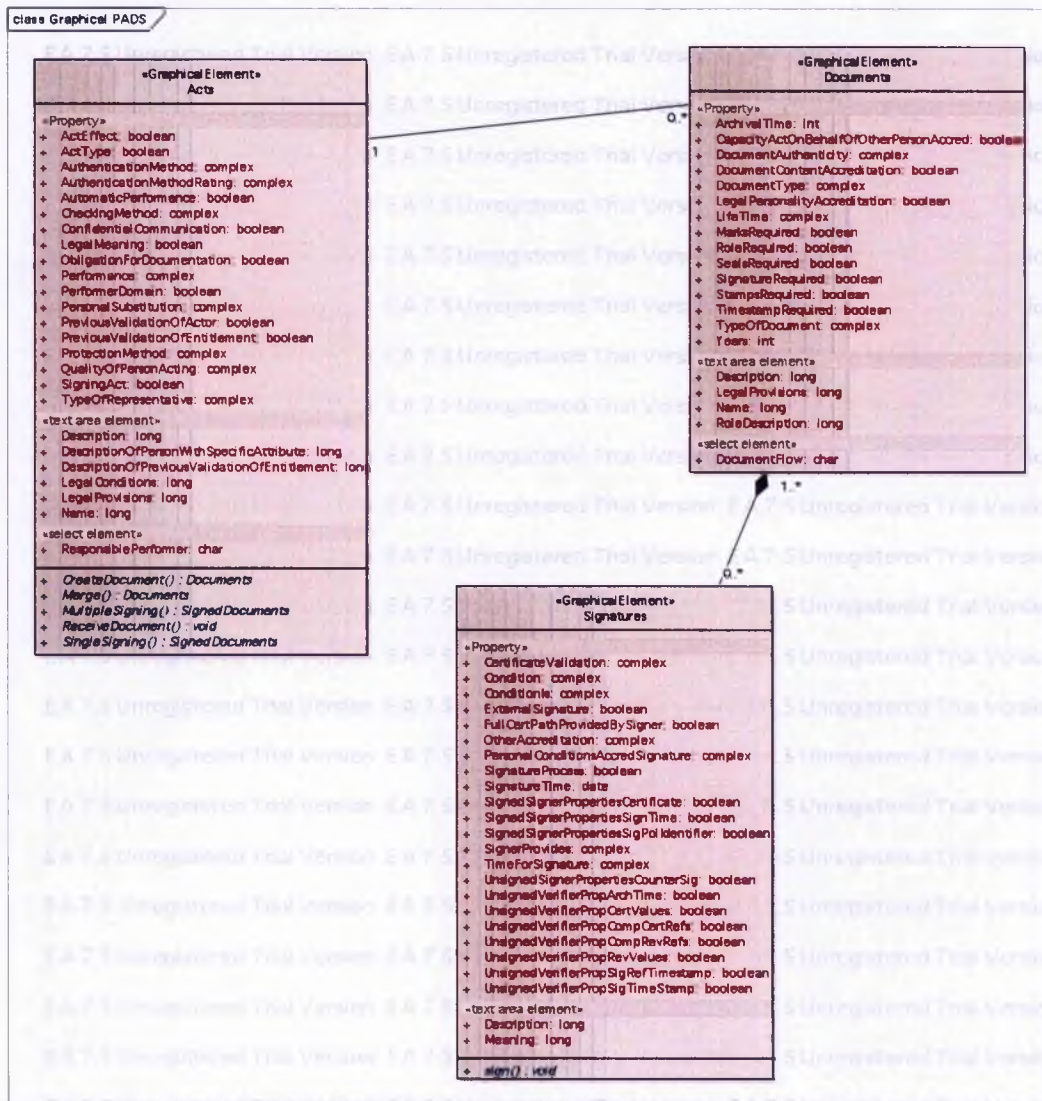

Figure 4-1: Metamodel of PADS and Digital Signature Policies

Note that in figure 4-1 above, Signatures are an 'Aggregation' (ibid.) of Documents and Acts can exist independently of Documents. It thus captures the fact that whilst an Act can exist without a document, a document can not exist without an Act. Similarly, a document is required for a Signature to exist. This decomposition of the data involved would later prove extremely useful.

Therefore, the development of PADS into a full-blown graphical representation of legal workflows was influenced by two major factors: the requirements of ultimately producing an ETSI compatible DSP, and the author's experience in business process modelling and in the toolkit used. The result is a business process modelling notation that is capable of capturing enough contextual information from a legal act's workflow in order to create a DSP that can conform to the ETSI standard. These results were arrived at through continuous exchange of emails, occasional phone calls, and a number of documents that were returned with detailed comments.

The following pages shall feature the re-worded version of the PADS questionnaire, as it is of key importance to the method since it is this questionnaire that is the vehicle of eliciting key requirements relating to the context within which DSPs are to be employed. Finally, the developed method shall be demonstrated using a sample process.

4.2 PADS Questionnaire

The following matrix is the expanded PADS questionnaire. As mentioned previously, the original questionnaire was found to be lacking in yielding sufficient data to satisfy the ETSI TR 102 038 data requirements. Therefore, the additions were aimed at yielding the required data. The original PADS Questionnaire can be found in Appendix A. Changes/new additions to the questionnaire are highlighted with italic font in the table below to aid understanding.

Question	Potential Answers
Process Analysis	
All questions were removed, since they are addressed through the graphical element - as explained above, the need to capture information on the sequence of events was addressed by implementing a graphical modelling notation	
Acts Analysis	
1. Which is the content of the Act?	• Act's description • Type of Act ○ Citizen Act ○ Administration Act ○ Other • Effect of Act on workflow ○ Initiates ○ Terminates ○ Other
2. Which is the regulation applicable to the act?	• Identification of the applicable legal provisions • Legal meaning of the act (regulated or discretional act, other) • Legal conditions required to perform the act • Legal or administrative obligation to document the act
3. Who performs the act?	• Natural person / citizen • Administrative Worker • Administrative Authority (Organ, Department)

Question	Potential Answers
	• *Specify entity that actor belongs to (department, etc)*
4. In which quality is the person acting? Is the person acting on his/her own behalf or on behalf of another person?	• On his/her own behalf • On behalf of a public or private legal entity, for which he/she is a corporate organ (organic representation) • On behalf of a public or private legal or natural person, for which he/she is a legal representative (legal representation) • On behalf of a public or private legal or natural person, for which he/she is a voluntary representative (notary or registry representation) • On behalf of a public or private legal or natural person, acting as a professional representative
5. Is personal substation allowed?	• Acts strictly personal • Any kind of representative • Any person with a concrete attribute (e.g. any worker belonging to a group or department)
6. Does the Act generate a new document, or is it added to a previous document, or is it added to an expedient or book?	• Generates a new document • It is added to a previous document • It is filed into a registry, without generating a new document
7. Does it require the previous validation of the person performing the act?	• Yes/No • Determination of the identification and authentication method of the acting person • Rating of the method, according to CATCert's classification scheme

Question	Potential Answers
8. Does it require the previous validation of the entitlement in which the person acts?	• Yes/No • Checking method of the personal condition, in case of organic or legal representatives • Checking method of the entitlement or authorisation, in case of voluntary representatives • Checking method of the professional condition, in case of professional representatives
9. Does it require a previous or posterior confidential communication?	• Yes/No • Determination of the protection method used
10. Is the act of automatic performance?	• Yes/No • Determination of mechanic or automatic treatment
Documents Analysis	

1. Which is the content of the document?	• Document's description
	
	• Type of document
	   o Private
	   o Administrative
	   o Public

2. Which is the regulation applicable to the document?	• Identification of the applicable legal provisions

3. Which formal requirements apply?	• Document needs to be:
	   o Original
	   o Simple Copy
	   o Authenticated Copy

Question	Potential Answers

	• Needs to incorporate a digital signature
	
	• Needs to incorporate:
	
	    o Marks
	
	    o Stamps
	
	    o Seals
	
	• Needs to be stamped with Date and Time
	
	• Needs to incorporate role or another personal attribute or condition

4. Which content accreditation requirements apply?	• Need to accredit legal personality • Need to accredit the capacity to act on behalf of another person • Need to accredit the document content
5. Which is the expected lifetime of the document?	• Active or semi-active term, in years • Archival term, in years
Signatures Analysis	
1. What is the legal meaning of the signature?	• Description of the legal meaning • Legal description of the signature, when it belongs to a signature process
2. Which personal condition accredits the signature?	• Author or another (substitution, delegation or another mechanism) • Acts on his/her own behalf, or on behalf of a third party • The condition (role, attribute) is certified or claimed
3. Is there a need to ensure signature time	• Yes/No

Question	Potential Answers
independently from the document time?	
4. Is there a signature process?	• Yes/No
5. What is the signature validity period?	• Provide Lifetime period
6. Is the signature external from the objects it signed?	• Yes/No
7. Is the signer providing the full certification path?	• Yes/No • Signer provides own/all certificates
8. Does the signer need to supply signed/unsigned properties?	• Signed: yes/no • Unsigned: yes/no
9. Does the verifier need to supply unsigned properties?	• Yes/No
10. How is the certificate to be validated?	• CLR/OCSP/EITHER/BOTH/NONE
11. What are the valid signing algorithms and their minimum key lengths?	• Specify 6 algorithms & key lengths

Table 4-1: New PADS Questionnaire

Thus, all necessary and relevant information in order to create a DSP is captured through the re-developed version of the questionnaire for the extended PADS methodology. It should be noted that the above questionnaire underwent several research iterations through the exchange of annotated documents, as described in figure 3-2, in order to ensure that all possible data requirements were covered. Below follows an example of feedback from the problem owner, agreeing to the removal of the first set of questions on processes (see Table 4-1, first entry):

> "In Fact, the only relevant practical question in this form is the third one, asking for a graphic representation of the workflow which we can draw using Processes and Acts diagram."

The questionnaire introduced above was of key importance when it came to developing the graphical Business Process Modelling Notation for the

extended PADS method, as it provided a guideline with regards to the kind of data required to capture by the notation. As explained earlier, the original PADS Questionnaire is included in Appendix A.

4.3 BPM Notation

The questionnaire introduced above covers the necessary contextual information to arrive at a signature policy in the ETSI standard. However, in order to be used in a graphical toolkit and thus make the process of creating signature policies more convenient, formal and controlled, graphical elements need to be introduced in order to carry and convey the information elicited through the questionnaire. The following sections will introduce a variety of graphical elements that are going to visually represent the information contained within a PADS questionnaire and thus ultimately the information contained within a DSP.
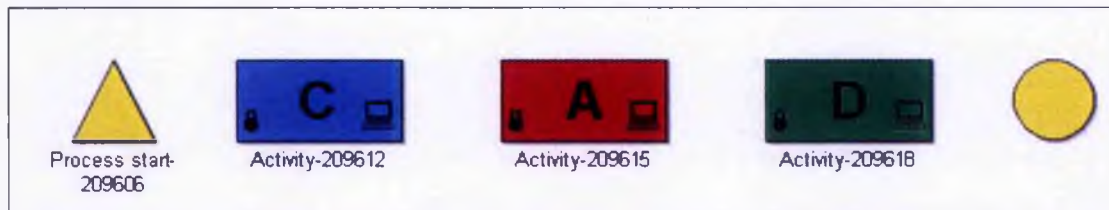
4.3.1 Acts

Figure 4-2: Acts Symbols

The above figure 4-2 represents the main symbols to be used in a Legal Workflow. From left to right, the symbols are:

1. Process Start Event

2. 3 Acts of different domains (more below)

3. End Event

The three Acts and their depiction represent question 3 from the Acts chapter of PADS and use colour coding to present the information required by that question. The symbols represent Processes and Acts within a legal workflow. Double-clicking on these boxes will call up an 'Adonis Notebook', containing elements that are described below. PADS differentiates between three different types of Actors (represented by the three different colours):

- Citizens

- Administrative Workers

- Administrative Authorities (such as governing organ, or a council department)

Due to the requirements of the ETSI DSP standard, a new element is added to PADS, which adds contextual information to the actors. The swimlane concept is to be used to denote the contextual work area of the different actors; that is, by using swimlanes (Seltsikas & Palkovits, 2006) the model will be able to differentiate between Administrative Workers in different offices or organs. This is less relevant to citizen actors, however, administrations require the differentiation between their different offices and departments. This explains the extended version of question 3 of the PADS questionnaire (see Table 4-1) and the graphical element therefore looks as follows:
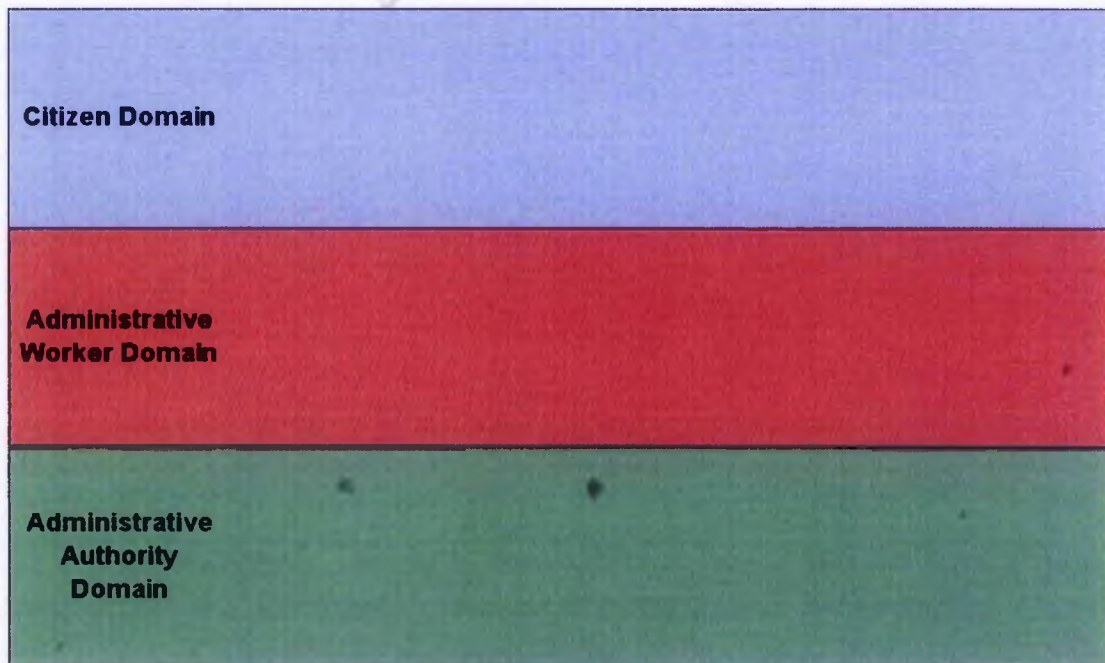
Figure 4-3: Swimlanes

As one can see, the actors' processes can be represented within separate swimlanes that denote the administrative departments the actors belong to through the different colours separating different organisational contexts. The different swimlanes, from top to bottom, are as follows:

- Citizen Domain: blue colour, denoting citizens
- Administrative Worker Domain: red colour, denoting that a process or act is being performed in an administrative worker domain
- Administrative Authority Domain: green colour, denoting that a process or act is being performed by an organisational unit (or within an organisational unit)

With the swimlanes separated like that, it is possible to ascertain the kind of activity performed by an actor within a particular domain. For example, a Citizen might be performing an activity within the Administrative Authority Domain, or vice versa. There is a distinct impact in choosing the actors, as the type of Digital Signature Policy will be different due to the fact that CATCert issue different certificates to different actor types. This is described

by feedback received in one of the research iterations when the researcher was trying to understand the significance of the concept of actor in this context:

> "The third question asks for who performs the act, and possible answers are Natural Person, Administration worker or Administrative Authority. Only for information purposes in order to build a signature policy, probably you have to know or certificate profiles for all of them. They are:
>
> Natural Person: No special certificate profile restriction. We issue certificates for citizens, called idCAT, but in any case, all the certificates issued by trusted certification authorities will be accepted.
>
> Administration workers: We offer a special profile for Administration Workers called CPISR. We have CPISR with and without entitlement. This entitlement is going to be needed when the act needs the participation of a specific person into administration (Major, Secretary, etc.)
>
> Administrative Authority: We have certificates for juridical persons but commonly acts carried out by administrative authorities could be performed automatically. In this case, a Application device certificate should be used. We call it CDA."

This shows the significance of choosing the correct actor for a specific Act.

As mentioned previously, a double-click on a process in Adonis calls up the 'notebook' feature; the notebook contains pertinent contextual information about a specific Act or Process and thus is the main bearer of the information required for a DSP. Since PADS is fairly extensive, a variety of 'tabs' are required to capture this information. Therefore, the following figure shall be representative of this feature; further examples are all provided in Appendix D.

Figure 4-4: Acts Notebook, Description Tab

Figure 4-4 shows the make up of the Description tab of the Act Notebook. It allows the user to select the actor responsible for performing the Act and also provides necessary input information for ADONIS. Under "Name", the name of the Act can be entered; this name is later displayed in the graphical overview

of the workflow and is a key component for linking Acts/Processes with Documents and Signatures. Also, the performer domain can be chosen, thus specifying the kind of actor performing the Act. Choosing the actor will result in the colour of the Act box changing, as outlined in figure 4-2.

Furthermore, question 1 of the Acts chapter in the PADS questionnaire is also represented within this notebook and allows the user to input contextual information about the following:

- A general description of the Act and its purpose in a legal workflow

- The type of Act (Citizen Act, Administration Act, Other)

- Act Effect on a workflow, or on a process (Initiates, Terminates, Other)

Finally, the tab offers a tickbox which is not related to PADS; this is the "Signing Act?" tickbox and it serves the programmatical purpose of indicating that this particular Act is performing the signing of a document, thus indicating that this Acts' contextual information is relevant and needs to be encoded in a Signature Policy. If a particular Act does not sign a document, then this tickbox must not be ticked. If the Act does sign a document, but the tickbox is not ticked, then a signature policy can not be created for this Act, therefore it is imperative to tick the tickbox if it signs a document. This particular approach is a necessary work around to overcome the tool's limitations.

This is merely an excerpt from the full range of screen options available in the developed BPM Notation. The remainders are demonstrated and explained in Appendix D.

4.3.2 Documents
This section describes how the Documents section of PADS is represented graphically in Adonis. The handling of documents is necessary since PADS

elicits information about document handling and when and how and under what legal conditions the documents in question are to be signed. Therefore, knowledge of the documents is necessary for a DSP.

The figure below displays the various document symbols to be used in the process model itself and denote the flow of the documents within a legal workflow.
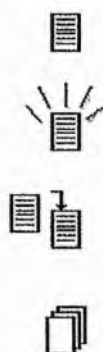
Figure 4-5: Documents Notation

The four symbols in the above figure are to be used in the main process model view and their meaning, from top to bottom, is as follows:

1. The standard document symbol; when located at the left edge of a process, it acts as an input to the process. When located at the right edge of a process, it acts as an output to the process

2. When a new document is created by a process, this symbol gets used to denote 'new' documents. This is different to obtaining a new document through a merge

3. This symbol indicates that a new document is created through a merge of documents

4. This symbol indicates that a document that was used by other processes is entering a finalised state of 'filed' or 'archived'.

As with the Acts introduced in Section 4.3.1, the Document symbols have a large number of data associated with them which can be accessed via a double-click on the Document symbol within the tool. The details of these can be found in Appendix D.

4.3.3 Signatures

This section describes the graphical implementation of the Signatures section of the PADS questionnaire within Adonis. The use of Signatures is important, since the Signature Policy is to govern how and when a Digital Signature is legally valid within the confines of the law. Therefore, knowledge about which signature is to be used for which Act and Process is important, as are the legal implications surrounding its use.
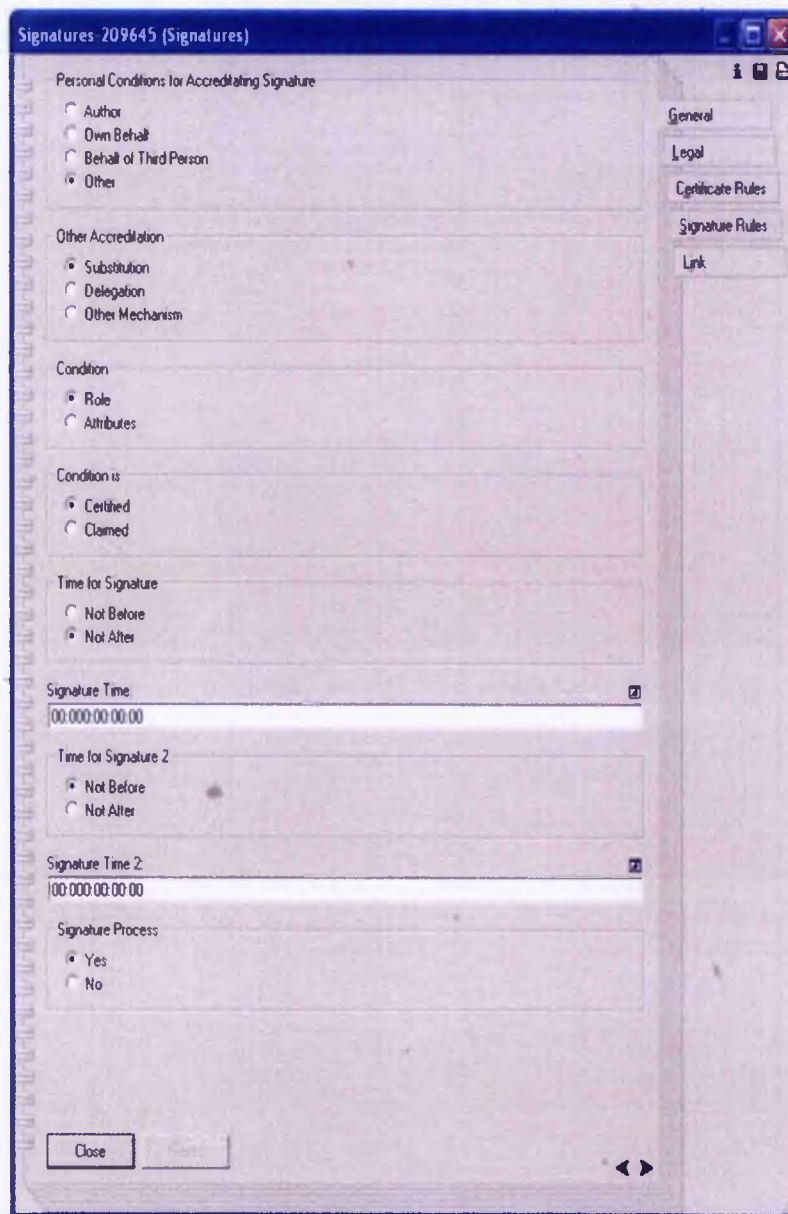
Figure 4-6: Signature Symbol and Signature Notebook – General Tab

Figure 4-6 is split in two parts; the left part shows the signature symbol that is utilised within the workflow to indicate the use/flow of a signature. Double-clicking that symbol loads up the Signature Notebook, whose "General" tab is shown on the right of figure 4-6.

The "General" tab shows how items 2, 3 and 4 of the Signatures section of the PADS questionnaire have been implemented. Thus, the user can select whether the author, a substitute, a delegate or another person accredits the

signature through the provided radio buttons. If "Other" is selected, the user can also select whether the condition (role, attributes – selected via radio buttons) is certified or claimed (selected through a drop-down menu). This covers the requirements for question 2 of the Signature section.

In the same tab, question 3 is addressed by providing a facility on providing the signing period through the two time-input facilities. One facility needs to have selected "Not Before", whilst the other has to have selected "Not After"; the order is not important. Also, the existence of a Signature Process can be confirmed through the use of radio buttons and thus question 4 of the Signatures section of PADS has also been addressed. Again, this view was modified over several research iterations. Below follows an example of how the problem owner clarified the use of the time fields and how this feedback helped shape the application of "Signature Time" in the metadata (see Figure 4-6):

```
"the "Signature Time" control is not needed, because we can't know the
exact moment of a concrete signature, and we can't describe a Signature
Policy for each document to be signed. In the Signature Standard, there is
the possibility to include the moment with "NotAfter" and "NotBefore"
controls. Perhaps you can use for Signature Time this kind of selector,
but taking into account that this is going to be optional."
```

As with the prior Act and Document symbols, the Signature symbol is a carrier for a large number of metadata, screenshots of which are illustrated further in Appendix D.

4.3.4 Combining the individual elements
This section will describe a workflow in its entirety and introduce the potential behaviours of Processes, Acts, Documents and Signatures within such a workflow. All processes and acts are combined together with all documents and signatures; all relevant and necessary information is input into the notebooks of the relevant elements. In other words, this is a global view of the entire workflow and the completion of this model will allow the export of the metadata to an ETSI DSP.
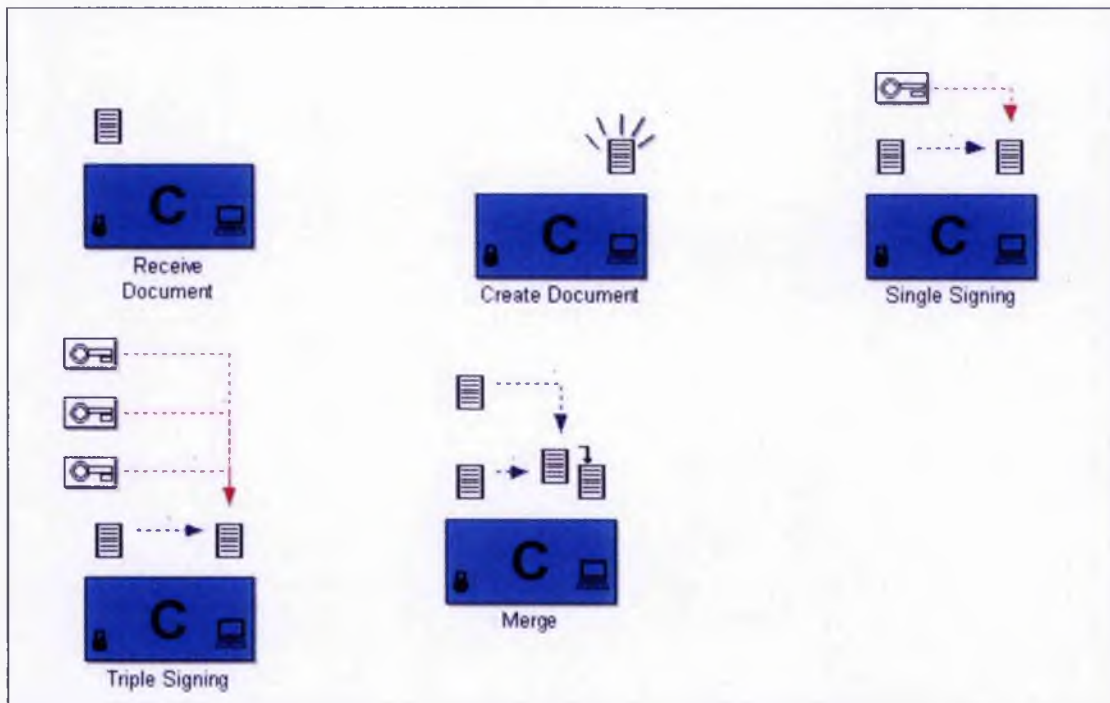
Figure 4-7: Document and Signature Operations

The above figure shows a range of permissible operations by Signatures and Documents within the main model view. As can be seen, there are 5 different operations, each of which shall be described below:

1. Receive document: This shows how a document or signature is used as an input. A document or signature always serves as an input to a process/act by being positioned at the left edge of the act/process box.
2. Single Signing: This shows how an actor digitally signs a document. The document and the signature serve as an input (by being on the left edge of the act – see below) whilst the signed document is the end state of the document.
3. Create Document: This shows how a new document is created by an actor which is subsequently used. Any signature or document serves as 'output' when positioned on the right hand side of a process/act box. This is further emphasised by the appropriate arrow pointing to the right, towards the next process/act affecting that document

4. Merge: This is how two documents acting as inputs are merged through a process/act; once the merge is complete, the document is used further in other processes.

5. Triple Signing: This shows how a document can be signed by more than one signature. It is very similar to item 1, denoting a single signature. Whilst three is used as an example here, any number of signings are possible.

These operations can be combined together to show a workflow that involves documents and signatures. In order to demonstrate these operations, a sample process was constructed, showing how these operations could be used. The swimlanes serve to emphasize the different actors and their organisational background. Below is a description of the sample process.
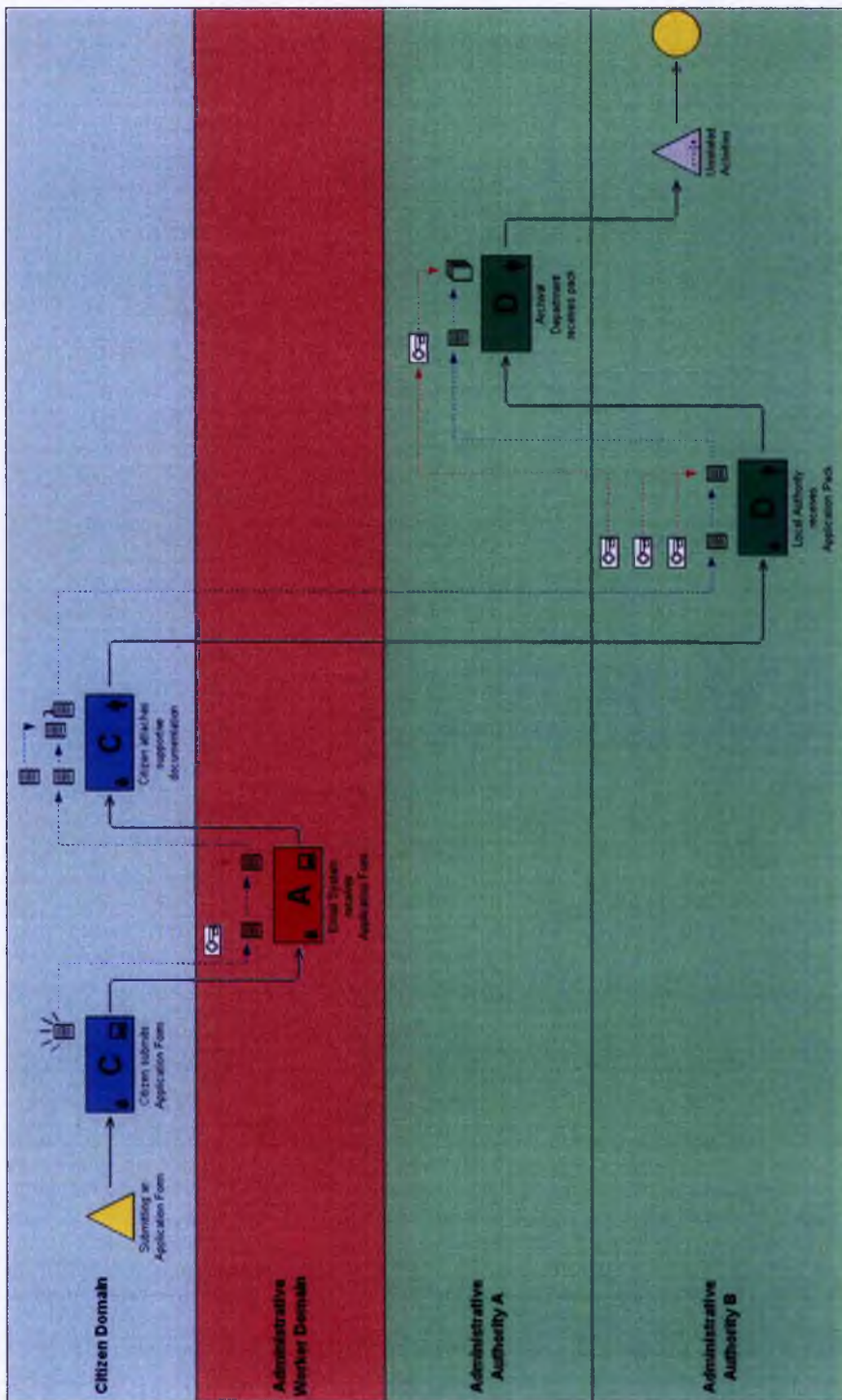
Figure 4-8: A Sample Process

The process description of the above depicted process is as follows:

1. A citizen creates a new document. The citizen needs this document to be recognised by an official authority, therefore approaches an Administrative Worker in the Administrative Worker Domain.

2. The Administrative Worker, having securely received the document, validates the document using his official signature and returns it to the citizen. This is automatic routine, assuming everything is in order with the document.

3. The citizen merges this document with another document, in order to hand in an application to Administrative Authority B. The merged documents are forwarded to Administrative Authority B.

4. Administrative Authority B receives securely the merged documents. This departmental unit examines the merged documents. For this document to be accepted, two signatures are required, which are provided.

5. The departmental unit is required to archive the citizen's application – the archival unit in Administrative Authority A not only requires the signed document, but also a third signature from Administrative Authority B in order to prove the authenticity of the request. So Administrative Authority B forwards to Administrative Authority A: a doubly-signed document (triple, if the original signature of Entity 2 is counted), and a signature that states the authenticity of the request.

6. Administrative Authority A archives the signed document, as well as Administrative Authority B's signature. Further, unrelated activities are performed, which are not relevant to this level of detail. The process ends

Within this process, it was demonstrated how documents and signatures act as inputs, as outputs, and how they are consumed by acts and processes. It was also shown how document and signature flow are all viewed together in the main model view and how they are handled by a variety of actors. Also, the use of both secure and non-secure communications, as well as the use of automated and manual processes was demonstrated. Therefore, a general

overview over the entire workflow was presented which demonstrated how different document and signature operations can be undertaken in a process.

A lot of information was entered in the above acts and documents. This information will not be presented here; however, the XML file generated by the sample process of figure 4-8 will be consumed further in subsequent chapters below.

4.3.5 Using the Modelling Notation

The previous sections have all introduced the graphical version of the methodology, the controls and functions employed by it and the information it captures. The question that remains is – how can this be employed to actually elicit information from a workflow and from acts and represent this information accurately? This section will provide a how-to guide on how the methodology can be used; it is by no means a rule book, merely a guide and one's individual preferences will influence how it is used and applied.

1. Restrict the domain and scope of the legal workflow to a specific problem or issue
2. Create a first sketch of the workflow and annotate specific acts that may influence individual processes (essentially, question 3 of the old PADS questionnaire in Appendix A)
3. Open Adonis and create a new model, saving it with a useful naming convention in a useful location
4. Identify the major actors and their departments – create their respective swimlanes
5. Arrange the workflow processes in the correct manner and name them appropriately
6. For each act in the workflow, attempt to answer the PADS questions, then fill them in by double-clicking on the individual act box

7. Add the documents to their respective locations within the workflow, then answer their PADS questions and fill in the information

8. Add the signatures to their respective locations within the workflow, then answer their PADS questions and fill in the information

9. Connect everything up – processes/acts, documents, signatures (including the signing processes)

10. Double-check the model for consistency and accuracy

11. Create the State Change Models – Adonis will create the correct number of models

12. Link the individual documents and signatures with their corresponding state change models – verify accuracy of document and signature flows

Apart from these general guidance notes, there are some extra instructions to facilitate the creation of accurate models that will allow their conversion to DSPs in XML format:

- Each document's and signature's Description box must have, as a first entry, the exact copy of the Act name that 'consumes' them

- Document/Signature information must only be entered where they are needed; that is, the left side of the Act that consumes them. This is because information entered into document/signature notebooks does not get 'passed down' in the workflow. Therefore, to cut down on model creation time, their information should only be entered when they get consumed by an Act (i.e. in their input stage)

- An Act can only perform 1 operation at a time; it can either merge 2 documents, or sign 1 document with multiple signatures. It can not sign 2 separate documents

- Only Acts that actually sign a document can have the "Signing Act?" tick box ticked. All other Acts and processes can not be ticked

The previous sections introduced an expanded version of the PADS questionnaire, which is a tool to assist an administrator with the construction of a legal workflow in Adonis. PADS was then expanded to a graphical component and the individual controls and functionality of the new business process modelling notation were introduced and demonstrated. A quick how-to guide was provided in order to equip a user with a starting point on using the methodology. This presents an important achievement in the process of creating DSPs, and the next section will outline the further steps required to turn the achieved process model into a DSP.

4.4 Converting Legal Text to Digital Signature Policies

4.4.1 Data Fields in ETSI TR 102 038 and their sources from PADS

The developed graphical workflow model can capture information relevant to the context that governs the use of DSPs. However, with the contextual information governing the use of Digital Signatures involved in a workflow encoded within a graphical workflow, the question arises on how this information can be retrieved from the graphical model and be inserted into a standards-compliant DSP. In other words, the next research problem requiring solving was the one of data flow: what is the data required, how is it captured in the PADS Questionnaire, how is it transformed as it passes through the graphical PADS notation to an XML representation of the graphical PADS notation and what does the data look like when it finally ends up within a DSP? These questions refer to the following diagram; note how the diagram uses a particular piece of data and applies it to the various 'stages' of the transformation process:
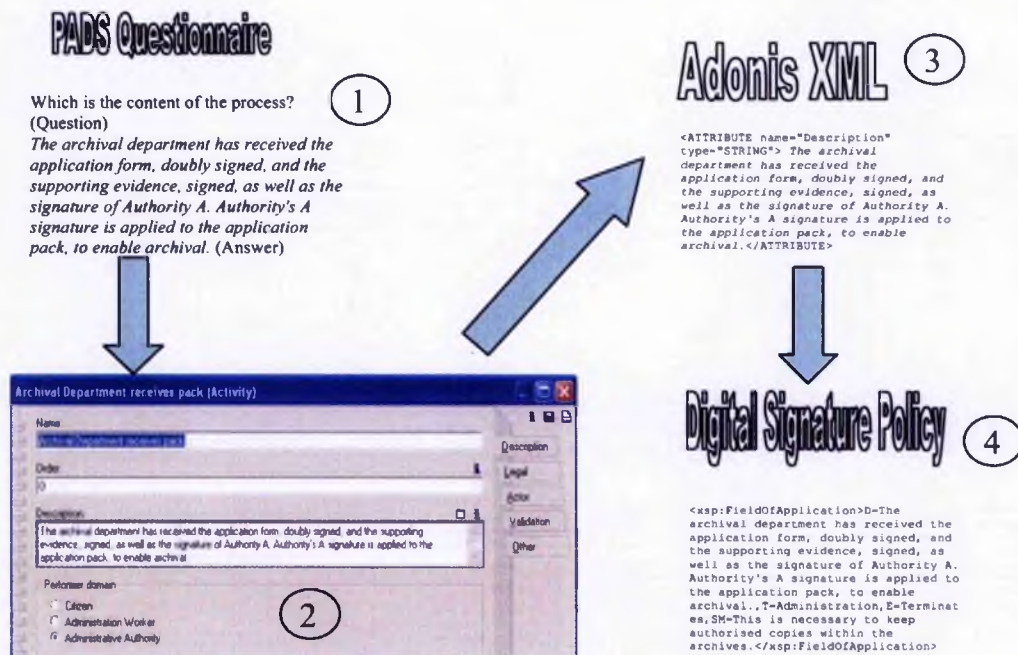
Figure 4-9: Converting Natural Language Text to XML Code

1. A PADS Questionnaire is completed about a particular legal process
2. The answer is entered into the appropriate field within the graphical workflow
3. The graphical workflow is turned into an XML representation using Adonis' proprietary XML standard
4. The extracted data needs to be entered into the appropriate XML tags within the DSP. In order to achieve this, however, each data element within the graphical workflow needs to be associated in a one-to-one relationship with each available tag in the ETSI DSP standard

This process was arrived at and solved as described below.

4.4.2 Data Fields in ETSI TR 102 038 and their sources from PADS

Developing a tool that allows for the XML output of the graphical PADS methodology to be converted into an ETSI TR 102 038 compliant DSP requires a data mapping between the data fields comprising the DSP standard and the data provided by the graphical PADS methodology. This data

mapping allows one to specify and comprehend the data source for each necessitated data field. Such an overview helps future designers to see potential problems in the current implementation and data mapping and allows for a quick analysis of whether data requirements have been met or not.

The following pages will be comprised of a table featuring the following elements:

- A description of the signature policy section being examined (c.f. ETSI TR 102 038)

- A description of the source of the data in the graphical PADS methodology

- A description of data transformation rules (incl. Conditional rules)

For space saving issues, the discussion is limited to the sections that contain unique data fields. References made to the "transformation software" refer to the tool performing the transformation of the PADS XML to ETSI XML, described in section 4.4.3.

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
SignaturePolicy Element			
SignPolicyDigestAlg	N/A	Hardcoded into transformation software as "SHA1"	None - Organisation specific
Ds:Transforms	N/A	Hardcoded into transformation software as "0"	None - Organisation specific
SignPolicyDigest	N/A	Hardcoded into transformation software as	None - Unique hexadecimal value

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
		"Digest Value here"	
SignPolicyInfo Element			
SignPolicyIdentifier	N/A	Hardcoded into transformation software as "Identifier here"	None - Organisation specific
DateOfIssue	Used system time at runtime	No source	None
PolicyIssuerName	N/A	Hardcoded into transformation software as "CATCert"	None - Organisation specific
FieldOfApplication	For Single/Strong Multiple Signature Policies, the value of this field is: "D=Description, T=C/A/O, E=I/T/O, SM=Meaning" Where D is the Act's Description, T for the different Act Types, E for the different Act Effects and SM is the Signature Meaning	D, T and E are taken from the **Description-tab** of the Act's Notebook, SM is taken from the corresponding signature's **Legal-tab.** For WEAK multiple signatures, SM is skipped.	A combination of "Acts Analysis, Question 1" and "Signature Analysis, Question 1"
SignatureValidationPolicy			

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
Element			
SigningPeriod	Signing Period of the signature; for WEAK multiple signatures, the Signing Period is the Signing Period of the UPPERMOST (i.e. the FIRST in the signing sequence) signature	Signature Notebook, **General-tab**	A combination of "Signature Analysis, Question 5" and "Document Analysis, Question5"
RecognizedCommitment Type Element	For WEAK multiple signatures *only*		
CommitmentIdentifier	XADES-compliant Object Identifiers	N/A	None
FieldOfApplication	Combination of Signature and Act Description	Signature Notebook, **General Tab;** Acts Notebook, **General Tab**	A combination of "Signature Analysis, Question 1" and "Acts Analysis, Question 1"
Semantics	Combination of Signature Meaning and Document Description	Signature Notebook, **Legal tab,** Document Notebook, **General tab**	A combination of "Signature Analysis, Question 1" and "Documents Analysis, Question 1"
SignerRules Element			
ExternalSignedObjects	N/A	Signature Notebook, **Signature**	Signature Analysis, Question 6

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
		Rules tab, Tickbox ticked for "Signature is external?" question	
QPropertiesListType	If corresponding tick box is ticked, then add URI.	Signature Notebook, **Signature Rules** tab, panels "Signed Properties for Signer", "Unsigned Properties for Signer" and "Unsigned properties for Verifier"	Signature Analysis, Questions 8 and 9
MandatedCertificateRef	N/A	Signature Notebook, **Signature Rules tab,** tickbox ticked for "Signer Provides full certification path?"	Signature Analysis, Question 7
MandatedCertificateInfo		Signature Notebook, **Signature Rules tab**, radio buttons (Signer Provides)	Signature Analysis, Question 7
SignerTrustTree Element			
TrustPoint	N/A	Hardcoded into	None - Organisation

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
		transformation software, using CATCERT Trustpoint	specific
AcceptablePolicySet	N/A	N/A	Organisation-specific ID numbers of related Policies
NameConstraints	Performer Domain for Act	Acts Notebook, **Description** tab, "Performer domain" panel	Acts Analysis, Question 3
CertificateRevReq Element			
EndRevReq	Change Radio button label text to conform to ETSI notation (e.g. CLR becomes clrcheck)	Signature Notebook, Certificate Rules tab, "Certificate Validation" radio button group	Signature Analysis, Question 10
CACerts	Copy EndRevReq	As above	As above
TimeStampTrustCondition Element			
TtsCertificateTrustTree	Copy from TrustPoint in SignerTrustTree	N/A	None - Organisation specific
TtsRevReq	Left as empty element	N/A	None - Organisation specific
TtsNameConstraints	Left as empty element	N/A	None - Organisation specific
CautionPeriod	Left as empty element	N/A	None - Organisation specific
SignatureTimeStampDelay	Left as empty	N/A	None - Organisation

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
	element		specific
RoleTrustCondition Element			
RoleMandated	Boolean; if un-ticked (i.e. false), leave tags empty. Otherwise, declare True and fill out remaining tags	Documents notebook, **Accreditation + Requirements tab**; Role? Is ticked, = TRUE	Signature Analysis, Question 2
HowCertRole	Enumeration type, values "CertifiedRole" and "ClaimedRole"	Signatures Notebook, **General tab**, "Condition: Claimed/certified" radio button. (Condition: "Role" radio button must be selected	Signature Analysis, Question 2
RoleConstraints	N/A	None	Organisation specific (link to URI), but known to incorporate the following information: - Acts Analysis, Questions 4, 5, 7 and 8 - Documents Analysis, Question 4

ETSI Field	Transformation Rules	Source in Graphical PADS	Source in PADS Questionnaire
			- Signature Analysis, Question 2
AlgorithmConstraintSet Element	Left Empty		

Table 4-2: Signature Policy Data Field Sources

The above table shows how information for each data field within the ETSI TR 102 038 standard is supplied by either the graphical PADS methodology, or through other, outside means.

