

https://dspace.org/

An analysis of electronic signature regulation in South Africa

Chetty, Prialoshni

2014-02-27
http://hdl.handle.net/10539/13973

Downloaded from a DSpace repository. https://dspace.org/

AN ANALYSIS OF ELECTRONIC SIGNATURE REGULATION IN SOUTH AFRICA

Pria Chetty

March 2013

A research report submitted to the Faculty of Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management (in the field of ICT Policy and Regulation).

ABSTRACT

This is a study of the effectiveness of e-signature regulation in South Africa. The primary objective is to analyse South Africa's e-signature regulatory frameworks and approaches in order to produce findings on its current status and its effectiveness. To do this, the research included the development of a conceptual framework that identifies key themes of analysis for effective electronic signature regulation and a research approach that produces findings from qualitative analysis of multiple sources of data. The report specifically considers the effectiveness of the regulation in rendering electronic signatures a legally valid, secure and trustworthy method of concluding electronic transactions as the key tenets of effectiveness. The report concludes that the regulation is ineffective in various aspects including outdated legislative approaches and technical standards as well as various delays and inefficiencies in implementing the regulations which detract from the regulatory intent.

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Master of management (in the field of ICT Policy and regulation) in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.

_____

Prialoshni Chetty

Student Number 521486

28 March 2013

DEDICATION

For my husband, best friend and co-conspirator, Josh, who is always with me at the starting and finishing line.

For my sister Kelen, and brother Laven, who are my heroes.

To my dearest friends - legends.

ACKNOWLEDGEMENTS

I am grateful to my supervisor, Charley Lewis, for his generous support and encouragement throughout the research. Mr Lewis provided deep and meaningful insights in our many discussions that steered me through times of indecision and uncertainty. As a teacher and supervisor, he encouraged an appreciation for the importance of the task at hand and inspired my best endeavour. I wish to also thank Luci Abrahams for her assistance with my research proposal. Her guidance in the foundation phase is sincerely appreciated. Without the assistance of Mr Lewis and Ms Abrahams, this research would not have been possible.

TABLE OF CONTENTS

TABLE OF TABLES x

TABLE OF ABBREVIATIONS xi

1 CHAPTER ONE – AN INTRODUCTION TO E-SIGNATURE REGULATION 1

1.1 The role of e-signatures in electronic commerce 1

1.2 An Introduction to E-signature Regulation in South Africa 3

1.3 Is the Regulation of E-signatures in South Africa Effective? 4

1.3.1 The Effectiveness of Regulation 4

1.3.2 Problem Context 6

1.3.3 The Problem Defined 8

1.4 Purpose of the Research 8

1.5 Audience and scope 9

1.6 E-Signatures and Advanced Electronic Signatures 10

1.7 Structure of this research report 10

1.8 Chapter Summary 12

2 CHAPTER TWO –LITERATURE REVIEW 13

2.1 Overview of the Chapter 13

2.2 Ensuring the Legal Validity of an E-signature 13

2.3 Expert Guidance on the importance of AeS Regulation 15

2.4 Model Law Approaches to Regulation of E-signatures 16

2.4.1 UNCITRAL Model Law on Electronic Commerce (1996) 16

2.4.2 UNCITRAL Model Law on E-signatures (2001) 16

2.4.3 EU E-signatures Directive (1999) 17

2.4.4 Specific regulation of the Service Provider 19

2.5 Regulation of E-signatures in the UK, Australia and China 21

2.5.1 UK 21

2.5.2 Australia 22
2.5.3 China 23
2.6 Emerging Typology of E-signature Regulatory Approaches - The Digital Signature, Two-Prong and Minimalist Approach 26
2.7 Extracting a Conceptual Framework 27
2.8 Application of International Theory and Expert Perspectives 29
2.9 Summary 30
3 CHAPTER THREE – METHODOLOGY AND RESEARCH DESIGN 32
3.1 Overview of the Chapter 32
3.2 Research Questions 32
3.2.1 Main Research Question 32
3.2.2 Research Sub Questions 33
3.3 Research Methodology– Qualitative with Case Study Components 33
3.3.1 Qualitative Study 33
3.3.2 Case Study Aspects 34
3.4 Research Design 35
3.5 Data Collection and Analysis Methods 38
3.5.1 Secondary Content Analysis: 38
3.5.2 Interviews: 39
3.5.3 Ensuring the Quality of the Analysis 42
3.6 Summary 43
4 CHAPTER FOUR: RESULTS ON REGULATION OF E-SIGNATURES IN SOUTH AFRICA 44
4.1 Overview of the Chapter 44
4.2 Legislative Analysis 44
4.2.1 Legal Validity of E-signatures in South Africa 44
4.2.2 Regulation of E-signature Products, Services and Service Providers 47
4.3 Case Law 55

4.3.1 Jafta v Ezemvelo Wildlife 56
4.4 Outcomes of Individual Interviews 58
4.4.1 Overview of Interviews 58
4.4.2 Summary of Interviews 60
4.5 Summary 75
5 CHAPTER 5 - ANALYSIS 77
5.1 Overview of the Chapter 77
5.2 Legal Validity of E-signatures 77
5.2.1 Legally Valid Substitution with Handwritten Signatures 77
5.2.2 Distinction in the Legal Validity of E-signatures 78
5.2.3 Other Factors impacting the legal validity of e-signatures 81
5.2.4 South African case law on the legal validity of e-signatures 82
5.3 Trustworthy E-signature Services 84
5.3.1 Essential attributes of e-signature services 84
5.3.2 Accreditation Regulation 86
5.3.3 Liability of the Accredited Service Providers 89
5.3.4 Analysis of the regulation of information security standards for e-signature products and services 90
5.3.5 The delay in the accreditation of the ASP 92
5.3.6 The effect of a single ASP 94
5.3.7 Foreign signature service providers 95
5.3.8 Oversight of E-signature Products and Services 97
5.4 Harmonisation of Approaches to Regulation of E-signatures 98
5.4.1 How do South Africa's approaches to e-signature regulation compare with international models and frameworks 98
5.4.2 How does South Africa's approaches to e-signature regulation compare with foreign country approaches? 101

5.4.3 Is South Africa's approach to e-signature regulation aligned with developments in regulatory approaches that advance electronic commerce? 104
5.5 Summary 106
6 CHAPTER SIX – CONCLUSIONS 108
6.1 How effective is the electronic signature legal framework for the promotion of legal confidence in electronic commerce transactions? 109
6.1.1 Effective Legal Validity 109
6.1.2 Ease of Substitution of Electronic Signatures – Case Law Perspectives 110
6.2 How effective is South Africa's regulation of electronic signature products and services to promote trust and information security in electronic commerce? 111
6.2.1 Partially Effective Regulations 111
6.2.2 Ineffective Regulatory Outcomes for Trust and Information Security Standards 112
6.2.3 Auditor Appointments and Knowledge 112
6.3 How effective are South Africa's electronic signature regulatory approaches when compared with primary international model laws? 113
6.3.1 Close Alignment with EU Directive but Ineffective Approaches 113
6.4 How effective are South Africa's electronic signature regulatory approaches when compared with other country frameworks and approaches? 114
6.5 How would South Africa be impacted by the continued reliance on the current electronic signature regulatory framework and approaches? 115
6.6 How effective is the South African electronic signature regulatory framework for promoting the adoption and use of electronic signatures to advance legal assurance, security, and trust in electronic commerce? 116
6.7 Limitations of the Study 118
REFERENCES 119
Annexure A – Interview Protocol 125
Masters Research Report: An analysis of electronic signature regulation in South Africa 127
ANNEXURE B: INTERVIEWEES 130

TABLE OF TABLES

Table 2.1: Conceptual Framework for Analysis of Effective Regulation of E-Signatures in South Africa 28