Performing the research on the data allowed the researcher to gain a greater understanding of the ETSI TR 102 038 DSP standard and this greater understanding served as a good input in improving the graphical workflow further so that it covers the required data more accurately. Thus, the individual research iterations continuously improved intermediate results. Below follows some sample data that showed how researcher and problem owner arrived at some of the data described in the above table:

```
"TrustPoint - Is a base64 certificate of the signer certificate root. Using
it, we can define that only CATCert certificates will be admitted.

AcceptablePolicySet - Is a list of Certification Policy Identifiers
admitted. Each certificate is issued according to a Certification Policy
which define its attributes. Each Certification Policy is identified by a
OID set of numbers. For instance, If we are accepting only CATCert
certificates, with this item we can specify that only CPSIR certificates
are accepted.

Nameconstraint - Is a list of concrete attribute values accepted. For
instance, if only we accept CATCert Certificates with CPSIR profile, with
elements like this we can specify that Organisation Unit has to be
"OU=Research Area".

This is the  kind of information that we can obtain from PADS. If signer
is a Administration Person, digital signatures must be produced using a
CPISR, and if the administrative act must be produced by the Secretary of
a City Hall, digital certificates must have a "OU=City Hall,
E=Secretary"."
```

4.4.3 The Transformation Software

The need for a Transformation Software arose when the need to transform PADS into an ETSI TR 102 038 compliant DSP became apparent. Due to the information and data structures supplied by PADS and due to the data requirements of the ETSI standard, it was realised early on that the data had to be handled and transformed in order to fill the relevant data fields within the standard. As PADS evolved and became an EPC-based graphical process modelling methodology (similar in spirit to BPMN, UML, and other similar notations), the transformation from graphical representation to standards-compliant XML code became an even bigger issue.

To take these factors into account, the decision was made to employ the tool ADONIS[4] for the implementation of the graphical PADS methodology. ADONIS features an "Export" feature, which creates an XML representation of selected process models authored within ADONIS. This feature is a big advantage, as the export feature reduces the data matching problem to a problem of converting XML files to a different standard; without this feature, there would have been a need to handle the data within its natural language form (as was indeed used in the previous method employing the PADS questionnaire). However, with the data now encoded in XML, the task of identifying relevant data and placing it within the correct data field within the standard is much reduced in complexity, due to the abundance of support tools for XML related operations.

The essential nature of the transformation software is therefore to convert the ADONIS created XML representation into ETSI compliant DSPs. In order to put the need for having this software in perspective, please refer to the following diagram, which describes the *overall* approach to the research conducted:

---

[4] http://www.boc-group.com/
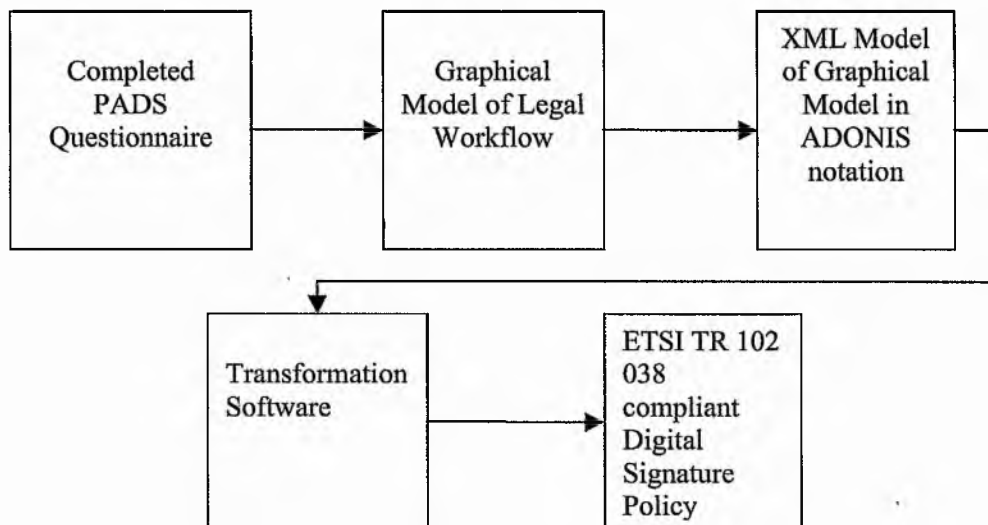
Figure 4-10: Flowchart outlining the method by which a Digital Signature Policy is arrived at

The above figure outlines the sequence of steps to arrive at an ETSI TR 102 038 compliant DSP. The first two steps, "Completed PADS Questionnaire" and "Graphical Model of Legal Workflow" have already been explained in detail in the previous chapters, whilst "XML Model of Graphical Model in ADONIS notation" and "Transformation Software" are covered in the following sections.

As a pre-condition, it is necessary to create an XML model of the legal workflow represented within ADONIS. ADONIS has an in-built XML export feature which should be used for this purpose.

The created XML file is written in ADONIS' native schema and contains a wide variety of information, such as location of processes within the drawing pane, colour of elements and other program internal data which is present in addition to the relevant data for PADS. A manual read of the file contents is difficult due to its cluttered nature and therefore a Transformation Software is essential in order to translate this to an ETSI compliant DSP.
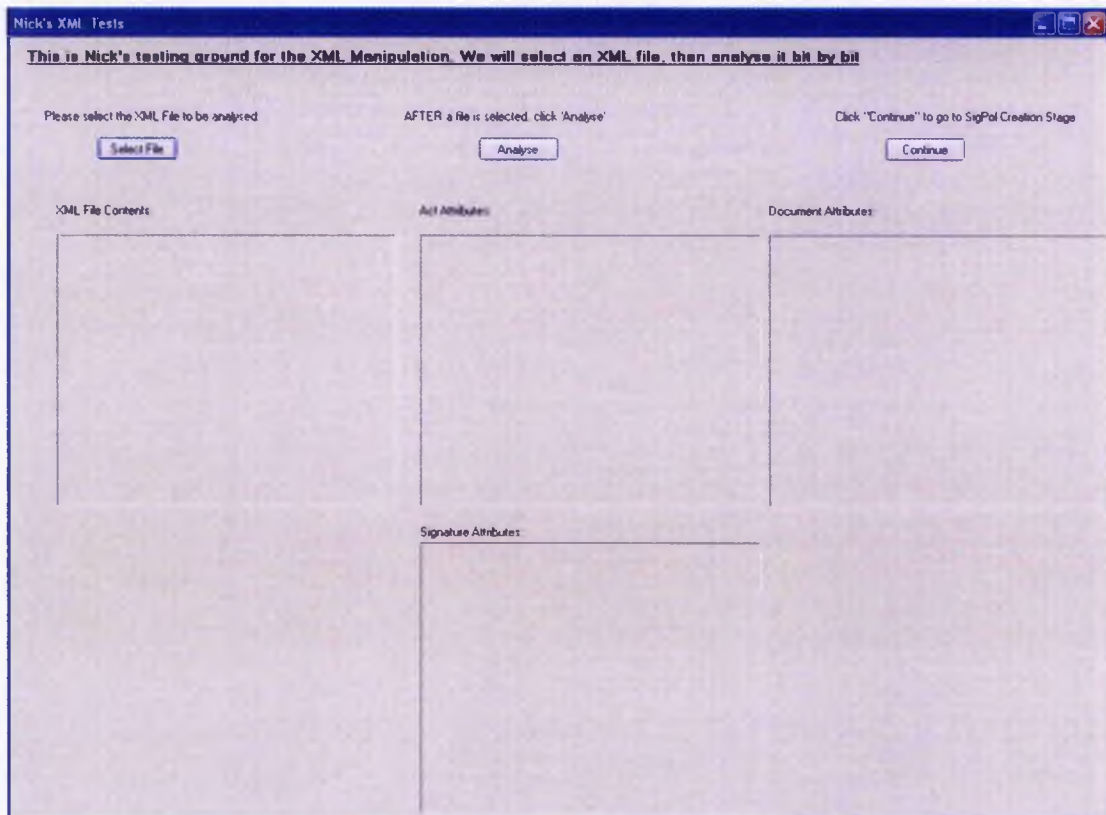
Figure 4-11: The initial screen of the transformation software

The transformation software uses XPath (W3C, 1999) to traverse the different XML tags within the file and to identify and extract the data relevant to PADS and DSPs. XPath and XML are supported technologies of .NET 2.0 (Willis et. al., 2004) and the software itself is implemented in VB.NET 2003 (Willis et. al., 2004). There are several forms guiding the user through the various steps, and a number of modules holding many important functions that provide functionality to the software.

The flow of creating signature policies is, in rough terms, as follows:

1. ADONIS is used to create an XML export of a selected workflow model
2. The transformation software is launched and the created model is loaded into the software

3. The transformation software identifies the relevant data fields and stores the data, whilst irrelevant data is discarded

4. The software presents a list of signing acts identified within the model and requests the user to select the act for which a signature policy is to be created

5. If there are multiple signatures being performed within a single act, the software will ask whether a Strong Signature Policy (i.e. a Signature Policy for each individual signature) or a Weak Signature Policy (i.e. a Signature Policy for all signatures applied in a given Act) is to be created

6. The signature policy is created and saved in the program's root directory

These details are merely scratching the surface of the Transformation Software functionality. As it is an involving piece of technology going into a lot of detail, its details will be presented in Appendix E.2 in order to not stray the focus of the research report.

5 Analysis and Discussion

Arriving at certain results can by no means be the end of a research intervention (Gray, 2004). In research, and especially in Action Research (McNiff and Whitehead, 2009), it is important to reflect on the achieved results and discuss their meaning, whether the original research question has been satisfied, whether improved practice was arrived at and whether the research was conducted in accordance with its methodological constraints. However, Baskerville (1999) noted that there is a "lack of generally agreed criteria for evaluating action research", which means that there is no prescribed method of evaluating Action Research and its success. Therefore, the researcher decided to evaluate the research from a number of angles.

Section 5.1 looks at the evaluation conducted as part of the Action Research cycle, where each instance of action was followed with an instance of evaluation. The section therefore contains the observations and conclusions that were made at the time of the ongoing research, and is mainly focused on the creation and iterative development of the artefacts.

Section 5.2 is a retrospective analysis of the conducted research and is mainly focused with establishing whether the research is methodologically and epistemologically consistent. This analysis looks at whether the methods of Action Research were applied correctly and whether this research may have been Design Science instead of Action Research. An element of this retrospective analysis compares the activities performed by the researcher against what literature defines as good Action Research and good Design Science. The justification for conducting this retrospective analysis on epistemological and methodological consistency is that Baskerville (1999) assets that Consultancy and Action Research "contain substantial similarities" (Baskerville, 1999) and showing that the conducted Action Research was methodologically consistent is a way of asserting the scientific foundation of this research.

Section 5.3, on the other hand, performs a retrospective analysis of the entire research intervention by assessing elements of the problem owner/co-researcher interaction and placing the research activity in the context of the epistemological and methodological boundaries of Action Research. Since Baskerville (1999) identified a lack of agreed evaluation criteria for Action Research, the Researcher applied a reflection technique developed by McNiff and Whitehead (2009) to strengthen the argument that the conducted research was consistent and methodologically sound Action Research. Part of this reflection also involved highlighting the learning that took place in both the researcher and the problem owner.

5.1 Artefact Analysis

Since the research intervention resulted in the creation of a number of artefacts as a way of results, these artefacts need to undergo analysis in order to assess whether they help satisfy the research question and identify their role in the research intervention. The researcher will also reflect on their functionality in the later sections.

5.1.1 Analysis and Reflection through Software Testing

The previous chapters introduced the PADS questionnaire and its transformation from a questionnaire to a Business Process Modelling Notation to an ETSI TR 102 038 compliant DSP. In particular, the chapters captured the precise data mapping between the data provided by the graphical notation, and the data required by the DSP standard. Furthermore, a tool which implemented the data transformation rules and was capable of transforming Adonis XML output into a DSP, compliant with ETSI TR 102 038, was introduced. Thus, the previous chapters represent the complete method, from filling out the PADS questionnaire, to creating a Legal Workflow model, to transforming model output into signature policy. This chapter captures the testing performed on the method and its component parts. Therefore, this

chapter proves that the tool and method function correctly and yield the expected results.

Building on the results reported by Wood et. al. (1997), namely that a combination of test strategies is likely to be more effective at uncovering errors than a single test strategy, it was decided to adopt a combination of white and black box testing. White box testing is a strategy that assumes the tester has full knowledge of the internal components of the software being tested, whilst black box testing is a functional analysis that ignores the internal functionality and instead focuses on the correct INPUT-OUTPUT pairing of data.

Due to the nature of the implementation of the methodology, it was decided to perform Black Box testing on the graphical notation, whilst the conversion tool was tested using the White Box testing strategy. The reasoning for this is that the graphical notation is implemented within Adonis, a proprietary program whose source code is not publicly viewable and thus it is not possible to view the programmatical structures behind the user interface - the tool is a "black box"; the developed conversion tool, on the other hand, allowed for white box testing as the source code was developed by the author and hence viewable.

The testing was performed in phases, with each phase testing the "as-is" state of the methodology, then looping to test the revised state of the methodology, dedicating one phase on the original error-input, to verify that the error had been eliminated, whilst another phase would then be dedicated on remaining input. In other words, the testing strategy followed the structure of Action Research by adopting a cyclical approach to testing, similarly to how the development of the methodology had been performed in the earlier chapters. The following figure summarises the cyclical testing strategy.
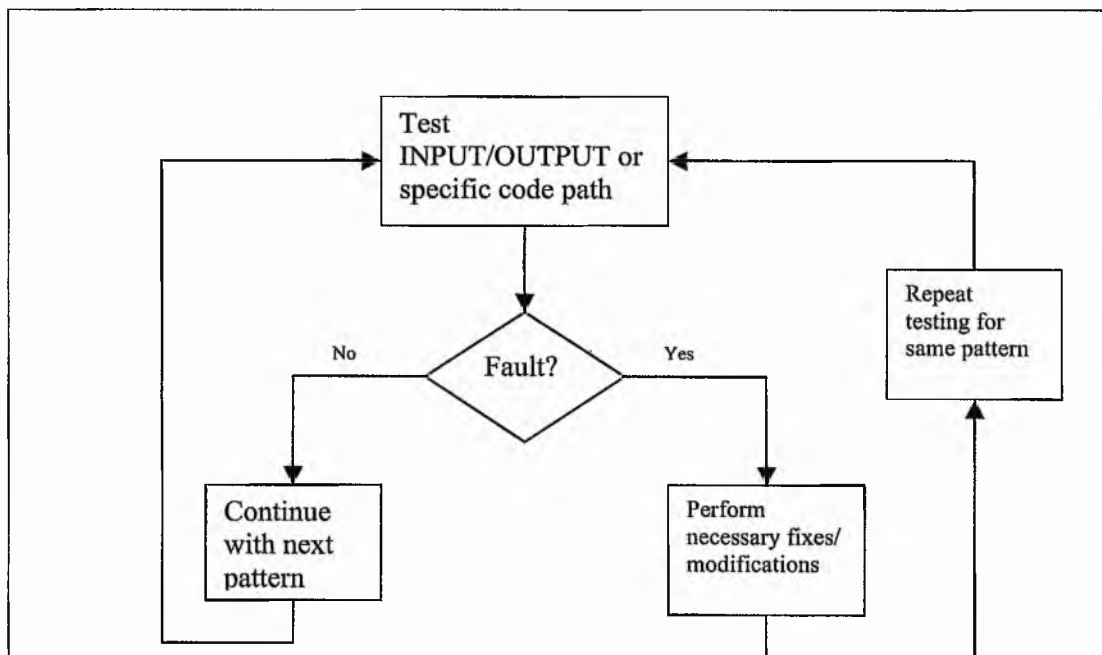
Figure 5-1: Testing Methodology

As can be observed from figure 5-1, this approach to testing allows testing to be performed with both Black Box and White Box testing methods, as the fault identification method is dependent on the type of testing performed, but independent from the testing methodology.

5.1.1.1 Testing the Graphical Notation

As mentioned above, the graphical notation was tested using Black Box testing techniques. The testing was limited to a functional level and tested the validity of a particular input resulting in a particular output. There were several phases of testing, dealing with several iterations of the notation.

Initial testing on the prototype methodology was aimed at verifying whether the methodology had been implemented according to the design specifications and whether all technical features were working correctly. This initial testing resulted in identifying a range of minor lay-out and organisation faults, as well as one technical fault (Error on selecting a radio button). The identified faults and errors were the first items tested on the updated

notation; on passing these tests, testing resumed with the remainder of available input values. These tests on the early notation were limited to ensuring the functionality of the notation. That is, it was tested whether all provided facilities (e.g. Notebook) worked and whether the particulars of the notation (different colours for different actors) were according to what had been specified.

On ensuring that all provided functionalities within the notation were working according to the specified design, a legal workflow was designed in such a manner as to test all available functionality and options of a legal workflow. In other words, use case testing was adopted to create a workflow featuring all possible states a workflow could take. Amongst others, the workflow included:

- Workflow spanning multiple swimlanes

- All available document operations; creating a document, merging a document, filing a document, "normal" document state, signing a document, passing a document from process to process

- All available signing operations; single signature signing 1 document, multiple signatures signing 1 document, sharing of signatures between actors

- Inclusion of sub-processes

Thus, the particular lay-out of the workflow also precipitated the use of boundary analysis, as the transformation software would need to be able to distinguish between 0, 1 and multiple signatures being applied. It should be noted that the sample workflow omitted the provision of inter-model links, as permitted for sub-processes and for links to state-change models. This decision was made due to inter-model links not adding anything of value to the understanding of the notation, as every 'level' of the workflow is a self-sufficient item that does not need to access resources on another level. The

fact that the links work was tested in the initial testing, however. Please see the figure below for the final appearance of the representative sample workflow.
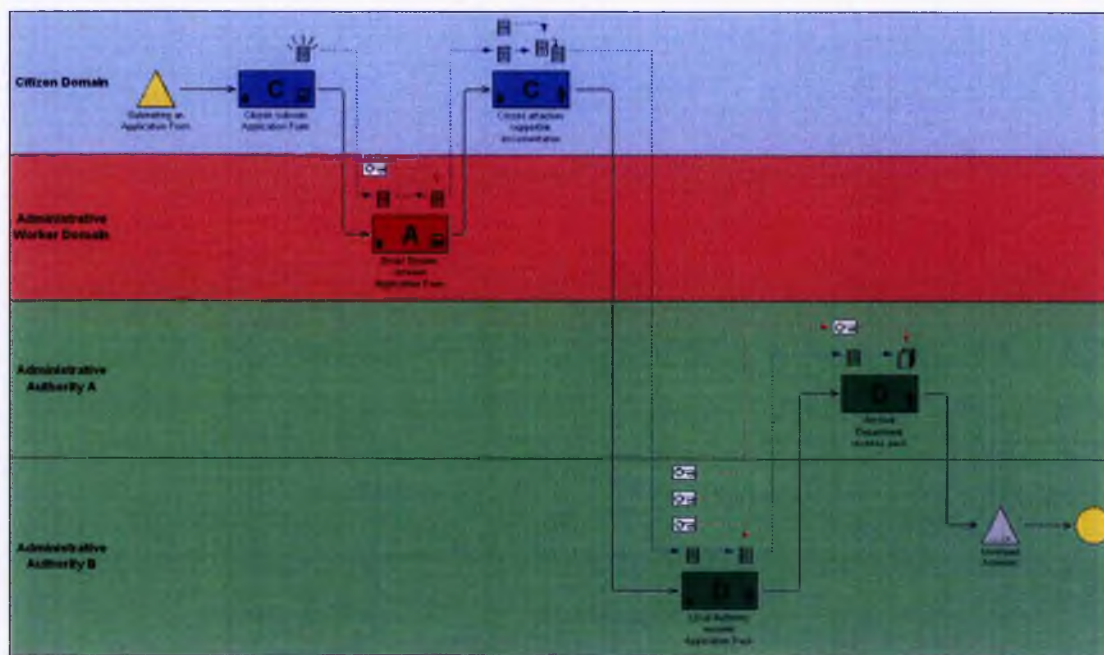
Figure 5-2: Representative Sample Workflow

Apart from the graphical side of the notation, the created workflow was also provided with a wide range of sample data. It should be noted that, initially, the provided sample data was semantically invalid and thus very unlikely to result in a semantically/legally valid DSP in the latter stage of XML output conversion. Instead, the sample data was aimed at functionality testing and thus attempted to trigger all possible input mechanisms, to ensure well-formed DSPs would be formed.

Results

The outcome of the creation of the representative workflow was observed in a two-tier method – firstly, occurrences within the graphical notation itself were noted, such as issues in creating such a workflow or observation of effects (difficult to copy data content when document 'flows' to another process). Further observation was performed by exporting the workflow

model to XML and inspecting the XML – this step was performed in order to gain experience with the Adonis XML syntax. With the workflow thus presented in two different tiers, a variety of results were observed.

Apart from cosmetic issues (such as colours causing difficulty in reading/identifying processes within a workflow), a range of technical observations were made. For example, it was identified that Adonis is not capable of "linking" documents and signatures to a particular act; that is, when an act signs a document, Adonis regards the act, document and signature as three separate entities. This also implied that Adonis was unaware of a signing process occurring. This necessitated the inclusion of a question in an act, asking whether the act was a "Signing Act", which could be used as a signal that this act was of interest. Also, in order to link Documents and Signatures with a particular Act, a workaround was developed that required a user to have that particular Act's exact name as the first entry in a Document's or Signature's description text box in order to allow a Document or Signature to be linked to that particular Act.

A different issue encountered was the issue of providing a valid signing time; originally, this had been a time entry facility (a standard control provided by Adonis) but subsequent examination of the XML code (and the use of various entries in this facility) resulted in a design change, requiring the use of two such controls, as well as two radio buttons indicating the values "Not Before" and "Not After" for each control, in order to be able to provide a meaningful statement. Further results and observations were made and noted, then implemented into new versions of the graphical notation. These new versions of the notation were then tested for the identified issues, before being examined further.

It has been demonstrated how functionality improvements resulted in updated versions of the graphical modelling notation. However, the graphical notation also underwent changes due to semantic and syntactic content. The

requirements set by the ETSI TR 102 038 standard were included in the notation without having had previous experience with the standard, but a peer review with the professionals that have established methods for implementing the standard, revealed that the notation, despite its functional integrity, did not meet all semantic requirements set by the standard. For example, signer and verifier requirements were not queried correctly, nor did the notation account for multiple or nil selections. Therefore, the graphical notation required yet another version upgrade, based on the semantic needs of the standard. The new notation was also tested using the testing methodology outlined in figure 5-1, with a focus on already identified issues in order to eliminate the possibility of old issues appearing again. This concluded the testing of the graphical notation and demonstrates how the Action Research Evaluation phase informed a further Build phase.

5.1.1.2 Testing the Transformation Software

As mentioned in the previous section, the transformation software was tested using a variety of White Box testing techniques. By testing, we do not include syntactical errors corrected during the development. Instead, the testing was limited to the logical flow of the software as well as the output provided and the ability to process the provided input. The testing methodology was the one depicted in the previous section. As with the graphical notation, there were several phases of testing. Furthermore, a series of phases was aimed at examining a particular item within the transformation software. Since the transformation software used the XML output from the graphical notation as input, any identified issue had to be cross-corroborated with the data entry in the graphical notation, in case the error originated from the notation, rather than the transformation software. As the testing did not include programmatical validity in terms of syntax, but did include programmatical validity in terms of programming logic, the main measure of correct operation was the yield of semantically correct, ETSI TR 102 038 compliant DSPs.

Results

The syntactical validity of the created XML code was inspected visually. On discovering syntax errors, first the code would be investigated to discover whether there was a programming logic fault, or whether the fault was related to the output mechanisms of the transformation software. On correcting the fault, the test would be repeated.

Apart from syntax testing, it was also investigated whether the programming logic was capable of handling the various elements of a signature policy in such a way as to correctly deal with different case scenarios. Through boundary analysis, it was determined during one run that whilst the flow of creating single signature policies had been successful, the software was still failing with multiple signatures. Such errors in the programming logic were also identified through the incorrect XML output of the transformation software. One notable case was the case of the Commitment Type element, which is used to indicate validation rules that apply to given commitment types. This element is very important for multiple weak signature policies, as it needs to capture the various validation rules, but it posed a difficult challenge to extend the transformation software such that it uses commitment rules correctly.

Finally, the transformation software allowed the researcher to identify some flaws with the graphical notation. For example, it was pointed out that the graphical notation was not able to link documents and signatures with acts and processes. This limitation was further emphasised when it came to developing the transformation software, as the linking between documents and signatures and acts was crucial for the XML transformation – it is from these tests that the requirement for putting the act name into documents' and signatures' description boxes originated from.

The testing of the transformation software also had a rectifying effect on the data mapping performed in the early stages of the development of the

transformation software. During the testing of the transformation software, some inconsistencies between the resulting signature policy and the actual requirements of the standard were revealed. Further investigation revealed that these were due to the wrong data being used by the transformation software. Modifications had to be performed that would map different kinds of notational data into the signature policy syntax, thus fixing the observed discrepancies. The revision in the data mapping prompted a further validation exercise of the data mapping and a clearer distinction in data understanding.

Summary

The testing reported in 5.1.1.1 Testing the Graphical Notation and 5.1.1.2 Testing the Transformation Software was at times performed concurrently with the development phases, at other times sequentially after the development phases. Whenever testing activities identified flaws or drawbacks, the affected item was re-developed and re-tested. In other words, there was a continuous set of activities that involved evaluating a developed artefact, analysing the feedback, implementing the feedback, followed by further evaluation, in line with the approach required of Action Research. The result was a set of continuously tested and updated artefacts which over time became more and more appropriate for improving the problem owners' state of dissatisfaction with existing practice.

The testing was vital, in that it achieved to show that the concept works. It was shown how PADS could be expanded into a graphical notation, and it was shown how this notation could then be turned into ETSI TR 102 038 compliant signature policies. The testing validated the correctness of both notation and transformation software, which was necessary to prove the concept.

The testing also highlighted some shortcomings in the current versions that ought to be addressed in future versions. In particular, the link between acts, documents and signatures needs to be stronger; relying on a character match

within a particular part of an entity is a not very user friendly and thus error prone method of creating such a link. Also, it should be born in mind that whilst the graphical notation underwent a semantic validity test, the transformation software did not perform such a test. In other words, the data used to create the signature policies is test data and thus holds no legal value. However, the true value of this work can not be judged fully until a semantically valid signature policy has been created. This requires a domain expert to supply such data, however. Such data was requested from the problem owner but the data was not suitable for testing; more details on this issue are provided later in this section.

5.1.2 Analysis of the Graphical Notation and its role in the Digital Signature Policy Creation Process

The graphical notation was developed with the aim of capturing legal information. The intention was to use the information, captured in legal process models, to create DSPs. The user of the notation is the research's problem owner which is a public sector body in the regional government of Catalonia and active in European research efforts (Seltsikas and Papas, 2008). As the researcher started the collaboration, it became clear that the problem owner was seeking a solution that was, from a perspective of technical sophistication, rather conservative. The problem owner insisted that the existing ad-hoc method be improved, in order to allow their administrators to quickly retrain without much investment. The researcher took this as a signal that innovative and technologically intensive solutions, such as the one suggested to the problem owner (Mercatali et. al., 2005), would not be acceptable. The researcher therefore decided to arrive at a solution that was on the one hand capable of addressing and solving the research question, but on the other hand not too challenging a technology that would risk getting rejected by the problem owner. The researcher therefore based the modelling notation on a notation previously utilised in eGovernment research that the problem owners had participated in. As a result, the problem owners felt

comfortable with the visual aspect, since, in spite of its adaptation for DSP concepts, it reflected concepts that were known to them.

Originally, this notation had been developed for modelling cross-border Identity Management processes (see Seltsikas and Palkovits, 2006) and had to be adapted for the DSP domain. However, the researcher identified that the adaptation could be done in a manner that would allow the notation to be used for other purposes and the collaborative effort on the notation was therefore directed towards retaining elements of the notation that are not directly linked to DSPs. The result is that the notation can capture and express information beyond its intended use for DSPs. As the results (and Appendix D) have shown, the notation can show swimlanes, various different actor types, it can capture a large variety of process metadata and can visualise different types of process behaviour, thus being a much more powerful tool than originally intended. Due to these features being inherent of the notation, it has the potential to be used by the problem owner for other purposes, such as business process re-engineering or an audit of internal processes.

With regards to DSPs, the notation is equipped with visual elements depicting documents and signatures and has the necessary metadata fields to hold signature and legal data. The data fields added to the notation were identified on the basis of the ETSI TR 102 038 technical standard and on the basis of the type of data provided by the PADS Questionnaire. As the notation has the necessary 'vehicle' to carry data relevant for DSPs, it is therefore capable of contributing to a DSP creation process.

With regards to implementing the notation into a process modelling tool, there are a myriad of products available that support process modelling work. The researcher and the collaborator agreed that a viable tool must permit the modification of a notation and the underlying metamodel, so that the notation can be implemented in full. Since DSPs are XML documents, there was a further requirement on a tool to be capable of exporting a model and its

associated data as an XML document. Finally, the tool was required to be user friendly and allow future users to start working quickly, without requiring users to perform needless and unnecessary procedures. Apart from such functionality concerns, there were budgetary limits as well and the problem owners set aside a budget of €30,000 for the purchase cost of tool and user licenses. It was for these reasons that Adonis was chosen as the process modelling tool, as it combines all of these features and, a feature that the problem owner thought was particularly useful, the capability to programmatically modify the notation, underlying metamodel and other aspects of both modelling notation used and tool behaviour. The problem owners saw this feature as important once realising that it was a tool feature, since it would enable them to continue refining the results after the period of collaboration ended - and later sections will show that this refinement did take place.

What this demonstrates is that a public sector organisation of a regional government may be reluctant to adopt state of the art solutions if the effort and cost of implementation is perceived to be prohibitively high, when simpler solutions for less effort could be obtained. It also shows that organisations participating in European research initiatives are learning from their engagements, as the familiarity with the notation demonstrates. These points may serve as a basis for future research into the behaviour of regional public sector organisations. On the other hand, the rationale for choosing the Adonis modelling tool demonstrates continued commitment to the technology of DSPs, and the commitment to developing the method for creating them further in the future. It thus shows that the organisation was able to appreciate that the results are not set in stone and could be developed further, as well as the ability to foresee the need for changes in the future.

5.1.3 Analysis of the Transformation Software and its role in the Digital Signature Policy Creation Process

The need for a Transformation Software emerged when the collaborative research effort realised that the XML export of process models from the Adonis modelling tool yielded an XML document that was highly complex and 'information heavy' (for example, the XML file created included information on the position of graphical model elements within the tool's drawing pane, references to colour schemes and other information not relevant to DSPs). Whilst Adonis only had a single option for exports, communication with the tool vendors revealed that exports were customisable, but that such a process was highly complex and required programmatical assistance from the tool vendor. Due to the limited budget and due to the fact the researcher was in a collaborative agreement with the problem owner, the problem owner opted for a functional solution that could be built by researcher and the collaborative problem owner. Therefore, this aspect of the developed method is born out of necessity of turning the Adonis-native XML format into standard-compliant DSPs. Nevertheless, the transformation tool can be adapted to work with the XML output of other modelling tools by modifying its data-field detection mechanism to look for the syntax of other modelling tools. This portability to other modelling tools was not a primary driver in its development, however.

Of greater importance to the method is the data analysis that was conducted by the researcher and the collaborators in order to enable the transformation tool to create accurate DSPs. This data analysis accurately traced the 'flow' of data from questionnaire to modelling notation to Adonis XML to Transformation Tool to ETSI-compliant DSP. This allowed the researcher and problem owner to identify some minor issues that led to some modifications and, more importantly, created a map of the data that traces the various 'locations' and data types as it passes from questionnaire to modelling notation and to DSP. This data mapping is therefore an important artefact that makes the whole method more agile, in that it provides the necessary information required to de-couple the method from the artefacts that were built in this research. Therefore, the method of creating DSPs can be

implemented in other tools with minor modifications, and this is therefore a significant finding of the research because not only is it capable of satisfying the specific issues of the organisation in question, but it can also be 'transferred' into a different environment (using different tools) and be applied there as well.

Therefore, what initially started out as a 'work-around' without much contribution to the overall method of creating DSPs, has led to developing an artefact (the data mapping table) that can be used to apply the developed method in other organisations using different tools.

To summarise, the repeated Action Research iterations developed the aforementioned artefacts further and further up to the point where a 'saturation point' was achieved; once it was shown that the artefacts were capable of creating standards-compliant DSPs, it meant that the extended research aims had been met as well. The PADS questionnaire and the graphical modelling notation contributed to meeting the research aim 'to develop a method enabling individuals to convert natural language legal acts and convert those to process models'. The transformation tool and the data mapping table met the research aim 'to develop tools and methods to convert the process models into a codified form', but also met the other research aim of complying with ETSI TR 102 038 through its inherent design. Finally, the structured and repeatable manner of the method to develop DSPs was demonstrated through testing of the aforementioned artefacts, as outlined in the previous section.

Later sections will show that the problem owner displayed the development of actionable knowledge on reaching the saturation point; that is, the problem owner took these final results and started modifying them to suit their organisation more closely. This is evidenced by the receipt of files that show the problem owner had started modifying some of the underlying meta-model in the graphical notation, such as the introduction of some Catalan terms. In

other words, the problem owner, following these repeated research iterations, had learned sufficient knowledge on the subject to have reached a position where the research output could be taken further.

5.2 Methodology Analysis

In Section 3.4 it was pointed out that the researcher thought that aspects of the research resembled the Design Science research methodology. This section now explores the analysis of whether this research can constitute Design Science and then explores the links between Action Research and Design Science, in order to arrive at a final conclusion of whether the research conducted was either Action Research, Design Science, or both. The issue is examined both theoretically (epistemologically) and practically (i.e. assessment of the actions taken by the researcher and collaborator). This is a retrospective analysis that will assert the scientific foundation of this research through showing epistemological and methodological consistency.

5.2.1 Is the research Design Science?

The Design Science research methodology was introduced in Chapter 3.4. Amongst others, two key authors were mentioned that have developed a Design Science research methodology (Peffers et. al., 2008) and a framework that examines whether a piece of research satisfies all necessary features of Design Science (Hevner et. al., 2004). As part of the initial post-hoc analysis, the researcher posits that if a piece of research was conducted according to Peffers et. al.'s activities, and the completed research shows evidence of Hevner et. al.'s identifying features, then it can be stated that the conducted research indeed constitutes Design Science research. The following section will apply Hevner et. al.'s and Peffers et. al.'s results to the research conducted in this project and show whether the research aligns with the Design Science research paradigm. These were applied to the conducted research after the intervention had finished; this is therefore a post-hoc analysis of the researcher's actions.

This chapter is a post-hoc analysis and justification to consider whether this research project constitutes Design Science research. Peffers et. al. (2008) were shown to have produced a Design Science methodology for IS and also outlined a mental model for Design Science research - their model will be applied to the research conducted and it will be evaluated whether the research was carried out in accordance with their model and methodology.

Following on from this, the research results of Hevner et. al. (2004) will be applied in order to investigate whether the research conducted exhibits the seven features identified by Hevner et. al. as 'identifying features'. This two-pronged approach will provide a degree of confidence in the assessment of whether this research conforms to the Design Science research paradigm since the project is being assessed from two different angles; on the one hand, the project is assessed with regards to its conformity to the Design Science research methodology and whether it was conducted in the manner commanded by the Design Science methodology developed by Peffers et. al. (2008). On the other hand, the research will also be evaluated from Hevner et. al.'s (2004) point of view in order to assess whether the research exhibits any of the seven features that Hevner demands of a Design Science research project.

The earlier mentioned 'degree of confidence' is obtained through the fact that the research is evaluated against a set of criteria only recently developed in the field of I.S., which is grounded in the beginnings of Design Science, as shown in the previous chapter. Both authors have identified and developed methods through which Design Science research can be identified. Therefore, applying these methods to this research will reveal how well this research fits with their definition of Design Science. The fact that this is done from two different angles (i.e., was it conducted in the manner befitting a Design Science research project? Does it exhibit all features of a Design Science

research project?) only serves to strengthen the assessment outcome, as the research is being evaluated through two different methods.

The following chapter shall now evaluate whether this research was conducted according to Peffers et. al.'s methodology.

Peffers et. al.

Applying the earlier stated result of the six key activities requiring to have been performed, this chapter will now evaluate how and to what extent each of the key activities were performed. The activities were explained and outlined above.

Activity 1: Problem identification and motivation:
The introductory chapter of this report summarises the motivation behind the research. It gives a very brief background on the technology itself, it provides a background on what the technology is to be used for and how there is a state of dissatisfaction with the current technology and method of using this technology within the specified organisation. The setting of the research problem is then re-visited in the section outlining Action Research (Chapter 3.2.2); an entire chapter is dedicated to assessing whether the research conducted fits in with the Action Research methodology, and an investigation is conducted on how certain elements of the research constitute Action Research. Part of that investigation focuses on the initial setting of the problem and whether the type of problem qualifies for an Action Research project. Thus the problem setting is explored even further in that chapter, using evidence from a contract document that explicitly captured the aims and objectives of the research.

Briefly, the basic description of the problem is that there is a state of dissatisfaction with the existing use of the DSP technology. The creation of this technology is based on the use of a questionnaire asking open-ended

questions and thus the development of DSPs is not consistent, as it depends on a user's knowledge of the administrative law surrounding that Digital Signature and the user's ability to arrive at sufficient information from completing that questionnaire. In practical terms, the problem owner has no confidence that this process is sufficient to create DSPs. The technology of DSPs is ultimately going to be used in the problem owner's new infrastructure, therefore the problem can be considered to be highly motivated and relevant and grounded in a real business problem, as the problem owner has no other method of creating DSPs.

It has been demonstrated how and where the research problem was described and analysed and where the motivation of the researcher was stated. Thus, the requirement of this Activity having been performed can be considered as fulfilled.

Activity 2: Define the objectives for a solution:

The objectives of the solution were hinted upon in Chapter 1 describing the approach to conducting the research, and were also explored in Chapter 4.1 where the problem owner and problem specifics are introduced. It was shown that the use of Soft Systems Methodology helped in eliciting the requirements and objectives of the solution in the initial research iteration, and these were:

- A methodology for transforming natural language legal acts into process models
- Tools to convert process models into "codified forms"
- At least some of the tools are to take the form of software
- The produced codified forms are to be used in a service platform, inferring that the created DSPs must be consistent, as otherwise a system would not be able to peruse such information

From this it becomes clear that the quality criteria were described in a qualitative fashion, which is a permitted approach according to Peffers et. al. (2008).

These topics are explored in the research approach section of the document and therefore the requirement of this activity having been performed can be considered as fulfilled.

Activity 3: Design and Development:

There is ample evidence of this having occurred in Chapter 4, where the creation of several artefacts is described, both the method by which they were created and the nature of the artefacts themselves. In short, the created artefacts are:

- A mapping document between the data created by the PADS questionnaire and the data required by the ETSI TR 102 038 standard
- A Business Process Modelling Notation that can be exclusively used for modelling legal workflows involving the electronic signing of documents
- A mapping document between the data captured by the Business Process Modelling Notation and the data elements within the ETSI TR 102 038 standard and how this data is transformed and where it is placed within that standard
- A software tool that performs the transformation of Business Process Model to ETSI TR 102 038-compliant DSP

In other words, there was plenty of Design and Development activity conducted and documented, thus fulfilling the requirement of performing this activity.

Activity 4: Demonstration:

At the end of the chapter outlining the performed technical work (see Chapter 4.4), the created artefacts are demonstrated and used in a Sample Process showing the various tools developed within the Process Modelling Notation and outlining how the Process Modelling Notation is to be used.

Furthermore, guidance notes are provided that list a range of suggestions on how to apply the developed artefacts. The developed software artefacts are also demonstrated in that chapter; all developed artefacts were also demonstrated to the problem owners, the future users and the problem owners' CEO, all of which provided valuable feedback on how to improve earlier iterations of those artefacts (c.f. Chapter 3.3 on the research methods and how the collaborative relationship enabled multiple cyclical development iterations), thus the research and the derived solutions were demonstrated both on paper within this document and also physically to key audiences.

Finally, Chapter 5 on 'Discussion and Evaluation' explicitly outlines how each of the requirements and quality criteria (c.f. Activities 1 and 2) were addressed through the various artefacts developed, which is an implicit demonstration of the solution's ability to address the research problem.

It has thus been shown how the current research approached and satisfied the requirements of this activity.

Activity 5: Evaluation:

The Action Research chapter demonstrated how reflection on intermediate results was used to arrive at improved results in an iterative fashion. Also, a project-wide Evaluation is conducted in Chapter 5, to demonstrate that the final solution represents an adequate method of addressing the research problem and addresses it according to the quality criteria defined (c.f. Activity 1 and 2). It is interesting to note that Peffers et. al. (2008) describe this activity as an iterative process which results in research work being conducted

further if the requirements of Activities 1 and 2 are not met, or that the research process moves on to Activity 6 once the requirements of Activities 1 and 2 have been met. This iterative approach is very similar to the Action Research approach on conducting reflection on intermediate results, a point to be furthered below.

Therefore, as iterative development utilised the evaluation of intermediate results against initial requirements and quality criteria, and since the overall outcome of the final solution was also assessed, it can be stated with confidence that this activity was satisfied.

Activity 6: Communication:

Two different kinds of communication and dissemination activities were performed during the course of this research project. The first kind involved stakeholders relevant to the problem owners only, namely future users, the problem owner's Management Team and finally their organisation's CEO. The aim of this dissemination was to transfer the results and gained knowledge over to the organisation owning the problem, to explain the functionality of the constructed solution artefacts, to provide an insight into the theoretical aspects involved in the domain and help the problem owner gain a greater insight into this domain from a scientific perspective. Also, dissemination to the future users was aimed at preparing them for the change and to provide them with confidence that the solution would be easy to use.

The second kind was along the more traditional lines of disseminating knowledge of the artefacts and the problem to the wider scientific community through the creation of conference and journal papers. One paper, introducing and explaining the Business Process Modelling Notation, was presented at the JURIX 2007 Conference; the full reference for this publication is as follows:

Alamillo, I., Martinez, D., Seltsikas, P. and Papas, N. "Designing a modelling methodology for legal workflows." JURIX 2007: The Twentieth Annual Conference in Legal Knowledge and Information System.

The second paper had a more theoretic approach, examining the role of artefacts in the context of interventionist research methodologies and constitutes an abbreviated version of Chapter 5. It is called "Legal Workflows and Digital Signatures in eGovernment: Action Research or Design Science?" and had been submitted to the EJIS-Journal. At the time of writing, no decision on acceptance had been reached yet. Another paper is in preparation, aimed at the more technical audiences of digital security and aiming to disseminate information on the actual artefacts and their role in creating DSPs.

In other words, activities were performed with the aim of engaging in the dissemination of the knowledge gained and putting it into perspective in comparison against other, existing knowledge.

Hevner et. al.

It was stated in the introduction of this sub-chapter that both Peffer's and Hevner's results would be used to evaluate the adherence of this research work to the Design Research paradigm. The above section covered the alignment of this work to Peffer's results; this section shall now cover the alignment of this work to Hevner's results.

Hevner et. al. identified seven specific guidelines that must be present in a piece of research in order to constitute Design Science, as explained in the earlier chapters. The various guidelines are now assessed with regards to whether they are present or not.

Guideline 1: Design as an Artefact:

Hevner et. al. (2004) state that the final output of a Design Research project must take the form of either a Construct, Model, Method or Instantiation (Hevner et. al., 2004). These forms were originally defined by March and Smith (1995) as follows:

Construct: The vocabulary of a particular domain, which is used to provide a conceptualisation that is used to describe and define the terms, and thus ultimately the knowledge, of a particular discipline.

Model: A description or representation of 'how things are', implemented such that the description is useful to a particular goal-oriented task; March and Smith (1995) used the example of "logical block access" models in database design as a model that is "extremely useful for feasibility assessment" but "inappropriate for physical database design" (March and Smith, 1995; using material from Teorey and Fry, 1982).

Method: An instruction of a number of steps required to perform a task. Methods are intrinsically linked (not necessarily in an explicit fashion) to "a set of underlying constructs and a representation of the solution space" (March and Smith, 1995, using material from Nolan, 1973). Thus, "methods are often used to translate from one model or representation to another" (March and Smith, 1995), using the common language (or constructs) that was applied to the description and definition of the solution space.

Instantiation: The implementation of an artefact in its environment, which "operationalises constructs, models and methods" (March and Smith, 1995), thus bringing the four main outputs together.

Using the above definitions, it then becomes clear how these were achieved in the research described in this document.

The constructs of this research domain had already been defined through the ETSI standards documents on DSPs. These documents defined terms and meaning and suggested a technology to implement this concept. As this research is focused on improving the technology suggested by the ETSI standards, it did not contribute to the constructs of the DSP domain. However, in Chapter 5.1 it is highlighted where the constructs need to be improved in order to provide a higher degree of alignment between construct and the technology implementing it. The particular example refers to the use of free-text fields in the XML-definition of the DSP which is prohibitive to automated processing.

As shown in Chapter 4.3, a business process modelling notation was developed (using the constructs defined by the ETSI standards documents), which provides a description of how Acts and Documents and Signatures interact and captures how the data is captured and split between the three entities. The goal of this notation is twofold:

1. It attempts to capture a legal workflow in which Digital Signatures are exchanged, such that the information in the DSPs can be derived and applied and cross-referred to the purpose of the Digital Signature
2. It attempts to provide a starting point from which the derived data referred to above can be processed further

Therefore, the model that was developed covered the relationships between data in the form of natural language, data as used in the process modelling notation, data in the form of XML and finally the transformation of data between these various stages. This model ensured that the data, as defined by the constructs, would remain consistent throughout its various transformations.

The research also arrived at a method; in fact, the key output of this research was a method. Chapter 4.4 describes the method in detail, which must be

followed in order to turn natural-language description of legal matters into a workflow model using the developed business process modelling notation and then into an XML file of a DSP. Therefore, the developed method describes the steps involved in creating DSPs.