Table 3.1: Phasing of the study 36

Table 3.2: Boundary setting with Yin's research design components 36

Table 3.3: Interview themes and questions 41

Table 4.1: Criteria for Accreditation 50

Table 4.2: Key regulatory provisions 52

Table 4.3: Interview themes and questions 59

Table 5.1: Distinction between E-signatures in South Africa 78

Table 5.2: Principles of interpretation of the ECT Act on e-signature validity 83

Table 5.3: Requirements for accreditation of the AeS in South Africa 85

Table 5.4: Comparison of SA regulatory approaches to e-signatures 103

TABLE OF ABBREVIATIONS

Abbreviation	Description
AeS / AES	Advanced Electronic Signature(s)
ASP / The ASP	Accredited Service Provider
Authority	The regulatory authority for electronic signatures in South Africa.
CA	Certification Authority
CSP	Certified Service Provider
DOC/DOC	Department of Communications
ECA	Electronic Communications Act
ECT Act	Electronic Communications and Transactions Act
E-commerce	Electronic commerce
E-signature	Electronic signature
ES Regulations	Electronic Signature Regulations
EU	European Union
ITU	International Telecoms Union
PKI	Public Key Infrastructure
RSA	Republic of South Africa
SA	South Africa
SAAA	South African Accreditation Authority
SAPO	South African Post Office
SMME	Small and medium enterprises
UK	United Kingdom
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law

1 CHAPTER ONE – AN INTRODUCTION TO E-SIGNATURE REGULATION

In this introductory chapter, the role and relevance of e-signatures and their regulation for electronic commerce in particular will be introduced, before positioning the research question concerning the efficacy of South Africa's approach to the regulation of e-signatures. This is followed by an outline of the scope and purpose of this research and an overview of the structure of this report.

1.1 The role of e-signatures in electronic commerce

A definition of an e-signature that has broad consensus is not apparent in the literature. The most fundamental of definitions of an e-signature, is a "computer based identity" including scans of handwritten signatures, biometric and digital signatures associated with public key cryptography (PKI) (Spyrelli, 2002, p1). Electronic commerce in equally fundamental terms is defined as "doing business over the internet" and "doing business electronically" (Aalberts & Van der Hof, 2000).
Perhaps one of the most significant characteristics of the relationship between e-signatures and electronic commerce is that e-signatures offer legally valid substitutes to handwritten signatures when entering into electronic transactions (Aalberts & Van der Hof, 2000). To facilitate the use of e-signatures in such legal facility, countries that have implemented e-signature regulation commonly (i) afford e-signatures a functional equivalence to paper signatures in law and/or (ii) provide for technology neutrality for the methods of assenting to contracts (Low & Christensen, 2004, Parry, James-Moore, Graves, Altinok, 2008).

E-signatures are further utilised as an important mechanism to address of barriers to electronic commerce through, the generation of trust in electronic commerce activities (Cogburn, 2003, Dagada, 2009, Kshetri, 2006, Cole et al, 2008 Low & Christensen, 2004) and through:

- addressing concerns of the identity of the transacting parties (Wang, 2007, Brazell, 2008), and
- attending to the security of the transactions being concluded (Kshetri, 2006, Dagada, 2009).

What renders electronic signatures suitable for this role? A succinct explanation is that of Mason who describes the attributes of an e-signature as:

- fulfilling the requirement of "authenticity" or verifying the identity of the sender of a communications;
- evidencing the "integrity and accuracy" of the information or communication i.e. it remains free from interference or alteration; and
- controlling against "non-repudiation" or denial that the relevant person was the sender of the electronic information or communication (2003, p20).

Collectively, therefore, the role of electronic signatures may be explained in the context of addressing issues of legal assurance, trust and security in e-commerce. Moreover the significance of e-signatures may be extracted as advancing electronic commerce through addressing such barriers that may otherwise inhibit consumer confidence in e-commerce transactions.

This significance may be extended to an impact on South Africa's information economy aspirations and broader socio-economic goals. In a 1999 collection of essays that spoke to the impact that electronic commerce could have in South Africa, a specific essay convincingly set out that whilst electronic commerce cannot deliver poverty alleviation in the short term, it could have immediate impact on SMME's (Miller, 1999). By promoting their ability to enter new international markets using electronic commerce, South Africa could take significant strides in poverty alleviation through SMME upliftment (Miller, 1999). At a similar time the Green Paper on Electronic Commerce Law in South Africa declared that electronic commerce did have a role to play in the economic stance of South Africa and has the potential to deliver equitable economic development in South Africa and in so doing, deliver a better quality of life for South Africans (RSA, 1999). This places e-signatures as a function of e-commerce advancement as a contributor, to South Africa's broader socio-economic pursuits associated with e-commerce success.

With the brief extraction of the significance above, an examination of the manner in which electronic signatures are regulated in South Africa and its association with the significance of electronic signatures is pursued in the section following.

1.2 An Introduction to E-signature Regulation in South Africa

Electronic signature regulation in South Africa is a subset of broader electronic commerce regulation (RSA, 2002). The approach emanated from the United Nations Commission on Trade Laws (UNCITRAL) Model Law on Electronic Commerce, published in 1996 - the central premise of which was that (i) uncertainty in national laws on the legal force and effect of electronic transactions may result in barriers to international trade and (ii) harmonised laws that remove inconsistencies in the legal treatment of electronic communications and transactions will enable countries to participate more effectively in international electronic commerce activities (UNCITRAL, 1996).

South Africa's electronic commerce law, the Electronic Communications and Transactions Act (the ECT Act) passed in 2002 pursues the benefits to national countries enacting electronic commerce law, as urged by the UNCITRAL Model Law. The Act principally afforded electronic communications and transactions legal force and effect (RSA, 2002). In following the example of the UNCITRAL Model Law, the ECT Act was South Africa's regulatory intervention to provide an enabling legal platform for the promotion of electronic commerce, providing regulatory guidance on electronic contracting, online consumer protection, and production of electronic evidence in courts and the subject of this research, e-signatures. In accordance with the role that e-signatures play as a facility for legal assurance in electronic commerce (Low & Christensen, 2004; Parry et al, 2008), South Africa's ECT Act deemed e-signatures to be the functional equivalent of paper signatures for the purposes of electronic contracting or trading (RSA, 2002) as an enabling approach.

The legislative provision on e-signatures in the ECT Act extends beyond the aspect of legally providing for functional equivalence to manuscript signatures. The ECT provided a differentiation between two categories of e-signatures. Firstly, an "e-signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature; and secondly, an "advanced e-signature" (AeS) intended as a more secure form of e-signature that results from a process which has been accredited by the accreditation authority described in the legislation (RSA, 2002, s1). An AeS is prescribed for instance, where there is a legal requirement for a signature to conclude a particular (electronic) transaction (RSA, 2002, s13) whilst parties may agree to the form of satisfactory e-signature otherwise. What emerges from the legislation is that the purpose of accreditation of the AeS is to promote the security of electronic transactions by providing for a more secure form of e-signatures. The hardware and software systems must for instance be "reasonably secure from intrusion and misuse", "provide a reasonable level of availability, reliability and correct

operation" and "be reasonably suited to performing their intended functions" (RSA, 2002, s38(3)). In terms of serving the fundamental role of an alternative to manuscript signatures for electronic transactions, the criteria for accreditation include that an AeS must demonstrate the manner in which the signature is uniquely linked to an identified user and the electronic communication or transaction in question. The Act provides for the issuing of further regulations by the Minister for further implementation of the Act and in particular the accreditation of the AeS (ECT, 2002, s 41).

The reading of section 13 of the ECT Act reveals that an AeS, albeit intended as having specific utility, application and regulatory implications as an advanced form of e-signature, in broad terms remains a category of e-signature with regulatory implications in such capacity (RSA, 2002, s13). In other words, the legislation intends that an e-signature, in general terms, would include an AeS.

The legislation further provides that other forms of expressions of intent made electronically that are not e-signatures may be used to infer a person's intent. Chapter 6 of the ECT Act provides for the establishment and powers of the authority that accredits an AeS as well the criteria for accreditation of the AeS (RSA, 2002 s13).