There are two main instantiations which were arrived at over the course of the research. The first instantiation, described in Chapter 4.3, is a business process modelling notation which is aimed at eliciting data relevant to the legality of Digital Signatures. The other instantiation, described in Chapter 4.4.3, is a software tool which transforms a business process model and the data contained within the process model into an ETSI TR 102 038 compliant DSP in XML format. Both instantiations represent key steps in the method arrived at earlier and can be seen as a proof of concept of the developed method - a valid aim of an instantiation, as claimed by March and Smith (1995).

As has been shown above, the research produced various artefacts that conform to the requirements of Design Science research. A number of instantiations were produced, satisfying the need of an instantiation artefact. A model was created, satisfying the need of a model artefact. Finally, a method was developed, satisfying the need for a method artefact. In other words, the research produced three out of the four acceptable types of artefacts and made suggestions for changes to the fourth type (constructs), thus satisfying the Guideline that stipulates that at least one of these artefact types must be produced in Design Science research.

Guideline 2: Problem Relevance:

This Guideline requires the research to provide a technology-centred solution to a relevant business problem, according to Hevner et. al. (2004).

The relevant business problem was stated, explained and outlined in the introductory chapter of this document (see Chapter 1 for details; further detail also in Chapter 4.1) and can be summarised as the need to replace a current business process, which is manual and both time and labour intensive, with a more automated procedure that reduces the use of both time and labour resources on the one hand, and on the other hand produces results that are more consistent.

This business problem is tackled through the use of technology; using and applying the aforementioned business process modelling notation requires the use of modern process modelling technology, whilst the use of a transformation software (c.f. Chapter 4.4.3) also implies the use of technology for the data conversion part of the developed method.

Thus, a relevant business problem is addressed through the application of a technology-centred solution and satisfies the requirements set up by Hevner et. al. (2004).

Guideline 3: Design Evaluation:

As mentioned in the previous chapter on conducting an evaluation of the performed research, an evaluation was carried out in this research to investigate "utility, quality and efficacy" of the design artefact, as required by Hevner et. al. (2004).

The chapter on the employed research methods (Chapter 3.3) demonstrated how reflection on intermediate results was used to arrive at improved results in an iterative fashion. Also, an Evaluation/Discussion activity is conducted in Chapter 5, to demonstrate that the final solution represents an adequate method of addressing the research problem.

The evaluation method applied is the method of Interpretive Evaluation. Hevner et. al. describe suitable evaluation methods for Design Science research (Hevner et. al., 2004; p. 86) and as can be seen in Chapter 5.2.1, both evaluation methods revealed that the artefacts sufficiently address the business problem and that the design artefacts possess utility, quality and introduce a higher degree of efficacy. In conclusion, this guideline can be deemed as having been satisfactorily applied and completed.

Guideline 4: Research Contributions:

The research conducted offered some contributions to knowledge, which is what this guideline requires a research project to do. Hevner et. al. (2004) set out four key areas in which a Design Science research project has to make a contribution and they state further that the project must make such a contribution in "one or more" of these areas (Hevner et. al., 2004).

These four key areas are:

- The Design Artefact: the design artefact itself represents a contribution through the application of new knowledge or the application of existing knowledge in new and innovative ways
- Foundations: the development and evaluation of novel constructs, models and method artefacts that extend and improve existing formalisms are regarded as significant contributions
- Methodologies: the application of and evaluation of new and existing evaluation methods are important parts of Design Science research
- Practical: the research must demonstrate a clear contribution to the business environment and solve the business problem

(adapted from Hevner et. al., 2004)

The research in this document has made several contributions. With regards to the practical key area, the evaluation of the research has shown how the

various artefacts developed contributed to solving the business problem. The developed method, models and instantiations are combined in order to tackle the problem of creating DSPs (c.f. Chapter 4.4 ff), and the evaluative chapter (c.f. Chapter 5) demonstrated how the research results satisfied the problem.

Finally, the complete design artefact (i.e. the developed models, methods and instantiations) also represents a contribution as existing knowledge was combined in new and innovative ways (process modelling and data transformation to XML are both known concepts that have been applied in past research, e.g. Mercatali et. al. (2005), Seltsikas and Palkovits (2006), Governatori (2004)) in order to tackle the business problem.

Note how Hevner et. al. restrict the contribution to "Methodologies" to the application and evaluation of "evaluation methods" (Hevner et. al., 2004). Taking the concept of "methodology" further, the author considers that contributions can be made to methodologies that go beyond the evaluation methods of research. As shown in the section on comparing Action Research and Design Science (c.f. Chapter 5.2.2), the author considers the research to have clarified some points on the crossovers between the Action Research methodology and the Design Science methodology, and to have raised some new issues with regards to the compatibility of these two research methodologies. If one were to apply Hevner's definition of possible research contributions to "methodology", then these would lose their validity. The author recommends that Hevner's definition of "methodologies" ought to be expanded such that it considers contributions to the understanding of the research methodologies applied by IS researchers to be valid contributions to the IS field.

Taking the above paragraphs in account, the author states with conviction that there has been contribution to the existing body of knowledge within the IS field, meaning that this guideline has been satisfied in this research.

<u>Guideline 5: Research Rigor:</u>

Of Research Rigor, Hevner et. al. (2004) demand that the research was conducted in "adherence to appropriate data collection and analysis techniques", but also warns that the developed artefacts may need to operate in an environment which does not lend itself to "excessive formalism" (Hevner et. al., 2004). Therefore, with regards to the activity of building the artefact itself, Hevner et. al. state that the applicability of rigor must be assessed "with respect to the applicability and generalizability of the artefact" (Hevner et. al., 2004). Finally, Hevner et. al. establish that "rigor is derived from the effective use of the knowledge base - theoretical foundations and research methodologies" (Hevner et. al., 2004).

Taking the above requirements with regards to research rigor into account, it becomes evident that the "effective use of the knowledge base" is being addressed in the preceding chapters on Action Research (c.f. Chapter 3.2.2 ff), and the earlier chapters on the background to the research domain (c.f. Chapter 2). The chapter on the employed research methods (Chapter 3.3) demonstrates the use of Action Research within this research project, particularly with how data was being applied to the continued research on both the models and the development of the business process modelling notation in the iterative manner typical for Action Research. On the other hand, the later chapters looking into the background of the research domain (and domains closely related to the research problem) establish the required "theoretical foundation" that Hevner et. al. referred to, showing that the basic concept of the research problem has been tackled before and that the artefacts developed as part of the research have a theoretical foundation (c.f. Chapter 2) from their applicability in a slightly different, yet related, domain (e.g. ARIS for Law as demonstrated by Sijanski and Münch (2005), or UML for Regulatory Compliance enforcement as demonstrated by Giblin et. al. (2005)).

With regards to the software artefact (c.f. Chapter 4.4.3) that transforms the output of the business process modelling notation into the ETSI TR 102 038 compatible DSP, this was constructed using the software development methodology known as "proto-typing" (Dennis and Wixom, 2000), which meant that the researcher would continuously liaise with the problem owners on completing minor stages in the artefact development in order to continuously evaluate the artefacts and allow the problem owners to retain greater control and influence on the design of the artefacts (Dennis and Wixom, 2000). Also, as prototyping is a cyclical and iterative activity, it mapped well against the overall Action Research approach.

Hevner et. al. (2004) talk about the "applicability and generalizability" of the developed artefacts, as mentioned above. With regards to the software artefact, there is little generalisability as it was developed with the specific purpose of converting the output of the developed business process modelling notation into ETSI TR 102 038-compatible XML. As the notation was implemented in the Adonis BPM Toolkit, the developed software artefact was developed such that it could input and analyse Adonis BPM Toolkit XML-output only. This lack of generalisability thus results in a large amount of applicability to the research problem, because the tool was developed with the specific requirements of the research problem and honed towards delivering an important part of the technical solution addressing the research problem.

On the topic of 'generalisability', this is defined by Polit and Hungler (1991) as the degree to which research findings can be generalised from the study sample to the entire population (Polit and Hungler, 1991; p. 645). However, this is a qualitative study and 'generalisability' is not a concept that bears much relevance in qualitative study anyway (Myers, 2000); Myers (2000) admits that "partial generalization may be possible to a similar population", but Adelman et. al. (1980) state that the knowledge generated by qualitative research on one particular sample is valid enough in its own right and does

not need to be generalised in order to gain further legitimacy (Adelman et. al., 1980), as is sometimes claimed by quantitative researchers (Yin, 1989). Therefore, 'generalisability' should be understood, in the context of this work, as partially applicable to similar organisations facing similar demands, not in the 'classical' quantitative way of making assessments of a complete phenomenon on the basis of a study of a component part of that phenomenon.

The developed business process modelling notation faces a similar issue, in that it has high applicability to the research problem due to its design as a particular link in a chain of technology artefacts addressing the research problem, but compared to the developed software artefact it has a greater degree of generalisability as its graphical design incorporates many basic elements of the flowchart notation (Goldstine, 1972), which could be re-used in different business settings. However, the data collection tools within the notation are not generalisable, due to their specific targeting of DSP data.

Whilst the developed artefacts lack some generalisability, they do possess a great degree of applicability to the research problem. It was also shown how the research is steeped in a sound theoretical foundation, both from a methodological point of view and also from the point of view of applying and interpreting past research results. Thus, Hevner et. al.'s requirements for this guideline have been met.

Guideline 6: Design as a Search Process:

Hevner et. al. (2004) refer to Simon (1967) when they talk about the search process being equivalent to the "Generate/Test Cycle", by which they mean that the research ought to undergo several iterations before an optimal or near-optimal solution is found (Hevner et. al., 2004). Furthermore, Hevner et. al. (2004) state that the test cycle ought to "establish that it [the artefact] *does* work...even if we cannot completely explain *why* it works" (Hevner et.

al., 2004; emphasis in original), thus demonstrating how Design Science takes a very practical approach towards research and is more concerned with utility than establishing truth, a theme originally explored by March and Smith (1995).

The iterative development of the artefacts comprising the solution to the research problem is obvious through the application of Action Research, as demonstrated in the previous chapters. Through its very nature, Action Research is an iterative research methodology that uses feedback to create new iterations, with each iteration coming closer to the solution (see Chapter 3.3.1 for a detailed description of how Action Research is applied in this research). The key activity in the Action Research process is the "Evaluate" activity, where the feedback on the created artefact iteration is gathered. This feedback then feeds further "build" activities (e.g. Baskerville and Wood-Harper, 1996). The previous chapter on Action Research shows how this was implemented, so the "Generate/Test Cycle" is present in this research.

With regards to whether the artefact works to solve the business problem, this theme was explored in the evaluation chapter (c.f. Chapter 5.1) and it is demonstrated there that the artefact does work and produces the required ETSI TR 102 038-compliant DSPs. Therefore, this guideline can be assumed to have been addressed and met.

Guideline 7: Communication of Research:

As mentioned as part of Activity 6 of Peffers et. al.'s Design Science research methodology activities, this research has been presented to a wider audience, such as the scientific community. However, Hevner et. al. (2004) see this guideline in a slightly different perspective, in that they prescribe the output of the research to be communicated effectively to the practitioners within the organisation in which the artefact is to be used (Hevner et. al., 2004). They make it a point to stress that the practitioners ought to be considered as two

disparate groups, the "technology oriented audiences" and the "management oriented audiences" (Hevner et. al., 2004).

The research team included, on the organisational side, both a management oriented team member as well as a technological oriented team member. The technological team member was involved in providing technical feedback and assisted in the artefact construction by providing specialist knowledge. The management oriented team member reviewed project progress and reviewed, commented and assessed the final artefact. Thus, the project was communicated to the two audiences required by Hevner et. al. (2004), but despite the two research team members being key members in their organisation as well, this guideline must be seen as the weakest of them all, since two organisational members can not possibly be regarded as a sufficiently-sized sample that would be capable of spreading the knowledge of the solution (both the technical as well as the managerial aspects) across the entire organisation, thus putting the solution at risk of not being accepted by the organisation (Laudon and Laudon, 2004). This topic is explored further in the chapter on the research's limitations in Chapter 6.3.

As mentioned above, this guideline was partially met but with some reservations.

Summary
From the above two sections on Peffers et. al.'s Design Science research methodology and Hevner et. al.'s guidelines on conducting Design Science research, it becomes apparent that as the research conducted meets all of the guidelines and activities laid out by Peffers and Hevner, this research could therefore be considered to be a valid example of Design Science.

Hevner et. al. (2004)	This Research	Peffers et. al. (2008)	This Research
Design as an artefact	Several artefacts were created, including a modelling notation, algorithmic methods and a software tool. There is a physical artefact, which is critical to Hevner et al.	Problem Identification and motivation	The problem owner identified that their existing DSP creation process was cumbersome, slow and error-prone, and sought an improved. Problem is highly motivated.
Problem relevance	The problem owner identified that their existing DSP creation process was cumbersome, slow and error-prone, and sought an improved method. Problem is relevant.	Define objectives for a solution	Objective was to develop an improved method to produce DSPs, but based upon some existing processes. A solution was sought and delivered.
Design Evaluation	Evaluation took place as part of the research cycle, including prototyping. The design was evaluated against the problem, and other research.	Design and development	Artefact development conducted using cyclic methodology including prototyping; artefacts exist and are in use.
Research Contributions	Domain contribution through the development and evaluation of artefacts solving a particular business problem. Research contribution through creation of a method for legal workflows and DSP that can be used elsewhere.	Demonstration	Internal meetings with stakeholders. Application of developed solution on a representative problem and creation of prototype output, then hand over to client.
Research Rigor	Demonstrated through the application of a methodology.	Evaluation	Continued evaluation took place as part of the research cycle.
Design as a Search Process	Demonstrated through the various iterations of the work, although limited in part by client requirements.	Communication	Internal communication to affected stakeholders. Funded by and reported to the problem owner's management team plus presentation to the CEO.
Communication of Research	See Alamillo et. al. (2006) for communication of prior technical outputs. Funded by and reported to the problem owner's management team plus presentation to the CEO. Also this article and internal communication to affected stakeholders.		

Table 5-1: Comparison of Research against Hevner et. al. and Peffers et. al.

To move beyond this comparison and post-hoc rationalisation, the researcher would need to consider some key areas of similarity and difference in an

effort to deepen understanding of both Action Research and Design Science. As a previous chapter established that this research was planned and conducted as Action Research, the obvious question is therefore: which of the two is this? Is it Action Research, or Design Science? Is it both, or are they mutually exclusive? What is the link between Action Research and Design Science? The researcher will focus on the role of the artefact, the research cycle, the evaluation of the research and the role of knowledge versus learning, as these emerged from reflections on the research effort.

5.2.2 How Similar are Design Science and Action Research?

In this chapter, the author will investigate some apparent similarities between the Action Research and Design Science research methodologies, followed by an analysis on what the similarities could mean and finally solve the question of whether this is an Action Research or Design Science research project.

Another possible interpretation of Design Science is provided below, based on the evidence provided in the previous chapter on Design Science. The possible interpretation is provided in the form of a diagram that captures the two key steps of Design Science - "Build and Evaluate", which is a literal quote from Hevner et. al. (2004), who was in turn quoting Markus et. al. (2002). As such, whilst most authors see more than two steps within the Design Science process, the steps can be grouped into the two activities shown in the diagram below.
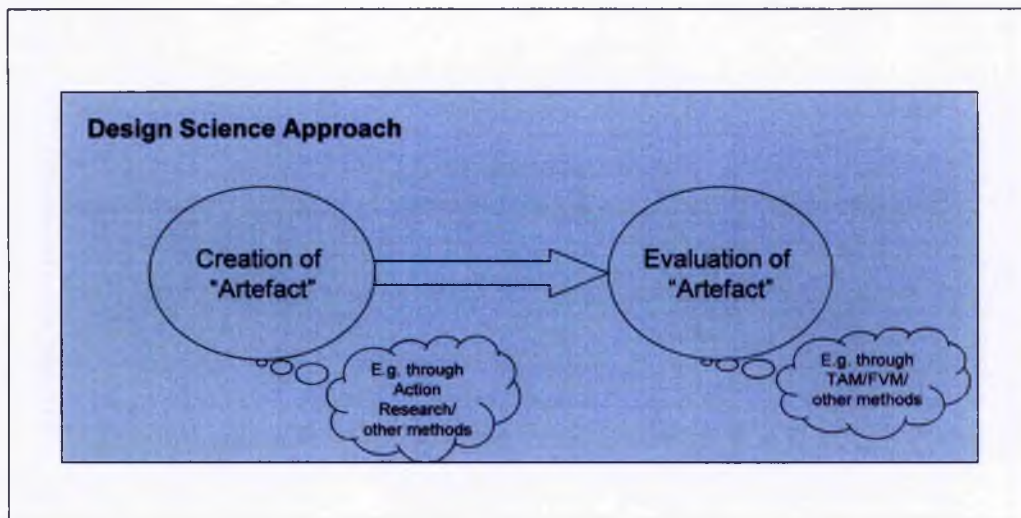
Figure 5-3: A possible interpretation of the Design Science approach

The basic idea is that an Artefact is created through some method, which is not specified (therefore, as the method of creation is not specified, Action Research could be a permissible method through which the Artefact can be created) and that the created Artefact is then Evaluated through some other method in such a way that the "research [is] evaluated in light of its practical implications" (Hevner et. al., 2004; p.77), which are (as stated previously), "identified organizational problems" (ibid.).

The author's confidence in portraying this generalised view stems from statements such as "The design process is a *sequence* of expert activities..." (emphasis added) and "This build-and-evaluate loop is typically *iterated* a number of times before the final design artefact is generated" (emphasis added, from Hevner et. al. (2004), quoting Markus et. al. (2002)) As can be seen from these statements, there is a lot of emphasis on sequences and iterations, which are also key aspects of Action Research, as demonstrated in Chapter 3.2.2 above.

Therefore, one could argue that Action Research is a form of Design Science through the fact that Action Research undergoes a similar cycle of evaluation

and continuous self-improvement. However, where Action Research and Design Science differ is through the fact that Design Science explicitly states that it is concerned with evaluating an Artefact against "identified organisational problems", whereas Action Research evaluation is more narrowly focused on improvement of a practice which may or may not be linked to a wider organisational problem. Peffers et. al. (2008) see "Action Research, as...an alternative or complementary paradigm through which to design IS research artifacts" (Peffers et. al., 2008), in their concluding remarks on their discussion of Design Science, without going into more depth of this theme.

The above theme has been picked up by other researchers in the IS field as well. For example, Järvinen (2005) states that "Action Research and Design Science are similar" (Järvinen, 2005), which is a similar statement to the researcher's assertion in the previous paragraph.

Järvinen builds his argument around a similar point as the researcher. Järvinen identified that Action Research is cyclical and quotes Susman and Evered's (1978) five-step cycle of diagnosis, action planning, action taking, evaluation and specifying learning (Järvinen, 2005, paraphrasing from Susman and Evered, 1978), which is a known approach of Action Research. Järvinen then compares this with Vaishnavi and Kuechler's (2004) view on a five-step Design Research cycle, where the individual stages are identified as problem awareness, suggestions, development, evaluation and conclusion (Järvinen, 2005, paraphrasing from Vaishnavi and Kuechler, 2004). Järvinen sees this as proof that Action Research and Design Research are similar, as he identified that "there are many similarities, e.g. five steps with different names but almost identical contents" (Järvinen, 2005). Järvinen then continues to identify key aspects of both Action Research and Design Research and identifies six areas where Action Research and Design Research yield equivalent, or very similar, results. This comparison of Action Research and Design Research, and the identification of so many common elements,

leads Järvinen to conclude that "Action Research and Design Science should be considered as similar research approaches" (Järvinen, 2005).

Similarly, Cole et. al. (2005) also see a close relationship between Action Research and Design Research. Cole et. al. (2005) choose a slightly different approach than Järvinen in order to construct their argument - they first identify key points of each research method, which in the case of Design Research they present Hevner's seven criteria for Design Research, which were discussed in detail in the previous chapter. For Action Research, on the other hand, Cole et. al. (2005) follow Järvinen's lead and use Susman and Evered's (1978) five step Action Research methodology and then apply Davison et. al.'s (2004) guidelines on conducting Canonical Action Research. The result is that Cole et. al. (2005) identify seven Design Research criteria and five Action Research criteria that they can use to classify research with. Their next step was to perform a "cross-application of criteria" (Cole et. al., 2005), meaning that the Action Research criteria would be applied to a notable Design Research paper and that the Design Research criteria would be applied to a notable Action Research paper; Cole et. al. would then use this cross-application to see to what extent the criteria are interchangeable between Action Research and Design Research and thus draw inferences on the similarity between the two approaches.

The results of their study indicate that Action Research and Design Research are similar on the levels of Ontology, Epistemology and Axiology. With regards to Ontology, Cole et. al. (2005) identified that both Action Research and Design Research follow into the "becoming" ontology, through the fact that the "phenomenon of interest does not remain static through the application of the research process" (Cole et. al., 2005), which in the case of Action Research is a logical necessity (the Action Research process aims at improving, and thus changing, a state of non-desirability, as shown in Chapter 3.2.2.1), whilst in Design Research the change occurs through the construction of an artefact (Cole et. al., 2005).

With regards to Axiology, Cole et. al. (2005) identify that "both value the relevance of the research problem, and emphasis on practical utility and theoretical knowledge simultaneously" (Cole et. al., 2005), thus showing their acknowledgement that both Action Research and Design Research have the same, common goal when applied to research - practical change, and contribution to existing theoretical knowledge.

However, Cole et. al. (2005) identify some issues with regards to Epistemological similarity. Whilst they posit that both Action Research and Design Research "assume a mode of knowing that involves intervening to effect change" (Cole et. al., 2005), thus excluding Epistemological positions that require non-intervention from the side of the researcher (e.g. Positivism), they also note that Epistemologically Action Research and Design Research can be placed in different positions. They reference Burrel and Morgan's epistemological framework (1979), which places Action Research into the neo-humanist, subjective-conflict position, whilst Design Research is regarded as functional, objective-order (Cole et. al., 2005, with adaptation from Burrel and Morgan, 1979). However, Cole et. al. argue that Design Research can be subjective as it is focused on one particular organisation, and that "functionalism can also encompass conflict" (Cole et. al., 2005, paraphrasing from Hirschheim et. al., 1989), thus cross-applying aspects of both Action Research and Design Research's epistemological positions to each other.

Cole et. al. (2005) use the above argument, namely the ability to cross-apply epistemological positions, to show that Action Research and Design Research are epistemologically similar. To further their argument, they quote Baskerville et. al. (2004), who identified Action Research within the IS context as belonging to the Pragmatist epistemological position, and also quote from Hevner et. al. (2004), who sees Design Research in IS to also sit under the Pragmatist school of thought - they take these arguments to posit that "the

common philosophy that Design Research and Action Research share is pragmatism" (Cole et. al., 2005).

In other words, Cole et. al. (2005) have identified key criteria that show that Action Research and Design Research are similar from the points of view of Ontology, Epistemology and Axiology. The impact of this finding on the research conducted within this document, and shown to have traits of both Action Research and Design Research, is that it can therefore be seen as both either Action Research or Design Research - or so it may seem at first sight. The important caveat in Cole's work is that Action Research and Design Research can only be considered similar if their posit of both Action Research and Design Research falling within the Pragmatist school of thought is accepted.

However, the author has keenly stressed in Chapter 3.1.2.1 that the author's Epistemoiogical position is Constructivism. The author has also shown how Action Research can also be considered a constructivist research methodology and has provided evidence on why the author considers this to be a valid statement. However, in order to present this work as a piece of research that satisfies both Action Research and Design Research criteria, the author must not only prove that Action Research and Design Research criteria can be applied to the research conducted (which was done in Chapters 3.2.2.4 and 5.2.1), but must also show that within the author's theoretical framework, Action Research and Design Research can be considered equal from the points of view of Epistemology, Axiology and Ontology, as done by Cole et. al. (2005). The crucial difference between this research and Cole's research is that Cole et. al. posit Action Research and Design Research to share a common Epistemology. As the author in this research posits Action Research conducted under the Constructivist paradigm, the author must therefore be able to demonstrate that Pragmatism, Design Research's Epistemoiogical position, does not conflict with Constructivism and that the two positions

share enough similarity amongst each other to allow the author to identify Pragmatist Design Research as similar to Constructivist Action Research.

Should the author not be able to do this, then the author can not describe this work as being both Action Research and Design Research, since the author would then be Epistemologically inconsistent. Therefore, it must be investigated whether Pragmatism and Constructivism share sufficient similarities to be considered equal.

Pragmatism vs. Constructivism

The question of whether the schools of Pragmatism and Constructivism have anything in common has been tackled by a range of researchers before, such as Neubert (2001) and Garrison (1997). Their work (as well as work they quote from other authors) considers John Dewey to be the 'father' of Pragmatism and use quotations of Dewey's to illustrate their point. Amongst the most commonly quoted works of Dewey by Neubert and Garrison are "The Quest for Certainty" and "Experience and Nature", which are therefore key to understanding the debate of Pragmatism vs. Constructivism.

It is somewhat surprising that Dewey could be considered as a source of showing a similarity between Pragmatism and Constructivism, especially when one considers the following quote: "It would be hard to find a more thoroughgoing confirmation than this conclusion provides of the complete hold possessed by the belief that the object of knowledge is a reality fixed and complete in itself, in isolation from an act of inquiry which has in it any element of production of change" (Dewey 1988, p.19, as quoted by Neubert (2001)). The reason that this is a surprising piece of evidence is the fact that the quote essentially describes a fixed, external world which is wholesome unaffected by an inquiry performed on it, which is contradictory to Constructivism's basic premise (see Chapter 3.1.2.1) and is a very positivistic perspective.

The key to Neubert's (2001) argument lies in the lines preceding Dewey's quote. Neubert (2001) quotes an entire paragraph, which contains phrases such as "The theory of knowing is modelled after what was supposed to take place in the act of vision" (Dewey, 1988), "The real object...is a king to any beholding mind that may gaze upon it" (ibid.) and "A spectator theory of knowledge is the inevitable outcome" (Dewey, 1988), all of which are pointing towards a point made by both Neubert (2001) and Anderson (1997), which is "pragmatism, in any of its forms, must take the view that we think best not alone, but as participants, as parties to an ongoing project of inquiry" (Anderson (1997), as quoted by Neubert (2001)). Adopting the view that there is participatory activity occurring in Pragmatism thus excludes Pragmatism from possibly being Positivistic and points at a different direction for it instead, which Neubert (2001) follows up to arrive at his first major reason for Pragmatism being similar to Constructivism. Dewey (1988) refers to actions that are connected with the act of vision, and vision is something that is undertaken by a spectator. Neubert (2001), therefore, sees a connection between the Deweyan spectator and the Constructivist 'observer' and explains that, in his opinion, observing in the context of Constructivism can mean "seeing, hearing, feeling, sensing, imagining....but acting and participating as well" (Neubert, 2001). Neubert therefore posits that "all claims to knowledge be seen as provisional constructions of observers that on principle should be kept open to further re/de/constructions by other observers" (Neubert, 2001). This quote signifies an important assumption about Pragmatism and puts it in line with Constructivist views - Neubert sees Dewey's concept of the spectator to be similar or equal to the Constructivist observer; furthermore, Neubert then sees knowledge being constructed through Constructivism, only to allow a Pragmatist to then 'observe' the constructed knowledge and test the validity of the constructed knowledge (Neubert, 2001).

Neubert (2001) uses the equalisation of the observer and spectator concept as the main building block for his further arguments. Neubert (2001) draws a conclusion from Dewey's "Theory of Experience" (Dewey, 1925), namely that Dewey focuses on "primary experience as the source and *telos* of all reflection" (Dewey, 1925; quoted by Neubert, 2001; emphasis in Neubert's quote) and thus showing that "This allows for the vision of a universe that is still 'in the making'" (Neubert, 2001). This argument essentially says that at any given time, there exists an incomplete picture of the world and that "primary experience", i.e. *a priori* knowledge, has constructed this picture which then leads to reflection on this picture and this reflection then leads on to the continued construction of further pictures. In the words of Neubert (2001), this is "a circular logic of observation...knowledge is actively constructed in processes of inquiry..." (Neubert, 2001; p. 4). The essence of these conclusions is that knowledge is continuously 'constructed', only for the Deweyan pragmatist spectator to come and reflect upon it, with a view of constructing new knowledge.

Neubert (2001) uses a similar argument to raise a further point that points to similarity between Pragmatism and Constructivism. Neubert (2001) mentions Dewey's view that "cultural viability rests on the operation of habits that inform our active capacities to master new situations" (Neubert, 2001; p. 5). In other words, a Deweyan Pragmatist can deal with new situations by reflecting on past knowledge. Neubert argues that from the point of view of a Constructivist, we 'deconstruct' our known and habitual ways in the light of new situations, we adapt our habits and 'construct' a new habit that can potentially deal with a new situation. This shows how Constructivism and Pragmatism are therefore closely linked.

Garrison (1997) has similar views on the similarity between Pragmatism and Constructivism. Garrison states that his version of "social constructivism [mirrors] the pragmatic tradition of John Dewey" (Garrison, 1997) and also acknowledges the earlier point that Dewey could be thought of as a positivist,

because "pragmatists generally reject representative realism or any epistemology that describes truth as correspondence to reality" (Garrison, 1997) and evidence of this view was provided earlier with a quote from Dewey.

Garrison's arguments for Pragmatism and Constructivism being similar are close to Neubert's (2001) views also. For example, Garrison uses Dewey's writings on the mind to show that Dewey believed in Constructivism. Specifically, "Through speech a person dramatically identifies himself with potential acts and deeds; he plays many roles, not in successive stages of life but in a contemporaneously enacted drama. Thus mind emerges" (Dewey, 1925, quoted in Garrison (1997). To Garrison, this means that Dewey believes that speech is the source of meaning and the fact that Dewey uses the verb "emerge", can be thought of as a synonym for "constructed" - to Garrison, this means that Dewey considered the mind to be "a social construction" (Garrison, 1997).

Garrison uses this premise for another piece of evidence pointing towards similarity between Pragmatism and Constructivism. Garrison quotes Dewey's statement that "Meanings do not come into being without language..." (Dewey, 1925); as "Meaning for Dewey was a social construction" (Garrison, 1997), it follows that Garrison considers Dewey to set out rules for Pragmatism that also apply to Constructivism - with knowledge (in this case, knowledge of the mind) being regarded as a construction out of, amongst others, speech.

Finally, Garrison (1997) picks up on a point that was also raised by Neubert (2001), which is related to the conduct of inquiry constructing new knowledge. Dewey is quoted by Garrison (1997) as saying "objects of our common sense...are not matters of knowledge...where they precede operations of...inquiry. But in the degree in which...affairs...are transformed by...consequences of operations [of inquiry]...they also are objects of

knowledge" (Dewey, 1925). To Garrison, this means that the act of inquiry and symbolic manipulation of objects results in the construction of knowledge and meaning of said objects. Therefore, Dewey is seen as recognising knowledge construction occurring through inquiry and Garrison therefore sees this as further evidence for the similarity between Pragmatism and Constructivism (Garrison, 1997).

To round off the discussion on the similarities between Constructivism and Pragmatism, consider these additional quotes; von Glaserfeld is quoted as saying "constructivism is a form of pragmatism" (von Glaserfeld, 1989), and Garrison is quoted in a different publication (Garrison, 1997b) as saying "Dewey was a 'social constructivist' decades before the phrase became fashionable" (Garrison, 1997b).

What this chapter has shown is that a range of philosophers have investigated similarities between Pragmatism and Constructivism and the conclusions of these philosophers have been shown as agreeing that Pragmatism share sufficient traits to be considered similar; in fact, Dewey was called a constructivist by one of the philosophers.

The meaning of the above paragraph shows that since Pragmatism and Constructivism are similar approaches and have similar views on the construction of knowledge, it can therefore be said that the view of Action Research and Design Science being similar can be considered as Epistemologically consistent, since it was shown that the two Epistemological views are similar to each other as well.

The immediate result is that the research work being presented within this document can be considered to be either Action Research, or Design Science, or both. The researcher therefore has the necessary methodological and epistemological alignment between the two approaches in order to make an

assessment of the two methods and make a judgment on whether the research intervention could be considered Design Science.

5.2.2.1 Deciding the methodological position of this research

The adherence to the Design Science methods, demonstrated in Section 5.2.2, can only be used to make a judgment on whether the research is Design Science at a superficial level. That is, the actions taken can be determined whether they were within the Design Science realm and post-hoc justifications of these actions can be made with regards to methods. However, deeper reflection and understanding is necessary in order to arrive at an answer, therefore this section shall consider the roles of the artefacts, the research cycle, the research evaluation and the role of learning (and the knowledge it generated) that took place.

The Role of the Artefacts

Section 3.4 introduced Design Science as a research methodology that aims to effect change through the design, build and implementation of an artefact capable of "serv[ing] human purposes" (March and Smith, 1995). Since the definition of artefact by March and Smith (1995) can cover constructs, models, methods and instantiations, it can be said that an artefact is any type of research product that serves human purposes and effects change.

On the other hand, Baskerville (2004) defines Action Research in the context of an IS research methodology as aiming to "solve current practical problems while expanding scientific knowledge" (Baskerville, 2008), which means that, axiologically, Action Research is about improved practices and problem solving. This highlights a key difference: whilst in Design Science the Artefact is the key vehicle 'administering' the change, in Action Research the existence of an artefact is not required, a fact observed by Henfridsson (2005), who found that "the IT-artefact has a marginal role in Information Systems Action Research" (Henfridsson, 2005).

Whilst this research has yielded physical artefacts, the problem owners actively pushed for "a kind of graphical tool" which they saw as a key driver for change; therefore, the problem owner's view of the research was more artefact oriented than the researcher's. This is exemplified through the following quote, showing how the problem owner was more concerned with the functionality of the artefacts in their ability to create DSPs:

> "At the end of this month, Nacho would like to do some kind of "concept test" of the methodology and the software. I'm preparing a "fake administrative process" to be loaded in ADONIS. The main goal of the test will be to obtain the XML description of the process and a "First Very Easy Signature Policy"."

On the other hand, the researcher was more concerned with developing an overall method that delivers DSPs and the design characteristics of the artefacts (see Section 5.1) support this claim; the researcher posits that the created artefacts can be seen as a meta-method that (with some modifications) can be transferred into different organisational settings where DSP creation is required.

The key question arising then is - does the development and delivery of the artefacts make the research Design Science? Since the researcher was highly focused on creating the improved method for creating DSPs, it could be said that the research's primary aim was the improvement of practice and not artefact design. Therefore, whilst the research approach is compatible with both Action Research and Design Science, the importance on the method of creating an improved DSP creation process by the researcher shows that the researcher conducted Action Research and not Design Science. However, it should be noted that the collaborator had a much greater interest in physical artefacts than the researcher and therefore would amount greater interest in the artefacts than the researcher.

Research Cycles and Development Methods

Chapter three discussed the two research methodologies and referred to some key characteristics, namely the fact that both Action Research and Design Science undertake multiple iterations of 'action' or 'design' cycles. It was also shown how both are interventionist methods that are sustained over a specific period of time and involve an element of collaboration.

A distinctive feature of this research is the double-iteration research loop, which had a double focus - one where the physical artefacts were generated through multiple iterations of Plan-Action-Evaluation, and an 'outer' iteration which focused on the complete method of generating DSPs and caused changes in all physical artefacts. The researcher sees this as a further argument that Action Research was conducted, since the 'inner' iteration loop focused on specific aspects of the intervention, whilst the 'outer' loop focused on the complete cycle from conceptualisation to the resulting artefacts. Thus, it could be said that the researcher collaborated with the problem owners to create the physical artefacts and also collaborated with the problem owners to create the overall method; the 'outer' iteration loop also had effects on the artefacts, which could be considered as evidence that the two research products were aligned with each other in order to deliver a more targeted intervention. What separates this from Design Science is the fact that the research did not stop at artefact creation, therefore the primary output of the research and development cycles were not actually artefacts, even though these artefacts form a *part* of the research output. This crucial difference shows that the research was Action Research and not Design Science.

5.3 Evaluation

The preceding chapters have managed to achieve a number of aims: they outlined the domain within which this research was carried out; they provided background information that narrowed and highlighted the scope for this research; they displayed the researcher's philosophical orientation and showed how the research approach was consistent with those philosophical views; an appropriate methodology was chosen and it was evaluated how the

research adhered to the principles, practices and procedures (Hevner et. al., 2004) of that methodology; finally, the research itself and its outcomes were conducted and demonstrated. The one important view missing from this list is whether the conducted research actually met its original aims and requirements and whether the research output (regardless of adherence to requirements) actually succeeds in achieving its stated aims. Originally, the aim of the research was to develop:

- A methodology enabling individuals to convert natural language legal acts and convert those to process models
- Tools and methods to convert the process models into a codified form
- Produce standards-compliant signature, evidence and archival policies (adhering to ETSI TR 102 038)
- The developed method should allow transformations in a structured and repeatable manner

These were born out of the original state of dissatisfaction with the existing manner of producing standards-complaint DSPs, which was an ad-hoc method that relied on individuals' skill in both understanding the legal text as well as the content of the DSP that had to encapsulate that text's meaning.

In order to be able to assess the success of the research, an evaluation must be carried out. According to Gray (2004), "Evaluation involves the systematic collection of data about the characteristics of a programme, product, policy or service", with the purpose of exploring (amongst other things) "whether there is evidence that change has occurred" (Warr et. al., 1970; paraphrased in Gray, 2004). In other words, evaluation is the process where the impact of research can be measured, including its effectiveness. This is similar to Clarke's (1999) view that "whilst the purpose of basic research is to discover new knowledge, evaluation research studies show how existing knowledge is used to inform and guide practical action" (Clarke, 1999; quoted by Gray, 2004), which essentially means that evaluating current knowledge can inform

and guide future action (e.g. research), which at the same time means that once new knowledge has been discovered and implemented, evaluating that knowledge can lead to further knowledge on whether further action is required or whether the implementation of the new knowledge was successful. This means that Evaluation must be considered as an essential element of research as it informs one of the success and impact of the research.

Within the discipline of IS, Evaluation is an accepted topic that has let to discussions on utilising evaluative techniques within the development process (c.f. Avison et. al., 1995), discussions on evaluating potential IS prior to development (c.f. Willcocks and Lester, 1991), and discussions on the process of evaluation itself (c.f. Hirschheim and Smithson, 1987; Powell, 1992; Symons and Walsham, 1988). According to Ballantine et. al. (2000), evaluation within the IS discipline can have many objectives depending on the interest of the stakeholders performing or requesting the evaluation, a view supported by Symons and Walsham (1988).

At this stage it should be noted that according to Easterby-Smith (1994), there are a various different approaches to evaluation, which are experimental, systems, illuminative and goal-free; Gray (2004) extends this list to include decision making, goal-based, professional review and interventionist (Gray, 2004). In other words, there are a number of different approaches towards conducting evaluations and this puts a potential evaluator (in this case, the authoring researcher) into a position where a choice needs to be made with regards to which approach to follow. In the previous paragraph, it was noted by Symons and Walsham (1988) that the objective (and thus the approach) of an evaluative method is based on the interest of the involved stakeholders. The existence of different schools of evaluation indicates that the choice is more complex, however.

In fact, Ballantine et. al. (2000) state that "a number of factors can be identified which will strongly influence the choice of an evaluation approach" (Walsham, 1993; paraphrased by Ballantine et. al., 2000); those factors are named as

1. Material resources required to conduct the evaluation
2. Ability and interests of the Evaluator
3. Organisation's style of Management
4. Organisation's culture
5. Distribution and exercise of power within the organisation
6. Philosophy underlying the evaluation approach

Adapted from Ballantine et. al. (2000)

Of the above factors, factor number 6 is of importance in this context of choosing the appropriate type of evaluation. Ballantine et. al. (2000) state on this point that the philosophy "has a great influence on how the evaluation is carried out... and the ways in which the goals of the evaluation are arrived at" (Ballantine et. al., 2000); thus, Ballantine et. al. (2000) identify that in order to carry out an effective evaluation, it must be consistent with the epistemological choices of the researcher, similar to how the choice of research methodology is influenced by the epistemological position of the researcher. In other words, the epistemological position determines the pool of possible evaluation techniques in the same manner as it determines the pool of possible research methodologies. Indeed, Ballantine et. al. (2000) identify "technical approaches to evaluation" as "positivist" (ibid.), whilst "moral approaches to evaluation....tend to be human centred" (ibid.), showing the influence of epistemology on the choice of evaluation technique.

Gray (2004) combines the viewpoints of Ballantine et. al. (2000) and Easterby-Smith (1994) to show the appropriateness for particular schools of evaluation under a given epistemological position, shown in a reproduction of a graph originally in Gray (2004):
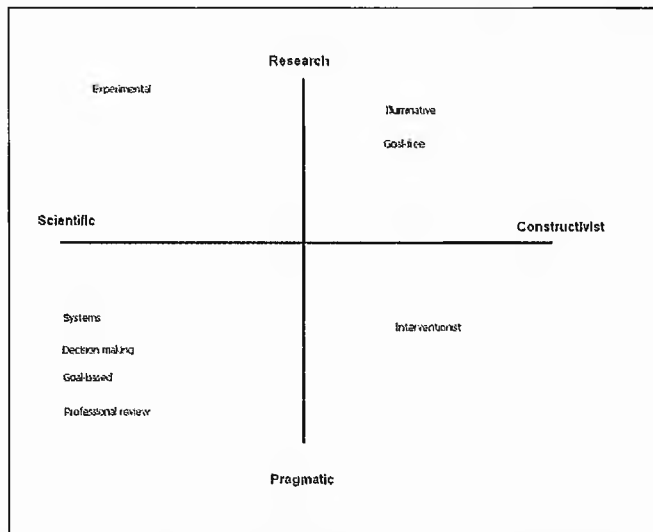
Figure 5-4: Model of schools of thought in evaluation (Reproduced from Gray, 2004).

As can be seen from figure 5-4, the various schools of evaluation have been categorised according to different epistemological positions.

Previous chapters have seen a debate as to whether the research conducted followed the Design Science research methodology or the Action Research methodology. These chapters also identified that the researcher's original epistemological position was Constructivism, whilst Design Science was identified as belonging to the Pragmatist school. Making the assumption that the research conducted followed the Pragmatist-Design Science route, then the acceptable evaluation techniques would be those that are marked by the red circle in figure 5-5:
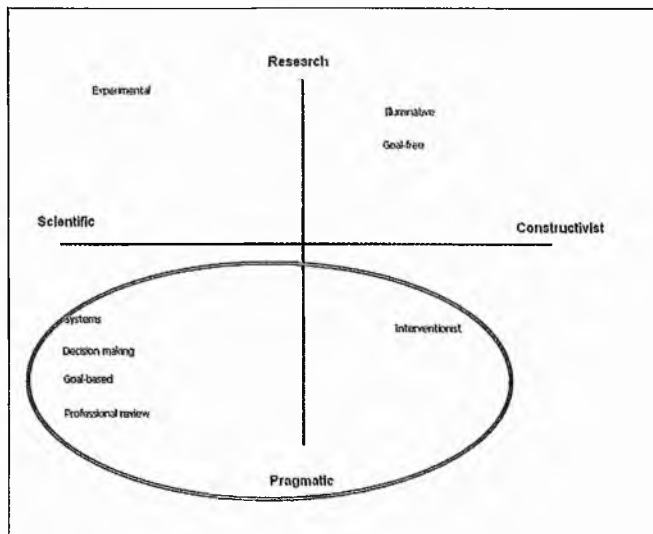
Figure 5-5: Evaluation techniques compatible with the Pragmatic epistemological position

On the other hand, if the assumption is made that the research conducted followed the Constructivist – Action Research route, then the acceptable evaluation techniques are those that are marked by the blue circle in figure 5-6:
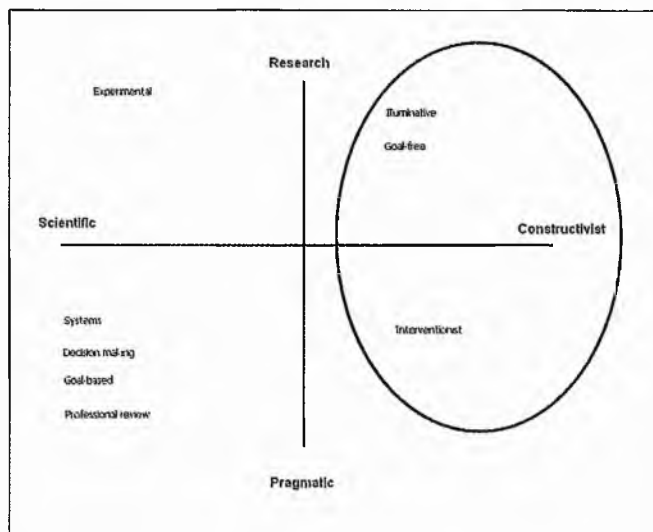

Figure 5-6: Evaluation techniques compatible with the Constructivist epistemological position

Thus, figure 5-5 and figure 5-6 show the range of evaluation techniques available if the assumptions stated on the previous page were true. However, the attentive reader will have noted that in Chapter 5.2.2, it was shown that Action Research and Design Science were two methodologies that were very

similar in their methods, but at odds in their Epistemological orientation, unless one made the assumption that Pragmatism and Constructivism were not mutually exclusive. This assumption was made and evidence from literature was brought forward that identified that Pragmatism and Constructivism could indeed be regarded as similar. Therefore, in order to accept this research as both Design Science and Action Research, one had to accept the stated argument of Pragmatism and Constructivism being similar.

The position developed and chosen in Chapter 5.2.2 has implications on the issue present within this chapter, namely the choice of evaluation technique. Adopting the position that Design Science and Action Research intersect in the same manner that Pragmatism and Constructivism intersect results in figure 5-7, where Pragmatism and Constructivism intersect to yield evaluation techniques in line with both philosophical positions:
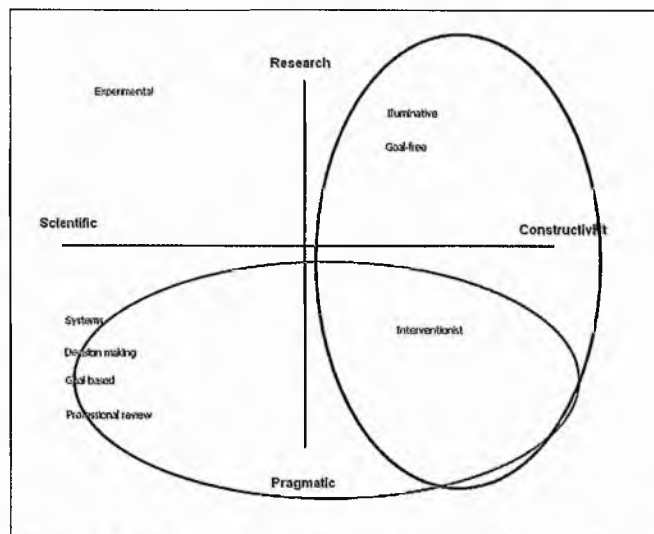

Figure 5-7: Intersection of Pragmatism and Constructivism

As can be seen from figure 5-7, the only evaluation technique available when Pragmatism and Constructivism are considered at the same time is the evaluation technique of 'Interventionist'; this is the necessary choice to remain consistent with the originally chosen epistemological position and

remain consistent with the research methodologies identified in previous chapters.

Interventionist evaluation is, according to Gray (2004), an approach that "has much in common with Action Research" (Gray, 2004; p. 164) because one "set[s] out to solve problems through planning, implementing and evaluating change processes and strategies" (ibid.), the main steps in an Action Research project. Through this close interaction between researcher and problem owner, "a commitment to achieve a direct impact on a programme and those involved in it" (ibid.) develops through the fact that there is a high degree of interaction between the researcher and the subject matter and interaction with the problem owners, or stakeholders. Thus, a solution developed through Action Research will undergo several planning-implementation-evaluation cycles (see Chapter 3.2.2), with each evaluation cycle containing feedback from the stakeholders and the analysis of the implemented intervention (Baskerville, 1999); since the evaluation-step informs the planning-step in an Action Research project (see Chapter 3.2.2), it means that the continued stakeholder input results in the stakeholders having a significant amount of input on the final artefact developed through the Action Research methodology, since it is their input that provides the researcher with the necessary data to be informed of the next planning and implementation steps (McNiff and Whitehead, 2002). Furthermore, McNiff and Whitehead (2002) explicitly state that each evaluation in a planning-implementation-evaluation cycle must evaluate whether there is "evidence of improvement", whether "the solution actually solves the problem" and whether a new plan is "clearly specified" or required (McNiff and Whitehead, 2002; p. 87). Baskerville and Pries-Heje (1999) expand on this point when they describe the evaluation cycle as an activity which must "specify the learning...if a new core category, or story line will emerge from the process" (Baskerville and Pries-Heje, 1999), meaning the evaluation cycle must determine whether new information was gained (i.e. whether learning took place); the evaluation phase must also determine whether the attained state

is satisfactory or not, for "If the results of the action do not reflect a satisfactory outcome, then this adjusted story line becomes the foundation for...a further iteration of the Action Research cycle" (Baskerville and Pries-Heje, 1999), which demonstrates that each evaluation-cycle examines not only whether and what kind of learning has occurred, but also whether a state of satisfaction (the ultimate goal) has been reached when compared to both the departure point (the original state of dissatisfaction) and the goal of the research (a state of satisfaction). This cycle is broken at a stage called 'termination point', when 'saturation' has occurred; in the words of Baskerville and Pries-Heje (1999), "The Action Research cycles reach a termination point when the categories reach saturation...[meaning] the evaluating and learning phases produce little change" (Baskerville and Pries-Heje, 1999), there is a point when the final goal is attained and this is evidenced by the fact that the evaluation yields little to no change in the state of the (in this case) artefact. According to Baskerville and Pries-Heje (1999), reaching 'saturation' is a valid "rationale for concluding the research project" (Baskerville and Pries-Heje, 1999).

To summarise, in an Action Research project, the evaluation of the overall project is not a necessity since the stakeholders have completed this evaluation already through the repeated evaluation steps that is one of the key steps in the Action Research cycle. Therefore, when an Action Research project concludes, it follows that the developed intervention has gained the necessary compliance with the stakeholder needs and views since the last evaluation step has not yielded a further planning step; in other words, it means that the developed intervention has developed into a state that sufficiently caters for the needs of the stakeholders, who continuously evaluated it - a state of saturation also known as the 'termination point', as outlined in the previous paragraph.

The same view can be taken towards this research project, as the 'final' evaluation stage resulted in no more feedback from the problem owners,

other than a literal "good job, well done" from the problem owners, indicating a state of satisfaction for the state of the developed artefacts. Therefore, as the research is conformant to the Action Research cycle, it can be concluded that the evaluation of the project has been conducted successfully as well. The proof is in the existence of the research outputs (the developed artefacts from Chapter 4), the fact that a method has been developed and has been shown to work, and the cessation of further feedback from the evaluating problem owners, which is a line of argumentation taken by many pragmatists when evaluating a pragmatic research project. In pragmatism, "what is true is what works" (Heikkinen et. al., 2001), which means that an artefact's utility can be determined because "'it is useful because it is true' or 'it is true because it is useful'" (Heikkinen et. al., 2001), meaning that from an epistemoiogical point of view, the fact that the developed artefact has ceased to yield any further feedback during the Action Research cycle and has entered 'service' with the problem owners (i.e. the artefacts and the method are now in use), it can therefore be evaluated as being 'true', i.e. artefacts that are appropriate and useful for the purpose they were developed. According to James (1994), "the verification process of an idea is practice and vice versa" (James, 1994; p. 98), which Heikkinen et. al. (2001) interpret as justifying "the quality of an Action Research project is its workableness" (Heikkinen et. al., 2001), i.e. when the output of an Action Research intervention is 'workable', it is then of quality.

There are (at least) two issues with this view; the first issue concerns the epistemological position of this research. It has been stated that this is a pluralist piece of research which adheres to the practices and processes of two research methodologies (Action Research and Design Science) that belong to two different epistemoiogical 'strands' (Constructivism and Pragmatism); it was also shown that, traditionally, these two epistemological strands were considered opposites, or mutually exclusives. This research has established, however, that under specific circumstances the two epistemological positions can be considered to not be dissimilar and this

argument has led to its natural conclusion earlier in this section, namely that an evaluation conducted under the 'combined' Pragmatist-Constructivist paradigm can only be successful if an evaluative method is applied that is applicable and valid for both epistemological positions. Clearly, the argument of utility ("it's good and the truth because it works") is at the core of Pragmatist philosophy and can not be considered appropriate from a Constructivist point of view. This leads to the second problem with taking this position, which is also identified by Heikkinen et. al. (2001), when they correctly identify that pragmatism "presupposes the criteria of usefulness and better practice" (Heikkinen et. al., 2001) and neither identifies "Who dictates the criteria" and "who validates them" (Heikkinen et. al., 2001), aspects that a Constructivist would want to capture.

This means that whilst Action Research can be validated and evaluated under the pragmatic paradigm by capturing its use and utility, it means that such an evaluation is at odds with the constructivist notion of evaluation. Where does this leave the evaluation for this research? On the one hand, it has been demonstrated that the Action Research cycle reached a state of 'saturation', a point at which research is terminated for no further learning or advances can be made, implicitly indicating that the research has reached a successful conclusion. However, at the same time it can not be said that the research has reached a successful conclusion because utilising the developed research output is not a sufficiently valid evaluative statement from a constructivist point of view (albeit it is from a pragmatist view).

On this unsettling and inconclusive state, List (2006) mentions in his conclusion of an Action Research project in the Futures discipline that whilst "it would be pleasant to be able to produce some concrete evidence that [the Action Research intervention]...was effective...other participative methods of social enquiry" (List, 2006) face the same problem: "it is simply not possible to 'prove', using the hypothetico-deductive paradigm, that a method is in some way effective" (List, 2006). In other words, the termination of Action

Research cycles due to saturation can not be considered successful evidence in determining the effectiveness of the intervention, when not considering any other evidence. What List is attempting to say is that success can not be deduced, it means that evidence for success needs to be gathered.

The impact for this research is as follows - as the research falls under a combined constructivist-pragmatist paradigm, only one evaluative technique is possible, the one of Interventionist (see beginning of this chapter). It has already been demonstrated how the Action Research cycle had reached saturation. Therefore, one can choose to ignore List and *deduce* it was a successful intervention, or one can conduct yet another Evaluation-step under the auspices of needing to analyse the "good job, well done" feedback - in other words, the problem owner's statement is evaluated ("Are you sure it's a good job?") and this is epistemological and methodological consistent because it represents a more detailed evaluation-step in the Action Research cycle; however, the researcher has already hinted on the fact that post-final iteration, the collaboration was ended abruptly without much in the way of evaluation, collaborative reflection or any kind of useful feedback other than "good job". The researcher attempted several times to elicit further information from both the collaborators and from potential users, but no response at all was received. This, then, created a dilemma for the researcher, for reaching the 'termination point' does not carry enough significance to show whether the research was successful. Other hints that the researcher received, such as the "good job, well done" comment and the fact that the problem owners had been seen to modify the research outputs may point towards adoption by the organisation and could be argued to constitute, at least at the surface, successful conclusion and a stage where the problem owner had learned sufficiently to be able to carry on the research internally by demonstrating actionable learning - one of the key outputs of Action Research, according to Baskerville (1999). But without a more formal way of eliciting the collaborators' and future users' views, this assessment will always remain in the realm of speculation.

The researcher did find some evidence in literature that the above assessment could be sufficient; for example, Gray (2009) mentions that Action Research "Validation can be quite an informal process" (Gray, 2009; p. 328) and goes as far as suggesting that some researchers may even take the stance that validation is neither "a necessary or feasible objective" (ibid.) in Action Research. However, the researcher is of the view that there needs to be some kind of further evidence that points towards the efficacy and applicability of the intervention. Gray (2009) paraphrases McNiff (1988) when saying that McNiff "suggests that the researcher needs to demonstrate publicly that he or she has followed a system of disciplined inquiry" (Gray, 2009; p. 328, paraphrasing from McNiff, 1988). The researcher agrees with this view, for the ability to demonstrate that the research was conducted in strict accordance with the methodological rules of Action Research can point towards success of the intervention; whilst this is not a fool-proof method of demonstrating that the intervention was a success, it can at least provide an estimate that the research had a chance of succeeding, because a research methodology which mostly leads to negative results is unlikely to be considered a useful methodology and is likely to be superseded with a more effective methodology that does yield positive results. Apart from the need to show the success of the intervention, it is also pertinent to show that the research was rigorous, as this is an important component in demonstrating the quality of qualitative research (Gray, 2009; pp. 189 ff.). Therefore, demonstrating whether (and how well) the research was conducted according to methodological requirements will present a good indication about the rigour of the conducted research.

Therefore, in order to demonstrate that the conducted research did not only constitute Action Research, but constituted *rigorous* and canonical Action Research, the researcher shall evaluate the research against what could be called Action Research quality criteria, developed by McNiff and Whitehead (2009) and called "the seven I's" (McNiff and Whitehead, 2009; p. 32 ff.).

They posit that these seven I's are actually seven different levels of reflection that an Action Research project must undergo in order to effectively communicate what actions a researcher took, why they were taken, what effect they had, what the meaning of the effect was and other such views, which in combination provide a full account of the intervention and demonstrate the reasoning, reflection and understanding of the intervention and its effects. The following table shall therefore show that these seven I's were met by the research.

Stage of Reflection	Type of Reflection	Evidence of achievement
Actor-Agent	Descriptive account, e.g. "X did this, and Y did that"	Chapter 3.3 - Research Design
Explanatory	Explanation for why certain actions were taken	Partially in Chapter 4 - Results, and Chapter 5.1 - Artefact Evaluation
Researcher	Reflection on quality of actions and quality of explanations	Most of Chapter 5 - Analysis and Discussion
Scholarly	Literature Review and claims validated against literature	Chapter 2 - Literature Review
Critically Reflexive	Reflection on biases and influences on the researcher	Chapter 6.3 - Research Limitations and Challenges
Dialectically Critical	Research limitations and influences	Chapter 6.3 - Research Limitations and Challenges
Meta-Reflexive	Analysis of the significance of the entire action-reflection process; how did this contribute to learning?	Chapter 6.1 - Contribution to Knowledge

Table 5-2: Action Research Reflection Stages (adapted from: McNiff and Whitehead (2009), pp. 33-34)

As can be seen from table 5-2, the research presented has undergone through all seven stages of reflection that McNiff and Whitehead (2009) posit forms part of well-formed and well-disciplined Action Research. The researcher posits that the fact that an artefact was changed after the final

research iteration loop, the fact that a "good job, well done"-type feedback was received, and the fact that the above table shows that the research adhered to Action Research quality guidelines all form sufficient strength to conclude with the assessment that the conducted research was well-formed Action Research that resulted in the implementation of an improved practice (of creating DSPs) and the creation of a number of technical artefacts.

This is not the only method through which rigour of qualitative design can be assessed; Gray (2009) mentions other methods, such as Skrtic (1985) who suggests rigour can be assessed through addressing issues of Transferability, Dependability, Confirmability and Credibility (Skrtic, 1985; quoted by Gray, 2009, p. 194).

In order to satisfactorily show that the research is rigorous, the following table shall highlight how each of the above criteria were successfully implemented in this study. The table itself is taken from Gray (2009), which in turn was adapted from Hoepfl (1997) and Lincoln and Guba (1994):

Rigorousness Criteria	Description of Criteria	Evidence of how it was achieved
Credibility	Examining the study design and methods used to derive findings	Chapter 5.2 and 5.3 Table 5-2
Transferability	Exploring the degree to which findings are context bound, so assessed by examining the characteristics of sample	Chapter 6.2
Dependability	Evaluating reliability of study's conclusion	Chapter 5.3; Chapter 6.3
Confirmability	Addressing the degree to which the steps of the study can be audited, confirmed or replicated	Appendices; Chapter 4; Chapter 5

Table 5-3: Criteria for Rigorous Qualitative Research (adapted from: Gray (2009), pp. 194)

As Table 5-3 shows, the criteria for rigorousness have been demonstrated to have been met, therefore it can be said that the research was rigorous. One final note on rigorousness is mentioned by Johnson and Harris (2002), who state that there is no standard practice for achieving rigorousness in qualitative research due to its variable nature and the fact that many research methodologies are relatively new (Johnson and Harris, 2002; quoted in Gray (2009), p. 195); Baskerville (1999) made a similar observation about Action Research when he observed a "lack of agreed evaluation criteria" (Baskerville, 1999).

5.4 Concluding the Analysis

As the above sections have shown, the question of whether this research is Design Science or Action Research has been resolved satisfactorily. It was interesting to note that collaborators and researcher had a seemingly differing epistemological footing, yet were able to work together successfully to deliver results. This may be down to Constructivism and Pragmatism sharing common features.

Another interesting aspect of the Analysis is that it was shown that Evaluation is an activity that is not essentially the formal activity that Design Science prescribes, but can be informal through the fact that the Action Research cycle *evaluates* achieved results, even if these are intermediate. It was shown, both from literature and from actual comments of the problem owners, that the success of the intervention could be shown through the fact that the produced artefacts were working as per expectation and through the fact that feedback ceased and that there were indications that the problem owners had started researching the topic further without the researcher's involvement. Whilst quite a pragmatic approach, other evidence (e.g. the exhibition of learning being turned into actionable knowledge through the modified XML file being sent from the problem owner for evaluation by the researcher; or the adherence to all of Action Research's quality criteria) points

towards the fact that the research was in line with methodological requirements and achieved its aim of developing a better method for creating DSPs.

Finally, known criteria for rigorousness were applied to the research in order to show that the research was not only methodologically consistent, but rigorous in relation to criteria of rigour for qualitative research. Baskerville's observation that there is a "lack of agreed evaluation criteria" (Baskerville, 1999) for Action Research was thus taken into account and responded to by applying various levels of evaluation and self-reflection that other researchers deem sufficient for evaluation of Qualitative and Action Research, thus demonstrating sufficient evaluation of the conducted research.

6 Conclusions and Further Research

This chapter shall summarise the work conducted into finding an answer to the research question and highlight how this research has contributed to knowledge, outline potential future research and conclude with a number of shortcomings that the researcher considers to be exhibited by the described research.

6.1 Contribution to Knowledge

The previous chapters have introduced a large amount of information, analysis, results and interpretations, all of which contribute in some manner to greater understanding of the Digital Signature domain within the wider discipline of IS. This chapter shall summarise and conclude the understanding gained and put it within the wider context set by the Introduction.

The previous chapters, in their combination, have managed to provide a number of strong statements and insights into a number of areas. In other words, they contributed to understanding and knowledge in a variety of ways. There are a number of key contributions, especially those that are technical and methodological. The technical contribution lies in the development of a method that allows the production of DSPs in a precise and repeatable manner which does not require domain-specific knowledge by potential users. The research produced a number of artefacts that are tools aimed to assist users in adopting and applying the developed method. As far as the researcher can ascertain, this formal approach to DSPs is the only known process with such a high degree of formalisation. The developed method, alongside the developed tools, can be considered as results that can be generalised; for example, the artefacts were developed in such a way that applying them in a different organisation using different tools should be possible with some modifications. Most process modelling tools allow the modification of the underlying metamodel and even the graphical elements, so 'transplanting' the developed process modelling notation into a different

tool should be a possibility. Furthermore, the developed data mapping between the questionnaire, the modelling notation and the transformation tool can be used to re-develop a transformation tool that can transform a different tool's XML into ETSI TR 102 038 compliant DSPs. As for the method, since the developed tools are one possible way of implementing it in an organisation and not the 'key constituents' of the method (i.e. the method of transforming the data is not dependent on the process modelling notation being implemented in Adonis, for example) it means that the method can also be applied in a different organisational setting; therefore, the contribution here could be thought of as a *meta*-method which in spite of being developed out of an individual organisation's research problem could be applied in different organisations.

The methodological contribution lies in the contribution to the current debate of Action Research vs. Design Science and how it was shown that research conducted strictly in accordance with Action Research methods could, superficially, be regarded as Design Science research. Epistemologically, it was shown that the two approaches are quite similar (as ought to be expected for two interventionist research methodologies) and that the importance of the artefact separates Design Science from Action Research. Therefore, future debate in this area can use this research as evidence of the similarities and differences between Action Research and Design Science and use the conclusions made here to take the debate forward.

There are a range of other contributions, albeit with a smaller impact factor than the ones above. This research has managed to highlight that there is precious little writing on the topic of DSPs and, presumably, little take-up of this technology as well. Raising awareness of this technology through this research may change the ubiquity and up-take of this technology.

Whilst investigating Digital Signatures, it came to the researcher's attention that the underlying technology of Digital Signatures is under threat by the

development of various methods aimed at defeating Digital Signatures' advantages. As Chapter 2.1.3 has shown, various methods have now been developed that allow an attacker to change a document or Digital Certificate and pass it off as valid to a validating entity. The ramifications are quite severe, in that if Digital Signatures can not be proven to be able to withstand such attacks, then it must be concluded that they are of little use. Whilst remedial work is underway in order to eliminate the inherent weakness shared by the various techniques employed in Digital Signature creation, the researcher is afraid that should these efforts fail, then Digital Signatures (and by extension, DSPs) are doomed to failure. Therefore, the researcher reported of this work in order to raise awareness of the threat against Digital Signatures, in the hope that this might encourage further efforts to safeguard the technology.

McNiff and Whitehead (2009) posit that good Action Research induces learning in its participants, a view originally laid out by Rapaport (1970) who developed the so-called Operational Research view of Action Research, a combination of Action Research and Action Learning (Revans, 1983) which brings together technical approaches and organisational methods in order to solve organisational problems through shared learning. Revans (1983) suggests that a key aspect of this learning is that communities, within and beyond the research, learn from interventions. This means that under the Operational Research view of Action Research, the key objective of Action Research is to produce learning in not only the research participants, but interested communities outside the research as well.

Within this research, then, it can be argued that the key learning was the researcher's learning on how to develop the necessary tools and workflows in order to produce DSPs, whilst the problem owners have learned on how to produce DSPs from natural language text in a more efficient and robust manner. Specific examples of this kind of learning are, for example, discussions that took place on definitions of data fields and the type of legal

information that had to be entered into those fields, as well as the format this data had to be in. These discussions led to the problem owner learning of the value of establishing and agreeing definitions and led to the publication of a schema that formalised these definitions. Thus, the problem owner moved from learning into actionable knowledge. Further evidence of this occurring is the fact that during the Artefact Analysis phase, the problem owners produced an XML file of a legal procedure through their copy of Adonis and requested the researcher to test whether the DSP created would match the legal requirements. To the researcher's surprise, the XML file produced differed significantly from those that the researcher had produced throughout. Following up on the differences, it was revealed to the researcher that the problem owners had started conducting their own internal investigations into the developed artefacts and had started introducing modifications, even as the development of the method and the Transformation Tool were coming to a close. This shows that the problem owners were indeed 'consuming' the shared learning into actionable knowledge and it shows that the research contributed significantly to the problem owners' learning and knowledge.

6.2 Further Research/Recommendations

The research work conducted herein has pushed the envelopes of knowledge in a number of areas, but as any kind of research limited by time and other resources, only so much 'envelope pushing' occurred, meaning that there is further scope for more research in this area. Nevertheless, a number of areas will be highlighted where other, future research could be undertaken for ever increasing understanding.

In Chapter 2.1.4 it was identified how there was great difficulty in obtaining literature on DSPs and in identifying other users of the standards documentation identified for this work. This could serve as a starting point for a domain survey to investigate the ubiquity of DSPs in the form discussed within this research and to investigate reasons for the (presumably) limited

use of this technology. The research work carried out could be used as a tool to educate the domain about the existence and use of this technology, assuming that current take up is low to non-existent. This would allow a researcher to understand reasons for why this technology has not become widely available, or whether it is available but under different names or guises. This kind of exploratory research could serve as the kind of market survey that could inform future suppliers on whether there is a market for a product applying the technology discussed within this document. Similarly, should such a study reveal that the uptake of this technology is actually a lot higher than the researcher was able to establish, then research focus could be placed on identifying why the researcher was not able to establish such wide use, and it could also focus on the practices, applications and methods employed in the marketplace and compare these with the developed method and practices of this study. This would highlight aspects of this particular domain and would show whether the researcher's approach was in line with industry's.

In the next chapter on the limitations of the research, it is going to be mentioned that the research was conducted following strict epistemoiogicai consistency within the paradigm of constructivism. As a result, this research lacks any kind of positivistic investigation and this could therefore be an area that a positivist researcher could exploit in the future, to gain further understanding of the subject by applying quantitative research and evaluation methods on both the technology itself and the developed method as it had been applied to the organisation, in order to gain an understanding on the subject, the success of the intervention and identify shortcomings from a positivistic viewpoint. The value of such research would lie in the fact that the same subject would have been investigated from two opposing epistemological positions, thus yielding a point of view that is more holistic than a purely constructivist or positivistic point of view could hope to achieve. This could then either strengthen or refute the conclusions and results drawn from this study, and yield further possibilities for further study of the subject

in question. An example of such a possible future positivistic study is Sunro and O'Keefe (1996), who investigated speed and accuracy improvements in knowledge-base maintenance. It is interesting to note that there are several authors that suggest combining qualitative and quantitative research methods may be beneficial and indeed desirable in a number of social settings; e.g. Flick (2006), Wilson (1982) and Baum (1995) all promote the view of quantitative and qualitative research methodologies being complementary, rather than competitive research methodologies (Flick, 2006; p. 41).

Part of this further investigation should also focus on the developed method's application in practice, in order to obtain real-world performance data and allow for measuring the performance and effectiveness of the developed method, as well as the acceptance by the users and any potential unforeseen problems. The real-world application of the method in practice ought to be studied using a variety of epistemologies and research methods in order to account for a more holistic view and understanding of the method, similar to the stated example of Sunro and O'Keefe (1996).

In Chapter 3.4 it was shown how this research can be considered as either Action Research, Design Science research, or both. Further research could focus on the current debate on Action Research vs. Design Science and ascertain the impact of this research on the debate, particularly from the point of view of Epistemological consistency and the impact on evaluation in such a pluralist approach, in order to take further the results the researcher captured in Chapter 5.2.1. Järvinen (2005) is a known proponent of the view that Action Research and Design Science are similar research methodologies, whilst Baskerville (2008) has posited that Design Science is neither a methodology nor equivalent to Action Research. This view is somewhat contrary to, for example, Peffers et. al. (2008) who identify Design Science as a research methodology and the researcher has contributed to this debate by stating that the difference between Action Research and Design Science

mainly lies in the importance of the artefact. These conclusions can be utilised for further, future debates on this topic.

On a more technical issue, the current method utilises a graphical process modelling notation in order to capture and organise legal data obtained from textual sources (see Chapter 4). It was demonstrated how a metamodel was developed that captures the breakdown and organisation of the data, whilst a table captured the data fields in their various formats (questionnaire, notation, ETSI Signature policy). However, no provisions were made either in the metamodel or in the transformation rules about exploiting the potential of 'sub-processes' (Seltsikas and Palkovits, 2006). In process modelling, sub-processes are utilised to hide layers of increasing complexity behind an individual symbol in order to keep a particular layer of functionality relatively simple without complicating it with more detailed functionality. An example could be an e-business model which is (at a high level) made up of three activities called 'Find object', 'purchase object' and 'receive object'. Clearly, finding, purchasing and receiving can be quite complicated mechanisms in an e-business, and the more detailed procedures (e.g. retrieve stock level details, process credit card, book delivery options) can be 'hidden' away behind the more high-level activities of find, purchase and receive (Dennis and Wixom, 2000). The developed notation, whilst it contains facilities for representing sub-processes, does not contain rules and linkage mechanisms to allow a user to create multiple DSPs, or policies from a sub-process because these were not thought relevant by the collaborators other than for organising the diagrams. Rather, the method is very sequential, in that a user needs to select a particular diagram and then needs to select the activity for which a policy should be created. What is missing is the ability to produce DSPs in bulk, including policies that may be 'hidden' away in a sub-process. Future researchers might want to investigate whether users would welcome such a facility and whether such a facility would provide meaningful benefit.

Another more technical aspect of future research is to consider testing the developed methods and tools in a more 'natural' environment, i.e. to test the results using real legislation. Preferably, this testing could be performed on legislation that has already had DSPs created for it using the previous manual approach, so that the results of this research can be assessed whether they can match or improve the results of the manual process. Further research could also widen the scope and investigate whether DSPs, created using the developed methods and tools, can be integrated and used by a wider computer system, such as Catalonia's new eGovernment infrastructure. Interestingly, this suggests that the future research ought to move away from Action Research and move to more formal field-testing, which is a natural step for attempts to generalise developed technological solutions.

Finally, future research should focus on investigating whether it is possible to utilise DSPs for purposes other than those captured within this research. Hernandez-Ardieta et. al. (2008) have already shown that it is possible to use DSPs as a token in a network exchange protocol.

DSPs are used to provide context to a particular Digital Signature by informing a validator of the purpose the Digital Signature is being utilised for and whether the signer has the authority to utilise a signature for the stated purpose. It also informs the validator of the legal situation and whether such utilisation is within the word and spirit of the law; in other words. The signer does have the authority to utilise a Digital Signature for the stated purpose, but is this a lawful application when examining it from a wider, legal perspective and examining the more minute details of the use of Signature and the purpose? The researcher suggests that the function of the DSP (i.e. to provide wider context to a particular statement) can have application in other areas. An area the researcher would encourage to research is the area of Identity Management. In many current applications, Identity Management is primarily concerned with establishing a person's "what you know" through the use of username/password questions (Clauss & Koehntopp, 2001). With

regards to establishing the permissions of what a person may do, however, many current applications revert back to the use of "Roles" and attempt to customise a person's content according to their particular role. Using an equivalent concept of a DSP, however, would provide an application owner with a far stronger and more versatile tool than a Role, since a Role is normally implemented as a single word that may encapsulate many different combinations for access to various parts of an application; an equivalent to a DSP could utilise the various fields related to legal context, legal meaning, legal provisions and similar to establish a highly customised access profile for an individual that ensures an individual is allowed to use a system in a prescribed manner, similar to the way that Clauss & Koehntopp (2001) envisage an Identity Management system to be comprised of rule-bases that determine access controls, privacy and other aspects of Identity Management issues (Clauss & Koehntopp, 2001). In other words, DSPs could be a possible technology for satisfying Clauss & Koehntopp's (2001) requirements for a multilateral Identity Management system. Whether such an application offers any advantage and/or improvements over the current use of Roles would be one of the key aspects of this potential research. Such an application would be closer to Hernandez-Ardieta et. al. (2008)'s suggested use as a token in a network exchange protocol, since in both cases the Signature Policy is carrying non-signature related information that informs a consumer of this information about procedural matters of the transaction that the consumer is engaged in.

6.3 Research Limitations and Challenges

As stated in the "Evaluation" chapter above (i.e. Chapter 5), the study was conducted in strict adherence to the Epistemological position of Constructivism and therefore the choice of research methodology, data collection and evaluation techniques were all restricted by this choice. The consequence is that insights that could be gained from a different epistemological position (such as Positivism) are therefore not captured by this study. A positivist researcher might find plenty of elements within the

study that could not be captured by a constructivist researcher who wishes to remain consistent in his research approach. For example, a positivist researcher might be interested to find out whether the actual time taken to complete the process of creating a DSP has been shortened using the new method, or whether the accuracy of created DSPs has been affected (and if yes, to what extent). An example for such a quantitative study is Sunro and O'Keefe (1996), who investigated speed and accuracy improvements in different methods for maintaining knowledge bases in expert systems; the relevance here is that the developed method for creating DSPs should have a similar impact on such variables (i.e. speed of creating a DSP, legal accuracy of created policy). Another similar study is Gibson and Senn (1989), who conducted a combined quantitative and qualitative study of software maintenance performance in complex systems.

Another limitation is that the instantiations developed to create DSPs have not undergone the required technological maturity expected of commercial products. For example, the Transformation Tool does not have any help functions associated with it, it doesn't allow the user to specify where they would like the created DSP to be placed and it does not perform input checks. Therefore, deploying the solution as it was developed within this research effort will require a little bit of investment into the technology to make it more robust and compliant with any regulatory requirements that may exist on software quality. However, the researcher does not consider this shortfall to have any kind of impact on the meaning and strength of the results reported in this study, as these are cosmetic and not functional issues.

A further limitation was the limited access granted to the organisation and non-organisational stakeholders by the problem owner. At the onset of the research, it had been explained to the researcher that DSPs would play a role in Catalonia's Digital Signature Validation infrastructure. At the time of research, this infrastructure was still in the design phase and the envisaged concept can be approximated through the figure below.
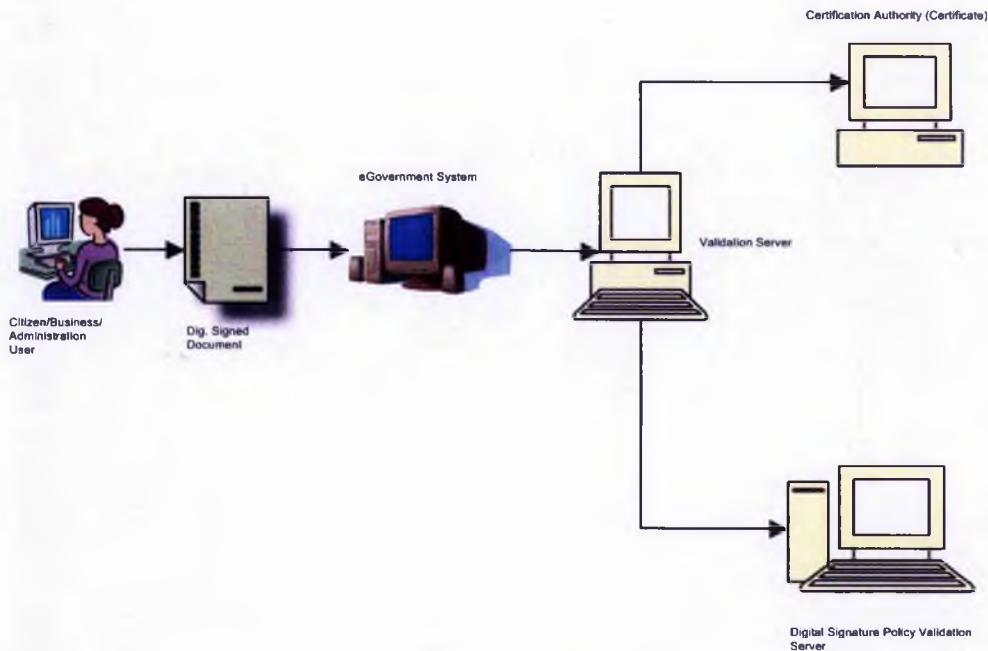
Figure 6-1: The future Catalan eGovernment System Infrastructure (Concept)

Please note that due to the sensitivity of the Information System as the future validation service for all eGovernment systems of the Catalan government, the above figure is highly conceptualised and abstract in order to protect the actual system topology and ensure the security and confidentiality of the system.

Figure 6-1 describes a conceptual application of DSPs. The figure shows how a User (who could be any one of Citizen, Business or Administration) submits a digitally signed document to an eGovernment application in support of a particular process or service. The eGovernment application utilises a validation service (whether it is an integrated part of the eGovernment application or a separate physical entity is not relevant; the importance lies in that validation must take place) to validate the digital signature by verifying the validity of the used Digital Certificate against an approved Certification Authority and verifies the Digital Signature against a particular DSP that is

invoked by the process/service that the documents are for. The research work conducted herein produces DSPs for the DSP validation service (at the bottom right of the above figure) that allows the service to verify whether submitted signatures have sufficient remit for their purpose.

This results in the following stakeholder groups having an interest in this work - firstly, the workers within CATCert that would produce the DSPs in the first instance; secondly, the owners of the Validation service; thirdly, the owners of the eGovernment service. However, as the previous chapters have shown, the researcher's interactions were mainly with the Head of Research and the Technical Lead at CATCert only; despite repeated lobbying by the researcher to gain access to the other stakeholder groups (i.e. the workers within CATCert who would use this technology, the validation service owners and the eGovernment service owners), this permission was denied and therefore their input could not be gained. The researcher referred to literature when warning that the introduction of this new Information System would have significant organisational impact through the change in processes, procedures and power relationships within the organisation and that such change "breeds resistance and opposition" if the organisational aspects are not considered (Laudon and Laudon, 2004; pp. 426-427). The fact that stakeholders from outside of the organisation were not considered either would only exacerbate the issue, but the researcher's pleas were ignored and it was stated that this system would be implemented regardless of people's attitudes towards it. The researcher's efforts to consider other relevant stakeholders in the Action Research cycle were therefore in vain and the researcher has doubts whether the Information System will be readily accepted by the stakeholders within and outside of CATCert without significant effort by the collaborators.

An interrelated problem was the ability to gain detailed feedback for each iteration of the research cycle, where the researcher had to expend significant effort in order to receive the kind of feedback that would be sufficient to advance to the next iteration cycle. The delays were attributed to the

Technical Lead having other responsibilities and expending some effort to discuss internally the received material (thus somewhat alleviating the issues in the paragraph above about stakeholder disregard, at least within the CATCert organisation); the researcher suggested conducting this internal consultation himself, but as mentioned above this was refused. The researcher felt that some of the feedback had been returned merely because of the researcher's continuous urging and not because the collaborators were ready, without the returned material having been assessed whether it actually provided the answer the researcher was seeking. Therefore, the researcher had to expend time and effort to obtain more feedback and information. Interestingly, a similar issue was encountered in face-to-face meetings (e.g. for presentations on progress updates), where the feedback would be limited to "good job, well done" and the researcher would be left to having to probe such answers further in order to obtain feedback that would be more enlightening. This was met with limited success and therefore, despite the seemingly successful evaluation, the researcher feels that another research iteration cycle could have been conducted to increase the quality of the end result further, as the researcher is unwilling to accept that the conducted research was as successful as the comments from the problem owner would suggest. Since Action Research is so dependent on collaborator feedback, the aforementioned reluctance to provide feedback at times was a real hindrance, which was confounded through other actions – for example, the problem owner delayed the start of the collaboration because the collaborators in question had lost contractual paperwork and legally they were not entitled to engage in the research collaboration without the paperwork being in place. This led to a delay of four weeks, in which the researcher had no assistance. Through the middle of the research, the collaboration seized for a period of six weeks when one of the key collaborators that the researcher was engaging with suddenly went off work with illness. The researcher was not notified of this and the prolonged period of non-responsiveness caused a great deal of anxiety and concern as the collaborators' help was required. In other words, there was a degree of unreliability with the collaborators'

responses and promptness of response, which the researcher feels impacted the research by restricting the opportunity to undertaking another Action Research iteration cycle in order to gain further confidence in the "good job, well done" comment. This is of concern as Action Research requires access to the organisation for the collaboration between researcher and client organisation to function effectively.

Further challenges were encountered through the choice of Action Research as the research methodology and the approach required to document the research. A significant challenge arose through the fact that Action Research is an iterative and cyclical methodology that undergoes several cycles of analysis, research intervention, evaluation and reflection. This is in contrast to more traditional approaches to research where the research typically follows just one such iteration. This distinction causes a challenge because in the traditional approach, one describes the research in a linear fashion that describes analysis, intervention, evaluation and reflection one after another; furthermore, the connections between these distinct phases of research are clear and can easily be highlighted. The cyclical nature of Action Research, however, does not permit this kind of approach. If a researcher chose to document each iterative cycle in the same detail as one would write up traditional research, the resulting volumes of information would become unmanageable. This causes dilemmas for authors writing up Action Research, because a trade-off must be achieved between adequately describing the overall research (i.e. what the combination of the various iterative research cycles achieved) but also some details on each individual iterative cycle.

From a presentation point of view, it then becomes difficult to find a good way of describing these two 'layers' of results. Does one choose a descriptive or a reflective account? How much data (and what kind of data) should be presented for each iterative cycle? How does one ensure to not lose the reader when switching from iterative cycle to iterative cycle, or from iterative cycle to the overall research? All these are challenges that have formed the

presentation of the research within this document. The researcher made the choice to concentrate more on discussing the overall research outcomes, and chose to reduce explanations and descriptions of the individual iterative cycles to a few paragraphs that describe how the 'intermediate' results were arrived at, using captured data from the intervention. This undoubtedly raises issues of its own, such as that some researchers reading this report may wish to focus on more detailed aspects of a minor iteration as opposed to the wider research outcomes. The researcher feels that McNiff and Whitehead's (2009) guidelines on presenting Action Research as a story of seven types of reflective account can help future researchers in structuring the various levels of analysis and reflection, but it does not provide an accurate methodology one can follow to structure a research report in a generic manner. Therefore, any Action Research report can be expected to contain highly individual characteristics and it makes it difficult for authors to follow a formulaic structure, especially when asked to do so by supervisors that may not be familiar with this method. However, whilst the structure may not be formulaic, the content may certainly be so – there are known guidelines on how to conduct rigorous qualitative research in a manner that satisfactorily resolves questions of validity, reliability, confirmability and credibility (Gray, 2009). Also, McNiff and Whitehead (2009) provide guidelines on what type of descriptions and reflections should be in an Action Research report, so there are guidelines on content if not on structure.

Another limitation identified by the author was caused by the data definition of the ETSI TR 102 038 standard. As shown in Appendix C, the DSP standard provides two data fields, "Field of Application" (the domain of its validity) and "Semantics" (the legal issues governing the use of a DSP); these fields are both defined as <xsd:String>, meaning that they are effectively a text box with arbitrary content. The author considers this a drawback, since DSPs are supposed to inform an Information System of legal information. In order to inform an Information System, the data must be computable; having string-fields in the policy, however, means that computation of the content in that

field is only possible if a strictly controlled data vocabulary is used. Allowing users to input any type of text would render the Signature Policy useless, therefore there must either be an initiative by an implementing party to define and structure a controlled vocabulary in order to ensure that DSPs can be processed, or a standards body like ETSI must develop an international standard on acceptable content for these fields, similar to how Signed and Unsigned Properties were agreed and can be referenced using a URI or similar method. This would ensure that these fields remain accessible to an Information System and thus an implementing party would encounter fewer complications when validating the content of these fields.

Whilst the above paragraphs show the external influences and limitations placed on the research, they do not show the internal influences and limitations on the research, i.e. limitations caused by the choice of the research design and the researcher's limitations placed on the research by his actions. Since Action Research is a research methodology that sees the researcher in close collaboration with collaborators that typically either suffer from a research gap themselves, or are tasked by their parent organisation of resolving a particular research gap, it follows that the researcher and the collaborators influence each other through choice of tools, methods and exchange of ideas. Whilst Action Research postulates that it is these exchanges that progress the research, these exchanges also threaten the researcher's neutrality with regards to the research being conducted. Particularly in this research, the researcher is aware of his own views influencing those of his collaborators with regards to the quality of the produced artefacts in an unconscious manner. Whilst the researcher undertook measures to ensure formal and written communications were free of judgmental comments on the quality of the output, the researcher can not say with full confidence that the same occurred in personal meetings or over the phone. The researcher is aware that, on occasion, the research artefacts may have been unconsciously lauded by the researcher and that these signals of laudation may have influenced the collaborators' view of the quality of the

artefacts. This could be called 'neutrality bias' and is frequently mentioned as a common criticism of Action Research as a whole (e.g. Gray, 2009; p. 314). However, the researcher considers the risk of neutrality bias having influenced the results as only minor, since the iterative nature of Action Research meant that the research underwent further adjustments following such meetings and that the ultimate goal (i.e. ETSI compliant DSPs) was a fixed entity that could not be changed; in other words, the artefacts *had* to produce a final output that was ETSI compliant and therefore neutrality bias could not have affected the research to an extent as to affect the final output.

One of the positivistic criticisms of Constructivism is that the notion of truth is not deterministic, but rather blurred and dependent on the subject's view of the world (e.g. Denzin and Lincoln, 2008) and therefore results gained through Constructivist, qualitative methods can not be generalised. In the context of the research results, therefore, this means that a positivistic interpretation of the results would conclude that the identified method of creating DSPs is the valid method to be used and that it should be applicable in other organisational settings and that the research should be able to provide empirical evidence of this being the case. However, as Constructivism supports the notion that "truth and meaning as constructed interpreted by individuals" (Gray, 2009; p. 201), it follows that the research results do not represent one method for an arbitrary number of organisations. The results must be interpreted with the Constructive paradigm in mind, which means that the method for creating DSPs is the one method that is appropriate to the studied organisation. The importance of the procedural aspect of Catalan law, the desire to utilise a process modelling notation and the stated objective of arriving at ETSI TR 102 038 DSPs are all specific to the organisation in question. Whilst the researcher has identified elements of the method that could be transplanted into other organisations, these organisations must still share certain attributes with this one; for example, the process modelling notation is dependent on other legal frameworks adopting a similar, process-oriented form. The data mapping table depends on the ETSI TR 102 038 DSP

standard being adopted. An organisation that operates in a legislative environment that can not be represented procedurally would struggle with adopting the modelling notation; similarly, an organisation may choose to adopt the ETSI TR 102 272 standard for representing DSPs, in which case much of the technical work would need to be re-done, though the existence of translators between XML and ASN.1 may help avoid extensive re-work (Imamura and Maruyama, 2001). Therefore, under the Constructivist paradigm it can be said that this method of creating DSPs is the one method that is appropriate for the organisation in question, due to the circumstances that have presented themselves through the course of the investigation. Whilst the results could be applied (with some adapting) to organisations operating with similar constraints, they can not be applied to organisations that operate under completely different constraints. Therefore, the research complies with its Constructivist notion and positivistic quests for generalisation are actually satisfied in identifying that the research can be applied in organisations that share a similar view of the 'truth', but that this truth is not shared by all organisations.

According to Cheek (2008), research can be funded in two different ways: either a researcher can be provided with a budget which the researcher has to expend in order to complete the research, or support to research can be offered 'in kind', meaning that instead of money the researcher is provided with assistance, e.g. access to laboratory equipment, or access to experts (Cheek, 2008). Cheek (2008) posits that this kind of arrangement is "not a neutral, value-free process" (Cheek, 2008; p. 45) and that "Would-be researchers must consider the potentially conflicting agendas of funders, participants, and researchers" (ibid., p. 62). In other words, funding can introduce elements of bias into the research objectives, research methods and research results, dependent on the values of the funders and participants and even the researcher's. Cheek (2008) mentions examples of research findings being 'steered' towards an 'acceptable' position, research reports being curtailed to state only 'acceptable' statements and potential pressure on

participants to not provide statements that may be seen as detrimental to the sponsor (ibid., pp. 65 f.f.). The researcher considered these influences throughout the research process, but considers such influence to have been minimal, mainly through the fact that the research methodology of Action Research actually reduces the power-influence of the sponsor by 'relegating' the sponsor to co-researcher status. Since problem-owner and researcher worked on the problem together, the power relationship was therefore quite egalitarian and this allowed the work to progress without the problem owner having to curtail elements of the research. It is true that there were instances where the researcher's suggestions were not taken up (e.g. data gathering with future users; more advanced technology), but this can be explained from the viewpoint that advanced technology and the associated higher cost of purchase and re-training may make an advanced solution prohibitive (therefore, it is an organisational requirement for the solution to be cost effective); with regards to the limited access to users and scope for evaluation, this may be explainable through the fact that the collaborators saw the ultimate output of the research to consist of technical artefacts, as hinted on earlier in Section 5. Therefore, the fact that a technical artefact had to be arrived at shows that it wouldn't be in the sponsors' interests to unnecessary curtail research activities, whilst the view that user access was not necessary can be explained from the more pragmatic viewpoint that the collaborators had adopted; they considered working technical artefacts as sufficient evaluation and sought to show the fact that the developed artefacts worked through a series of case studies, such as the XML file that was sent to the researcher for evaluation (See Chapter 6.1). Therefore, the researcher sees these influences as the epistemological position of the collaborators and the organisation's limited resources, not a value-based influence on the research in order to present facts in a certain light or serve some ulterior motive.