An early statement of objectives of the ECT Act is to promote legal certainty and confidence, and a trusted and secure environment for electronic commerce (RSA, 2002 s2). From the cursory review of the e-signature legislative provisions above, the promotion of the utility of e-signatures to improve the security, trust and legal confidence of electronic transactions is directly associated with such objective. This objective arguably underpins the e-signature regulatory framework.

1.3 Is the Regulation of E-signatures in South Africa Effective?

1.3.1 The Effectiveness of Regulation

Exploring the efficacy of South Africa's e-signature regulation is the very core of the research constituted in this study. Chapter Two, comprising the review of literature on effective electronic signature regulation is focussed on producing in the conceptual framework a specific map of inquiries that relate to effective e-signature regulation. In general terms, however, what is meant by effective regulation and how is regulatory effectiveness probed?

Makaya undertaking a study on the determinants of regulatory effectiveness concluded that the literature reviewed does not provide unequivocal methods of assessing regulatory effectiveness (Makaya, 2001). Rather Makaya argues that the central tenets pertains to the "accomplishment of policy goals" and the pursuit of the associated "policy objectives" (2001, p5). She cites the manner in which the regulation provides for the accomplishment of such goals such as its ability to produce "efficient results" is a key inquiry as well as the "simplicity and predictability" of the regulation as contributing to its success (Makaya, 2001, p5). Bundchuh-Rieseneder shared the view that effective regulation is associated with the securing of policy goals through "clear and achievable objectives". (Bundchuh-Rieseneder, 2008, p30). The focus should be on "performance and outcomes" but clarity is also needed on the influences extraneous to the regulation that will secure its success (Bundchuh-Rieseneder, 2008, p30). Conversely, navigating barriers to the success of the regulation, which may include ease of compliance, enforcement, costs associated with the regulation should be considered to promote its effectiveness (Bundchuh-Rieseneder, 2008, p30).

On the issue of assessing regulatory effectiveness, there have been several studies that propose metrics and indices to assess regulatory effectiveness, each placed in particular regulatory topics and sectors. In the communications sector, the ECTA Report for instances considers the regulatory environment in several European countries, Norway and Turkey to assess the effectiveness in pursuing the objectives of the EU electronic communications regulatory framework analysing institutional, legal efficacy and implementation effectiveness of the relevant regulators (Scorecard, 2005). This study deployed methods of comparative analysis to consider the regulatory approaches and produce conclusions and recommendations (Scorecard, 2005). Another study involved the compilation of an index of the effectiveness of the institutional approaches of telecommunication regulators of 142 countries to measure general political governance and correlate issues of governance and political transparency. Another empirical assessment of effectiveness of regulatory agencies relied on outcomes in the relevant markets associated with the regulatory measures introduced by the relevant regulatory agencies (Lupi, Manenti, Sciala, & Varin, 2011). While this study is not related to the measure of market outcomes, particular institutional effectiveness or regulatory governance, what emerges from the above studies is a clear need to develop an objective measure of regulatory effectiveness to guide any analysis of regulatory effectiveness.

A proposition can be extracted from the above theory of regulatory effectiveness that in general terms, assessing the effectiveness of regulation should be concerned with both the intended outcomes, results and goals associated with the relevant regulation including specific policy objectives as well as the employment of a model or index of considerations to

factors that will be used to assess success of the regulation. In the context of e-signature regulation, the intended outcomes and the model for analysis and assessment is pursued in the literature review and conceptual framework constituting Chapter 2. An analysis of the efficacy of the regulation in securing such outcomes and the factors promoting or inhibiting its effectiveness is then be pursued toward the conclusion on the regulatory effectiveness of South Africa's electronic signature regulation.

1.3.2 Problem Context

A study published in 2007, 5 years post the passing of the ECT Act, on e-commerce activity in South Africa showed that the adoption of e-commerce was met with several barriers including privacy, concerns surrounding the security of transactions and consumers' resistance to change (Warden & Motjolopane, 2007). Dagada too, 2 years later, noted that the new "e-market culture" (i) presented concerns surrounding information security and trustworthiness in the electronic environment and; (ii) that the market remained cautious about information security breaches (2009, p3). Given that these studies were concluded 5 and 7 years following the passing of the ECT Act, what, if any, effectiveness has electronic signatures had in addressing issues of information security, trustworthiness etc. in e-commerce? This query can be extended to enquire from a regulatory perspective - how effective has the regulation been in securing e-signature adoption to address such inhibitors of e-commerce?

Another aspect of concern is the delayed accreditation of an AeS. It was only in March 2012 that the Department of Communications duly accredited the current single accredited AeS service provider (ASP/ the ASP) for the provision of accredited e-signatures (ITWeb, 2012). This delay, in line with the discussion above pertaining to the role of e-signatures and e-signature regulation has resulted in a corresponding lack of availability of an accredited e-signature that each contribute to addressing barriers to electronic commerce in South Africa.

That the availability of an AeS is fundamental to improving the security, trust and legal confidence in electronic transactions was further entrenched in the online article published following the accreditation of the AeS (Perry, 2012). The article quoted the Director General of the DOC emphasising the importance of the accreditation in line with the legislative requirement stipulated in the ECT Act. According to the Director General, "it is a national obligation and one of the initiatives

that will contribute to increasing confidence and trust in the use of online platforms in South Africa…advanced e-signatures ensure authenticity, credibility and security of transactions and information on the internet...this increases the reliability of online information...ultimately, this would enhance the public's confidence in internet based information and services government provides to its citizens" (Perry, 2012).

With this in mind, and accounting for the commencement of the ECT Act in 2002, why has it taken the Department nearly ten years to accredit the signature or service provider? Is the regulation frustrating e-signature services in the market by unduly restricting accreditation of e-signature service providers? Christi Peens, Managing Director of the accredited service provider, the ASP, noted that, "the process to achieve this accreditation was a long and expensive one" (ITWeb, 2012). Associated with the above, an associated concern is that should the accreditation requirements be too cumbersome, what are the implications? Should no further service providers be accredited, perhaps a market monopoly will result for the ASP and South Africans access to an AeS will be subject to the conditions associated with such market structure.

From the above, questions surrounding the effectiveness of the current regulatory approaches are revealed. There are, however, several related queries that require consideration:

- The ECT Act provides that the facilitation of electronic transactions and communications in the public interest by promoting electronic transactions that conform to the highest international standards and ensure compliance with accepted international technical standards. In view of the ECT Act coming into force in 2002, has South Africa kept pace with international standards?
- Snail also raised the issue of the legislature doing away with the stringent requirements of an advanced e-signature for certain transactions - making provision for the use of internationally recognised e-signatures that used advanced encryption mechanisms in order to follow the international standard of technologically neutral e-signatures as an approach more conducive to electronic commerce advancement (Snail, 2008).
- One of the key issues is that the UNCITRAL Model Law on E-signatures was to facilitate international electronic commerce through the recognition of foreign e-signature technologies which were as reliable as required in the national jurisdiction (UNCITRAL, 2001). In the absence an express provision in the ECT Act providing for recognition, the position on the recognition of foreign e-signatures is uncertain.

In 2010, the South African Law Reform Commission published an Electronic Evidence Issue Paper highlighting aspects of electronic evidence law for public consultation and discussion (SALRC, 2010). One of the issues discussed was that of the current regulation of e-signatures. This Issue Paper further endorses a necessary examination of electronic signature regulation in South Africa in the context of its effectiveness.

Pertaining to the effectiveness of electronic signature regulation, international studies consider the nature of the institutions established to administer and regulate the accreditation of so called advanced e-signatures (Blythe, 2007, Cole et al, 2008) and the progress made in implementing the regulation (Parry et al, Cole et al and Low et al). Limited prior research makes it impossible to determine whether South Africa has had institutional effectiveness. Speculation from the delayed accreditation of the ASP would signal concerns with the effectiveness of the implementation of the accreditation regulations. These issues should also be examined.