Flick (2006) mentions that Expert Interviews may be problematic because they are prone to blocking by the expert being interviewed through the

realisation that they may not have had the relevant expert knowledge after all and that there may be an occurrence of role diffusion, where the interviewee may try to either talk more about current conflicts in his area of work or where the interviewee may switch between expert and private person and thus not contribute as much to the topic the expert is being interviewed for. However, the researcher did not experience these issues since the researcher used directive probing (a permissible method, according to both Flick (2006) and also Meuser and Nagel (2002)) to return the interview back on topic when there was a danger of the interview focus being lost. Since the interviewee was the collaborator, the interview was never at risk of being blocked since the collaborator was well versed in the research problem itself and therefore constituted a valid expert.

6.4 Summary

This section shall summarise the overall document. Originally, this document set out with a specific research question asked of the researcher, which read as follows: "How can the current method of creating Digital Signature Policies be improved such that Digital Signature Policies in ETSI TR 102 038 format are created in a reproducible and more formalised manner that allows users without legal training to use it?" The document then outlined, stage by stage, the activities undertaken by the researcher in order to find an answer to this question. Attached to this research question were four research aims, which were stated to be as follows:

- To develop a method enabling individuals to convert natural language legal acts and convert those to process models
- To develop tools and methods to convert process models into a codified form
- To produce standards-compliant signature, evidence and archival policies (adhering to ETSI TR 102 038)
- The developed method should allow transformations in a structured and repeatable manner

Whilst Chapter 1 summarised the entirety of the research and stated the research question, Chapter 2 then outlined the problem domain that the research question is rooted in. It highlighted what DSPs are and how they are different to Digital Signatures and Digital Certificates; in particular, it highlighted the type of legal issues that this technology makes explicit electronically and the data it captures to achieve this. Finally, the chapter investigated the literature on this technology, but failed to find much material of relevance. As a result, the discussion was limited on examples of imparting legal knowledge to IS, which served to inform the researcher on successful techniques tried in the past and thus offering potential for helping to solve the research question and meet the research aims.

Chapter 3 described the Research Design adopted by the researcher in order to find a solution to the research question. It highlighted the researcher's philosophical positions and identified a research methodology (namely Action Research) suited to the wording of the research question. It also introduced the chosen research methodology in detail and explained how and why the research methodology is suitable to solving the research question. Finally, the precise research methods employed in solving the research question were introduced and detailed, highlighting how the research aims would be solved also. The chapter rounded off by pondering whether the research was conducted in accordance with an alternative research methodology known as Design Science, but limited itself to merely introducing the methodology without much analysis; the researcher considered Chapter 5 to be a more suitable vehicle for this analysis of suitability.

Chapter 4 introduced the solutions that had been arrived at and explained how applying the developed solutions solves the research question. It highlighted the fact that the solutions were a mixture of instantiation artefacts and a method and described some of the technical aspects of the solutions.

However, the majority of the technical detail has been confined to the Appendices.

Chapter 5 is a central section that analysed the arrived-at results and showed whether, and to what extent, the results solve the research question. It also analysed whether the research design was appropriate for this study and whether the research was conducted on a sound base. It also identified why the research was Action Research, and not Design Science as Chapter 3 assumed. It highlighted how the artefact-based research aims were met in Chapter 5.1.

Chapter 6 concluded the document by highlighting how the conducted research contributed to knowledge, what restrictions the researcher had to cope with whilst doing the research and how these limited aspects of the research. Finally, the research identified a number of aspects suitable for further research and briefly explained why these were worthwhile research efforts.

7 References

Adams, S. and Allday, J. (2000). *Advanced Physics*. Oxford: Oxford University Press.

Adelman, C., Kemmis, S., and Jenkins, D. (1980). Rethinking the case study: Notes from the second Cambridge conference. In H. Simons (ed), *Towards a science of the singular*. Norwich: CARE.

Alamillo, I. (2007). N. Papas. Barcelona: Private Discussion between Ignacio Alamillo and Nikolaos Papas on the topic of Digital Signature Policies. Ignacio Alamillo raised several key points about Digital Signature Policies, including statements on why they are needed, how current technology does not provide sufficient weight in certain business contexts and how Digital Signature Policies can address this issue.

Alamillo, I., Martinez, D, Seltsikas, P. and Papas, N. (2007). *Designing a Modelling Methodology for Legal Workflows*. Presented at "Jurix 2007: The Twentieth Annual Conference". Leiden, Netherlands, December 2007.

Aleven, V. and Ashley, K. D. (1997) *Teaching Case-Based Argumentation through a Model and Examples - Empirical Evaluation of an Intelligent Learning Environment*. PhD Thesis, University of Pittsburgh, PA.

Aleven, V. and Ashley, K. D. (1993). *What law students need to know to WIN*. Proceedings of the fourth International Conference on Artificial Intelligence and Law, Amsterdam, ACM: pp. 152-161.

Aleven, V. and Ashley, K. D. (1997). *Evaluating a Learning Environment for Case-Based Argumentation Skills*. Proceedings of the sixth International Conference on AI and Law, Melbourne, Australia: pp. 170-179.

Alsaid, A. and Mitchell, C. J. (2005). Dynamic content attacks on digital signatures. *Information Management & Computer Security*. Vol. 13, No. 4: pp. 328-336.

Anderson, C. W. (1997). Pragmatism, Idealism, and the Aims of Liberal Education. In R. Orrill (ed), *Education and Democracy. Re-Imagining Liberal Learning in America*. New York: College Entrance Examination Board.

Atkinson, T. E. (1953). *Handbook of the Law of Wills*. 2nd Edition. St. Paul, MN: West Group.

Avison, D., Horton, J., Powell, P. and Nandhakumar J. (1995). *Incorporating evaluation in the information systems development process*. 3rd Evaluation of Information Technology Conference. Henley, UK.

Ballantine, J., Levy, M., Martin, A., Munro, I. and Powell, P. (2000). An ethical perspective on information systems evaluation. *International Journal of Agile Management Systems*. Vol. 2, No. 3: pp. 233-241.

Banville, C. and Landry, M. (1989). Can the Field of MIS be Disciplined? *Communications of the ACM*. Vol. 32: pp. 48-61.

Bariff, M. L. and Ginzberg, M. J. (1982). MIS And The Behavioral Sciences: Research Patterns and Prescriptions. *ACM SIGMIS Database*. Vol. 14, No. 1: pp. 19-26.

Baskerville, R. L. (1999). *Investigating Information Systems with Action Research*. Available at http://www.cis.gsu.edu/~rbaskerv/CAIS_2_19/CAIS_2_19.html [Accessed on 19/04/2007].

Baskerville, R. L. (2008). What design science is not. *European Journal of Information Systems*. Vol. 17, No. 5: pp. 441-443.

Baskerville, R. L. and Pries-Heje, J. (1999). Grounded Action Research: a method for understanding IT in practice. *Accounting Management and Information Technologies*. Vol. 9: pp. 1-23.

Baskerville, R. L. and Wood-Harper, T.J.M (1996). A Critical Perspective on Action Research as a Method for Information Systems Research. *Journal of Information Technology*. Vol. 11: pp. 235-246.

Baum, F. (1995). Researching Public Health: Behind the Qualitative-Quantitative Methodological Debate. *Social Science and Medicine*. Vol. 40: pp. 459-468.

Bench-Capon, T., Doutre, S., and Dunne, P.E. (2007). Audiences in Argumentation Frameworks. *Artificial Intelligence*. Vol. 171, No. 1: pp. 42-71.

Bench-Capon, T. J. M. (1997). *Arguing With Cases*. In Oskamp, A., et al.(eds), JURIX 1997, Nijmegen, Gerard Noodt Instituut: pp. 85-99.

Bench-Capon, T. J. M. (1997). Argument in Artificial Intelligence and Law. *Artificial Intelligence and Law*. Vol. 5, No. 4: pp. 249-261.

Bench-Capon, T. J. M. (2002). *Representation of Case Law as an Argumentation Framework*. JURIX 2002: The Fifteenth Annual Conference, Amsterdam, IOS Press.

Bench-Capon, T. J. M., Atkinson, K., and McBurney, P. (2005). *Generating intentions through argumentation*. The Fourth International Joint Conference on Autonomous Agents and Multi Agent Systems, Utrecht, The Netherlands.

Bench-Capon, T. J. M., Atkinson, K., and Modgil, S. (2006). *Argumentation for Decision Support*. DEXA Conference, 2006.

Berkeley, G. (1993). *Philosophical Works*. London: J. M. Dent.

Blythe, S.E. (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security. *Richmond Journal of Law & Technology*. Vol. 11, No. 2: pp. 1-20.

Bons, R. W., Lee, R. M., Wagenaar, R.W. and Wrigley, C.D. (1995). *Modelling Inter-organizational Trade Procedures Using Documentary Petri Nets*. International Conference on System Sciences (HICSS '95), Hawaii, IEEE.

Booch, G., Rumbaugh, J., and Jacobson, I. (1998). *The Unified Modelling Language User Guide*. Reading, Mass.: Addison-Wesley.

Borges, F., Borges, R., and Bourcier, D. (2003). *Artificial Neural Networks and Legal Categorization*. JURIX 2003: The Sixteenth Annual Conference, Amsterdam, IOS Press.

Bostrom, R. P. and Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. *MIS Quarterly*. Vol. 1, No. 3: pp. 17-32.

Bostrom, R. P. and Heinen, J. S. (1977). Part II: The Application of Socio-Technical Theory. *MIS Quarterly*. Vol. 1, No. 4 : pp. 11-28.

Broderick, M. A., Gibson, V. R., and Tarasewich, P. (2001). Electronic signatures: they're legal, now what? *Electronic Networking Applications and Policy*. Vol. 11, No. 5: pp. 423-434.

Burrel, G. and Morgan, G. (1979). *Sociological Paradigms and Organizational Analysis*. Portsmouth, NH: Heinemann.

Chadwick, D.W. and Mundy, D. (2003). *Comparing the performance of Abstract Syntax Notation One (ASN.1) vs. eXtensible Markup Language (XML)*. Trans-European Research and Education Networking Association Conference, Zagreb.

Chang, S.-J. and Dworkin, M. (2005). *Workshop Report - The First Cryptographic Hash Workshop*. Gaithersburg, MD: Information Technology Laboratory, National Institute of Standards and Technology.

Chatterjee, S., Tulu, B., Abhichandani, T. and Li, H. (2005). SIP-Based Enterprise Converged Networks for Voice/Video-Over-IP: Implementation and Evaluation of Components. *IEEE Journal on Selected Areas in Communications*. Vol. 23, No. 10: pp. 1921-1933.

Checkland, P. and Scholes, J. (1990). *Soft Systems Methodology in Practice*. Chichester: J. Wiley.

Cheek, J. (2008). The Practice and Politics of Funded Qualitative Research. In N.K. Denzin and Y.S. Lincoln (eds), *Strategies of Qualitative Inquiry*. Los Angeles: Sage Publications: pp. 45-74.

Chia, R. (2002). The Production of Management Knowledge: Philosophical Underpinnings of Research Design. In D. Partington (ed), *Essential Skills for Management Research*. London: SAGE Publications.

Christie, G. (2000). The Notion of an Ideal Audience in Legal Argument. Dordrecht: Kluwer Academic.

Clarke, A. (1999). Evaluation Research: An Introduction to Principles, Methods and Practice. London: SAGE Publications.

Clauss, S. and Koehntopp, M. (2001). Identity Management and its support of multilateral security. *Computer Networks*. Vol. 37: pp. 205-219.

Coghlan, D. and Brannick, T. (2009). *Doing Action Research in Your Own Organisation*. London: SAGE Publications.

Cole, R., Purao, S., Rossi, M. and Sein, M.K. (2005). Being Proactive: Where Action Research meets Design Research. *International Conference on Information Systems (ICIS 2005) Proceedings*, Paper 27.

Creswell, J. W. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. London: Sage Publications.

Crotty, M. (1998). *The Foundation of Social Research: Meaning and Perspectives in the Research Process*. London: Sage Publications.

Culnan, M. J. and Swanson, E. B. (1986). Research in Management Information Systems, 1980-1984: Points of work and reference. *MIS Quarterly*. Vol. 10, No. 3: pp. 289-302.

Curd, M. and Cover, J. A. (1998). *Philosophy of Science - The Central Issues*. New York: W. W. Norton & Company.

Daskalopulu, A. (2000). *Model Checking Contractual Protocols*. JURIX 2000: 13th Annual Conference, Frontiers in Artificial Intelligence and Applications Series, IOS Press.

Daskalopulu, A. (2000). *Modelling Legal Contracts as Processes*. 11th International Conference and Workshop on Database and Expert Systems Applications, IEEE C. S. Press.

Daskalopulu, A. and Sergot, M. (1995). *A Constraint-Driven System for Contract Assembly*. Fifth International Conference on Artificial Intelligence and Law, College Park, Maryland: ACM Press.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*. Vol. 13, No. 3: pp. 319-340.

Davison, R. M., Martinsons, M. G., and Kock, N. (2004). Principles of Canonical Action Research. *Information Systems Journal*. Vol. 14, No. 1: pp. 65-86.

de Santillana, G. and Zilsel, E. (1970). *The Development of Rationalism and Empiricism*. Chicago: University of Chicago Press.

Deng, R. H., Gong, L., Lazar, A.A. and Wang, W. (1996). Practical protocols for certified electronic mail. *Journal of Network and Systems Management*. Vol. 4, No. 3: pp. 279-297.

Dennis, A. and Wixom, B. H. (2000). *Systems Analysis and Design*. New York: John Wiley & Sons, Inc.

Denzin, N. K. and Lincoln, Y. S. (1998). *The Landscape of Qualitative Research: Theories and Issues*. London: SAGE Publications.

Denzin, N. K. and Lincoln, Y. S. (1998). *Strategies of Qualitative Inquiry*. London: SAGE Publications.

Denzin, N. K. and Lincoln, Y. S. (2008). Introduction: The Discipline and Practice of Qualitative Research. In N.K. Denzin and Y.S. Lincoln (eds), *Strategies of Qualitative Inquiry*. Los Angeles, Sage Publications: pp. 1-44.

Descartes, R. (1984). *The Philosophical Writings of Descartes*. Cambridge: Cambridge University Press.

Dewey, J. (1925). Experience and Nature. In J.A. Boydston (ed), *John Dewey: The Later Works 1925-1953*. Carbondale and Edwardsville: Southern Illinois University Press.

Dewey, J. (1988). The Quest for Certainty. In J.A. Boydston (ed), *The Later Works*, Volume 4. Carbondale and Edwardsville: Southern Illinois University Press.

Diffie, W. and Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*. Vol. 22, No. 6: pp. 644-654.

Duffy, T. M. and Jonassen, D. H. (1992). *Constructivism and the Technology of Instruction: A Conversation*. Hillsdale, New Jersey: Lawrence Erlbaum Associates, Publishers.

Dumas, M., van der Aalst, W. M. P., and ter Hofstede, H.M. (2005). *Process-Aware Information Systems: Bridging People and Software through Process Technology*. Hoboken, New Jersey: John Wiley & Sons.

Dung, P. M. (1995). On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming, and N-person games. *Artificial Intelligence*. Vol. 77: pp. 321-357.

Dunne, P. E. and Bench-Capon, T. J. M. (2004). Identifying Audience Preferences in Legal and Social Domains. *Database and Expert Systems Applications*. Lecture Notes in Computer Science, Volume 3180/2004: pp. 518-527.

Easterby-Smith, M. (1994). *Evaluations, Management Development, Training and Education*. Aldershot: Gower.

Easterby-Smith, M., Thorpe, R., and Lowe, A. (1991). *Management Research: An Introduction*. London: SAGE Publications Ltd.

ECRYPT-Project (2005). *Recent Collision Attacks on Hash Functions: ECRYPT Position Paper*. Revision 1.1. Available at http://www.ecrypt.eu.org/ecrypt1/documents/STVL-ERICS-2-HASH_STMT-1.1.pdf. [Retrieved on 08/2008].

Eden, C. and Huxham, C. (1996). Action Research for Management Research. *British Journal of Management*, Vol 7: pp. 75-86.

Eder, W. E. (1998). Design Modeling - A Design Science Approach (and Why Does Industry Not Use It?). *Journal of Engineering Design*. Vol. 9, No. 4: pp. 355-371.

Edlund, K., Michelsen, A. G., and Rudie, K. (2006). *Supervisory Control of Flowlines By Modelling the Legal Language as Inequalities*. Wodes 2006: Eighth International Workshop on Discrete Event Systems: pp. 15-20.

Eekels, J. and Roozenburg, N. F. M. (1991). A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. *Design Studies*. Vol. 12, No. 4: pp. 197-203.

Elliot, J. (1997). Action Research for Educational Change. In C. Day (ed), *Developing Teachers and Teaching*. Milton Keynes: Open University Press.

Empiricus, S. (1961). *IV - Against the Professors*. Cambridge, Mass.: Harvard University Press.

European Commission. *ICT Task Force*. Available at http://ec.europa.eu/enterprise/ict/policy/taskforce/taskforce_en.htm. [Retrieved on 23/08/09]

European Commission. (2005). *What is the Manchester eGovernment Ministerial Declaration on the European Union: Frequently Asked Questions*. Available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/446&format=HTML&aged=0&language=EN&guiLanguage=en. [Retrieved on 06/2008].

European Commission. (2006). *ICT and Lisbon Strategy*. Available at http://ec.europa.eu/information_society/eeurope/i2010/ict_and_lisbon/index_en.htm. [Retrieved on 06/2008].

European Commission. (2007). *The User Challenge: Benchmarking the Supply of Online Public Services*. Available at http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf. [Retrieved on 06/2008].

European Telecommunications Standards Institute (2002). *ETSI TR 102 038: Electronic Signatures and Infrastructures (ESI); XML format for signature policies*.

European Telecommunications Standards Institute (2002). *ETSI TR 102 041: Signature Policies Report*.

European Telecommunications Standards Institute (2003). *ETSI TR 102 045: Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model.*

European Telecommunications Standards Institute (2003). *ETSI TS 101 733: Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats.*

Fernandes, M. R. (2006). *A proposal of model of signature policy,* University of Sao Paulo. Masters Degree Dissertation.

Fink, A. (1998). *Conducting Research Literature Reviews - From Paper to the Internet.* London: SAGE Publications.

Flick, U. (2006). *An introduction to Qualitative Research* (3rd Edition). London: Sage Publications.

Forouzan, B. A. (2001). *Data Communications and Networking* (2nd Edition). Boston: McGraw Hill.

Fulcher, A. J. and Hills, P. (1996). Towards a strategic framework for design research. *Journal of Engineering Design.* Vol. 7, No. 2: pp. 183-194.

Galliers, R. and Land, F. (1987). Choosing Appropriate Information Systems Research Methodologies. *Communications of the ACM.* Vol. 30: pp. 900-902.

Garner, B. A. (2001). *A Dictionary of Modern Legal Usage.* New York: Oxford University Press.

Garrison, J. (1997). An Alternative to Von Glaserfeld's Subjectivism in Science Education: Deweyan Social Constructivism. *Science & Education.* Vol. 6: pp. 543-554.

Garrison, J. (1997b). *Dewey and Eros. Wisdom and Desire in the Art of Teaching.* New York and London: Teachers College Press.

Giblin, C., Liu, A. Y., Muller, S. and Pfitzmann, B. (2005). *Regulations Expressed As Logical Models (REALM).* JURIX 2005 Conference, Brussels.

Gibson, V. R. and Senn, J. A. (1989). System Structure and Software Maintenance Performance. *Communications of the ACM.* Vol. 32, No. 3: pp. 347-358.

Goldstine, G. (1972). *The Computer from Pascal to Von Neumann.* Princeton University Press.

Golinski, J. (1998). *Making Natural Knowledge - Constructivism and the History of Science.* Cambridge: Cambridge University Press.

Gonzales-Cadenas, C., Cruellas, M., Oliveras, F. and Alamillo, I. (2005). *eXtended Signature Services (XSS) - Profile of the OASIS Digital Signature Service (DSS).* Working Draft 02, OASIS.

Governatori, G. and Rotolo, A. (2004). *Modelling Contracts Using RuleML.* JURIX 2004: The Seventeenth Annual Conference, Amsterdam, IOS Press.

Graca, N. and Quaresma, P. (2003). *How to model legal reasoning using dynamic logic programming: a preliminary report.* JURIX 2003: The Sixteenth Annual Conference, Amsterdam, IOS Press.

Graca, N. and Quaresma, P. (2003). *Using dynamic logic programming to model legal reasoning.* APPIA-GULP-PRODE (Joint Conference on Declarative Programming).

Gray, D. E. (2004). *Doing Research in the Real World*. London: SAGE Publications.

Gray, D. E. (2009). *Doing Research in the Real World* (2nd Edition). London: SAGE Publications Ltd.

Graziano, A. M. and Raulin, M. L. (1989). *Research Methods - A Process of Inquiry*. New York: Harper & Row Publishers.

Grosof, B. N. and Labrou, Y. (2000). An Approach to Using XML and a Rule-Based Content Language with an Agent Communication Language. In F. Dignum and M. Greaves (eds), *Issues in Agent Communication*. London: Springer-Verlag. Volume 1916: pp. 96-117.

The Internet Society – Network Working Group (2001). *RFC 3125: Electronic Signature Policies*.

The Internet Society – Network Working Group (2002). *RFC 3280 - Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*.

Halsey, A. H., Heath, A. F., and Ridge, J.M. (1980). *Origins and Destinations: Family, Class and Education in Modern Britain*. Oxford: The Clarendon Press.

Harre, R. (1981). The Positivist-Empiricist Approach and its Alternative. In P. Reason and J. Rowan (eds), *Human Inquiry: A Sourcebook of new Paradigm Research*. New York, John Wiley.

Hart, C. (1998). *Doing a Literature Review - Releasing the Social Science Research Imagination*. London: SAGE Publications.

Hart, H. L. A. (1961). *The Concept of Law* (2nd Edition). Oxford: Clarendon Press.

Hawking, S. (1996). *A Brief History of Time*. New York: Bantam Books.

Hazari, S. (2002). Challenges of implementing public key infrastructures in Netcentric enterprises. *Logistics Information Management*. Vol. 15, No. 5/6: pp. 385-392.

Heikkinen, H. L. T., Kakkori, L., and Huttunen, R. (2001). This is my truth, tell me yours: some aspects of action research quality in the light of truth theories. *Educational Action Research*. Vol. 9, No. 1: pp. 9-24.

Henfridsson, O. (2005). *Information Systems Action Research: State of the art and future directions*. Seminar at LSE on 04/11/05. Available at http://personal.lse.ac.uk/SORENSEC/download/OlaHenfridssonSlides.ppt. [Accessed on 12/11/09].

Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., and Alvarez, B.R. (2008). An optimistic fair exchange protocol based on signature policies. *Computers & Security*. Vol. 27: pp. 309-322.

Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*. Vol. 28, No. 1: pp. 75-105.

Hirschheim, R. and Klein, H. K. (1989). Four Paradigms of Information Systems Development. *Communications of the ACM*. Vol. 32, No.10: pp. 1199-1216.

Hirschheim, R. and Smithson, S. (1987). Information Systems Evaluation: Myth and Reality. In R. Galliers (ed), *Information Analysis - Selected Readings*. Wokingham: Addison-Wesley.

Hoepfl, M. C. (1997). Choosing qualitative research: a primer for technology education researchers. *Journal of Technology Education*. Vol. 9, No. 1: pp. 47-61.

Housley, R., Ford, W., Poik, T. and Solo, D. (2002). *Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile*. Available at http://tools.ietf.org/html/rfc3280#page-128. [Retrieved on 30/07/2007].

Hubka, V. and Eder, W. E. (1996). *Design Science: introduction to the needs, scope and organization of engineering design knowledge*. London: Springer-Verlag.

Huff, A., Tranfield, D. and van Aken, J. (2006). Management as a Design Science: Mindful of Art and Surprise. *Journal of Management Inquiry*. Vol. 15, No. 4: pp. 413-424

Imamura, T. and Maruyama, H. (2001). *Mapping between ASN.1 and XML*. Proceedings of the 2001 Symposium on Applications and the Internet (SAINT 2001): pp. 57-64.

Irani, Z. and Love, P. E. D. (2000). The Propagation of Technology Management Taxonomies for Evaluating Investments in Information Systems. *Journal of Management Information Systems*. Vol. 17, No. 3: pp. 161-177.

James, W. (1994). *Pragmatism, a New Name for Some Old Ways of Thinking and The meaning of truth, a Sequel to Pragmatism*. Cambridge, MA: Harvard University Press.

Jarvinen, P. (2005). *Action research as an approach in design science*. The European Academy of Management Conference, Munich.

Jensen, K. B. (1991). Humanistic Scholarship as Qualitative Science: Contributions to Mass Communication Research. In K. B. Jensen and N. W. Jankowski (eds), *A Handbook of Qualitative Methodologies for Mass Communication Research*. New York, Routledge: pp. 17-43.

Johnson, P. and Harris, D. (2002). Qualitative and quantitative issues in research design. In D. Partington (ed), *Essential Skills for Management Research*. London, SAGE Publications.

Jouve, D., Amghar, Y., Chabbat, B. and Pinon, J.M. (2003). Conceptual Framework for Document Semantic Modelling: an Application to Document and Knowledge Management in the Legal Domain. *Data & Knowledge Engineering*. Vol. 46: pp. 345-375.

Kaminsky, D. (2004). *MD5 To Be Considered Harmful Someday*. Available at http://www.doxpara.com/md5_someday.pdf. [Retrieved on 16/08/07].

Kant, I. (1965). *Critique of Pure Reason*. New York: St Martin's Press.

Kemmis, S. and McTaggart, R. (1992). The Action Research Planner. In *Action Research and the Critical Analysis of Pedagogy* (3rd Edition). Victoria, Australia: Deakin University.

Kemmis, S. and McTaggart, R. (2008). Participatory Action Research: Communicative Action and the Public Sphere. In N. K. Denzin and Y. S. Lincoln (eds), *Strategies of Qualitative Inquiry*. Los Angeles, Sage Publications: pp. 271-330.

Kerlinger, F. N. (1986). *Foundations of Behavioral Research*. New York: Harcourt Brace.

Kisswani, N.M. and Al-Bakri, A.A. (2010). Regulating the use of electronic signatures given the changing face of contracts. *Macquarie Journal of Business Law*. Vol 7: pp. 53-65.

Knackstedt, R., Brelage, C., and Kaufmann, N.C. (2006). Entwicklung rechtssicherer Web-Anwendungen. Strukturierungsansatz, State-of-the-Art und ausgewaehlte Aspekte der fachkonzeptionellen Modellierung. *Wirtschaftsinformatik*. Vol. 48, No. 1: pp. 27-35.

Kratovil, R. (1946). *Real Estate Law*. Prentice-Hall.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd Edition). London: SAGE Publications.

Kuhn, T. S. (1962/1970). *The Structure of Scientific Revolutions* (2nd Edition). Chicago: University of Chicago Press.

Kumar, R. (2005). *Research Methodology - A step-by-step guide for beginners* (2nd Edition). London: SAGE Publications Ltd.

Landesman, C. (1997). *An Introduction to Epistemology*. Oxford: Blackwell Publishers, Ltd.

Laudon, K. C. and Laudon, J. P. (2004). *Management Information Systems - Managing the Digital Firm* (8th Edition). Upper Saddle River, New Jersey: Pearson Education Inc.

Lee, A. (1999). Inaugural Editor's Comments. *MIS Quarterly*. Vol. 23, No. 1: pp. v-xi.

Lee, S. and O'Keefe, R. M. (1996). The Effect of Knowledge Representation Schemes on Maintainability of Knowledge-Based Systems. *IEEE Transactions on Knowledge and Data Engineering*. Vol. 8, No. 1: pp. 173-178.

Lenstra, A. and de Weger, B. (2005). *On the possibility of constructing meaningful hash collisions for public keys*. ACISP Conference, Brisbane, Australia.

Lethbridge, T. C. and Laganiere, R. (2001). *Object-Oriented Software Engineering*. London: McGraw-Hill.

Lewin, K. (1946). Action research and minority problems. *Journal of Social Issues*. Vol. 2: pp. 34-46.

Liang, T.-P., Huang, C.-W., Yeh, Y.-H. and Lin, B. (2007). Adoption of Mobile Technology in Business: A fit-viability Model. *Industrial Management & Data Systems*. Vol. 107, No. 8: pp. 1154-1169.

Lincoln, Y. S. and Guba, E. G. (1985). *Naturalistic Inquiry*. London: Sage Publications.

Lincoln, Y. S. and Guba, E. G (1994). *Naturalistic Inquiry* (2nd Edition). London: SAGE Publications.

List, D. (2006). Action research cycles for multiple futures perspectives. *Futures*. Vol. 38: pp. 673-684.

Mann, W. C. and Thompson, S. A. (1987). Rhetorical Structure Theory: A Theory of Text Organization. In L. Polanyi (ed), *The Structure of Discourse*. Norwood, N.J., Ablex Publishing Corporation.

March, S. T. and Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*. Vol. 15: pp. 251-266.

Markus, M. L., Majchrzak, A., and Glasser, L. (2002). A Design Theory for Systems that Support Emergent Knowledge Processes. *MIS Quarterly*. Vol. 26, No. 3: pp. 179-212.

McCarty, L. T. (1989). A Language for Legal Discourse - I. Basic Features. *Proceedings of the 2nd International Conference on Artificial Intelligence and Law.* Vancouver, BC, Canada: ACM, pp. 180-189.

McNiff, J. (1988). *Action Research: Principles and Practice.* London: Routledge.

McNiff, J., Lomax, P., and Whitehead, J. (1997). *You and Your Action Research Project.* London: Routledge.

McNiff, J. and Whitehead, J. (2002). *Action Research - Principles and Practices* (2nd Edition). London: Routledge.

McNiff, J. and Whitehead, J. (2009). *Doing and Writing Action Research.* London: SAGE Publications.

McPhee, K. (1996). *Design Theory and Software Design.* Technical Report, The University of Alberta, Department of Computing Science.

Mercatali, P., Boschi, L., Romano, F. and Spinicci, E. (2005). *Automatic Translation from Textual Representations of Laws to Formal Models through UML.* JURIX 2005 Conference. Brussels.

Meuser, M. and Nagel, U. (2002). ExpertInneninterviews - vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion. In A. Bogner, B. Littig and W. Menz (eds), *Das Experteninterview.* Opladen, Leske & Budrich: pp. 71-95.

Mikle, O. (2004) *Practical Attacks on Digital Signatures using MD5 Message Digest.* ePrint Archive. Report 2004/356. Available at http://eprint.iacr.org/2004/356. [Retrieved on 16/08/07].

Moore, J. D. and Pollack, M. E. (1992). A Problem for RST: the Need for Multi-level Discourse Analysis. *Computational Linguistics.* Vol. 18, No. 4: pp. 537-544.

Myers, M. (2000). Qualitative Research and the Generalizability Question: Standing Firm with Proteus. *The Qualitative Report.* Vol. 4, No. 3/4.

Nechvatal, J. and Chang, S.-J. (2006). *Workshop Report - The Second Cryptographic Hash Workshop.* Gaithersburg, MD: Information Technology Laboratory, National Institute of Standards and Technology.

Neubert, S. (2001). *Pragmatism and Constructivism in Contemporary Philosophical Discourse.* Available from www.uni-koeln.de/hf/konstrukt/texte/download/pragmatism%20constructivism.pdf. [Retrieved on 27/04/09]

Newman, I. and Benz, C. R. (1998). *Qualitative-Quantitative Research Methodology - Exploring the Interactive Continuum.* Carbondale: Southern Illinois University Press.

Nolan, R. L. (1973). Managing the Computer Resources: A Stage Hypothesis. *Communications of the ACM.* Vol. 16, No. 7: pp. 399-405.

Nunamaker, J. F., Chen, M., and Purdin, T.D.M. (1990). Systems Development in Information Systems Research. *Journal of Management Information Systems.* Vol. 7, No. 3: pp. 89-106.

OASIS (2005). *eXtended Signature Services (XSS) Profile of the OASIS Digital Signature Service (DSS).*

OASIS (2007). *Advanced Electronic Signature Profiles of the OASIS Digital Signature Service.*

OASIS (2007). *Digital Signature Service: Core Protocols, Elements and Bindings.*

Olsen, F. (2005). *Hashing out encryption.* Available at http://www.fcw.com/fcw/articles/2005/0207/web-hash-02-07-05.asp. [Retrieved on 12/08/07].

Pasquier, J. and Devoret, F. (2006). *Re-enforced Electronic Signature.* European Patent Office. Application Number WO2006106224 (A1).

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems.* Vol. 24, No. 3: pp. 45-77.

Petri, C. A. (1962). *Kommunikation mit Automaten.* PhD Dissertation. Bonn: Institut fuer Instrumentelle Mathematik.

Pettigrew, A. M. (1997). What is Processual Analysis? *Scandinavian Journal of Management.* Vol. 13, No. 4: pp. 337-348.

Pfeiffer, A. (1966). *Dialogues on Fundamental Questions of Science and Philosophy.* Oxford: Pergamon Press Ltd.

Polit, D. and Hungler, B. (1991). *Nursing research: Principles and methods.* New York: JB Lippincott.

Popper, K. R. (1991). *Conjectures and Refutations: The Growth of Scientific Knowledge* (5th Edition). London: Routledge.

Potter, W. J. (1996). *An Analysis of Thinking and Research about Qualitative Methods.* Mahwah, New Jersey: Lawrence Erlbaum Associates.

Powell, P. (1992). Information technology evaluation: is it different? *Journal of the Operational Research Society* Vol. 43, No. 1: pp. 29-42.

Prakken, H. and Sartor, G. (1997). *Reasoning with Precedents in a Dialogue Game.* ICAIL Conference, Melbourne, Australia, ACM: pp. 1-9.

Preston, M. and Mehandjiev, N. (2004). *A Framework for Classifying Intelligent Design Theories.* Workshop on Interdisciplinary Software Engineering Research, Newport Beach, California, USA.

Breaking Barriers to eGovernment Project (2007). *Administrative Law.* Available at http://www.egovbarriers.org/?view=subject&subject=law. [Retrieved on 25/07/2007].

Randall, J. and Szydlo, M. (2004). *Collisions for SHA0, MD5, HAVAL, MD4 and RIPEMD, but SHA1 Still Secure.* Available at http://www.rsa.com/rsalabs/node.asp?id=2738. [Retrieved on 14/08/07].

Rapaport, R. N. (1970). Three dilemmas in Action Research: With special reference to the Tavistock experience. *Human Relations.* Vol. 23: pp. 499-513.

Reason, P. and Bradbury, H. (2008). *The Sage Handbook of Action Research: Participative Inquiry and Practice.* London: Sage Publications.

Reed, C. A. and Daskalopulu, A. (1998). Modelling Contractual Arguments. ISSA-98 Conference. *Proceedings of the 4th International Conference on Argumentation*: pp. 668-692.

Revans, R. W. (1983). What is Action Learning? *Journal of Management Development*. Vol. 21, No. 1: pp. 39-50.

Rissland, E. L., Ashley, K. D., and Loui, R.P. (2003). AI and Law: A fruitful synergy. *Artificial Intelligence*. Vol. 150: pp. 1-2.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method For Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*. Vol. 21, No. 2: pp. 120-126.

Robiette, A. (2001). Digital Certificates and Public Key Infrastructure. *VINE*. Vol. 31, No. 2: pp. 42-49.

Rorty, R. (1982). *Consequences of Pragmatism*. Minneapolis, MN: University of Minnesota Press.

Ross, A. (1968). *Directives and Norms*. London: Routledge & Kegan Paul.

Rossi, M. and Sein, M. K. (2003). *Design Research Workshop: A proactive research approach*. 26th Information Systems Research Seminar in Scandinavia. Porvoo, Finland.

Rouse, J. (1987). *Knowledge and Power: Toward a Political Philosophy of Science*. Ithaca, NY: Cornell University Press.

Ryan, S. D. and Harrison, D. A. (2000). Considering Social Subsystem Costs and Benefits in Information Technology Investment Decisions: A View from the Field on Anticipated Payoffs. *Journal of Management Information Systems*. Vol. 16, No. 4.

Sadler-Smith, E. (2006). *Learning and Development for Managers: Perspectives from Research and Practice*. Oxford: Blackwell Publishing.

Safire, W. (1984). *I stand corrected*. New York: Times Books.

Scharl, A. (1998). *Reference Modeling of Commercial Web Information Systems Using the Extended World Wide Web Design Technique (eW3DT)*. Thirty-first Hawaiian International Conference on System Sciences: pp. 476-484.

Scheer, A. W., Thomas, O., and Adam, A. (2005). Process Modeling Using Event-Driven Process Chains. In Dumas, M., W. van der Aalst and A.H.M. ter Hofstede (eds), *Process-Aware Information Systems: Bridging People and Software through Process Technology*. New Jersey, John Wiley and Sons: pp. 119-146.

Scott, J. (1990). *A Matter of Record - Documentary Sources in Social Research*. Cambridge: Polity.

Seltsikas, P. Personal Communication: Exchange of ideas on the nature of philosophy and epistemological effects of ontologies.

Seltsikas, P. and Palkovits, S. (2006). *Process Modeling Notation for eGovernment: an Assessment of Modeling Notations for Identity Management and GUIDE's Methodology in Practice*. eGov Interop Conference, Bordeaux.

Seltsikas, P. and Papas, N. (2008). *Developing User Requirements for Trans-National Government Information Systems*. 42nd Hawaii International Conference on Systems Sciences, Hawaii, USA.

Shao, J. and Cao, Z. (2006). A traceable threshold signature scheme with multiple signing policies. *Computers & Security*. Vol. 25: pp. 201-206.

Siau, K. and Rossi, M. (1998). *Evaluating Information Modeling Methods - A Review*. 31st Hawaii International Conference on System Sciences (HICSS-31), Big Island of Hawaii.

Sijanski, G. and Münch, S. (2006). Modelling Legal Proceedings. *JurPC* Issue 28/2006.

Simon, H. A. (1969). *The sciences of the artificial* (3rd Edition). London: MIT Press.

Skrtic, T. M. (1985). Doing naturalistic research into educational organizations. In Y. S. Lincoln (ed), *Organizational Theory and Inquiry*. Newbury Park, CA: SAGE Publications.

Soriano-Meier, H. and Forrester, P. L. (2001). A Model for Evaluating the Degree of Leanness of Manufacturing Firms. *Integrated Manufacturing Systems*. Vol. 13, No. 2: pp. 104-109.

Sotirov, A., Stevens, M., Applebaum, J., Lenstra, A., Molnar, D., Osvik, D.A. and De Weger, B. (2008). *MD5 considered harmful today - Creating a rogue certificate*. 25th Annual Chaos Communication Congress. Berlin.

Sunro, L. and O'Keefe, R. M. (1996). The effect of knowledge representation schemes on maintainability of knowledge-based systems. *IEEE Transactions on Knowledge and Data Engineering*. Vol. 8, No. 1: pp. 173-178.

Susman, G. I. and Evered, R. D. (1978). An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly*. Vol. 23: pp. 582-603.

Symons, V. and Walsham, G. (1988). The evaluation of information systems: a critique. *Journal of Applied Systems Analysis*. Vol. 15: pp. 119-132.

Teorey, T. J. and Fry, J. P. (1982). *Design of Database Structures*. Englewood Cliffs, N.J.: Prentice-Hall, Inc.

University Press, Cambridge. *Cambridge Dictionaries Online*, Cambridge University Press. Accessed on 20/04/2007.

Van Aken, J. (2005). Management Research as a Design Science: Articulating the Research Products of Mode 2 Knowledge Production in Management. *British Journal of Management*, Vol. 16: pp. 19-36

Van de Ven, A.H. and Johnson, P.E. (2006). Knowledge for Theory and Practice. *Academy of Management Review*, Vol. 31: pp. 902-921.

Vaishnavi, V. and Kuechler, W. (2004, Last update: 29/06/2007). "Design Research in Information Systems." Available at http://www.isworld.org/Researchdesign/drisISworld.htm. [Retrieved on 13/08/2008].

Various. (2007). *DMReview Glossary*. from www.dmreview.com/glossary/a.html.

Venkatesh, V., Morris, M. G., Davis, G.B. and Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*. Vol. 27, No. 3: pp. 425-478.

von Glaserfeld, E. (1989). Cognition, Construction of Knowledge, and Teaching. *Synthese*. Vol. 80, No. 1: pp. 121-140.

W3C. (1999). *XPath*. from http://www.w3.org/TR/xpath.

Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*. Vol. 3, No. 1: pp. 36-59.

Walls, J. G., Widmeyer, G. R., and El Sawy, O. A. (2004). Assessing Information System Design Theory in Perspective: How Useful Was Our 1992 Initial Rendition? *Journal of Information Technology Theory and Application*. Vol. 6, No. 2: pp. 43-58.

Walsham, G. (1993). *Interpreting Information Systems in Organisations*. Chichester: John Wiley & Sons.

Wang, X., Feng, D., Lai, X. and Yu, H. (2004). *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD*. CRYPTO Conference, Santa Barbara, CA.

Wang, X., Yin, Y. L., and Yu, H. (2005). *Finding Collisions in the Full SHA-1*. RSA Conference, San Francisco.

Wang, X. and Yu, H. (2005). How to Break MD5 and Other Hash Functions. EuroCrypt Conference, Springer LNCS.

Warr, P., Bird, M., and Rackman, N. (1970). *Evaluation of Management Training*. Aldershot: Gower.

White, S. A. *Introduction to BPMN*. Available at http://www.bpmn.org/Documents/Introduction%20to%20BPMN.pdf. [Retrieved on 25/07/2007].

Whitehead, A. N. (1933). *Adventures in Ideas*. London: Cambridge University Press.

Willcocks, L. and Lester, S. (1991). Information Systems investments: evaluation at the feasibility stage of projects. *Technovation*. Vol. 11, No. 5: pp. 283-302.

Willis, T., Crossland, J., and Blair, R.D. (2004). *Beginning VB.NET 2003*. Indianapolis, Indiana: Wiley Publishing, Inc.

Wilson, S. (1997). Certificates and trust in electronic commerce. *Information Management & Computer Security*. Vol. 5, No. 5: pp. 175-181.

Wilson, S. (1999). Digital signatures and the future of documentation. *Information Management & Computer Security*. Vol. 7, No. 2: pp. 83-87.

Wilson, T. P. (1982). Quantitative 'oder' qualitative Methoden in der Sozialforschung. *Koelner Zeitschrift fuer Soziologie und Sozialpsychologie*. Vol. 34: pp. 487-508.

Winter, M. C., Brown, D. H., and Checkland, P. (1995). A role for soft systems methodology in information systems development. *European Journal of Information Systems*. Vol. 4: pp. 130-142.

Wood, M., Roper, M., Brooks, A. and Miller, J. (1997). *Comparing and combining software defect detection techniques: a replicated empirical study*. 5th ACM SIGSOFT International Symposium on Foundations of Software Engineering.

World Wide Web Consortium (1998). *Extensible Markup Language (XML)*.

Yin, R. (1989). *Case Study research design and methods*. Newbury Park, CA: SAGE Publications.

Appendix A: Original PADS Questionnaire

This is the *original* form of the PADS questionnaire.

Cert

**Agència Catalana
de Certificació**

Analysis questionnaire of PADS methodology

Questionnaire of PADS methodology

PROCESS ANALISYS

Processes are, in a very simplified view, sequences of events which drive to a concrete result. Those events should be considered as facts or actions which arises out a step beyond or after into the process.

Administrative process is a good example of process, which is regulated, total or partially, by law, which determines its workflow, its contents and effects.

With administrative procedures, we should find processes for public or private services provision by public administrations or their organizations.

Analysis of each process should consider:

1. Which is the content of the process?	- Process description
	- Type of process (private service, public service, administrative procedure).
	- Process effects.
2. Which is the applicable regulation to the process?	- Applicable rules identification.
	- Process legal meaning.
	- Legal conditions needed for the process.
3. Which is its workflow?	- Graphic or list of events which form the process, with its relevant acts and facts, and their connections.

CAT Cert
Agència Catalana
de Certificació

Analysis questionnaire of PADS methodology

ACTS ANALISYS

When the process is identified, the next step is the analysis of its acts/events.

Acts are the verbs of an action (of citizens, administrations or third persons or entities) which initiates, impulses or terminates the process. Usually, acts should be documented, unlike material facts or omissions, which are usually not.

Analysis of <u>each act</u> should consider:

1. Which is the content of the act?	- Act's description. - Type of act (citizen act, administration act, other). - Effects of the act inside the procedure (initiates, terminates, other).
2. Which is the regulation applicable to the act?	- Identification of the applicable legal provisions. - Legal meaning of the act (regulated or discretional act, other). - Legal conditions required to perform the act. - Legal or administrative obligation to document the act.
3. Who performs the act?	- Natural person (citizen). - Administration worker. - Administrative authority (organ).
4. In which quality is the person acting? Is he/she acting on behalf of another person?	- On his/her own behalf. - On behalf of a public or private legal entity, for which he/she is a corporate organ (organic representation). - On behalf of a public or private legal o natural person, for which he/she is a legal representative (legal representation). - On behalf of a public or private legal or natural person, for which he/she is a voluntary representative (with notarial or registral title).

CAT Cert

Agència Catalana
de Certificació

Analysis questionnaire of PADS methodology

	- On behalf of a public or private legal or natural person, acting as a professional representative.
5. Is personal substitution allowed?	- Acts strictly personal.
	- Any kind of representative.
	- Any person with a concrete attribute (ex. Any worker pertaining to a group).
6. Dos it generate a new document, or is it added to a previous document, or is it added to a expedient or book?	- Generates a new document.
	- It is added to a previous document.
	- It is filed into a registry, without generating a new document.
7. Does it require the previous validation of the person performing the act?	- Yes/No.
	- Determination of the identification and authentication method of the acting person.
	- Rating of the method, according to CATCert's classification scheme.
8. Does it require the previous validation of the entitlement in which the person acts?	- Yes/No.
	- Checking method of the personal condition, in case of organic or legal representatives.
	- Checking method of the entitlement or authorization, in case of voluntary representatives.
	- Checking method of the professional condition, in case of professional representatives.
9. Does it require a previous or posterior confidential communication?	- Yes/No.
	- Determination of the protection method used.
10. Is the act of automatic performance?	- Yes/No.
	- Determination of mechanic or automatic treatment.

CAT Cert
Agència Catalana
de Certificació

Analysis questionnaire of PADS methodology

DOCUMENTS ANALISYS

In respect to the acts to be documented, whereas in independent documents or in collections of documents (like electronic books), whereas in electronic registries, it is necessary to identify the documental outputs generated in the execution of the process, and the formal requirements upon the documents.

Analysis of each document should consider:

1. Which is the content of the document?	- Document's description.
	- Type of document (private, administrative, public).
2. Which is the regulation applicable to the document?	- Identification of the applicable legal provisions.
3. Which formal requirements apply?	- Need to be original, simple copy or authenticated copy.
	- Need to incorporate a signature.
	- Need to incorporate marks, stamps or seals.
	- Need to stamp date and time.
	- Need to incorporate role or another personal attribute or condition.
4. Which content accreditation requirements apply?	- Need to accredit legal personality.
	- Need to accredit the capacity to act on behalf of another person.
	- Need to accredit the document content.
5. Which is the expected lifetime of the document?	- Active or semi-active term, in years.
	- Archival term, in years.

CAT Cert
Agència Catalana
de Certificació

Analysis questionnaire of PADS methodology

SIGNATURES ANALISYS

Finally, according to the act and document identified requirements, it is necessary to determine the concrete signature specific requirements, is any.

Analysis of each signature should consider:

1. What is the legal meaning of the signature?	- Description of the legal meaning.
	- Legal description of the signature, when it belongs to a signature process.
2. Which personal condition accredits the signature?	- Author or another (substitution, delegation or another mechanism).
	- Acts on his/her own behalf or on behalf of a third person.
	- The condition (role, attributes) is certified or claimed.
3. Is it a need to ensure signature time independently from the document time?	- Yes/No.
4. Is there any signature process?	- Yes/No.
	- Description of the signature flow.

Appendix B: Technical Analysis of Digital Signatures

Digital Signatures are functionally defined in ETSI TS 101 733. This technical standard describes different types of Digital Signatures and refers to DSPs and how they are represented within a Digital Signature.

Basic Electronic Signature

According to ETSI TS 101 733, a Basic Electronic Signature (BES) is, as the name suggests, the minimum format for an electronic signature to be generated by a signer. It provides basic authentication and integrity protection. An illustration of a BES can be viewed below:

Basic Electronic Signature (BES)
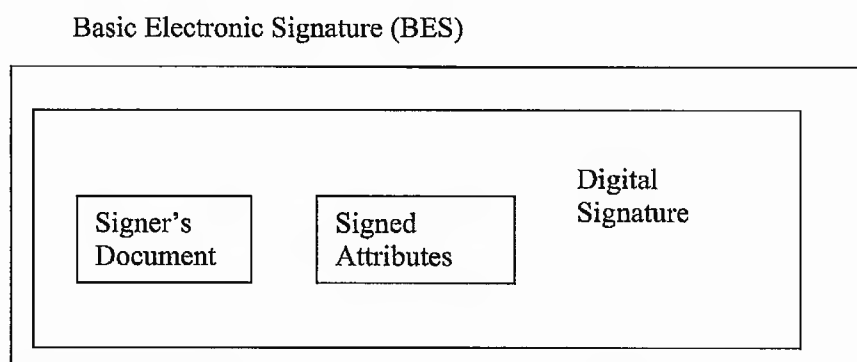
Figure B-1: Basic Electronic Signature

ETSI TS 101 733 states that the Signed Attributes are defined by RFC 3369 and RFC 2634 and consist of Mandatory and Optional Signed Attributes. Further details can be found in ETSI TS 101 733, page 14.

Explicit Policy Electronic Signatures (EPES)

An Explicit Policy Electronic Signature (EPES), according to ETSI TS 101 733, incorporates an additional signed attribute (when compared to a BES) which indicates that a signature policy is mandatory to validate the signature and explicitly states the signature policy that must be used for validation. The

signed attribute is protected by the digital signature. An illustration of an EPES is provided below:
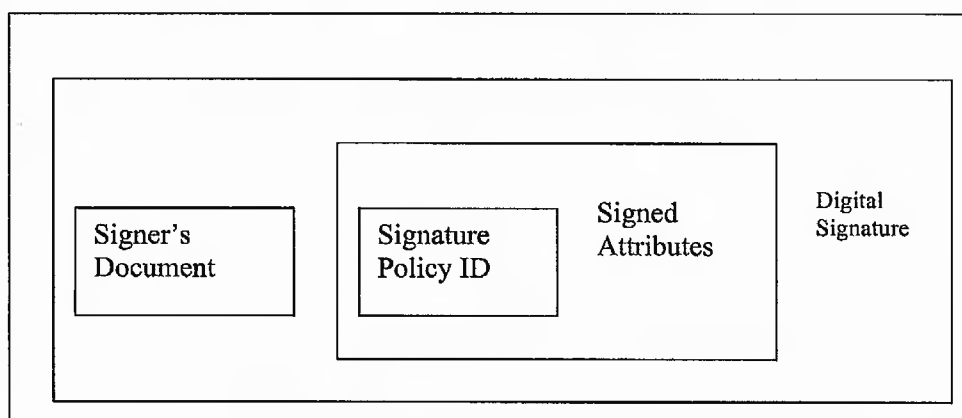
Explicit Policy Electronic Signature (EPES)

Figure B-2: Explicit Policy Electronic Signature

The Signed Attributes of the EPES consist of the same attributes that are used in the BES, with an added element indicating the Signature Policy ID to be used for signature validation. Further details can be found in ETSI TS 101 733, p. 16.

Electronic Signature with Time (ES-T)

ETSI TS 101 733 also describes an Electronic Signature with Time consisting of a BES or an EPES that have had a trusted time added to them. Trusted time provides the validity period of signature and there are two ways of adding trusted time to an electronic signature:

- As an unsigned attribute value, added at signing time
- A time mark provided by a trusted service provider, in this case a Time Stamp Authority (TSA)

If adding the time stamp through an unsigned attribute value, the token is added to within the signature policy as an unsigned attribute by the signer's software. On the other hand, if using a TSA, the TSA adds its own evidence of a time mark externally to the signature policy. An ES-T is illustrated below:
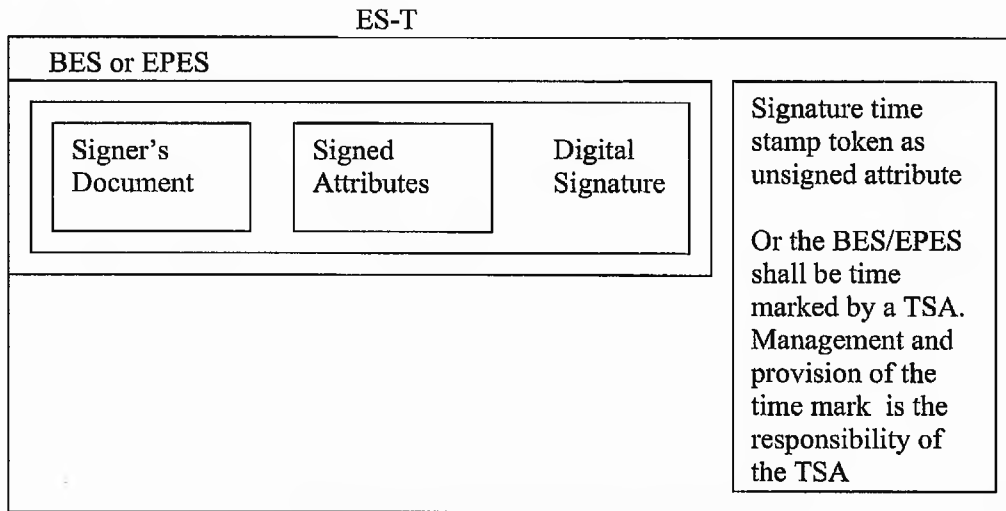
ES-T

BES or EPES	
Signer's Document **Signed Attributes** **Digital Signature**	Signature time stamp token as unsigned attribute Or the BES/EPES shall be time marked by a TSA. Management and provision of the time mark is the responsibility of the TSA

Figure B-3: Electronic Signature with Time

In case of an EPES being used as part of an ES-T, the Signed Attributes of the EPES will contain a reference to the Signature Policy ID that is included as part of the ES-T and which contains either the TSA information, or the unsigned attribute of the time stamp token. It should be noted that in order to reduce the risk of repudiation of the signature, the trusted time indication must be as close as possible to the time the signature was created. It is pertinent that an ES-T trust time indication must be created before a certificate has been revoked or expired. Further details can be found in ETSI TS 101 733, p.17 ff..

Electronic Signature with Complete validation data references (ES-C)

An Electronic Signature with complete validation data references (ES-C) extends an ES-T by adding references to all certificates present in the certification path used for verifying the signature and by adding revocation

information as well. ETSI TS 101 733 describes how the use of the references allows the actual values of the certification path and revocation information to be stored elsewhere, reducing the size of a stored electronic signature format. The structure of an ES-C is illustrated below:
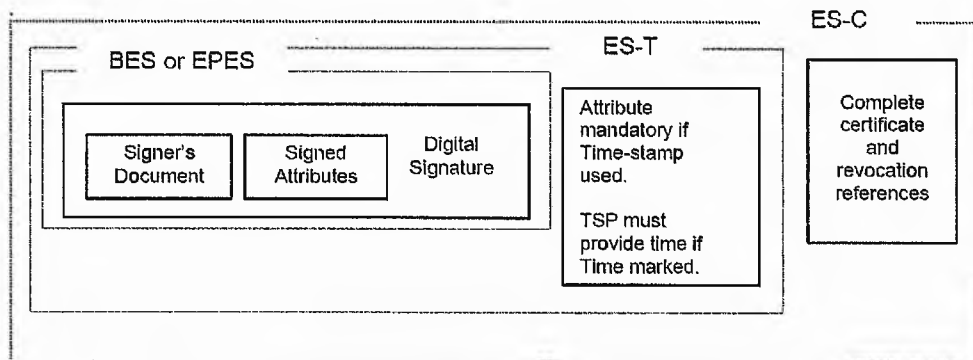

Figure B-4: Electronic Signature with Validation Data References

The complete certificate and revocation references are added to the ES-T as unsigned attributes. It is recommended that a grace period is observed between creating the signature and adding the certification and revocation references to the ES-C in order to allow the certificate revocation information to propagate through the revocation processes. The signature policy may define specific values for grace periods, which are described and defined in ETSI TS 101 733, pp. 17 ff.

Extended Long Electronic Signature (ES-X Long)

ETSI TS 101 733 describes the Extended Long Electronic Signature (ES-X Long) as extending the ES-C by supplementing the certificate and revocation references with their actual values. Thus, the ES-X becomes a repository holding the certificate and revocation information required to validate an ES-C. The following figure illustrates the concept of the ES-X Long.
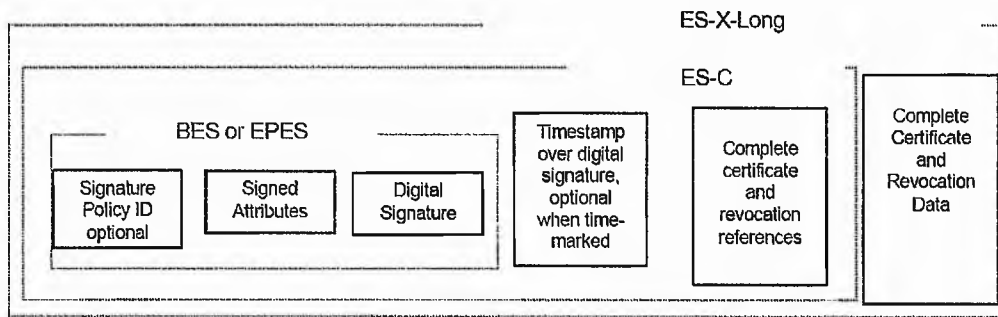
Figure B-5: Extended Long Electronic Signature

The complete certificate and revocation data would be added to the signature policy in the form of unsigned attributes, as per the description in ETSI TS 101 733, pp. 19 ff.

Extended Electronic Signature with Time Type 1 (ES-X Type 1)

This is an extension of the ES-C, where an ES-C and all of its contents have been time-stamped. This provides trusted time protection over the certificates and revocation information in case of the compromise of a Certification Authority key compromise. The schema of this signature is illustrated below:
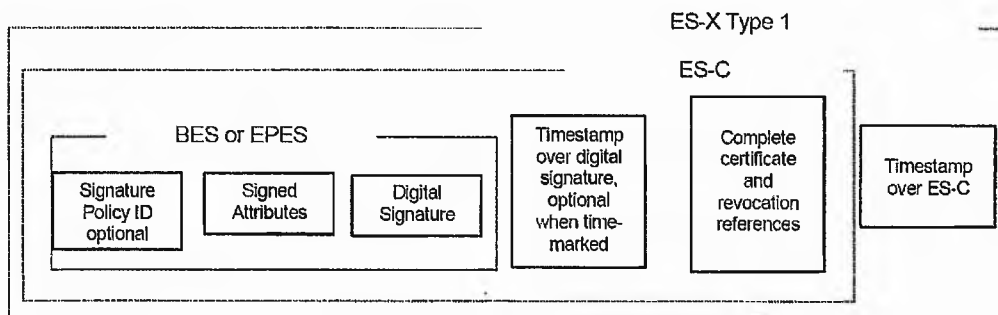
Figure B-6: ES-X Type 1

For more information, please refer to ETSI TS 101 733, pp. 19 & 37.

Extended Electronic Signature with Time Type 2 (ES-X Type 2)

This is an extension of the ES-C; unlike ES-X Type 1, this signature has a time-stamp token that is applied to the certification path and revocation information references only. Therefore, this provides trusted time protection to the certificate and revocation references only. Both ES-X Type 1 and ES-X Type 2 counter the same threats (Certification Authority key compromise) and the preference of one over the other is context dependent. ETSI TS 101 733 specifies that ES-X Type 1 be used when the revocation response is defined to be in the OCSP format, whilst ES-X Type 2 is to be used when the revocation response is defined to be in the CRL format. More information is in ETSI TS 101 733, page 69. The following illustration represents ES-X Type 2.
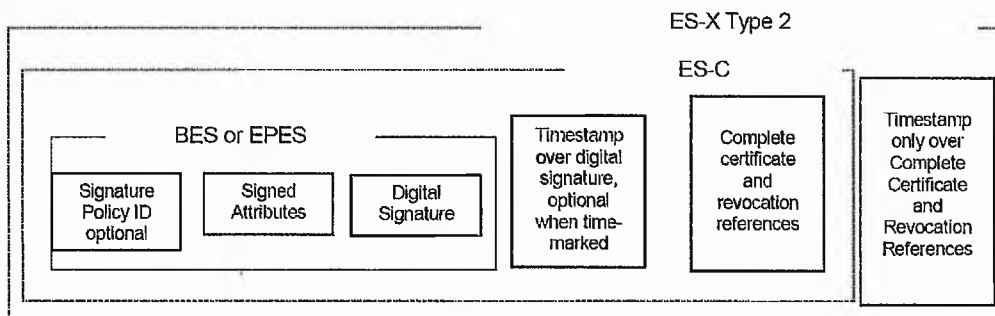
Figure B-7: ES-X Type 2

Extended Long Electronic Signature with Time (ES-X Long Type 1 or 2)

This signature combines ES-X Long with either ES-X Type 1 or ES-X Type 2. It offers protection against TSA key compromises and more information can be read in ETSI TS 101 733, p. 72. The schema is illustrated below:
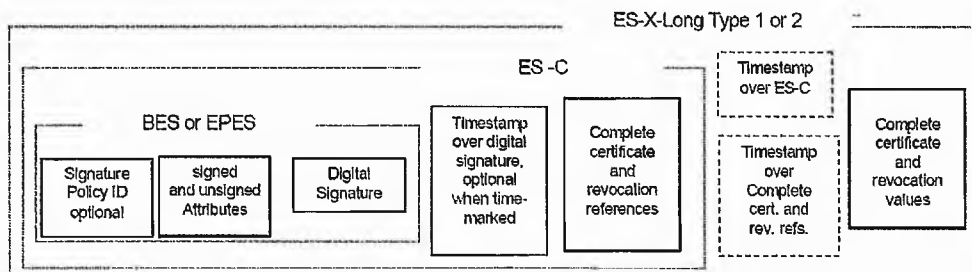

Figure B-8: ES-X Long Type 1 or 2

Archival Electronic Signature (ES-A)

This signature is an extension of either an ES-X Long, ES-X Long Type 1 or ES-X Long Type 2 and is used for archival uses of long-term signatures. Through successive time-stamps, the entire signature is protected against hashing algorithms becoming vulnerable over time or the breaking of cryptographic material or algorithms. Below is an illustration of an ES-A:
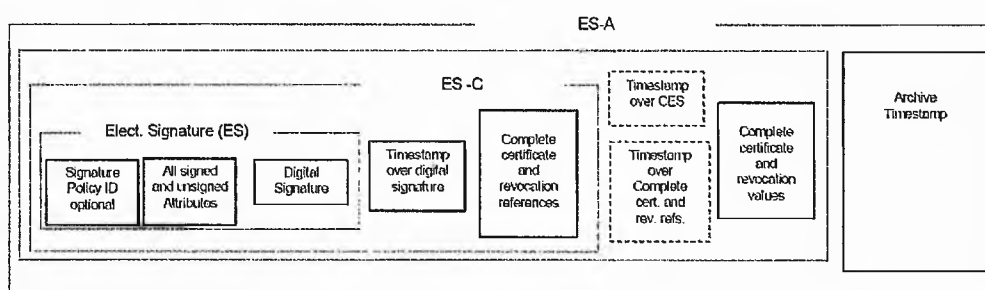

Figure B-9: Archival Electronic Signature

In the case of ES-A, the archive time stamps are timestamp tokens that may themselves include unsigned attributes required to validate the archive timestamp token. More information is found in ETSI TS 101 733, p. 21.

This type of Digital Signature is of key importance, as it represents the most complete set of information on a Digital Signature's validity and therefore presents the most legal weight a Digital Signature can produce. Furthermore, it exhibits the inclusion of a 'Signature Policy ID'-field, which allows this Signature to be verified and evaluated against a DSP. More importantly, as will be demonstrated later on within this chapter, a DSP has a variety of fields that provide further legal weight against the fields that are described in the ES-A, such as Timestamps, certificate and revocation information, as well as archival information. The full relevance of these fields will become clearer in the chapter on DSPs, which explains their meaning further.

Appendix C: Technical Analysis of Digital Signature Policies

This section will introduce the technical syntax of DSPs, as defined in ETSI TR 102 038. The standard defines DSPs in XML and the document is split into several elements; several of these elements in combination will result in yielding a DSP in the format introduced above – this point will be expanded on once the Signature Policy technical structure has been introduced.

The elements of the DSP XML specification will now be introduced in a sequential, top to bottom approach – **all technical information in the following section is taken directly from ETSI TR 102 038**.

Namespace Definitions

The following namespace definitions will apply to any DSP:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:ds="http://www.w3.org/2000/02/xmldsig"
xmlns="http://uri.etsi.org/2038/v1.1.1#""
xmlns:xsd="http://www.w3.org/2000/10/XMLSchema"
xmlns:XAdES="http://uri.etsi.org/01903/v1.1.1#"
targetNamespace="http://uri.etsi.org/2038/v1.1.1#"
elementFormDefault="qualified">
```

The SignaturePolicy element

This is the root element of a DSP and its schema definition is as follows:

```
<xsd:element name="SignaturePolicy"
type="SignaturePolicyType"/>
<xsd:complexType name="SignaturePolicyType">
<xsd:sequence>
<xsd:element name="SignPolicyDigestAlg" type="ds:DigestMethodType"/>
<xsd:element ref="ds:Transforms" minOccurs="0"/>
<xsd:element name="SignPolicyInfo" type="SignPolicyInfoType"/>
<xsd:element name="SignPolicyDigest" type="ds:DigestValueType"/>
</xsd:sequence>
</xsd:complexType>
```

The data fields have the following meanings:

SignPolicyInfo: Contains the computer processable information of the signature policy

`SignPolicyDigestAlg`: Indicates the digest algorithm used to compute a digest value for the unique binary encoded value of the definitive form of the signature policy

`ds:Transforms`: Optional element which can be used to specify a chain of transformations that have to be applied to the data before being digested

`SignPolicyDigest`: Contains the aforementioned digest value. The signer shall include it so that I can be verified that the policy selected by the signer is identical to the one being used by the verifier.

`SignPolicyInfo`: Specified below.

The `SignPolicyInfo` **element**

The XML schema of this element is as follows:

```
<xsd:element name="SignPolInfo"
type="SignaturePolicyInfoType"/>
<xsd:complexType name="SignaturePolicyInfoType">
<xsd:sequence>
<xsd:element name="SignPolicyIdentifier"
type="XAdES:ObjectIdentifier"/>
<xsd:element name="DateOfIssue" type="xsd:timeInstant"/>
<xsd:element name="PolicyIssuerName" type="xsd:string"/>
<xsd:element name="FieldOfApplication" type="xsd:string"/>
<xsd:element name="SignatureValidationPolicy"
type="SignatureValidationPolicyType"/>
<xsd:element name="SignPolExtensions"
type="SignPolExtensionsListType minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="SignPolExtensionsListType">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name=SignPolExtension type="XAdES:AnyType"/>
</xsd:sequence>
</xsd:complexType>
```

The data fields have the following meanings:

`SignPolicyIdentifier`: A unique identifier for a Signature Policy

`DateOfIssue`: The date the Signature Policy was issued

`PolicyIssuerName`: Identifier for the body responsible which issued the Signature Policy. It may be used by the signer or verifier to decide if a policy is to be trusted, in which case the signer/verifier shall authenticate the origin of the signature policy as coming from the identified issuer.

`FieldOfApplication:` Defines, in general terms, the general legal/context/application contexts in which the signature policy is to be used and the specific purposes for which the electronic signature is to be applied.

`SignatureValidationPolicy:` Definition of the validation rules, further defined below. Fully processable to allow the validation of electronic signatures issued under that signature policy.

`SigPolExtension:` A set of extensions that can be of any type (i.e. no set definition) This is a data element present in other signature policy elements, but will not be described further as its meaning and type does not change.

The `SignatureValidationPolicy` **element**

The signature validation policy defines a number of rules that have to be followed by both the signer when producing the electronic signature and by the verifier when verifying such an electronic signature. These rules refer to a number of different commitments being supported by electronic signatures produced under the security policy. The XML schema definition for this element is as follows:

```
<xsd:element name="SignatureValidationPolicy"
type="SignatureValidationPolicyType"/>
<xsd:complexType name="SignatureValidationPolicyType">
<xsd:sequence>
<xsd:element name="SigningPeriod" type="TimePeriodType"/>
<xsd:element name="CommonRules" type="CommonRulesType"/>
<xsd:element name="CommitmentRules" type="CommitmentRulesListType"/>
<xsd:element name="SignPolicyExtensions" type="XAdES:AnyType"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="TimePeriodType">
<xsd:sequence>
<xsd:element name="NotBefore" type="xsd:timeInstant"/>
<xsd:element name="NotAfter" type="xsd:timeInstant" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

The data fields are as follows:

`SigningPeriod`: Identifies the date and time before which the signature policy should not be used for creating signatures, and an optional date after which it should not be used for creating signatures.

`CommonRules`: A list of rules to be applied to the commitment types present (defined below).

`Commitment Rules`: A list of specific rules that only apply to certain given commitment types (defined below).

The `CommonRules` **element**

As mentioned above, this element specifies rules that are common to all commitment types. The rules are defined in terms of:

- Rules for signer and verifier (`SignerAndVerifierRules` element)
- Trust conditions for certificates (`SigningCertTrustCondition` element)
- Trust conditions for timestamps (`TimeStampTrustCondition` element)
- Trust conditions for roles (`RoleTrustCondition` element)
- Constraints on Algorithms (`AlgorithmConstraintSet`)

Furthermore, if a field is present in `CommonRules` then the equivalent field shall not be present in any of the `CommitmentRules`. If any of the following fields are not present in `CommonRules` then it shall be present in each `CommitmentRule`:

- `SignerAndVerifierRules`
- `SigningCertTrustCondition`
- `TimeStampTrustCondition`

Finally, the XML schema definition for this element is as follows:

```
<xsd:element name="CommonRules"
type="CommonRulesType"/>
<xsd:complexType name="CommonRulesType">
<xsd:sequence>
<xsd:element name="SignerAndVerifierRules"
type="SignerAndVerifierRulesType" minOccurs="0"/>
<xsd:element name="SigningCertTrustCondition"
type="SigningCertTrustConditionType"
minOccurs="0"/>
<xsd:element name="TimeStampTrustCondition"
type="TimeStampTrustCondition" minOccurs="0"/>
<xsd:element name="RoleTrustCondition"
type="RoleTrustConditionType" minOccurs="0"/>
<xsd:element name="AlgorithmConstraintSet"
type="AlgorithmConstraintSetType" minOccurs="0"/>
<xsd:element name="SIgnPolExtensions"
type="SignPolExtensionsListType" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="SignerAndVerifierRulesType">
<xsd:sequence>
<xsd:element name="SignerRules"
type="SignerRulesType"/>
<xsd:element name="VerifierRules"
type="VerifierRulesType"/>
</xsd:sequence>
</xsd:complexType>
```

The `CommitmentRules` element

This element specifies the validation rules that apply to given commitment types. It is a sequence where each element has the same contents as the `CommonRules` element, plus the `SelCommitmentTypes` element. The XML schema definition is as follows:

```
<xsd:element name="CommitmentRules"
type="CommitmentRulesListType"/>
<xsd:complexType name="CommitmentRulesListType">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name="CommitmentRule" type="CommitmentRuleType"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="CommitmentRuleType">
<xsd:sequence>
<xsd:element name="SelCommitmentTypes"
type="SelectedCommitmentTypes"/>
<xsd:element name="SignerAndVerifierRules"
type="SignerAndVerifierRulesType" minOccurs="0"/>
<xsd:element name="SigningCertTrustCondition"
type="SigningCertTrustConditionType" minOccurs="0"/>
<xsd:element name="TimeStampTrustCondition"
type="TimeStampTrustConditionType" minOccurs="0"/>
<xsd:element name="RoleTrustCondition"
type="RoleTrustConditionType" minOccurs="0"/>
<xsd:element name="AlgorithmConstraintSet"
```

```
type="AlgorithmConstraintSetType" minOccurs="0"/>
<xsd:element name="SignPolExtensions"
type="SignPolExtensionsListType"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

The SelCommitmentTypes **element**

This element is used to indicate the commitment taken by a certain agent under the signature policy being specified. The XML schema definition is as follows:

```
<xsd:element name="SelCommitmentTypes"
type="SelectedCommitmentTypeList"/>
<xsd:complexType name="SelectedCommitmentTypeList">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name="SelCommitmentType"
type="SelectedCommitmentType">
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="SelectedCommitmentType">
<xsd:choice>
<xsd:element name="Empty"/>
<xsd:element name="RecognizedCommitmentType"
type="CommitmentType"/>
</xsd:choice>
</xsd:complexType>
```

The semantics of the list of selected commitments is given in the RecognizedCommitmentType elements.

If a certain SelCommitmentType contains an empty element, it indicates that this rule is applied when a commitment type is not present in the electronic signature (i.e. the type of commitment is indicated in the semantics of the message). Otherwise, the electronic signature shall contain a commitment type indication that shall fit one of the commitment types that are mentioned in the RecognizedCommitmentType elements.

The RecognizedCommitmentType **element**

This element contains the semantics of each of the commitments taken by certain agents under the specified signature policy. The XML schema definition is as follows:

```
<xsd:element name="RecognizedCommitmentType"
type="CommitmentType"/>
<xsd:complexType name="CommitmentType">
<xsd:sequence>
<xsd:element name="CommitmentIdentifier"
type="XAdES:ObjectIdentifierType"/>
<xsd:element name="FieldOfApplication"
type="xsd:string" minOccurs="0"/>
<xsd:element name="Semantics" type="xsd:string"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

- `CommitmentIdentifier` identifies the commitment present in the signature policy
- `FieldOfApplication` and `Semantics` elements define the specific use and meaning of the commitment within the overall field of application defined for the policy

The `SignerRules` **element**

The signer rules identify:
- If the signed objects are external to the Signature element (`ExternalSignedObjects`)
- The signed qualifying properties that shall be provided by the signer under this policy (`MandatedSignedQProperties;` shall include identifier for all required signed qualifying properties)
- The unsigned qualifying properties that shall be provided by the signer under this policy (`MandatedUnsignedQProperties;` shall include identifier for all unsigned qualifying properties)
- Whether the certificate identifiers from the full certification path up to the trust point shall be provided by the signer in the

SigningCertificate   qualifying   property
(MandatedCertificateRef)

- Whether a signer's certificate, or all certificates in the certification path to the trust point, shall be provided by the signer in the `KeyInfo` element of Signature (`MandatedCertificateInfo`)

The XML schema definition of this element is as follows:

```
<xsd:element name="SignerRules"
type="SignerRulesType"/>
<xsd:complexType name="SignerRulesType">
<xsd:sequence>
<xsd:element name="ExternalSignedObjects"
type="xsd:boolean" minOccurs="0"/>
<xsd:element name="MandatedSignedQProperties"
type="QPropertiesListType"/>
<xsd:element name="MandatedUnsignedQProperties"
type="QPropertiesListType"/>
<xsd:element name="MandatedCertificateRef"
type="CertificateReqType"/>
<xsd:element name="MandatedCertificateInfo"
type="CertificateReqType"/>
<xsd:element name="SignPolicyExtensions"
type="SignPolExtensionsListType" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="QPropertiesListType">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name="QPropertyID"
type="xsd:anyURI"/>
</xsd:sequence>
</xsd:complexType>
<xsd:simpleType name="CertificateReqType">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="signerOnly"/>
<xsd:enumeration value="fullPath"/>
</xsd:restriction>
</xsd:simpleType>
```

The `VerifierRules` **element**

This element identifies the unsigned qualifying properties that shall be present under this policy and shall be added to the electronic signature by the verifier, if not added by the signer. The XML schema is as follows:

```
<xsd:element name="VerifierRules"
type="VerifierRulesType"/>
<xsd:complexType name="VerifierRulesType">
```

```
<xsd:sequence>
<xsd:element name="MandatedQUnsignedProperties"
type="QPropertiesListType"/>
<xsd:element name="SignPolicyExtensions"
type="SignPolExtensionsListType" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

The type `QpropertiesListType` is defined in the previous element, whilst `SignPolExtensionsListType` is defined in the `SignPolicyInfo` element.

The `SigningCertTrustCondition` element

This element identifies the trust conditions for certificate path processing used to validate the signing certificate (`SignerTrustTrees` element) and the minimum requirements for revocation information (`CertificateRevReq` element). The XML schema definition is as follows:

```
<xsd:element name="SigningCertTrustCondition"
type="SigningCertTrustConditionType"/>
<xsd:complexType name="SigningCertTrustConditionType">
<xsd:sequence>
<xsd:element name="SignerTrustTrees"
type="CertificateTrustTreesType"/>
<xsd:element name="SignerRevReq"
type="CertificateRevReqType"/>
</xsd:sequence>
</xsd:complexType>
```

The `SignerTrustTrees` element

This element identifies a set of self-signed certificates for the trust points used to start (or end) certificate path processing and the initial conditions for certificate path validation. Therefore, this element is used to define policy for validating the signing certificate, the TSA's certificate and attributes certificates. The XML schema definition for this element is as follows:

```
<xsd:element name="SignerTrustTrees"
type="CertificateTrustTreesType"/>
<xsd:complexType name="CertificateTrustTreesType">
<xsd:sequence maxOccurs="unbounded">
```

```
<xsd:element name="CertificateTrustPoint"
type="CertificateTrustPointType"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="CertificateTrustPointType">
<xsd:sequence>
<xsd:element name="TrustPoint"
type="ds:X509CertificateType"/>
<xsd:element name="PathLenConstraint"
type="xsd:integer" minOccurs="0"/>
<xsd:element name="AcceptablePolicySet"
type="AcceptablePoliciesListType" minOccurs="0"/>
<xsd:element name="NameConstraints"
type="NameConstraintsType" minOccurs="0"/>
<xsd:element name="PolicyConstraints"
type="PolicyConstraintsType" minOccurs="0"/>
</xsd:sequence> ·
</xsd:complexType>
<xsd:complexType name="AcceptablePoliciesListType">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name="AcceptablePolicy"
type="XAdES:ObjectIdentiferType"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="NameConstraintsType">
<xsd:sequence>
<xsd:element name="PermittedSubtrees"
type="GeneralSubTreesListType" minOccurs="0"/>
<xsd:element name="ExcludedSubtrees"
type="GeneralSubTreesListType" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="GeneralSubTreesListType">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name="GeneralSubTree" type="GeneralSubTreeType"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="GeneralSubTreeType">
<xsd:sequence>
<xsd:element name="Base" type="xsd:string"/>
<xsd:element name="Minimum" type="xsd:integer" default="0"/>
<xsd:element name="Maximum" type="xsd:integer" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="PolicyConstraintsType">
<xsd:sequence>
<xsd:element name="RequireExplicitPolicy" type="xsd:integer"
minOccurs="0"/>
<xsd:element name="InhibitExplicitPolicy" type="xsd:integer"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

The data fields have the following requirements:

TrustPoint: gives the self signed certificate for the CA that is used as the trust point for the start of certificate path processing.

`PathLenConstraint`: gives maximum number of CA certificates that may be in a certification path following the trustpoint. A value of 0 indicates that only the given trustpoint certificate and an end-entity certificate may be used. If present, the field value shall be greater than or equal to 0. Where the field is not present, there is no limit to the allowed length of the certification path.

`AcceptablePolicySet`: identifies the initial set of certificate policies, any of which are acceptable under the signature policy.

`NameConstraints`: indicates a name space within which all subject names in subsequent certificates in a certification path shall be loaded.

`PolicyConstraints`: constrains path processing in two ways. It can be used to prohibit policy mapping, or require that each certificate in a path contain an acceptable policy identifier. If present, this element specifies requirements for explicit indication of the certificate policy and/or the constraints on policy mapping.

`InhibitPolicyMapping`: If present, the value indicates the number of additional certificates that may appear in the path (incl. the trustpoint's self certificate) before policy mapping is no longer permitted.

`RequireExplicitPolicy`: If present, subsequent certificates shall include an acceptable policy identifier. The value of the element indicates the number of additional certificates that may appear in the path before an explicit policy is required.

The `SignerRevReq` **element**

This element specifies requirements regarding the checking methods for certificate validity. These rules specify the mandated minimum checks that shall be carried out. Revocation information in the certificate may supersede this element provided it does not conflict with the signature policy revocation rules. The XML schema definition is as follows:

```
<xsd:element name="SignerRevReq" type="CertificateRevReqType"/>
<xsd:complexType name="CertificateRevReqType">
<xsd:sequence>
```

```
<xsd:element name="EndRevReq" type="RevocationReqType"/>
<xsd:element name="CACerts" type="RevocationReqType"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="RevocationReqType">
<xsd:sequence>
<xsd:element name="EnuRevReq"
type="EnuRevReqType"/>
<xsd:element name="exRevReq" type="SignPolExtensionsListType"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:simpleType name="EnuRevReqType">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="clrcheck"/>
<xsd:enumeration value="ocspcheck"/>
<xsd:enumeration value="bothcheck"/>
<xsd:enumeration value="eithercheck"/>
<xsd:enumeration value="nocheck"/>
<xsd:enumeration value="other"/>
</xsd:restriction>
</xsd:simpleType>
```

Certificate revocation requirements are specified in terms of checks required on:

- End certificates (e.g. signer's certificate, attribute certificate, timestamping authority certificate)
- CA certificates

Revocation requirements are specified in terms of:

- `clrCheck` (check against current Certificate Revocation Lists)
- `ocspCheck` (check using Online Certificate Status Protocol)
- `bothCheck` (check using both methods)
- `eitherCheck` (check using either CRL or OCSP check)
- `noCheck` (no check is mandated)

The `TimeStampTrustCondition` element

This element identifies trust conditions for certificate path processing used to authenticate the timestamping authority and constraints on the name of the timestamping authority. The XML schema definition is as follows:

```
<xsd:element name="TimeStampTrustCondition"
```

```
type="TimeStampTrustConditionType"/>
<xsd:complexType name="TimeStampTrustConditionType">
<xsd:sequence>
<xsd:element name="TtsCertificateTrustTrees"
type="CertificateTrustTreesType" minOccurs="0"/>
<xsd:element name="TtsRevReq" type="CertificateRevReqType"
minOccurs="0"/>
<xsd:element name="TtsNameConstraints" type="NameConstraintsType"
minOccurs="0"/>
<xsd:element name="CautionPeriod" type="DeltaTimeType"
minOccurs="0"/>
<xsd:element name="SignatureTimeStampDelay" type="DeltaTimeType"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="DeltaTimeType">
<xsd:sequence>
<xsd:element name="DeltaSeconds" type="xsd:integer"/>
<xsd:element name="DeltaMinutes" type="xsd:integer"/>
<xsd:element name="DeltaHours" type="xsd:integer"/>
<xsd:element name="DeltaDays" type="xsd:integer"/>
</xsd:sequence>
</xsd:complexType>
```

If `TtsCertificateTrustTrees` element is not present then the same rule as defined in Signing `CertTrustCondition` element applies to certification of the timestamping authority's public key.

The `TsRevReq` element specifies minimum requirements for revocation information, obtained through CRL and/or OCSP responses, to be used in checking the revocation status of the time stamp that shall be present in the signature.

If `TtsNameConstraints` is not present then there are no additional naming constraints on the trusted timestamping authority other than those implied by `TtsCertificateTrustTrees` element.

The `CautionPeriod` element specifies a caution period after the signing time that it is mandated the verifier shall wait to get high assurance of the validity of the signer's key and that any relevant revocation has been notified. The revocation status information forming an ES-C shall not be collected and used to validate the electronic signature until after this caution period.

The `SignatureTimeStampDelay` element specifies a maximum acceptable time between the signing time and the time at which the signature timestamp, as used to form the ES-T, is created for the verifier.

The `RoleTrustCondition` **element**

This element specifies whether claimed or certified roles are permitted under the signature policy. The element's XML schema definition is as follows:

```
<xsd:element name="RoleTrustCondition"
type="RoleTrustConditionType"/>
<xsd:complexType name="RoleTrustConditionType">
<xsd:sequence>
<xsd:element name="RoleMandated" type="xsd:boolean"/>
<xsd:element name="HowCertRole" type="HowCertRoleType"/>
<xsd:element name="AttrCertTrustTrees"
type="CertificateTrustTreesType" minOccurs="0"/>
<xsd:element name="RoleRevReq" type="CertificateRevReqType"
minOccurs="0"/>
<xsd:element name="RoleConstraints" type="RoleConstraintsType"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:simpleType name="HowCertRoleType">
<xsd:restriction base="xsd:string">
<xsd:enumeration value="ClaimedRole"/>
<xsd:enumeration value="CertifiedRole"/>
<xsd:enumeration value="Either"/>
</xsd:restriction>
</xsd:simpleType>
<xsd:complexType name="RoleConstraintsType">
<xsd:sequence >
<xsd:element name="RoleTypeConstraint"
type="XAdES:ObjectIdentifierType" minOccurs="0"
maxOccurs="unbounded"/>
<xsd:element name="RoleValueConstraint" type="XAdES:AnyType"
minOccurs="0" maxOccurs="unbounded"/>
</xsd:sequence>
</xsd:complexType>
```

If `RoleTrustCondition` is not present, then any certified roles within an attribute certificate may not be considered to be valid under the validation policy.

If `RoleMandated` is TRUE, then a role, certified within the following constraints, shall be present. If FALSE, then the signature is still valid if no role is specified.

The HowCertRole element specifies how the roles must appear with the signature – uncertified claimed roles, or certifies roles within an attribute certificate, or either.

The AttrCertTrustTrees element specifies certificate path conditions for any attribute certificate. If not present the same rules apply as in SigningCertTrustCondition.

The RoleRevReq element specifies minimum requirements for revocation information, obtained through CRL and/or OCSP responses, to be used in checking the revocation status of attribute certificates, if any are present.

If RoleConstraints is not present, then there are no constraints on the roles. That may be validated under this policy.

If a RoleTypeConstraint element is present within the RoleConstraints element, it specifies a role type that is considered valid under the signature policy. Any value for that role is considered valid.

If a RoleValueConstraint is present within the RoleConstraints element, it specifies a specific role value that is considered valid under the signature policy.

The AlgorithmConstraintSet **element**

If this element is present, it identifies the permitted signing algorithms (hash and encryption algorithms) that may be used for the specified purpose, as well as specifying the permitted key lengths. If this element is not present, there are no constraints on algorithm and key length.

The XML schema of this element is as follows:

```
<xsd:element name="AlgorithmConstraintSet"
type="AlgorithmConstraintSetType"/>
<xsd:complexType name="AlgorithmConstraintSetType">
<xsd:sequence>
<xsd:element name="SignerAlgConstraints"
type="AlgConstraintsListType" minOccurs="0"/>
<xsd:element name="EeCertAlgConstraints"
type="AlgConstraintsListType" minOccurs="0"/>
<xsd:element name="CACertAlgConstraints"
```

```
type="AlgConstraintsListType" minOccurs="0"/>
<xsd:element name="AaCertAlgConstraints"
type="AlgConstraintsListType" minOccurs="0"/>
<xsd:element name="TSACertAlgConstraints"
type="AlgConstraintsListType" minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="AlgConstraintsListType">
<xsd:sequence maxOccurs="unbounded">
<xsd:element name="AlgAndLength" type="AlgAndLengthType"/>
</xsd:sequence>
</xsd:complexType>
<xsd:complexType name="AlgAndLengthType">
<xsd:sequence>
<xsd:element name="AlgId" type="xsd:anyUri"/>
<xsd:element name="MinKeyLength" type="xsd:integer" minOccurs="0"/>
<xsd:element name="Other" type="SignPolExtensionsListType"
minOccurs="0"/>
</xsd:sequence>
</xsd:complexType>
```

This summarises the discussion of the individual elements in a DSP adhering to the ETSI TR 102 038 standard.