Another unsettling predicament is that several countries and regions have recognised e-signature regulation as critical including United Kingdom, European Union, Australia, Malaysia, Hungary, Greece and China, and have undertaken studies of the effectiveness of the e-signature regulation (Blythe 2005, Wang, 2007, Blythe 2007) whereas South African has not. The presents a gap in local understanding of electronic signature regulatory effectiveness that should be addressed.

1.3.3 The Problem Defined

From the above, e-signatures appear to not be reaching their full potential in facilitating improved trust, security and legal confidence in electronic commerce. Further, the widespread use of e-signatures may be impeded by ineffective regulatory approaches. Should the dearth of analysis persist, an opportunity to understand and address areas of ineffectiveness and promote the effectiveness of e-signatures in advancing electronic commerce in South Africa will be missed.

1.4 Purpose of the Research

Research that analyses the current regulations and the effectiveness of South Africa's approach to the regulation of e-signatures is absent. This gap in understanding needs to be addressed.

Is the manner in which South Africa classifies the forms of e-signatures aligned with international frameworks? What is the impact of the accreditation of an advanced e-signature and the (signature) authentication service provider, the ASP? What are the reasons for the delayed accreditation and resulting delay in the availability of an AeS associated with higher levels

of security and trust? Is there a need to amend the e-signature regulatory framework? Can a different regulatory approach to e-signature regulation produce more positive outcomes for electronic commerce?

The primary objectives of the study, therefore, are to:

(i) *analyse the current state of e-signature regulation in South Africa, and*

(ii) *analyse the effectiveness of the frameworks and approaches for the improvement of e-signature regulation in South Africa.*

Earlier in this Chapter the association between electronic signature regulatory effectiveness and broader socio-economic goals associated was made. Seen in this light, the impact of ineffective e-signature regulation is not restricted to mere negative outcomes for electronic commerce but notably, negative outcomes for South Africa's socio-economic goals and aspirations of for instance, SMME participation in information economies. The ECT Act endorses this view in the statement of objectives of the legislation as promoting an information economy for the economic and social prosperity of South Africa (RSA, 2002, s2).

Additionally, speaking to the low adoption of electronic commerce in South Africa versus comparable jurisdictions in a 2007 study, Warden cautioned that the electronic commerce trends in developing countries such as South Africa were reflective of a gap between information rich and information poor countries (Warden, 2007). Furthermore, a number of other international commentators establish that a country's use of e-signatures is a central issue in facilitating a country's participation in global electronic commerce (Parry, et al). The purpose of this research while examining the effectiveness of e-signature regulation directly may, therefore, further, be associated with broader socio-economic pursuits for South Africa including the pursuit of meaningful participation in information economies and global electronic commerce.

1.5 Audience and scope

It is intended for the outcomes of the research to be made available to the relevant policy-makers as a primary stakeholder to consider the findings. Perspectives of various stakeholders including lawyers, information security experts, electronic commerce experts etc. are impacted by the effectiveness of e-signature regulation and need to be consulted for the study

but will also as stakeholder groups, be target audiences. The research may also be of interest to international stakeholders looking to compare South Africa's approaches to other jurisdictions.

The topic for this research was selected initially to provide clarity on an issue that to date has not had appropriate investigation. It was also a topic of much personal interest to the researcher as an ICT lawyer. However, as the background research progressed for this Chapter One, it became clear that the results could contribute to the current dialogues on ICT policy matters.

Importantly, the scope of this research is focused on the 10-year period from 2002 and 2012. The approaches to provide a regulatory environment over the period provide key insights to inform current and future policy decisions. This is an industry that moves rapidly, as with any technology dependent sector. Any developments in 2013 and beyond were not considered.

1.6 E-Signatures and Advanced Electronic Signatures

This Report refers through the Chapters to the regulation of e-signatures in broad terms in reference to all forms of e-signatures and to the regulation of advanced electronic signatures (AeS) in specific terms in reference to a specific form of e-signature, as defined in the ECT Act. In accordance with the definitions of the ECT Act, the presumption that e-signatures include the AeS is intended unless a specific exclusion or distinction is contained in the relevant section of the report.

1.7 Structure of this research report

The study consists of six chapters. An outline and summary of the chapters is provided hereunder:

Chapter One: Background	This Chapter introduces the study by providing an overview of the e-signature regulatory environment at an international level. This Chapter also briefly outlines the significance of effective e-signature regulation and a cursory overview of the regulation of e-signatures in South Africa. The Chapter ends with an outline of the aims and objectives of the study through the statement of the problem and the purpose of the study.
Chapter Two: Literature Review	This Chapter provides a theoretical framework for the study, which includes review of theories of regulatory approaches, review of international regulatory approaches to e-signatures and the topics of analysis of e-signature regulation emerging from the literature considered. The

	insights associated with approaches in certain countries and related commentary available in the literature is cited. As such, this chapter introduces key definitions, terminology and approaches that are the analysis apparatus regarding South Africa's e-signature regulatory frameworks and approaches.
Chapter Three: Methodology	This Chapter details the methodology applied for this research. The Chapter will describe the research question and sub-questions that inform the qualitative study. This chapter speaks to the methods deployed to ensure the quality of the research, including triangulation and the development of research propositions in a conceptual framework that guides the boundaries of the case study. The research design provides for the logical planning of the study and the sustained reference to a conceptual theoretical framework emanating from the literature review.
Chapter Four: Results	This Chapter is comprises the results of the research. This chapter includes the findings on South Africa's current e-signature regulatory framework. This chapter reports on the results and outcomes of the interviews with key interviewees selected.
Chapter Five: Analysis	This Chapter is an analysis of the results of the previous Chapter in response to the research questions that frames the study. This involved the situating of the findings in the context of the conceptual framework to analyse the effectiveness of e-signature regulation developed at the conclusion of the literature review.
Chapter Six: Conclusions and Recommendations	This Chapter presents the conclusions and recommendations emanating from the study. This Chapter answers the research questions and sub-questions. The conclusions and recommendations consider the interests of the identified audience, the primary target audience being the Department of Communications. Finally, an outline of the limitations of the study is provided as well as the emerging research questions for future studies.

A full bibliography of all sources and references is included. Annexure A consists of the interview protocol used for the interviews conducted. Annexure B contains a reference list of the interviewees for this research.

1.8 Chapter Summary

In this chapter, an overview of the role of e-signatures within the electronic commerce landscape was provided; key reasons why their existence and effective regulation are important were introduced. The research problem statement is notably presented, before positioning the research question around regulatory effectiveness. A summary of the content each chapter of this report concludes this Chapter.

With this context in place, a comprehensive Literature Review describing the approaches taken in their pursuit of effective e-signature regulation will be provided to extract a conceptual framework for the study.

2 CHAPTER TWO –LITERATURE REVIEW

2.1 Overview of the Chapter

The problem statement and purpose of this research have presented propositions for the study of the electronic signature regulatory environment in South Africa - particularly its effectiveness in promoting greater adoption of electronic transactions through promoting trust, security and legal confidence in electronic commerce in South Africa. Further, the gap in knowledge for the country's policy-making community is to be addressed. The object of this Chapter is to consider a global context in expert insights and other relevant studies; approaches in model laws; and case studies as the basis for a conceptual model to guide the research and analysis concerning effective e-signature regulation and ultimately respond to the research questions. This Chapter builds, particularly, on the relationship between the electronic signature and electronic commerce to query within the literature the metrics for assessing how the regulation would support electronic signature effectiveness.

2.2 Ensuring the Legal Validity of an E-signature

When Kshetri discusses the barriers to electronic commerce and competitive business models in developing countries, the author relates that one such barrier is the lack of laws that provide legal validity to e-signatures (2006). Kshetri's paper included discussion of a survey conducted among Brazilian consumers that indicated that low electronic commerce adoption was related to concerns about government regulations on security (2006).

Other authors too point to the significance of the regulation ensuring the legal validity of electronic signatures as the fundamental enquiry of effectiveness (Blythe, 2007, Brazell, 2008, Wang, 2007). In China the absence of transactional and institutional trust due to a lack of rules and laws was a significant barrier to electronic commerce (Kshetri, 2006). Concurrently, Blythe's paper on China's new e-signature law and certification authority regulations described the development as a "catalyst for dramatic future growth of electronic commerce" (Blythe, 2007).

Brazell referenced the intent of UNCITRAL and European Commission's regulation of e-signatures as facilitating approval and affording legal validity to electronic documents in a manner representative of the nature and legal utility of traditional hand-written signatures for paper documents (Brazell, 2008).

Commencing with the enquiry of whether the law affords e-signatures legal validity, the enquiry extends in the views of other experts to whether parameters or conditions are placed on the legal validity (Forder, 2010, Menzel &Schweighofer, 1999) or a further functional analysis inquiry (Aalberts & Van Der Hof,2000) as to whether this legal validity is effectively provided for.

Forder cautions that in legal terms, the extent to which the (electronic) method is accepted where a legal requirement for signature is present is the critical inquiry (2010) i.e. whether any conditions or parameters are placed on the legal validity afforded to electronic signatures. Furthermore, what level of validity is afforded to e-signatures that are not constituted by encryption technological methods? Menzel and Schweighofer, in a 1999 paper prior to the key international frameworks for e-signatures being adopted, dealt with the issue of whether digital signatures (one form of e-signatures) may meet the legal criteria of determination of a person's identity in order to be substituted for hand-written signatures (1999). The authors concluded that digital signatures relying on asymmetric cryptography do in fact offer the "authentication" necessary and that together with certificates issued by trusted third parties which verify the identity of the relevant persons may indeed present an electronic equivalent to hand written signatures (Menzel & Schweighofer, 1999). Relating this to Mason's description of the attributes of signatures that renders them suitable for purpose, the need for technical or other standards for the legal validity of an electronic signature may be necessary.

Aalberts and Van Der Hof established a functional analysis inquiry consisting of three sub-queries to establish the validity of e-signature(s) (2000). This test commences with establishing the laws in a legal system that require a signature for certain legal transactions (Aalberts & Van Der Hof, 2000). The functions and characteristics that were necessary for the requisite signatures to must then be established, and finally extent to which the functions can be replaced by an electronic signature/ must be examined (Aalberts & Van Der Hof, 2000). Where the e-signature satisfies the performance of the functions, the e-signature is indeed a substitute for the traditional manuscript signature (Aalberts & Van Der Hof, 2000). The authors added that the prevalent legal theories of a country that construct the definitions of writing and signatures are influential for this inquiry and should be reviewed to fully contextualise and understand e-signature regulation (Aalberts & Van Der Hof, 2000). What emerges is that while the law is required as a first step to provide for the legal validity of electronic signatures, a significant next step inquiry is need to contextualise such validity and in so doing understand the effectiveness of the regulation in this area.

2.3 Expert Guidance on the importance of AeS Regulation

In Chapter One, a particular approach in establishing a form of signature with higher levels of assurance, the AeS in South African regulation was introduced. Even the Director General of the DOC is quoted as specifying the AeS as the key tool for promoting trust, security and legal assurances in e-commerce. This section equally emphasises issues of regulation of this particular e-signature in considering how e-signature products and services are regulated.

The point is made in the literature that for e-signature regulatory effectiveness the issue of accreditation of so-called advanced e-signatures is important (Blythe, 2007, Cole et al, 2008) and the progress made in implementing the regulation (Parry et al, Cole et al and Low et al) is also a critical perspective. The abovementioned literature reference the need to assess the effectiveness of regulation of e-signature products and services, particularly accredited services to deliver the trust and legal certainty associated with the products and services. There are several aspects to this quadrant of analysis. According to Kuechler and Grupe, the implementation challenges of (digital) signatures in any jurisdiction are constituted not only by technical issues but also by the legal authority that may be provided to regulatory bodies and legally binding agreements (2003). What is called for according to the American Bar Association is a framework of identity authentication that enables multilateral transactions via electronic commerce to address authentication and non-repudiation requirements, achieving the signatures function in the relevant society (American Bar Association, 2001). Kuechler and Grupe too refer to multiple aspects of regulation that would need to be assessed including: the reliability and security of the service provider; whether such provider adequately gathers the information to identify and verify the relevant person; the procedures when a certificate are no longer valid or the service provider closes its business; and the liability of the service provider; (2003). Another issue is the governance of such advanced e-signature service providers Kuechler and Grupe, note that they are "trusted holders of electronically accessible information on the companies that subscribe to their services" (2003, p25). Such service providers hold and make available key information as the primary constituent of the authentication system including the keys that encrypt and decrypt digital signatures. They also hold the identity data of the certificate holders including personal information (Kuechler, 2003).

From the above, a set of factors to assess the completeness and adequacy of electronic signature regulation in how it regulates the AeS service provider emerges. In the section below, model law approaches are consulted on guidance on the approaches taken, at times aligned and at times in variance, to guide national legislators on how to promote the

effectiveness of their respective e-signature regulation. As such, a scan of model law provisions for key principles and approaches, and at times, expert commentary is set out in 2.4 to be consulted in the analysis of South Africa's approaches.

2.4 Model Law Approaches to Regulation of E-signatures

2.4.1 UNCITRAL Model Law on Electronic Commerce (1996)

According to Fischer, the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce "intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of formats" (Fischer, 2001)

In addition to providing a general legal framework for electronic commerce, the Model Law provides a general legal construct for signatures in the electronic realm (UNCITRAL, 1996, art 2, 6, 7). Article 7 provides that where the law requires a signature of a person, that requirement is met if a method is used to identify that person's approval of the information contained in the data message (UNCITRAL, 1996). Further, the method must have been as reliable as was appropriate for the relevant purpose of generating or communicating the data message in light of the circumstances and any agreement (UNCITRAL, 1996). According to Brazell, this approach borrows from the traditional requirements for a handwritten signature otherwise referred to as a manuscript signature with the focus of the provision being identification of a person, assurance that the person intended to sign and connect the person with the electronic document (2008). Blythe refers to this approach as a "technologically neutral" approach as the Model Law consists of "broad guidelines" and not detailed requirements and as such is not specific to any technological circumstance (Blythe, 2005 p6).

2.4.2 UNCITRAL Model Law on E-signatures (2001)

The UNCITRAL Model Law on E-signatures was adopted in 2001 to provide supplementary provisions to the abovementioned model law in relation to e-signatures (Blythe, 2001). The Model Law defines an e-signature as "data in electronic form in, affixed to or logically associated with a data message, which may be used to identify the signatory in relation to the data message and indicates the signatory's approval of the information contained in the data message UNCITRAL, 2001, art 2(a)" Additionally the Model Law refers to a certificate which, is "a data message or other record confirming the link between a signatory and signature creation data (UNCITRAL, 2001, art 2(b)". The Model Law on E-

signatures re-emphasises the issue of reliability of the e-signature as per Article 6 and provides a reliability test that inquires, for instance, whether the alteration to the e-signature following the time of signing is detectable and whether signature creation data was at the time of signing, under the control of the signatory and no other person (UNCITRAL, 2001). Brazell relates that this approach of the Model Law was a restrictive approach with the primary focus on public key encryption. In the end, the Model Law established a two-tier system – a tier of signatures developed to meet the reliability requirements whilst subject to rebuttal of legal validity and a second tier of signatures that will have to be assessed regarding the reliability in the circumstances. Blythe's view is that the technologically neutral approach of the electronic commerce model law was preserved, however, standards were introduced for under which different e-signature technologies should be used (2005).