Appendix D: BPM Notation Extra Details

D.1: Acts
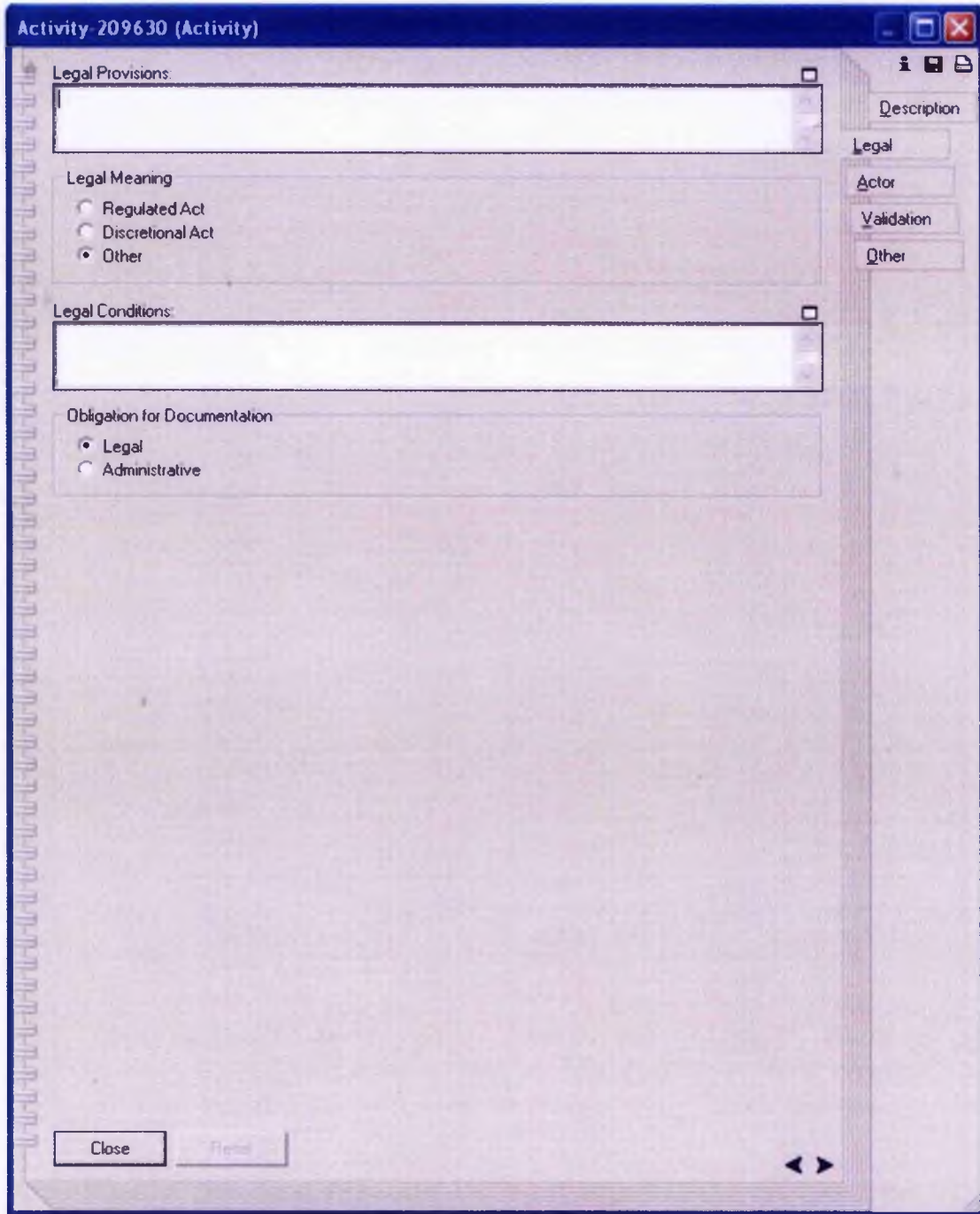
Figure D-1: Acts Notebook, Legal Tab

Figure D-1 represents the contents of the "Legal" tab, which in turn represents question 2 of the Acts part of the PADS questionnaire (see Table 4-1) and is therefore entirely concerned with the regulations that are applicable to a specific act. The information caught and represented by this element can therefore be summarised as follows:

- Identification of the Legal Provisions; representation mechanisms other than textboxes are too awkward, as the law is huge and changes constantly.
- The legal meaning of the act
- Legal conditions that must have been met for the act to be performed – as before, textbox offers the greatest flexibility
- Legal obligation to document the act

Figure D-2: Acts Notebook, Actor Tab

Figure D-2 shows the contents of the "Actor" tab in the Acts notebook, which concerns itself with contextual information relating to the actor of the act. This tab addresses questions 4 and 5 of the PADS questionnaire. The information in this tab is relevant for the permissions that are governed by a

signature policy. The information in this tab consists of two major areas, Legal Quality of Person Acting, and Personal Substitution. Since an actor can only be of one legal quality, and since an Act can have only one type of substitution regulation, all selections are as radio buttons. However, a text box for specific attributes has been added to allow for further information to be encoded when the actor has to have a specific attribute to execute the Act.
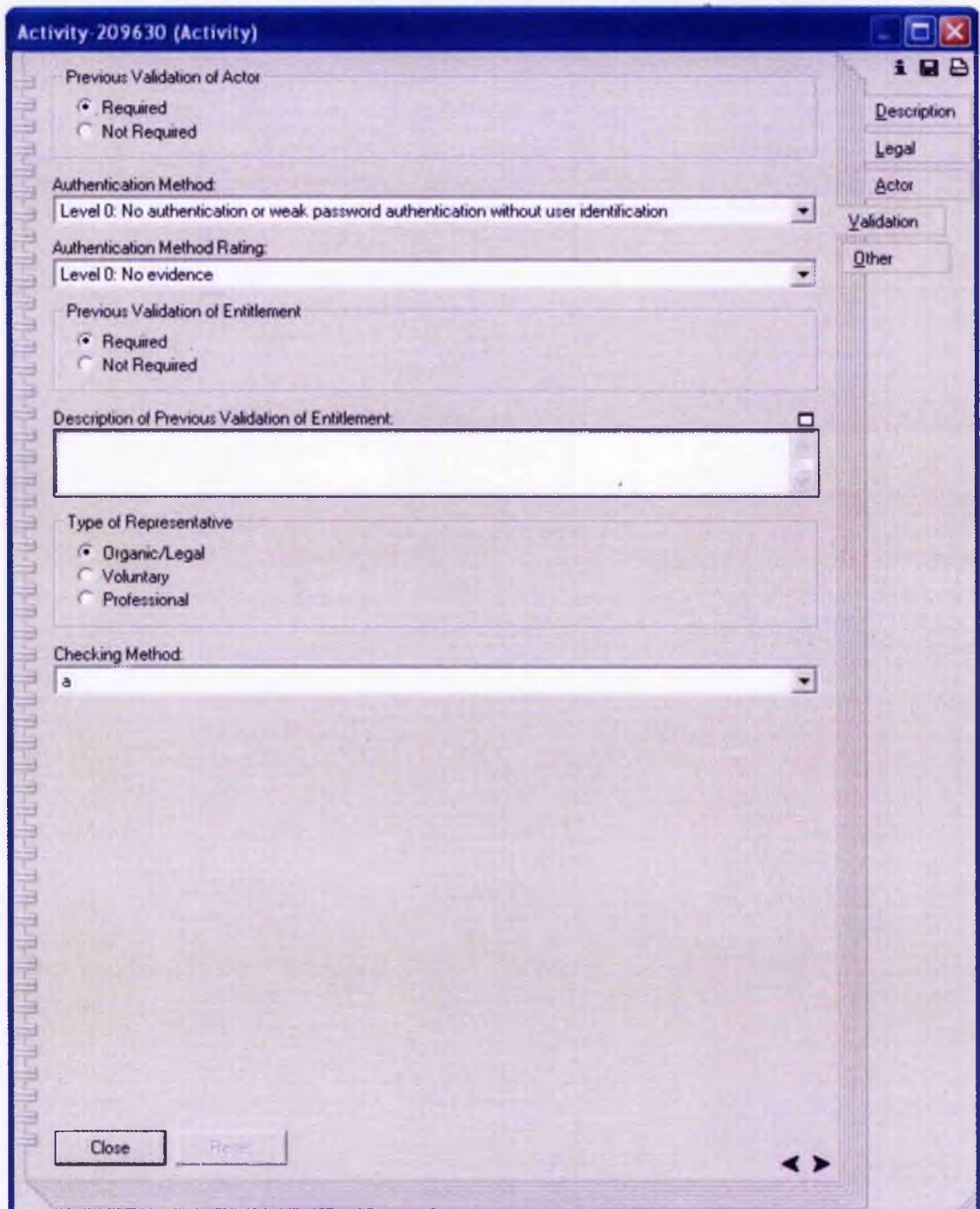
Figure D-3: Acts Notebook, Validation Tab

Figure D-3 shows the content of the "Validation" tab of the Acts notebook, which addresses items 7 and 8 of the Acts section of the PADS questionnaire. As such, it is concerned with the validation of actors and their entitlements.

Item 7 firstly establishes whether validation of the actor is required or not (through using Radio Buttons in the graphical methodology) – should it be required, it then allows the user to select the method by which the actor is to be authenticated, and the strength of the authentication method to be used. These are drop-down menus since there will only be a select few methods used by CATCERT – these methods were defined by CATCERT as follows:

Authentication Methods:
- Level 0: No authentication or weak password authentication without user identification
- Level 1: User and password with user identification
- Level 2: User and password with user identification as SSL Server authentication
- Level 3: Digital Signature
- Level 4: Digital Signature using recognised digital certificates
- Level 5: Digital Signature with verification data
- Level 6: Digital Signature with timestamp

Authentication Method Ratings:
- Level 0: No evidence
- Level 1: Evidence of Entity
- Level 2: Evidence of Data Source
- Level 3: Evidence of Document Authenticity
- Level 4: Digital Signature Evidence Level
- Level 5: Complete Digital Signature Evidence
- Level 6: Long Duration Digital Signature Evidence

Item 8, which deals with entitlement, queries the user as to whether the previous validation of entitlement is required or not (again, through radio buttons). Should validation of entitlement be required, then the type of representation that needs to be checked needs to be selected, followed by providing a textual description of the previous validation of Entitlement.

Thus, this tab establishes whether validations and authentications of actor and entitlement are required to take place, and if yes, the method by which they are validated or authenticated can be specified.
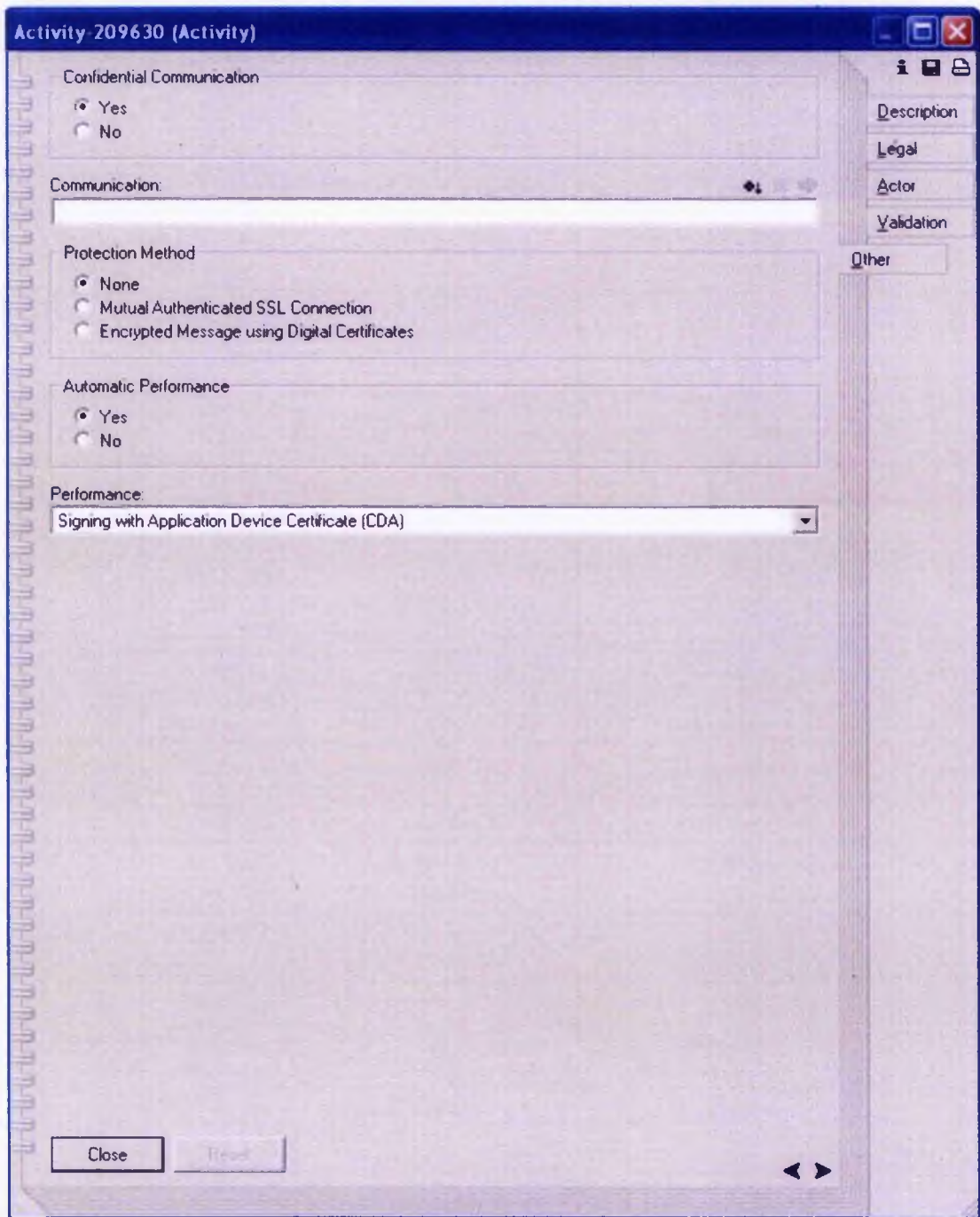
Figure D-4: Acts Notebook, Other Tab

Figure D-4 shows the contents of the "Other" tab, which is data that relates to the process itself. As can be seen from the figure, it takes account of items 9 and 10 of the Acts section of the PADS questionnaire.

Item 9 deals with the question of whether confidential communication is required; should it be required, the box describing the process/act (and thus containing the particular instance of the notebook) is changed in appearance through the addition of a little padlock in the bottom-left corner. Therefore, simply from a quick glance at the model it can be established where secure communications are required. Also, the "link" control (which provides a link to a different Adonis Process Model using the same notation and library) allows the user to link to a PADS process model depicting the communication process. Furthermore, a set of radio buttons are provided to indicate whether the Confidential Communication uses any kind of protection mechanisms to secure this communication.

Item 10, on the other hand, is concerned with whether the process of signing is automated or manually handled. Again, selecting either option will result in a change of the process box; automated performance will result in the display of a computer icon at the bottom-right of the box, whilst manual performance will result in the display of a 'sticky man' in the same place. If it is automatic signing, then the user has to specify whether the signing process adds an 'Application Device Certificate (CDA)' to the signature or not; if it is not automated signing, then "No Signing" can be selected with the drop-down menu.

This concludes the implementation of the Acts section of the PADS questionnaire. The next section to be discussed is the section of Documents.

D.2: Documents

Figure D-5: Documents Notebook – General Tab

Figure D-5 shows the contents of the "General" tab of the notebook that gets called up when double-clicking on a Document symbol. This tab accounts for questions 1 and 5 in the Documents section of the PADS questionnaire.

The textbox allows the entering of a general purpose description of a document. It is imperative that the first entry within this textbox is an exact copy of the name of the Act that this document gets signed by! This is to be

able to link a Document and an Act together. It is possible to add any string after the Act name to the description box, but the Act name must always be the first entry if the document is being signed by that act. This is another workaround to overcome the limitations of the tool.

Also, the type of document type can be specified through radio buttons, as it can only be of one type.

The documents' life –and archival times can also be set, and drop-down menus are used as Catalonia has different archival times for different documents, all of which ought to be specified in law.

The radio buttons denoting the type of document serve to select the correct graphic for the document symbol. Therefore, selecting "New Document" results in the appropriate symbol being displayed in the graphical overview of the workflow.
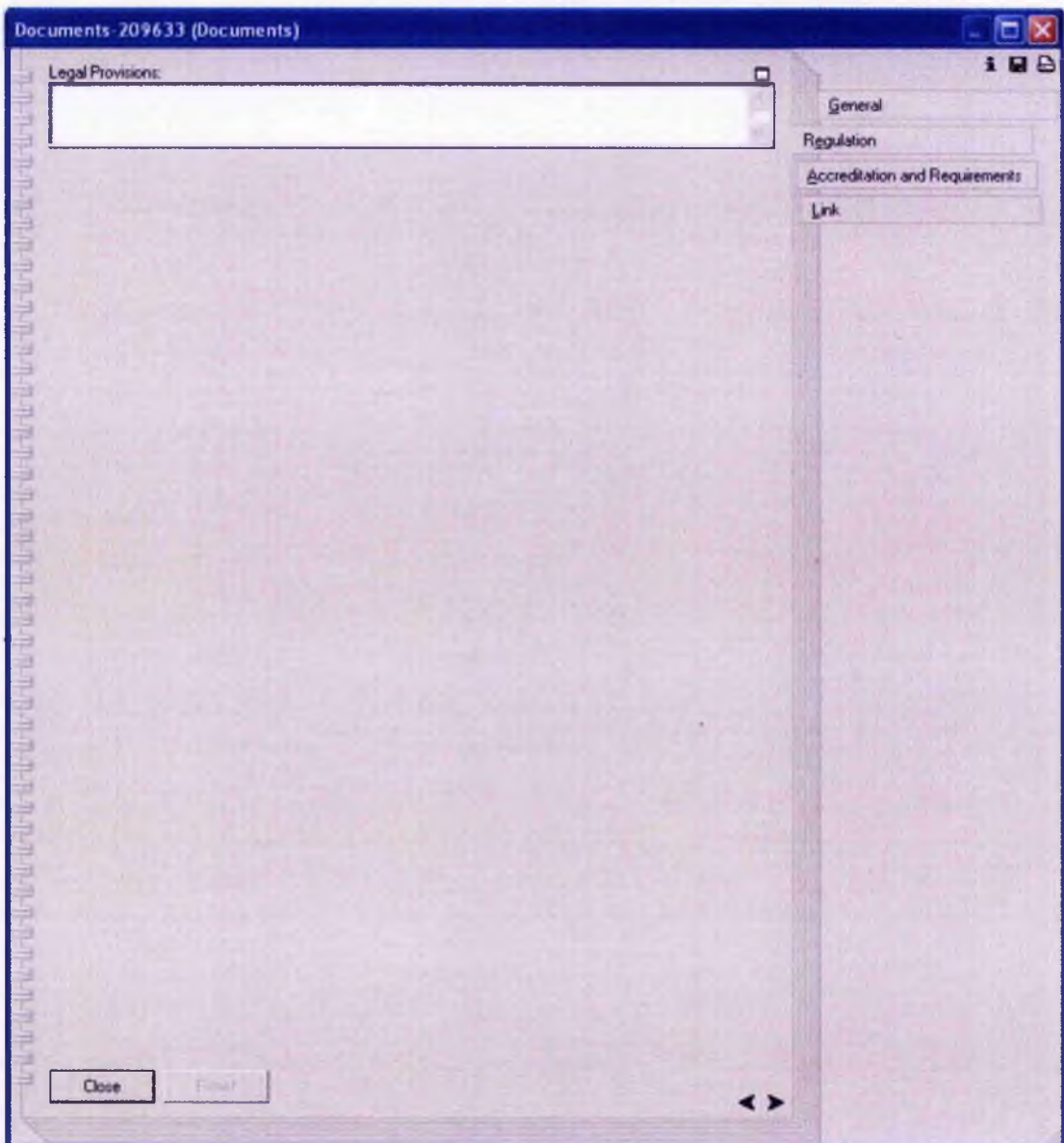
Figure D-6: Documents Notebook – Regulation Tab

The above Figure D-6 shows the contents of the Regulation tab, which encapsulates question 2 of the Documents section of the PADS questionnaire. This question centres on Legal Provisions affecting and regulating the document and its use. The textbox contains textual information relating to Legal Provisions that govern the use of this document.

Figure D-7: Documents Notebook – Accreditation & Requirements Tab

Figure D-7 shows the contents of the "Accreditation and Requirements" tab, which addresses questions 3 and 4 of the Documents section of the PADS questionnaire. Question 3 deals with a range of formal requirements with regards to document authenticity, which can be selected with radio buttons, whilst question 4 enquires on content accreditation requirements and provides the ability to select different options via tick boxes (as more than one, or none, can be applicable).

Documents can be one of three types: original, simple copy, authenticated copy, and since only one of these can apply, radio buttons were chosen as a selection method.

On the other hand, the requirement for a signature is optional, hence the use of a tick box. Furthermore, a document can be marked, stamped, sealed or a combination thereof, hence again the use of tick boxes.

The need for a timestamp is also optional, therefore again a tick box indicating this requirement, whilst a tick box for role enables the user to enter a role or personal attribute in the text box that specifies what that role requirement actually is.

As for the accreditation requirements, there are three distinct possibilities for these, and it is also possible for a document not to have any accreditation requirements, hence the use of tick boxes allows for the greatest amount of flexibility.

This leaves the final tab, the "Link" tab. This entry contains an intra-model link to the document flow model of a particular document.
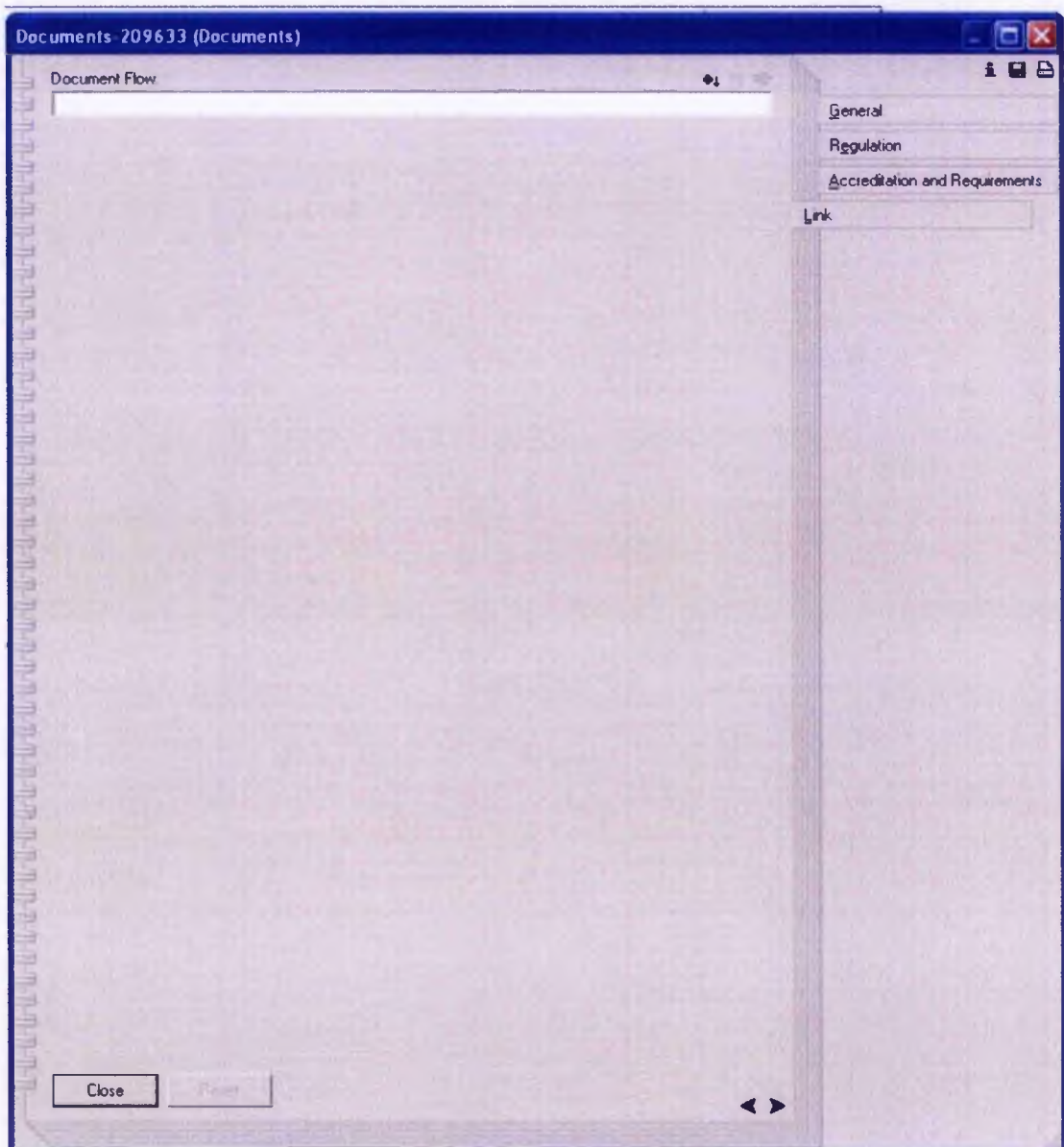
Figure D-8: Documents Notebook – Link Tab

The above figure shows the active "Link" tab. The only entry in this tab is an Adonis "Model Link" control, which allows the user to link to a different model (a Document State Change model) and then, by clicking the arrow pointing to the right, it is possible to follow that link. This allows the user to follow a particular document's passage through a legal workflow.

This concludes the description of the Documents section of the graphical version of the PADS questionnaire. This leaves one section remaining, that of Signatures.

D.3: Signatures
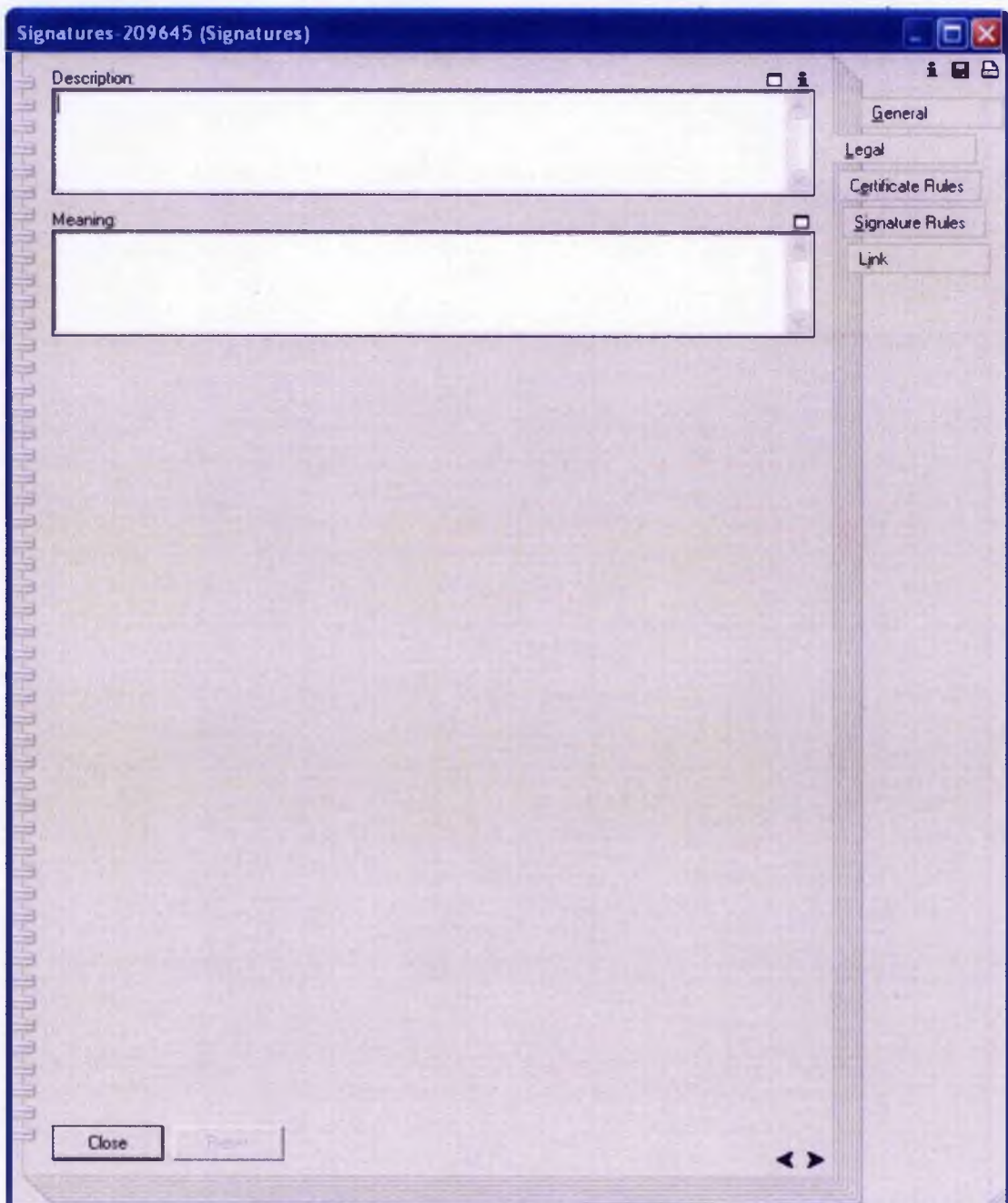
Figure D-9: Signature Notebook – Legal Tab

The above figure addresses question 1 of the Signatures section of the PADS questionnaire and offers textbox facilities to enter the legal description and legal meaning of the digital signature in question. It is pertinent that the first entry within the Description box is the name of the Act (exact character match) that 'consumes' the signature in a signing process, in order to 'link' the signature with the relevant Act. This is due to a workaround to overcome the limitations of the tool.
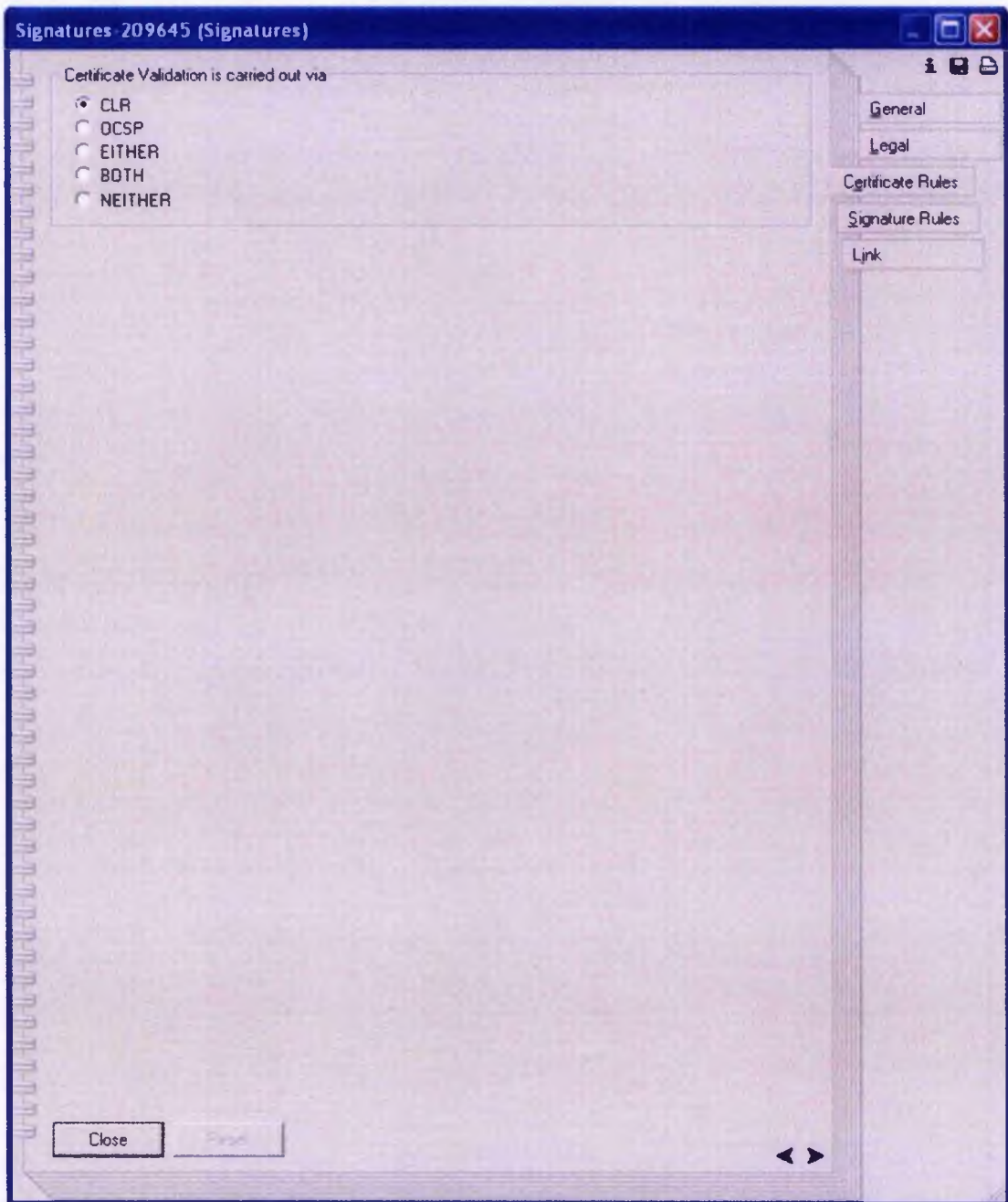
Figure D-10: Signature Notebook – Certificate Rules Tab

The above figure shows the contents of the "Certification Rules" tab. It addresses the question of the Signature section of the PADS questionnaire which concerns itself with the certificate validation mechanisms. The certificate validation mechanism can be selected via a range of radio buttons,

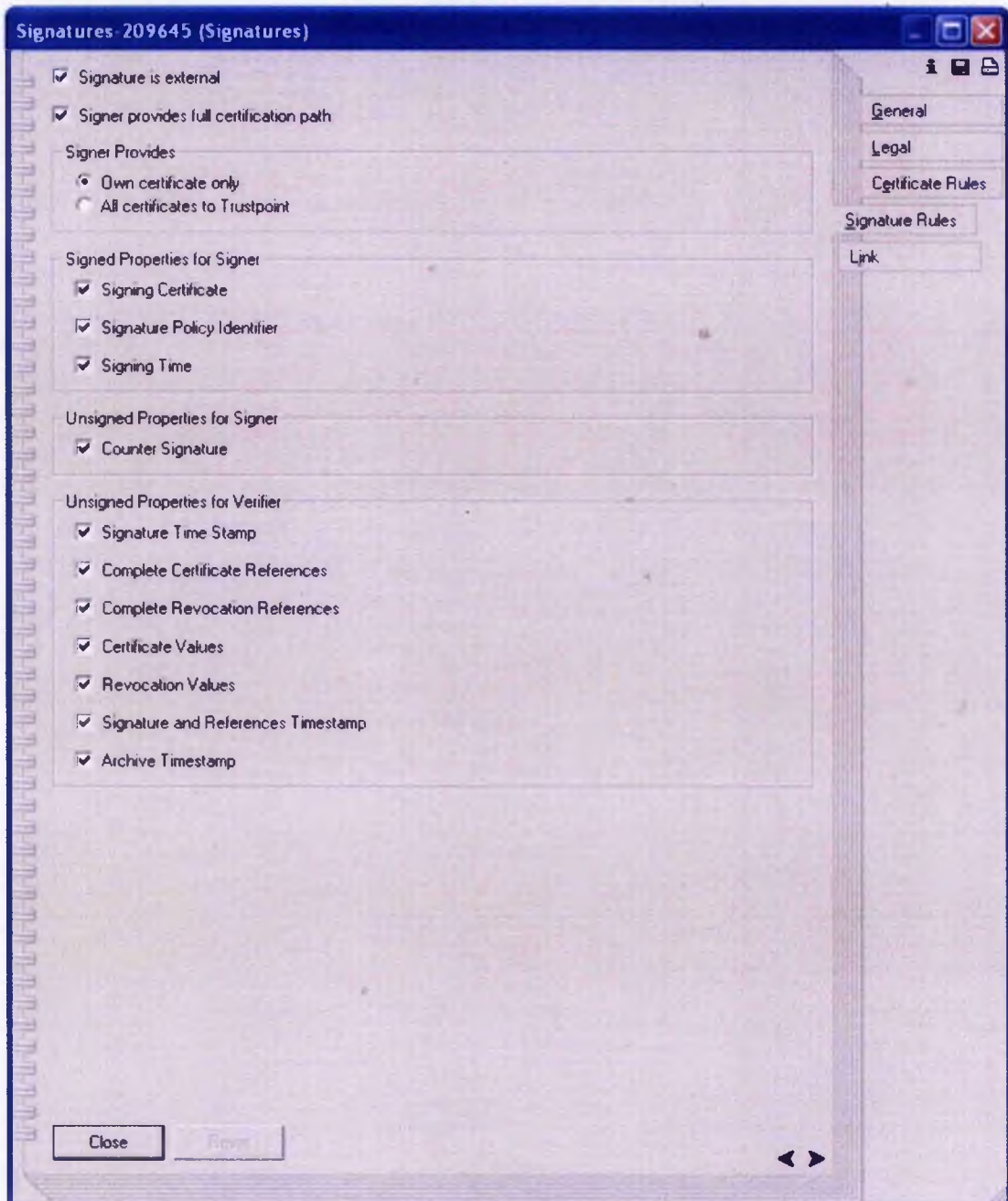since only one value is possible. It is assumed that the certificate validation mechanisms apply to both Signer certificate and CA certificate.

Figure D-11: Signature Notebook – Signature Rules Tab

The above figure shows the content of the "Signature Rules" tab, which covers questions 6 to 9 from the Signature section of the PADS questionnaire.

Question 6 investigates whether the Digital Signature is to be external from the objects it signed or not, hence the use of a tick box.

Question 7 addresses whether the signer is to provide the full certification path or not (using the tick box provided) and whether the signer is to provide his own certificate only, or all certificates up to the trust point (selectable through the provided radio buttons).

Also, it can be specified whether the signer is bound by any signed and/or unsigned properties – if he is bound, they can be selected via the provided tick boxes. The properties are defined in another ETSI specification, namely ETSI TS 101 733.

Furthermore, it might be the case that the verifier is required to abide to unsigned properties, which can also be selected via the provided tick boxes. As the signer properties, these were also defined in ETSI TS 101 733.

This leaves the final tab, the "Link" tab. This entry contains an intra-model link to the signature flow model of a particular signature. The make-up and functionality of this type of model is explained in the later chapter on state change models – please refer to it to understand the model that this link links to. The looks of this tab are the same as the same tab in the documents section – please refer to Figure D-8 for the looks of this tab.

As can be seen, there is the possibility to add a link to the model that shows the flow and state-change of a particular signature. This allows the user to follow a particular signature's passage through a legal workflow.

Thus, all necessary and relevant information is captured through the various elements of the graphical version of the extended PADS methodology.

D.4: Other Aspects of the Process Modelling Notation

Sub-processes

As has been shown in Figure 4-8, the main model view captures all Processes, Acts, Documents and Signatures involved in a legal workflow. However, the provided example is very simple. In some cases, legal workflows can contain

dozens of acts and processes, which would clutter and obscure the main model view such that it would not be readable anymore. In order to account for such scenarios, the concept of a sub-process is introduced. A sub-process means that a model can 'hide' complex functionality behind a symbol in order to ease the reading of a model (Dennis and Wixom, 2000). Analogies are sub-routines from the area of programming, or the use of "levels" from the systems design domain. In the graphical version of PADS, sub-processes shall be represented by a grey triangle. Within Adonis, clicking on the triangle shall allow the user to 'dive' into the lower level of the model and view more complex functionality than what is displayed on the higher level. One example of sub-processes is provided in Figure 4-8, labelled "Unrelated Activities"; this could be related to the actual processing of the application form 'within' other departments in Authority B. To further illustrate the point, please refer to the figure below.
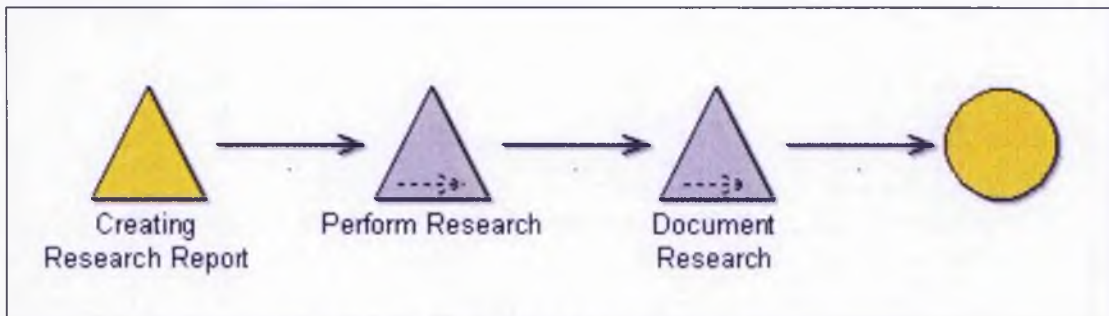

Figure D-12: An Example of Sub-processes

Figure D-12 shows a process consisting of two sub-processes, labelled "Perform Research" and "Document Research". This process 'hides' the complex functionality of actually performing research (a very complicated process!) and also the complex functionality of documenting research. Without the sub-processes, the resulting process model would be extremely complex and difficult to understand quickly, thus negating the advantage of using a graphical process modelling methodology. Therefore, the ability of sub-processes to 'hide' complexity but still retaining information about these complicated activities taking place is of invaluable advantage for future models, where complexity can be organised between several layers of detail.

However, there is still a need to be able to capture the state change of a document or a signature through the workflow. Whilst the above main view allows one to view the use of all documents and signatures, it does not allow a view of a single signature or document. Therefore, a new model is proposed, namely a "State Change Model", which is introduced in the next section.

State Change Model

As stated above, there is a need to capture the state change of a document or a signature as it is affected by a process or act. Therefore, one state change model for each document and signature used has to be created. These models are linked to using the "Link" tab in the document/signature notebooks, as explained above. The resulting model will be the main view model, but without any documents or signatures; instead, each process affecting a document or a signature will be followed by a state-change element, informing a user of how the document/signature was changed by that particular element. In order to demonstrate this concept, the sample process introduced in the previous chapter (see Figure 4-8) shall serve as a demonstrator for the state change model. The element whose state change is to be monitored is the main document used throughout the process.

Figure D-13: State-change Model

Figure D-13 shows the State Change Model of the main document used in the sample process in Figure 4-8. This State Change Model is specific to each individual document or signature, therefore each document and each signature will all have one individual State Change Model each. Only one State Change Model is shown.

Every time the document in question is affected by a process, Adonis will add a state change symbol, the white circles with the number within. The state change symbol is then required to capture what the state change was – therefore, after the very first process, the document's state change occurred through the document's creation. In the next process in Entity 2, the document was then signed. This continues for all processes that affected the document. The numbers represent the order of the state changes (it is optional to enter this information).

A state change model for the signature used by Entity 2 would contain just one state change symbol, which would be placed right after the use of the signature. Or to put it differently, the total number of state change models for the sample process in Figure 4-8 is six – two documents, and four signatures all underwent a state change.

These State Change Models thus capture the document and signature flow of individual documents throughout a complete legal workflow and provide a good overview of how each document and signature are affected individually by individual processes and acts.

Appendix E: Transformation Software Technical Details

E.1 User Guide

A pre-condition for the use of the Transformation Software is that the relevant legal workflow has been exported from ADONIS.

Once this has been performed, the software can be launched and the user will experience the main screen, which is shown in the figure below.
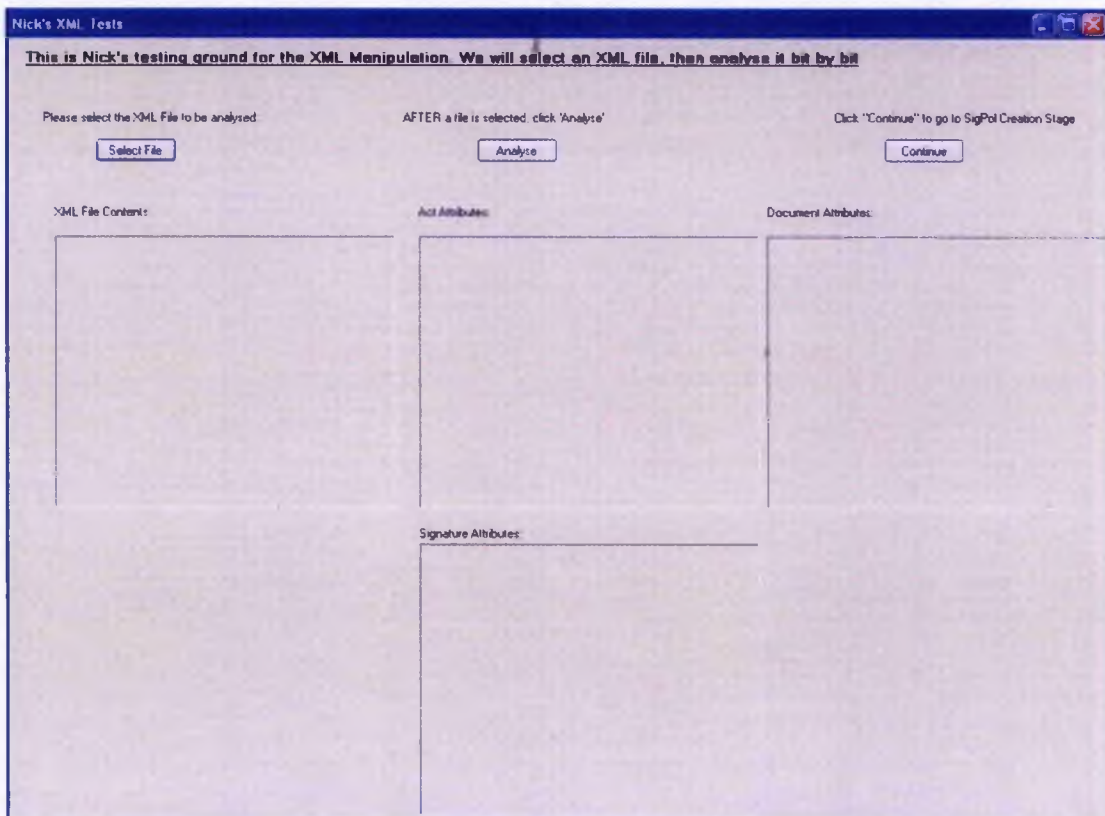

Figure E-1: The initial screen of the transformation software

The software was implemented with a minimal amount of functions and options, in order to keep the learning curve and complexity low. The reasoning behind this decision was the fact that along with the improved method for creating DSPs, CATCERT had an aspiration to assign the process of DSP creation to non-specialist office workers without knowledge of XML or

the DSP syntax. As a result, the decision was made to simplify the interface as far as possible. The simple interface means that the buttons must be pressed in the correct sequence (left to right) in order for the transformation to go ahead.