On the issue of trustworthiness, as described in the earlier section on Certification Authorities, the Model Law stipulates that it is the certification service provider that is assessed for trustworthiness on a variety of criteria (UNCITRAL, 2001).

2.4.3 EU E-signatures Directive (1999)

Probably the first significant aspect is that the Directive provides a differentiation between an e-signature and an advanced e-signature:

- An e-signature refers to "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication";
- An advanced e-signature (based on a qualified certificate) is uniquely linked to the signatory and; is capable of identifying the signatory; it is created using means that the signatory can maintain under his sole control; and is linked to the data to which it relates in such a manner that any subsequent change of the data (EU Commission, 2000, art 5)

Then specific mention is made of electronic signature certificates. A certificate is defined as "an electronic attestation which links signature-verification data to a person and confirms the identity of the person (EU Commission, 2000, art 5). According to Brazell, the definition would include standardised certificates such as the ITU X.509[1] format and a qualified certificate is one that meets the requirements set forth in Annex I of the Directive including the identification of the

1

certification service provider, signature verification data which correspond to signature creation data, an indication of the period of validity and identity code of the certificate (2008).

A further distinction is made. Article 5 of the requires Member States to ensure that: advanced e-signatures (AeS), based on a qualified certificate and created by a secure signature-creation device, meet the legal requirements of a signature in relation to electronic documents in an equivalent manner to hand-written signatures for paper and are admissible as evidence. This, however, is subject to a caveat - the legal validity and admissibility of an electronic signature should not be denies solely because: the signature is in electronic form; is not based on a qualified certificate or a certification service provider; or the certificate was not created by a secure signature creation device (EU Commission, 2000)

Forder described the EU Directive approach as a two-tier approach where that e-signatures should not be invalid purely for their electronic form; or purely because failure to qualify as an advanced e-signature and commended the approach as a an open and less restrictive approach when compared to the 1996 UNCITRAL Model Law approach (2010). Winn suggests that the E-Signature Directive actually culminated as an attempt to accommodate government's polar approaches of being technology neutral by countries such as the UK and technology specific approaches by countries such as Germany (2010). According to Winn, the EU Directive had to respond to the reality that while certain countries looked to substantive regulation for additional certainty, other countries looked to the private sector to self-determine the rules of the Internet economy (2010). Notwithstanding the regulation, market adoption of advanced e-signatures has, however, remained low (Winn, 2010) A recent online article announced that the EU Commission has announced a review of e-signature laws (Evans, 2011). According to the article, the review of e-signature laws is a much-needed update to cope with the changes in regulatory demands of electronic commerce. According to a Commission statement reported in Evans article, "Low levels of consumer and business confidence when making transactions online are one factor holding back the development of the EU's online economy...Relying on secure, trustworthy and easy to use online services is vital for a strong and healthy European Digital Single Market." The Commission's statement further spoke to issues of regional co-operation to promote the effectiveness "electronic signatures and electronic identification and authentication can be an important tool to enable both users and providers to rely on secure, trustworthy and easy-to-use online services but must work in all Member States to be effective." (Evans, 2011).

On the outset, the Model Laws reveal a number of significant approaches to the regulation of e-signatures. The almost instinctive response of the UNCITRAL Model Law on Electronic Commerce provides a broad acceptance of electronic

methods of signing electronic documents conducive to the legal validity of electronic transactions. The subsequent UNCITRAL Model Law on E-signatures has a deeper focus on the security and authenticity of the method of signing. Referring to public key infrastructure, several aspects of the digital certificate that is the advanced e-signature are detailed - the security and authenticity of the relevant electronic transaction is linked to the assessment of the way in which the digital signature is able to identify a signatory and associates or verifies the data. The Model Law on E-signatures further provides the criteria for the assessment of the relevant AeS to which the service provider must adhere for accreditation. A dependency on the certification process emerges in the regulation, which will in turn determine the availability of the AeS in the market.

The EU E-signature Directive, also a subsequent model law to the UNCITRAL Model Law on Electronic Commerce, takes a similar approach to the Model Law on E-signatures. Both the UNCITRAL Model Law on E-signatures and the EU E-signature Directive reveal a reluctance to restrict e-signatures to such advanced digital certificates and remain open to other forms of e-signatures. As a result they establish two-tiers of e-signatures that have varying legal validity. These tensions between the forms, functions and legal validity have resulted in a typology of approaches to the regulation of e-signatures discussed below. Finally, the inquiry of effectiveness of approaches is noted in the commentary on the Model Laws with market adoption of e-signatures in the EU is low. Commentators vary in their favour of technologically neutral approaches or the endorsement of digital signature approaches.

2.4.4 Specific regulation of the Service Provider

As stated above, there is particular emphasis on the regulation of the AeS service provider. The European Commission E-signatures Directive provides that a certification service provider is defined as “an entity or a legal or natural person who issues certificates or provides other services related to e-signatures” (EU Commission, 2000). Under the Directive the certification service provider may issue qualified certificates subject to meeting the criteria specified in Annex II of the Directive (EU Commission, 2000). The criteria include: (i) ensuring precise determination of the data and time when a certificate is issued or revoked; (ii) appropriate verification (per national law), the identity and if, applicable attributes of the person to which the qualified certificate is issued; (iii) employing persons with the relevant and necessary knowledge experience and qualifications necessary, (iv) maintaining sufficient financial resources for its functions and obligations; (v) using trustworthy systems and products protected from modification, (iv) taking measures against forgery and guaranteeing

confidentiality (EU Commission, 2001). Whilst the Member States are precluded from such certification service providers be accredited or licensed or registered (EU Commission, clause 12, art 3(1)), Brazell contends that Member States are, however, permitted to establish independent standards and methods of enforcing the requirements on certification service providers (2008). With this insight, the possibility of self-regulation of service providers is observed as permissible in the EU.

The EU Directive also deals with the issue of liability of the certification service providers. The providers may be liable for damages suffered by any person (natural or legal person) relying on the qualified certificate for accuracy or assurance of signature related information or that the signature was not revoked (EU Commission, 2000, art 6).

Article 7 of the EU Directive pertains to foreign certification service providers providing for bilateral or multilateral agreements that provide for recognition of the foreign provider's certificates and vice-versa (EU Commission, 2000). Member states are required to provide equivalent legal validity to providers outside the EU subject to the provider meeting the requirements of Annex III and being accredited under a voluntary accreditation scheme or an EU provider guarantees that the foreign certificate meets the requirements of Annex III or the certificate or provider is recognised under a bi-lateral or multi-lateral agreement. (EU Commission, 2000).

Comparatively, the other Model Law that considers such service providers is the UNCITRAL Model Law on E-signatures which is focussed on the issue of trustworthiness, and that the certification service provider is assessed for trustworthiness (UNCITRAL, 2001). According to Article 10, the certification service provider's financial and human resources, quality of hardware and software as well as procedures for processing of certificates are included in the assessment of the certification service provider's trustworthiness (UNCITRAL, 2001).

It appears that the regulation casts a spotlight on the service providers that offer advanced electronic signatures, referred to in certain of the model frameworks as CA's or certificate service providers. Furthermore that e-signature regulation effectiveness has a particular component of effectiveness in how it is able to provide for efficiencies and assurances regarding the AeS. For instance, significant review of the procedures and processes of the service provider, the liability of the service provider, whether the country permits self-regulation and recognition of foreign providers all describe at least the adequacy of the regulation in dealing with such areas. The analysis of the approaches and whether the key requirements are provided for should then be analysed for effectiveness.

2.5 Regulation of E-signatures in the UK, Australia and China

The following examination of e-signature regulation in three distinct jurisdictions establishes central tenets in the e-signature regulation: a primary law that provides for the legal validity of the e-signature, typically associated with one or other Model Law and regulations that provision the role of an e-signature certification authority or certification service provider.

2.5.1 UK

In the UK, the Electronic Communications Act 2000 (ECA) and the E-signatures Regulations 2002 which implement European Union (EU) Directive on E-signatures govern e-signatures (Arias, n.d). An e-signature is defined in the ECA as "electronic data that is attached to or logically associated to other electronic data and that serves as method of authentication" (Arias, n.d. p1). In accordance, the UK's ECA is described by Brazell as minimalist as it does not assign or distinguish legal validity of different forms of e-signatures. The 2002 Regulations, however, refers to an 'Advanced E-signature' (AES) with the following key features: (i) it is capable of identifying the signatory; (ii) is uniquely related to the signatory; (iii) is under the sole control of the signatory; (iv) the signature attaches to the communication or data in a manner that allows future changes to be detected (UK, 2000).

The Regulations have been described as having limited scope and application. According to a commentary on legal website, www.outlaw.com, the Regulations primarily speak to issues of the regulation of certification service providers (CSPs) or "businesses that issue certificates in support of e-signatures" (Outlaw, 2008) and the process of verifying a person's identity by the CSP (Outlaw, 2008). The Regulations provide that the Secretary of State is given the duty of reviewing CSP activities and setting up a register of CSPs that issue qualified certificates to the public. There is an industry run scheme known as the tscheme for accreditation (www.tscheme.org). According to Brazell, under section 16(4) of the Electronic Communications Act, the administration of accreditation was left with tscheme for five years and the time for the government to establish its own scheme has lapsed.

The Regulations also impose liability on CSPs to the extent that they either issue or guarantee qualified certificates to the public. The liability of certification service providers is aligned with section 6 of the EU Directive with additional liability for failure to provide information as required in Annex I of the Directive (Schedule 1 of the Regulations). In such

circumstances, a CSP is liable to anybody relying on the certificate for, among other things, the accuracy of the information contained within the certificate at the time of issue (Outlaw, 2008)

The Act does not provide for recognition of foreign certificates or certification service providers (Brazell, 2008)

Other legislation such as the Consumer Credit Act governing certain credit and hire contracts with consumers was amended to permit the use of e-signatures Brazell, 2008, p 200). In the UK, the substantive legislation is supported by relevant cases. In one case - the court deliberated on whether a name typed at the end of a telex was a signature as an acknowledgement of debt and determined it did, to the second case concerned an automatically added email header constituted a signature and the court found it not as it was not consciously added by the signatory (Brazell, 2008).

2.5.2 Australia

The Australian Electronic Transactions Act, 1999 provides that e-signatures shall possess the legal validity of hand-written signatures for the purpose of Commonwealth legislation (Australia, 1999) The descriptions of e-signatures closely resembles the UNCITRAL Model Law on Electronic Commerce and is described by Brazell as being technologically neutral, by virtue of the lack of prescription of any specific technology (Brazell, 2008). While primarily implementing the 1996 UNCITRAL Model Law on Electronic Commerce, the legislation has two points of departure; the beneficiary of the communication in question to which the signature is attached should consent to the use of the e-signature and critically, the method of signing must be appropriately reliable (Forder, 2010). The prescribed conditions for reliability include:

- the method must have been used to identify the person and indicate the person's assent of the relevant information; and
- the method was reliable with regards to the purpose of the communication and the relevant circumstances;

Specific technological requirements of the commonwealth entity are met alternatively, where the entity is not a commonwealth entity, such person consents that a method was used to identify a person and indicate their assent to the information (Brazell, 2008).

Forder's criticism of the Australian Electronic Transactions Act is that the legislation does not offer much in the way of regulating e-signatures and projects that signature users are likely to be required to evidence the reliability of the particular type of e-signature used (2010). One such case determined a typed name in an email was a signature as relevant for the purpose and another case determined that an email header can function as an e-signature (Forder, 2010). This judgement

together with Forder's argument offers the question as to whether the Australian ETA tenders much in the way of e-signature regulation or whether the reliance is mainly on the common law.

Brazell provides that while the Electronic Transactions Act does not provide for the regulation of certification service providers, an accreditation programme, Gatekeeper, was established for providers of services to public administration (Brazell, p 334).

Forder, in speaking to the inadequacy of the legislative response to e-signatures in Australia based largely on the 1996 Model Law on Electronic Commerce, extracts the following as the primary challenges with such approach: (i) through technological developments, myriad signature technologies would offer the "appropriate reliability", however, the need to explain the manner in which this is achieved presents a technical evidence challenge (ii) the evidence necessary to satisfy variable reliability requirements for the various transactions represents a second uncertainty (iii) the apparent duty to present such evidence for each relevant inquiry is "tedious and "wasteful of time" and (iv) the apparent reliance on legal cases to provide the clarity required is not a suitable response (2010, p12-13)

Forder in the review of the Australian legislation and approach to the regulation of e-signatures suggests as opposed to a two-tier approach, a multi-tier approach. According to Forder, while a top tier might still address the least flexible transactional requirements through a digital signature and bottom tier required a mere technology that satisfied the reliability requirement, between these levels, a manner of assessing signatures for reliability according to intended transactions accommodating of technological advancements but speaking to authentication, security and reliability would provide signature users with guidance on the choice of signature for specific transactions(who are further able to rely on the guidance to evidence that it was suitable or fit for purpose) (Forder, 2010, p13).

2.5.3 China

China's E-signature Law2 (ESL) of 2005 had three primary intentions (i) granting e-signatures legal validity equivalent to the manuscript or handwritten signature (ii) provision of the processes surrounding the use of e-signatures and (iii) providing for the rights and responsibilities of various parties including the parties to an electronic transaction (Blythe, 2007, Brazell, 2008).

[2] Order (No. 18) of the President of the People's Republic of China, LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON E-SIGNATURE

The definition of an e-signature provided by Srivastava (2005) is aligned with the definition in model frameworks but Wang criticised the exclusion of the requirement of a signature date to be logically associated with the message from the definition as in other countries and cautioned that this exclusion may create confusion as the judiciary may not find signatures sent separately to the message as acceptable under the law (2007). Articles 13 to 26 are premised on the reliability of e-signatures, e-signature certification service providers and e-signature certificates. Article 13 connects the reliability of an e-signature to the requirements of an Advanced E-signature in the EU Directive and affirmative responses to the following inquiries: whether the data used for creating the e-signature is exclusively owned and controlled by the electronic signatory and whether the signatory can trace or retrieve modifications to the e-signature or the electronic message following the signing (Srivastava, 2005). Srivastava extracts that while such reliable e-signatures may refer in practicality primarily to digital signatures, there is a rationale for not using the term digital signatures which is a reluctance on the part of the regulator to hinder the use of other signature technologies and secondly to limit the outdating of the legislation in the face of new technologies (2005). Blythe nevertheless asserts that China has offered a superior standing to the digital signature in its regulation (2007). In relation to Article 16, that typically requires the authentication of the e-signatures to be conducted by the certification authorities established in accordance with the law, Srivastava's challenge is that it is unclear which transactions would require a certified signature and secondly which category of signature requires certification (Srivastava, 2005). Wang, however, refers to this approach as affording the Chinese public the autonomy to select the appropriate e-signature technology that meets the reliability requirement and the autonomy to decide whether to use an e-signature at all (Wang, 2007. Other salient provisions in the context of this study, noted by Srivastava are (i) the regulatory standards established for CSPs typically including competent human resources, financial sustainability, and the imposition of security standards (ii) legal recognition of foreign e-signature certificates issued by CSPs outside China following approval after a relevant agreement or where there is a principle of reciprocity of recognition and (iii) uniquely, three conditions in which an electronic signatory shall be liable for damages where the signatory is aware that e-signature creation data (private key in case of digital signatures) has been descrambled or may have been descrambled but fails to inform the relevant parties in a timely manner and fails to stop its usage, failure to provide accurate information when applying to the CSP and commission of a fault resulting in loss to parties relying the signature or to the CSP.