Therefore, the first button to be pressed is the "Select File" button, which will be used to locate the created XML model of the ADONIS workflow model. Clicking it results in a screen like the one shown in the next figure.
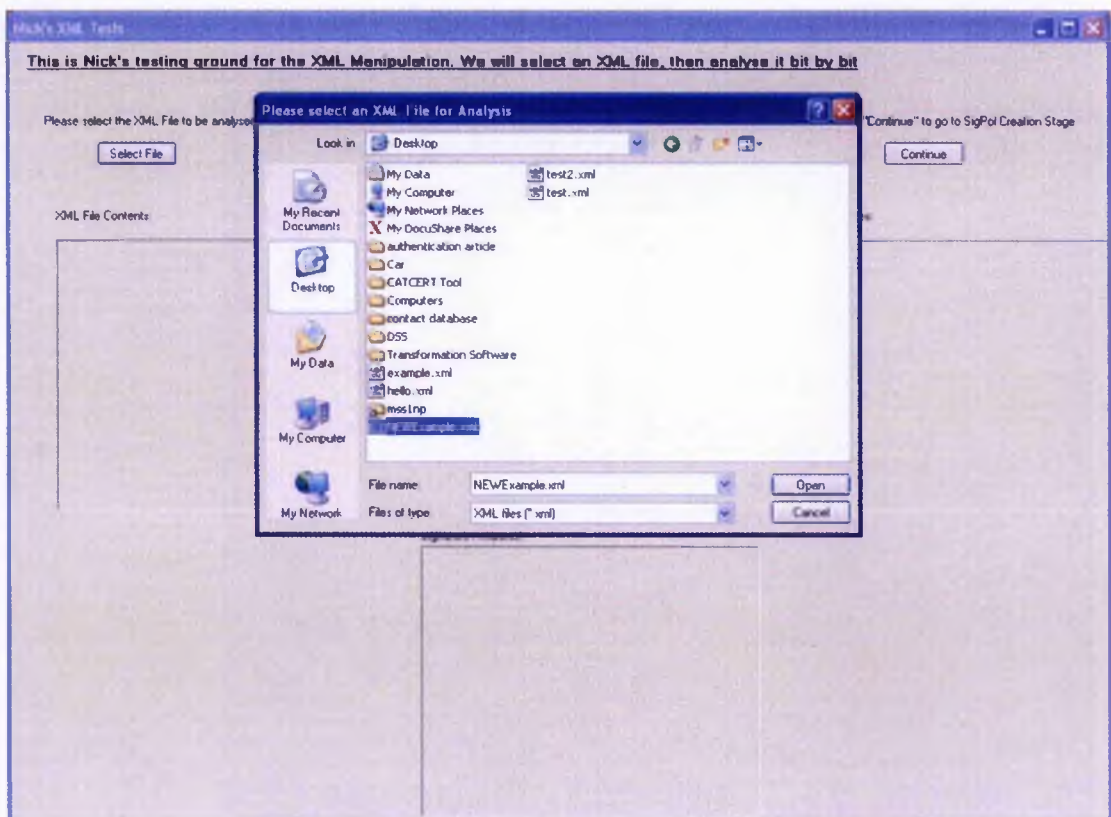

Figure E-2: The user selects a process model

As can be seen, clicking the "Select File" button opens the standard Windows "Open File" dialogue. Use the dialogue to select the correct model. On clicking "Open" in this dialogue, the main screen of the transformation software changes as follows:
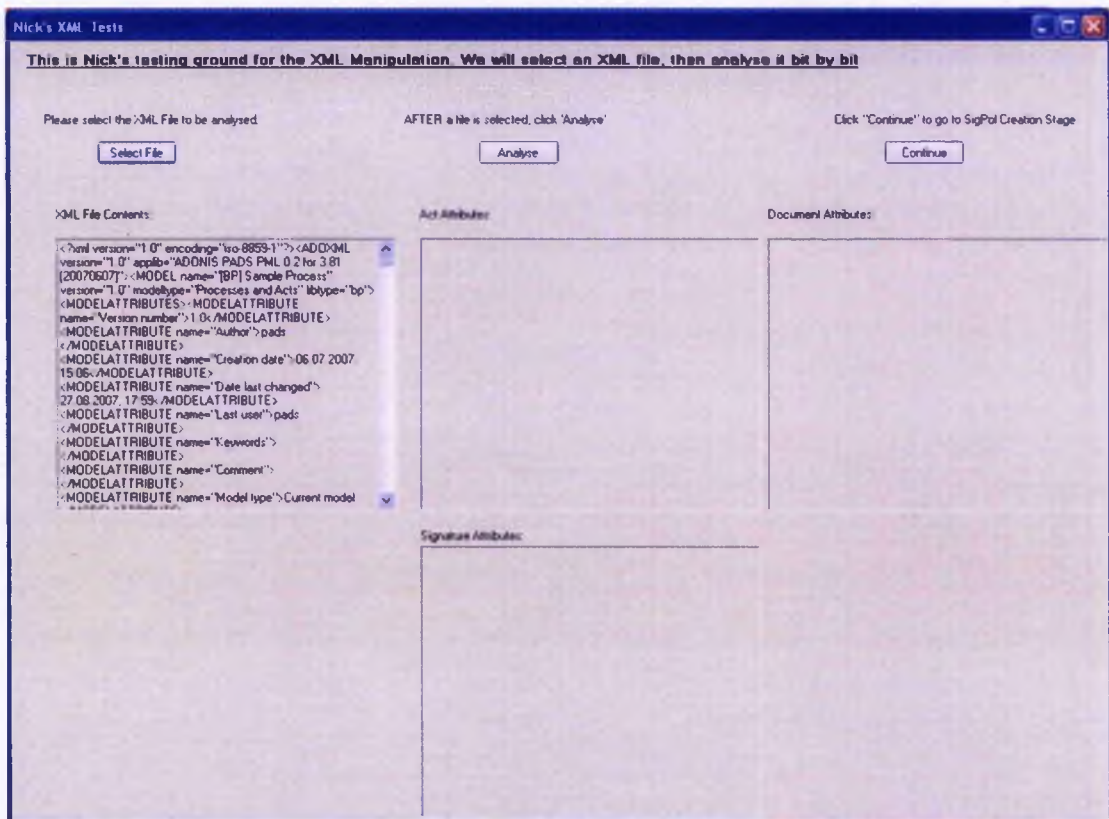
Figure E-3: The Transformation Software has successfully opened the process model XML file

The selected file is opened and the contents of the XML file are copied into the first text box of the transformation software. The text box is read-only to prevent the user from inserting comments; the text box is used as a diagnostic tool, to give the user the ability to inspect the opened XML file. It is also computationally more effective to perform one I/O operation to load the file into memory and only then manipulate it, rather than applying the manipulation operations as the file is being opened.

With the file opened and present in the text box, the user can then press the "Analyse" button to perform an analysis of the XML file. The analysis routine examines the loaded XML file and separates unwanted data (ADONIS specific data) from wanted data; wanted data (the Acts, Documents and Signatures present within the workflow, as well as their associated Notebook entries) is then placed within the individual text boxes. Again, these text boxes are read-

only. The outcome of pressing the "Analyse" button is shown in the figure below.
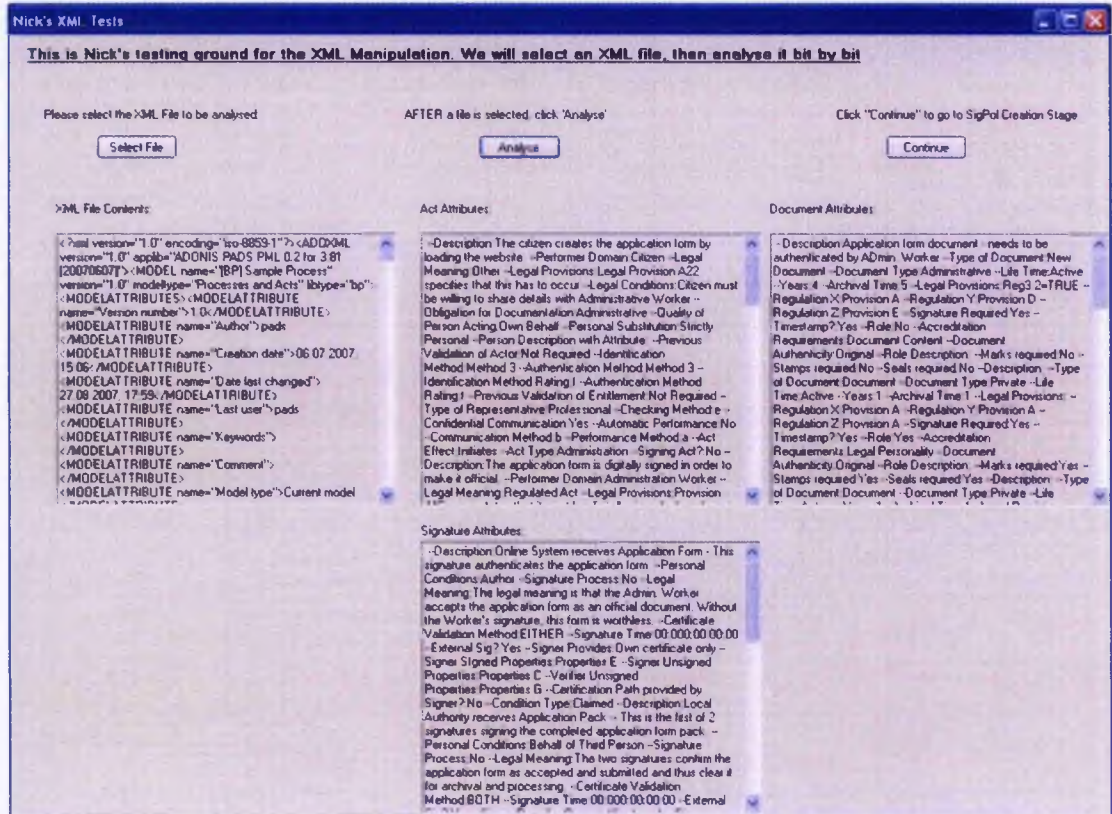

Figure E-4: The Transformation Software has analysed and decomposed the process model into the PADS component parts of Act, Document and Signature

As can be seen, the data is segregated by source (Act, Document, Signature) and by data type (Description, Performer Domain, other source specific data). This allows easy inspection of the data, if wanted by the user. The population of the text boxes also serves as an indication that the analysis phase has been completed, and that the software is ready to continue with the next step, which is the pressing of the "Continue" button. Pressing the "Continue" button loads the screen shown below.

Figure E-5: The Transformation Software has identified signing processes and requires the
user to select which Signature Policy ought to be created

The new screen presents a list of "signing acts", i.e. a list of Acts that sign a
document one or more times. Since DSPs are applied to govern and describe
signatures, it makes no sense to have DSPs for Acts that do not result in
signing (thus, use of digital signatures), therefore non-signing Acts are
discarded from this list. In order to select a signing Act for which a DSP is to
be created, the user must select an Act in the combo box. The Act name will
be highlighted, the Act name will also be copied into the button on the right,
and the number of signatures used by an act is shown below the combo box.
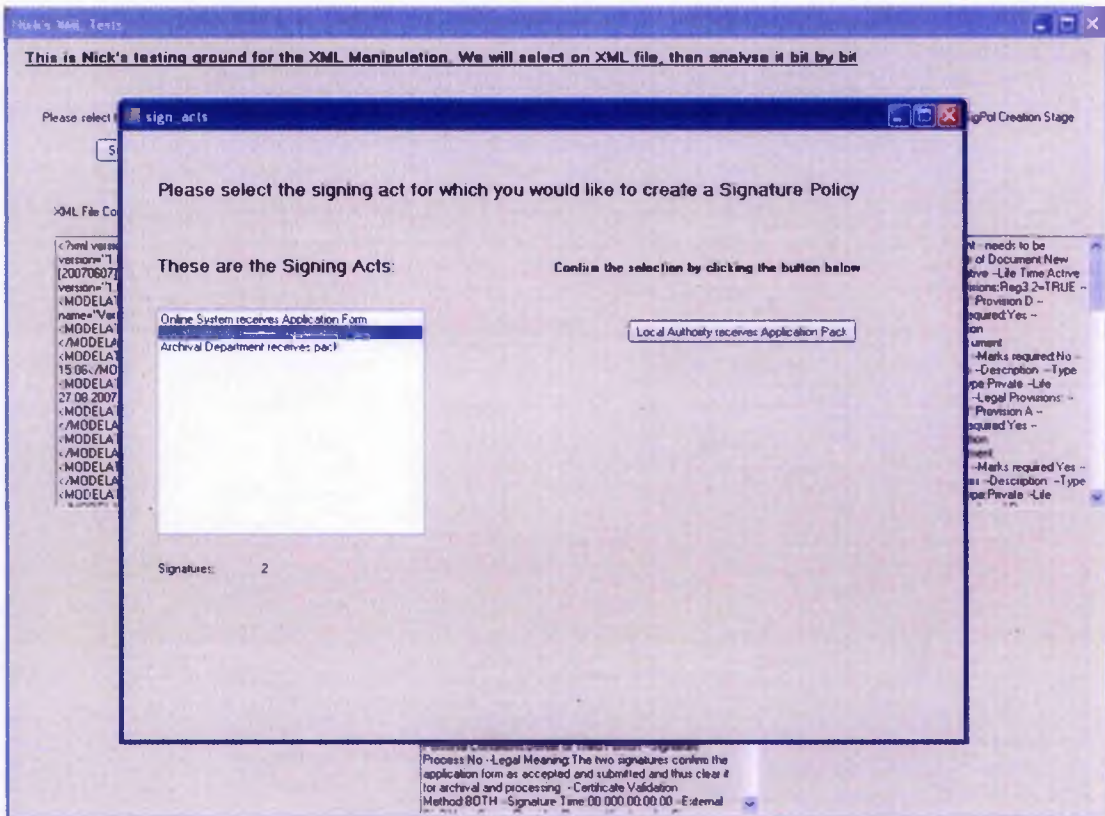In other words, the screen would look like the screen in the figure below.

Figure E-6: Confirming the selection

As can be seen, the selected Act's name was copied into the button on the right, and the number of signatures is shown below the combo box. At this stage, the remaining program functionality depends on whether the particular signing act governs the use of one, or multiple signatures. If there is just one signature, then clicking the button on the right will result in the relevant signature policy being created. However, if the act governs multiple signatures, then clicking the button will result in yet another window coming up, asking the user whether Weak or Strong Signature Policies are desired. It would like the window in the following figure.
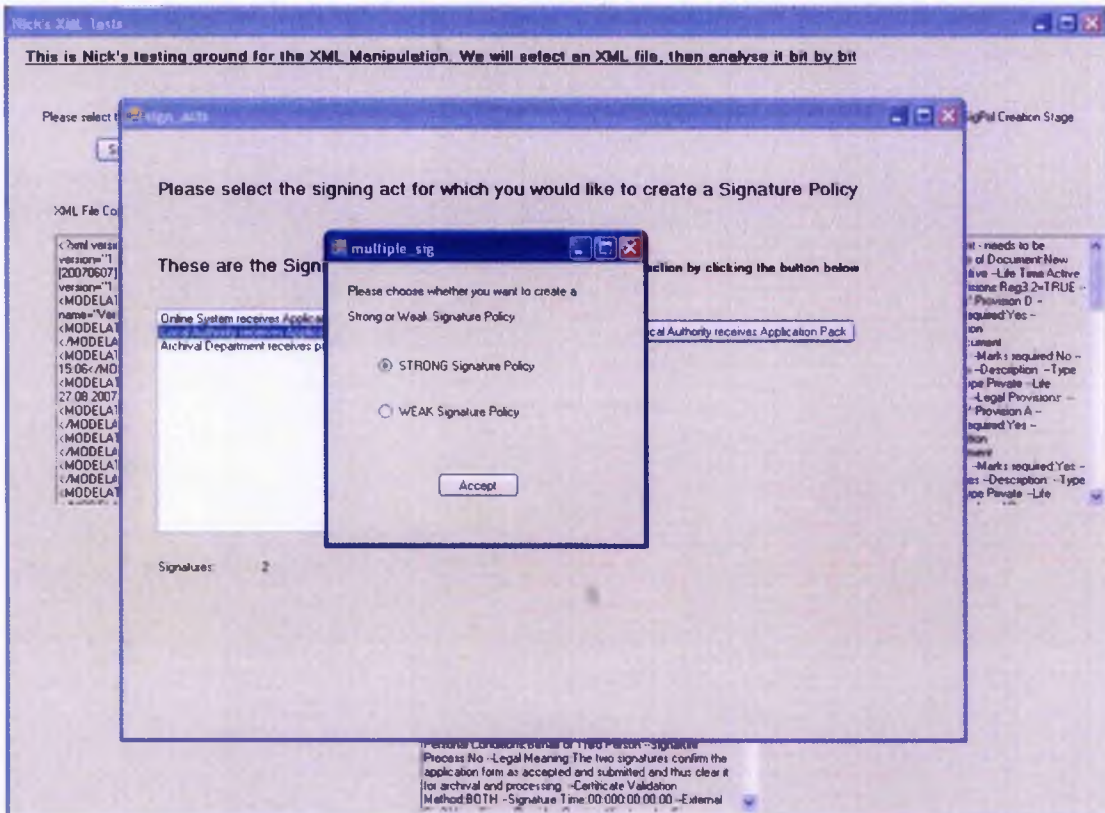
Figure E-7: The Transformation Software has identified multiple signatures - this allows the user to choose between a "Strong" and "Weak" signature policy

Selecting "Strong" signature policies will result in the creation of separate signature policies for each signature applied during the particular Act. Selecting "Weak" signature policies, on the other hand, will result in the creation of one individual signature policy describing all applied signatures in the particular act. On clicking "Accept", the Digital Signature Policy/policies will be created. For each created signature policy, a message box is displayed, such as the one in the figures below.
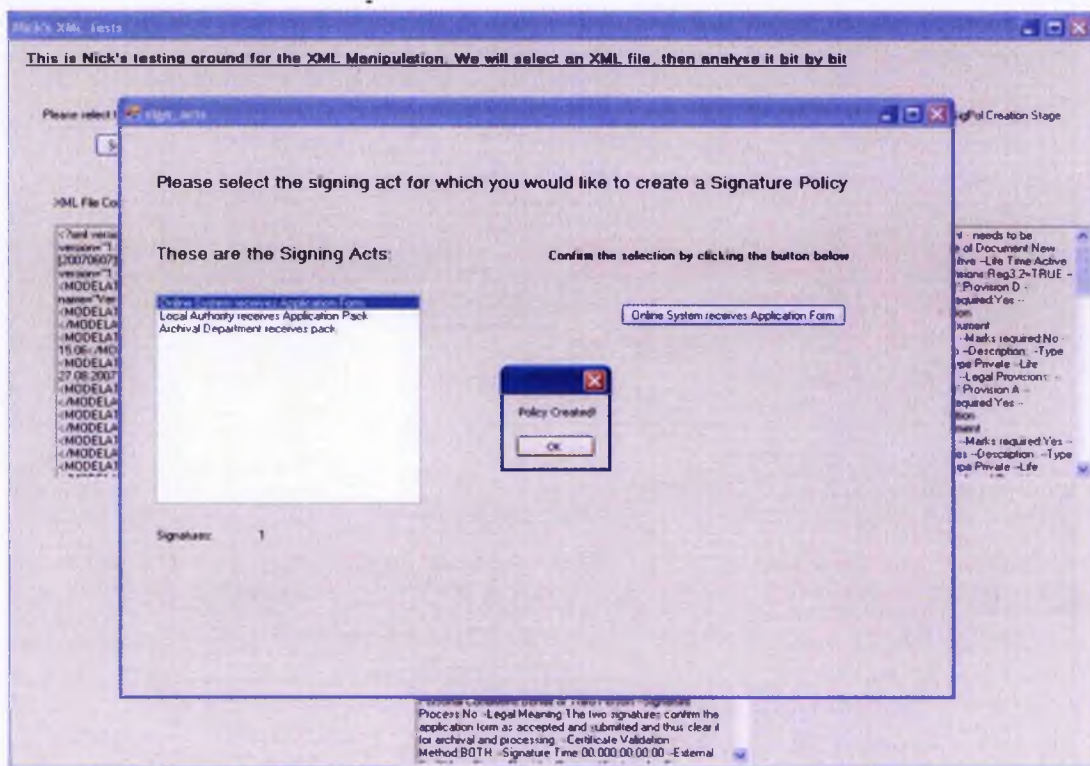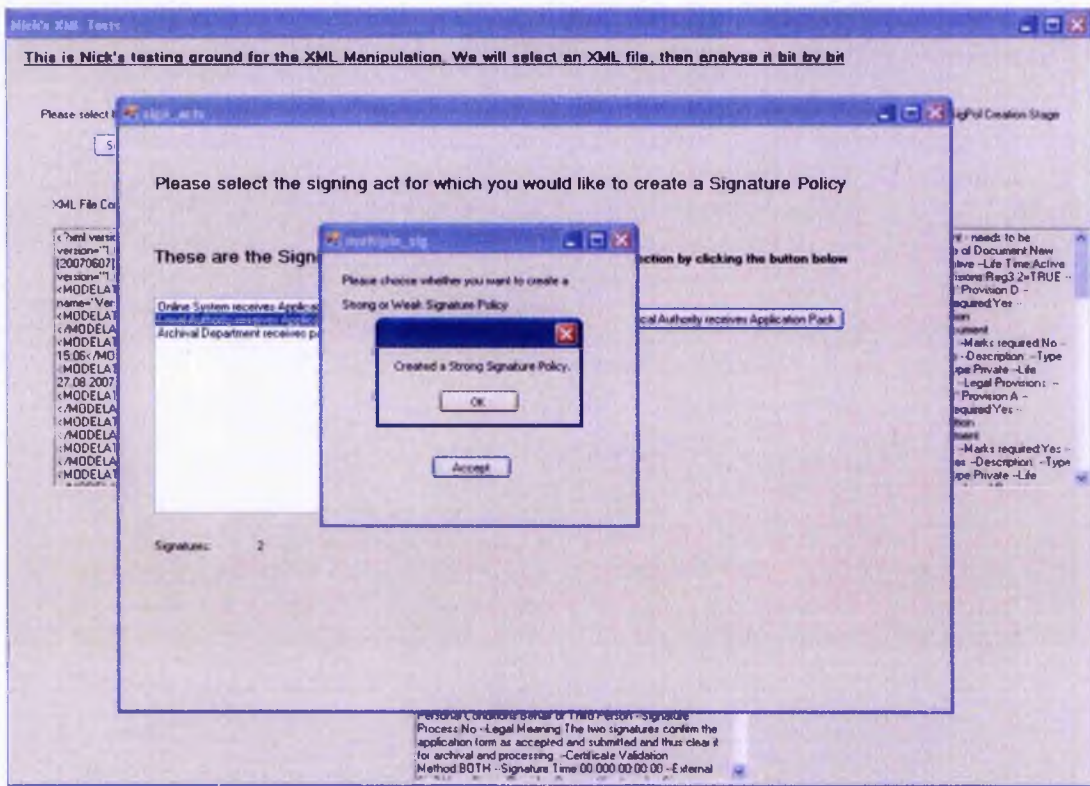
Figure E-8: The Transformation Software has successfully created a Digital Signature Policy

The DSP is created in the root folder of the application and the signature policies are named "actname.xml". It is recommended to move the signature policies out of the root folder once they have been created. Once all the required policies have been created, the program's windows can be shut by pressing the red button in the top-right hand corner.

This section demonstrated the usage of the transformation software to create DSPs. The order in which certain buttons are to be pressed was demonstrated. The simple interface was designed explicitly to keep user errors to a minimum and maximise user acceptance. What this section was lacking was a description of the technology behind the screens, how and why the application behaves the way it does and how data is handled program internally. This in-depth technical view (essentially a 'programmer's guide') is presented in the following sections.

E.2 Technical Details

As mentioned above, the transformation software is implemented in VB.NET 2003. This section assumes basic knowledge of programmes written in this language.

In VB.NET, human-computer interfaces are known as "Forms" and all windows in Windows are implemented using the Form construct. Within VB.NET, Forms have a Design view and a Code view. The Design View allows for visual, high-level manipulation of Form controls (items such as buttons, text boxes, combo boxes, etc.) whilst the Code View allows for the implementation of functionality of that form's controls (e.g. the effects of a button press).

Additionally, VB.NET contains facilities known as "Modules", which are files that contain code that can be executed from anywhere within a VB.NET project. Usually, modules contain a variety of classes of similar functionality.

In the following sections, each individual form or module will be introduced. First, the forms will be covered, in the order in which they appear in the User Guide. Where a form uses code from another form or module, a cross reference is provided. The modules are covered after the forms, and again cross-references are provided where necessary. Important variables for individual forms or modules are also introduced and described.

Form1.vb

This is the first form in the transformation software. The form is called "XMLTestStart", therefore all controls within that form are members of that class.

The button "Select File" is labelled btnSelFile and the code governing its behaviour is standard code for a "File Open" dialogue in Windows. This is a re-usable form which does not need to be created and documented within a VB.NET project. For the code to run, System.IO must be imported, as this is the header file describing the functionality of the "Open File" dialogue window.

The code should not be changed or edited, as it is standard code for using such a dialogue. There are two variables that can be modified:

- .Filter: In its current form, this restricts the "Open File" dialogue to see either XML files or All Files.

- txtBoxCont: This is the text box control into which the contents of the file are read.

The use of Try and Catch is a common construct for providing the program with facilities for error recognition and error output.

Button "Analyse" is labelled btnAnalyse and it calls function analyse_xml() to analyse the loaded XML. This function is present in module xml_extract.vb and will be discussed later. For this button to function correctly, an XML file using the PADS-workflow notation as

implemented in ADONIS must have been loaded already. Pressing it will populate the remaining text boxes with relevant data.

Button "Continue" is labelled `Button1` and performs three important functions. Firstly, it creates an array (called `res`) that holds the signing acts of the workflow (actually, their array subscripts within the `acts_array`; see below) by calling `find_signingact()` (a function described in `tools.vb`); this is a necessary step in order to complete the next function, which is to populate a list box (called `lstSignAct`) with all signing acts. The code to achieve this is as follows:

```
For i = 0 To UBound(res)
            'for all found signing acts, add them to listbox in form
sign_acts

sign_acts.lstSignAct.Items.Add(acts_array(res(i)).getName)
Next
```

The `for`-loop will cycle for as many iterations as there are elements in the array `res`. In each iteration, the list box `lstSignAct` in the next form `sign_acts` is populated with members of the array `acts_array` (an array containing all workflow acts, declared in `xml_extract.vb`); the members of `acts_array` that are added are determined by the contents of the `res` array, which contains the array subscripts of the signing acts within the `acts_array`. The call to method `.getName` adds the Act's name to `lstSignAct`. Method `.getName` and other methods relating to Acts functionality is contained within `acts_class.vb`. Finally, the line `sign_acts.Show()` loads the form named `sign_acts`.

Sign_acts.vb
This is the second form in the transformation software and it is called "`sign_acts`". All elements are enclosed within this class.

The population of the list box is explained in the previous section. The subroutine `lstSignAct_SelectedIndexChanged()` governs the behaviour of the form when a user selects an item within the list box, which is to identify how many signatures are performed by an act and to copy the Act name into the button labelled `btnSel`.

Button `btnSel`, which has a variable name depending on which Act has been selected in `lstSignAct`, performs three functions. Firstly, it creates a link between selected Act and Signatures and Documents associated with it (this requires all Signatures and Documents used in an Act to have the exact Act name (including capitalisation) as the first entry of their description boxes) so that the transformation software can see which signature is used in which Act. This is done by creating an array `temp_sig` which contains all signatures whose descriptions contain the Act name within them (due to `find_signatures()` in `tools.vb`).

Secondly, a check is performed to see whether there is one or more signatures and thus a need for one or more signature policies. This is done through the line

```
tmp = InStr(lblNumSig.Text, 1)
```

where `InStr()` is a string comparison function that compares the two strings supplied to it, in this case `lblNumSig.Text` and 1. The first string represents the number of signatures for an act, which is added to that label when the user clicks on an Act's name (see `lstSignAct_SelectedIndexChanged()`) When there is a match between the first and second string supplied to `InStr()`, the temporary variable `tmp` takes a value of 1 (match = successful); this will happen only when there is 1 signature for a particular act. On the other hand, if there is no match between the two strings (i.e. there is more than 1 signature used in that Act) then `tmp` will remain 0. This allows the software to construct a

signature policy, or to identify the need for further queries (when there is more than 1 signature).

Thirdly, once it has been established whether there is 1 signature or more per Act, the software either calls `create_sigpol()` (located in `policy_write.vb`) to create the signature policy, or it calls the form `multiple_sig` to get further data from the user.

The subroutine `exec_strong_sig()` is called from "`multiple_sig.vb`" and is the routine that governs the creation of signature policies when a strong signature policy has been selected by the user. The routine will loop as many times as there are signatures, creating a signature policy for each individual signature.

Subroutine `exec_weak_sig()` is also called from "`multiple_sig.vb`" and is the routine that governs the creation of signature policies when a weak signature policy has been selected by the user.

Multiple_sig.vb
This form is called "`multiple_sig`". Its function is to assess whether the user wishes to create a Strong or Weak DSP. It does this via the `weak` Boolean variable, which is declared in `policy_write.vb`. Depending on which radio button has been selected, the appropriate signature policy creation subroutine located in `sign_acts.vb` is executed.

Acts_class.vb
This is a public class that contains all relevant data for a particular Act. The class acts as a data storage facility and for each item of data, a pair of `set` and `get` methods are provided. There is no other functionality within this class.

Documents_class.vb

This is a public class that contains all relevant data for a particular Document. The class acts as a data storage facility and for each item of data, a pair of `set` and `get` methods are provided. There is no other functionality within this class.

Signature_class.vb

This is a public class that contains all relevant data for a particular Signature. The class acts as a data storage facility and for each item of data, a pair of `set` and `get` methods are provided. There is no other functionality within this class.

Xml_extract.vb

This module is tasked with extracting relevant data from the ADONIS XML file and adding it to the appropriate class instance of Acts, Documents and Signatures. The extraction is called through the method `analyse_xml()`, which is called when the "Analyse" button in `Form1.vb` is pressed. In order, the method does the following:

- Loads the ADONIS XML as an XML Document

- Identifies the relevant data items within the XML

- Copies the relevant data items into appropriate class instances

Method `load_xml()` creates a new XML object in memory (this requires `System.XML` to be imported) and loads the ADONIS XML into this object. The source of the ADONIS XML is the `txtBoxCont` control in `Form1.vb`. Using an XML object allows the use of XPath to query the XML, as will be shown in the following methods.

Method `select_nodes_Acts()` (and the equivalents for Documents and Signatures) then use XPath to identify Acts/Documents/Signatures within the loaded XML. The way XML support is utilised in .NET is that each tag is considered as a node and by using XPath expressions appropriately, it is

possible to navigate to the appropriate nodes (or tags) within a given XML document. The XPath provided within the code of the transformation software is dependent on the structure of the document used. That is, an ADONIX XML output file will have tags of type "ADOXML", tags of type "MODEL", tags of type "INSTANCE" and tags of type "ATTRIBUTE". There are other tags also, but they are not relevant in this case. What the used XPatch expression extracts from the XML are all attributes (the entries within the ADONIS notebook, in other words) belonging to different Acts/Documents/Signatures.

Method `loop_nodes_PADS_Signatures()` (and the equivalents for Acts and Documents) creates an array to hold all Signatures/Acts/Documents present within the ADONIS XML. The arrays (called `signature_array`, `documents_array`, `acts_array`) are declared within this module as being arrays of object type Signature/Act/Document (as applicable); in other words, the arrays hold objects of the appropriate type.

The array's size depends on the number of Acts/Documents/Signatures present within the XML. The current mechanism is to count the total number of attribute tags within all Acts/Documents/Signatures and divide this number by the number of attribute tags that make up one Act/Document/Signature. This is possible as `m_nodelist` contains a list of all attribute tags of Acts/Document/Signature, due to how XPatch extracts the information.

After setting the size of the array, it has to be re-initialised with the correct objects as `ReDim` statements in VB.NET destroy its data type and data contents (`PRESERVE` preserves the contents but not the data types if it is an empty array at the time of `ReDim`).

With the array in place, the method then goes through each `m_node` (that is, through each tag extracted from the XML) and looks for the string given in the `if`-statement; the string is constructed in such a way that it picks up the correct data and so that detection of the elements is done correctly (only one tag can have the value `name="Description"`). For each match, the node

has its `InnerText()` extracted, which is the location of the data of the tag in question, and the extracted data is added to the relevant text box in `Form1` (e.g. `txtBoxSig`). Furthermore, the data is added to the array by using the class' `set`-Method. The array subscript, set to 0, is increased every time the `for`-loop finishes examining a particular Act/Document/Signature; as the analysis is top-to-bottom, the last match of tags thus marks the end of one particular Act/Document/Signature and the next tag to be examined therefore belongs to the next Act/Document/Signature captured.

The use of `.AppendText()` is to avoid overwriting already added data within the text boxes and is irrelevant to the addition of the data to the array.

The above approach is slightly different for `loop_nodes_PADS_Acts()`; since the name of an Act is presented in a different XML tag than any of the notebook data, a separate XPath query is necessary to extract the Act name from the XML. Therefore, once the size of the `acts_array` has been set and initiated with Array objects, the array objects are firstly populated with the Act names found by the separate XPath query. Once this has been achieved, the array subscript is re-set, and the method then adds data to the different object instances as explained above.

Tools.vb

This module contains several methods aimed at aiding the software's operation. They are all public functions so that these aids are available to all modules and forms within the software.

Since the graphical PADS methodology does not provide a facility for assigning names to Documents and Signatures, it is necessary to develop a work around to be able to link up Documents and Signatures with the Act that consumes them. For this purpose, it is pertinent that all Documents and Signatures consumed by an Act, must have an exact copy of the Act name as the first entry of their "Description" text box. Other information can, of course, be added but the first entry in a Description box must be the exact copy of the Act name.

It is for this reason that `find_docs()` and `find_signatures()` use the act name as a variable to start the location process of documents and signatures. The methods take the act name as a variable, and then for the entire size of the document/signature array, the method evaluates whether there is a match between the "Description" text box and the referenced Act name. This comparison is performed on this line:

```
res = InStr(documents_array(i).getDescription, act_name)
```

The built-in `InStr()` method takes the content of the Description as the first input, and compares it with the Act Name (which is the second input). If a match is made (i.e., if input 2 (Act Name) is matching input 1 (Description text)) the function returns a positive integer; if there is no match, `res` remains 0.

If there was a match, then the value of the current iteration is copied into the temporary results array, as that is the index value of the found signature/document within their respective arrays. The results array is then increased in size. Since the last match leaves an empty entry in results, the last entry is cut off before results is returned to the caller; thus, these `find()` methods return an array of results.

Apart from these two methods, there is also a method called `find_signingact()`. It works on the same principle as the `find()` methods described above, but the search is actually focussed on finding those Acts that perform a signing. This is indicated through the "Signing Act?" question in the 'General' tab of the Act Notebook entry. Therefore, the method checks for the value of that tick box and if it is ticked, the method creates the array based on the earlier principle and returns it as before.

The final method in this file, `find_actindex()` works on a similar principle. It is given the name of an act as a variable and the function returns a single variable `i`, which indicates the position of the sought Act within the

`acts_array`. It uses the same pattern matching function as the other find-functions described above.

Policy_write.vb

This module creates the DSP. It imports "`System.io`", in order to access methods related to file creation. There are four public variables that are initialised at the start of the module. The three index-variables are tasked with indicating the position of a particular act/signature/document within their respective arrays (thus they are crucial to linking these elements together), whilst the Boolean variable `weak` indicates whether the user wishes to create a strong or weak signature policy when an act signs a document multiple times. This variable is actually set in "`multiple_sig.vb`" through the radio button selection. The index variables are set in "`sign_acts.vb`" and utilise the `find`-tools discussed in the earlier chapter. It should be noted that in its current stage, the software only supports 1 document being signed during a particular act, but it can be signed by an arbitrary number of signatures.

The remainder of the module consists of one public subroutine, `create_sigpol()`, which is called in "`sign_acts.vb`" to start the signature policy creation process, and a range of private subroutines that create the different sections of a signature policy, according to the order of the different elements as they appear within the ETSI TR 102 038 standard. Due to the complicated nature of this module, each subroutine will be explained in a sub-section of its own.

Create_sigpol()

This public subroutine is called in "`sign_acts.vb`". Its first action is to check whether, within the application's rootfolder, a signature policy exists of the same name. If it does, variable `nameExtension` is increased and the file is created in the format of "`ActName`" + "`nameExtension`".`xml`.

The subroutine then creates a new filestream with the above name and sets the access mode to write. A streamwriter is declared and linked to the

filestream. These are standard .NET access methods to create new files and, apart from the filename, nothing should be changed.

With the filestream and streamwriter set up, the subroutine then calls `add_namespace()` and `add_signaturepolicyelement()`. Both subroutines get passed the name of the streamwriter, in order to allow these subroutines to add their XML code to the file. On completion of these subroutine calls, the file is closed (no further access is possible) and the signature policy creation process is considered to be complete. The remaining signature policy code is called from `add_signaturepolicyelement()`, similarly to how the policy elements are explained in the ETSI TR 102 038 standard.

Add_namespace()
This subroutine provides the signature policy namespace. It is hardcoded, as it is not expected to change much, if at all. The method by which the XML code is added to the open filestream is to use the `WriteLine` method and submit as a reference the code. A new `WriteLine` call would create new code in the same space, therefore each time `WriteLine` is used, `BaseStream.Seek` is used the way it is used in the code in order to move the "cursor" to the end of the newly appended file. The outcome is that rather than overwriting existing code, new code is appended to the end of the file.

Add_signaturepolicyelement()
This routine adds the signature policy element to the file. Digest algorithm SHA-1 is hardcoded. No value for the actual hash value is provided. It also calls the next subroutine, `add_signaturepolicyinfo()`.

Add_signaturepolicyinfo()
This adds the signature policy info element. The value for the 'Identifier' is taken as the selected Act's name. The 'Date of Issue' is set to the current run time. The 'Policy Issuer Name' is hardcoded as "CATCert". The 'Field of Application' field is populated depending on whether a strong or weak signature policy is being created. For a single/strong signature policy, the content is the selected Act's 'Description' text box, the selected Act's 'Act

Type', the selected Act's 'Act Effect', and the associated Signature's 'Signature Meaning'. For a weak signature policy, the signature meaning is skipped (the remaining data remains the same). The data is encoded in the following way:

$$D=VALUE, T=VALUE, E=VALUE, SM=VALUE$$

where `value` takes the values mentioned above.

The subroutine then prints all this data, within its correct XML tags, to the file and calls the `add_signaturevalidationpolicy()` routine. Once that call is complete, the signature policy info tag is closed.

Add_signaturevalidationpolicy()

This subroutine adds the signature validation policy element. The signing period is the signing period assigned to the signature associated with the selected Act. In case of weak signatures, it is the top-most signature that determines the signature policy's signing period. The signing period is determined by checking the value of the Not Before/Not After radio buttons; depending on which one is pressed, the appropriate XML code is added to the signature time indicated within the signature notebook.

The signing period is then added to the actual signature policy being created and the subroutine then calls `add_commonrules()` and `add_commitmentrules()` to add the common rules and commitment rules elements respectively. On completion of these calls, the signature validation closing tag is added to the file and the subroutine has finished.

Add_commonrules()

The subroutine adds the opening tag of the common rules element. Then the routine checks on whether a weak signature policy is required; if it is, the signer and verifier rules element is not added to the common rules (instead, it will be added to the commitment rules), otherwise it will be added. Furthermore, the routine also calls for the addition of the signing cert trust condition element, the time stamp trust condition element, the role trust condition element and the algorithm constraint set. All these are added in the

common rules, as it is not anticipated that these will change for the case of weak signatures.

Once all these calls have been performed, the routine adds the common rules closing tag to the file and the routine has finished.

Add_signerandveriferrules()

This subroutine adds the opening tag of the signer and verifier rules element. After adding this tag to the file, it then calls `add_signerrules()` and `add_verifierrules()`, to add signer rules and verifier rules respectively. As mentioned above, this subroutine places itself (and its content) either within the common rules for single and strong signature policies, and into the commitment rules for weak signature policies.

Once the signer rules and verifier rules elements have been added, the routine adds its element's closing tag to the created signature policy file.

Add_commitmentrules()

This routine is called by the signature validation policy element. There are two functionalities, depending on whether weak signature policies are required to be produced or not. If they are not required (i.e. the signature policy in creation is either single or strong), then this subroutine creates an empty commitment rules block, with the associated tags and no data contained in those tags.

On the other hand, if weak signature policies are being created, then the commitment rules tags will look differently as they will be populated with data. The ETSI standard specifies that within the commitment rules tags, there is a cycle of commitment rule elements. Furthermore, within that commitment rule, there is a cycle of sel commitment type elements, of signer and verifier rules elements, and other elements which are not added in this software.

The understanding of the author based on the published standards is that for each signature being compiled and decomposed and to be added to a weak signature policy, a 'commitment rule' must be created. The contents of the

'commitment rule' are determined by how similar the signatures are with each other. If they are very similar to each other, most signature details can actually be captured within the 'common rules'. For this reason, elements such as the 'algorithm constraint set' and the 'role trust condition' element, are present within the 'common rules', rather than the 'commitment rules'. In other words, within this software the only contents of the 'commitment rule' element are the 'sel commitment types' elements and the 'signer and verifier rules' element. This understanding has been converted into the following functionality.

The software will open a new commitment rules tag; within this 'commitment rules' tag, a `for`-loop will cycle for as many signatures as there are for a given Act. For each cycle, a new 'commitment rule' block will be created. Within each of these 'commitment rule' blocks, a 'sel commitment type' element and a 'signer and verifier rules' element are added, using calls to the subroutines that create these elements. The signatures that are used as data source for these elements are the signatures that are addressed by the for-loops control variable. Since the `for`-loop cycles through the `temp_sig` array, it means that the `for`-loop cycles through all signatures associated with the selected Act (selected in "`sign_acts.vb`"); the public variable `sigIndex` is changed, but this is permissible in this case as the commitment rules are the last major element to be added to the signature policy.

Add_recognizedcommitment()
This subroutine adds the recognized commitment elements to weak signature policies. There are no conditional elements since this subroutine only gets called when the user has selected the creation of weak signature policies.

The value of the commitment identifiers is a hardcoded string, as the information is context dependent and not determined by legal information alone.

The value for 'Field of Application' is a combined string (separated by a comma) of the description text box of the particular signature and the description text box of the selected Act.

The value for 'Semantics' is also a comma separated string that consists of the 'Signature Meaning' text box of the particular signature and the description text box of the document being signed.

All of these data are added to their appropriate tags; all tags are printed to the created file and the subroutine finishes operation.

Add_signingcerttrustcondition()

This subroutine adds the 'signing cert trust condition' element. Essentially, the routine opens the tags associated with this element, performs calls to the creation of the 'signer trust tree' and 'signer rev req' elements, then closes the associated tags and writes the tags to the created file.

Add_signertrusttree()

This subroutine adds the 'signer trust tree' element to the signature policy being created. The routine adds a trust point, which is hard coded to be CATCert's trust point (found at the bottom of this file). The routine also adds a hard coded value of '1' to the path length constraint tags, whilst a string is added to the 'acceptable policy set', asking for the OID numbers to be inserted here (these are organisation specific).

For the 'Name Constraints' tags, the routine first checks if the document being signed requires a specific Role; if it does, the description of the role is added to the 'Name Constraints'. On the other hand, if Role is not required, then the name constraints consist of the 'Performer Domain' of the Act only. The data is encoded in the following manner:

```
OU=Performer Domain, E=Role Description
```

where "E=" may be skipped if no Role is specified.

Add_signerrevreq()

This sub routine adds the 'signer rev req' element to the signature policy. Firstly, the value of the selected certificate validation method is assessed. Then, depending on that value, the routine adds the semantics specified in the ETSI TR 102 038 standard to both signer certificate validation element

and the CA certificate validation element. It is assumed that a certificate issued by a particular CA to a signer would necessitate the same certificate validation method as the CA's own certificates.

Add_timestamptrustcondition()
This subroutine adds an empty 'Time Stamp Trust Condition' element to the signature policy.

Add_roletrustcondition()
This sub routine adds the 'role trust condition' element to the signature policy. The routine first checks whether the role is mandated, and if it is, it checks whether it is claimed or certified. If it is not mandated, however, then an empty 'HowCertRole' tag is added instead.

The 'AttrCertTrustTrees' tag is left empty (with a string message) as this value has to come from an attribute certificate. The same approach was taken for the 'rolerevreq' tag. On the other hand, communication on 'Roleconstraints' indicated that this was an open issue to be discussed further within CATCERT, therefore an appropriate string was left in that tag.

Add_algorithmconstraintset()
This subroutine adds an empty 'algorithm constraint set' element to the signature policy.

Add_signerrules()
This subroutine adds the 'Signer Rules' element to the signature policy. Firstly, it adds signed and unsigned properties, all of which are taken from the "Signature Rules" tab within the signatures notebook in the graphical methodology. For each ticked tickbox, the correct URI for that particular property is added. Secondly, it checks whether the signer provides the certificate identifiers for his own certificate only, or whether the signer provides certificate identifiers for the complete certificate path, as specified in the ETSI standard. Finally, the routine checks whether the signer provides his own certificate only, or whether he provides all certificates in the certificate path up to the trust point. The source for these data is again the same tab as the signed and unsigned properties.

Add_verifierrules()

This subroutine adds the 'Verifier Rules' element to the signature policy. As there is only one verifier rule that might be ticked within the graphical methodology, the routine simply checks for whether that rule has been ticked; if it has been, then the correct URI is added, otherwise empty tags are added.

Apart from all of these methods, the module also contains a string variable called `TrustPoint`, which is the representation of the Trust Point representing CATCERT.

Summary

This chapter has provided an overview over how the data necessitated by the ETSI TR 102 038 standard was provided by the graphical methodology. This mapping is a very important reference source for the future, as it will serve as the main input for new implementations of the XML Transformation process. The document also provided an explanation of one suggested XML Transformation software implementation, which should not be considered binding or as a standard. It is merely a demonstration of how to transform between Adonis XML created by PADS and an ETSI-compliant DSP.