In China, questions as to other inhibitors to the success of electronic commerce and e-signatures are also widely discussed. Blythe comments that fundamentally, the Chinese people are reluctant to transact online or through credit or debit cards and prefer cash transactions. Underdeveloped credit rating systems and inefficient postal services further inhibit

electronic commerce (2007). Blythe was, at the time of writing the article, confident that e-signature law and the certification authority regulations are conducive to promoting secure and trusted payment systems and would catalyse electronic commerce success in China (2007).

Whether this confidence was well placed is a critical inquiry. On the one hand, Wang referred to a Research Report on the Development of Electronic Certification Service in China 2004 where the following emerged - China had over 100 certification authorities and each of these authorities issued between 1000 and 600,000 certificates (2007). The above statistics were, however, qualified by the fact that 80% of the certificates issues are for use in e-government and in 2006; there were only 20 licensed certification authorities (2007). Winn and Song's 2007 research queried the efficacy of electronic commerce law reform for positive electronic commerce outcomes concluding "dim prospects" (2007, page). Winn and Song provided that law reform was a policy instrument with limited measure of results while transitioning to a market economy asserting that Chinese businesses would benefit from legislation that accounts for unique Chinese conditions rather than transplantation of foreign approaches with the primary criticism being (i) the promotion of a technology that is not broadly used, consequently, while the law intended to be technology neutral it actually leaned heavily toward a single technology (Winn and Song, 2007).

To summarise, each of the countries examined established a hierarchy of forms of e-signatures associated with levels of reliability or security and trust. In each case, the opinion of the authors assessed is that a more trusted signature references the attributes of a digital signature while not being prescriptive of particular digital signature technologies. Fundamentally, the advanced signature is certified as using acceptable technology that increases the security of the message and forms a reliable method of identifying the signatory. What results is described by Blythe as a system constituted by requirements for (i) the advanced signature (ii) the technology (iii) the certification service provider. In accordance, the primary laws that govern e-signatures are supplemented by regulations that govern the certification and certification service providers of so called advanced signatures. Furthermore, in the UK and Australia, there is a reliance on the common law for deciding on the acceptance of the e-signature, which leads to the understanding that the legal prescriptions and regulation are additionally joined by the decisions of courts to provide a body of reference on the regulation of e-signatures. Finally, in certain countries, commentators have challenged the approaches, with China's regulation being arguably insufficiently responsive to the needs of the market and Australia's legislation criticised for the lack of legal certainty and a reliance on case law for the determination of the reliability of e-signatures.

2.6 Emerging Typology of E-signature Regulatory Approaches - The Digital Signature, Two-Prong and Minimalist Approach

From the above, it is apparent, that e-signature regulation has been a subject of regulatory interest and concern in the context of promoting electronic commerce. What is sought ultimately is an understanding of whether the approaches to regulation are effective or in need of amendment to accommodate either technological change or to address legal and market issues arising in the countries. It is clear that interest on this subset of electronic commerce regulation is generating not only focussed regulatory experts but also a typology of approaches to e-signature regulation as a frame of reference for comparison.

Chronologically, Blythe refers to three eras of e-signature laws since 1995 (2007). The earliest of which referred to digital signatures only, followed by a more open approach towards various forms of e-signatures, followed by a third approach that moderates the first two providing legal validity to several forms of e-signatures but a higher level of preference for digital signatures (Blythe, 2007).

Aalberts and Van Der Hof establish the distinction in the approaches as follows:

- The digital Signature approach is technology specific. Regulation is focused on legal and evidentiary validity of the digital signature as a method of authentication;
- The two-prong approach provides technological criteria for e-signatures, but also allows for new technologies. A distinction is made between those that satisfy the basic requirements and additional legal authority is provided for e-signatures that exceed the authentication criteria; and
- The minimalist approach is technology neutral. It focuses on the functions of an e-signature, which may be applied to various signature formats to determine their legal validity.

According to Smedinghoff and Bro, the approaches can be arranged according to the level of regulatory control. In the minimalist approach, this is a mere authorisation in law for e-signatures. The second level is law that offers “evidentiary presumptions and default provisions” subject to change by consensus between the persons entering into the transaction. The third is “highly regulated” approach associated with digital signature technologies and certification authorities (1999, p5).

What is the significance of the difference between technologically neutral, technology specific or the two-prong approaches? Aalberts and Van Der Hof describes the tension between technology neutral and technology specific legislation as (i) the tension between the need to ensure that legislation responding to new technologies is not soon outdated or irrelevant on the one hand, and (ii) the need to ensure that adequate legal consequence and assurance is prescribed for the relevant emerging technology on the other hand (2000). According to the authors:

- technology specific legislation is relevant where for instance specific insights are necessary for complex technologies and technology neutral legislation provides inadequate security for the rights and duties of the relevant stakeholders and the benefit is that case law will not be required to determine the legal position as the legislation offers the necessary clarity;
- technology neutral legislation, however, provides functional equivalence to e-signatures regardless of form, often supplemented by affording the relevant government the authority to issue further regulations, as necessary (2002).

From the above, the foremost insight is the reluctance in the regulation to prescribe e-signature technologies. However, this reluctance can render e-signature regulation out-dated and unable to provide adequate legal certainty. The result is regulated standards for e-signatures appropriate to the security or authenticity requirements of the electronic transaction as a key requirement and an openness to further determination by case law or further regulations. Irrespective of the approach, however, Smedinghoff and Bro asserted that ultimately, the intent of the regulation should be measured by the ability to "remove barriers to e-commerce", and facilitate electronic commerce through the promotion of trust and certainty (1999, p5). The purpose of the above inquiry of the approaches is, therefore, whether the regulatory approach taken, in this study in South Africa, is suited to deliver e-signatures that create trust in electronic commerce transactions and legal certainty that in turn, promote electronic commerce.

2.7 Extracting a Conceptual Framework

The analysis of the literature concerning e-signature regulation reveals notable depth and diversity in approaches. However, key components, approaches and terminology emerge that define and distinguish the regulation of e-signatures as set out below:

Table 2.1: Conceptual Framework for Analysis of Effective Regulation of E-Signatures in South Africa

Analysis of Electronic Signature Regulation in South Africa		
Legal Validity of Electronic Signatures	**Regulation of Electronic Signature Products and Services**	**Harmonisation of Approaches to Regulation of Electronic Signatures**
• How does South Africa n law provide for the legal validity of electronic signatures? • How does South Africa define and distinguish between the forms of electronic signatures and what is the impact of such definitions on the validity of electronic signatures? • How does South African case law deal with the legal force of electronic signatures?	• How are electronic signature products and services, particularly advanced electronic signatures regulated? • How does South Africa deal with foreign signature service providers? • How does South Africa' regulation provide for the information security standards for electronic signature products and services?	• How does South Africa's approaches to electronic signature regulation compare with international frameworks and foreign regulatory approaches? • Is South Africa's approach to electronic signature regulation aligned with developments in regulatory approaches that advance electronic commerce
Advancement of trust, legal confidence and security in electronic commerce		

The conceptual framework above represent the themes and inquiries associated with the analysis of e-signature regulation in the context of electronic commerce objectives stemming from the literature review, with a South African perspective. Notably, the frames for analysis of the effectiveness of the regulation of e-signatures pertain to issues of legal validity, the nature of regulation of the e-signature products and services to promote trust and security and the level of harmonisation and currency with international developments as well as lessons learnt. This conceptual framework will be used to examine

the regulation of e-signatures in South Africa in Chapter Four and will be used in Chapter Five to support the analysis of South Africa's regulatory approaches.

This framework tends to align to a large extent with Guermazi and Satola's encapsulation of the components of the regulatory framework for e-signatures including approaches to (i) affording legal force (validity) to e-signatures whether by form or function, (ii) incorporating standards for e-signature technologies and the accreditation of so-called e-signature service providers and government approval of technologies (2006). The added pillar in this study is the consideration of the level of harmonisation of approaches. This additional pillar is in relation to the aspect of the research undertaking pertaining to policy and regulatory recommendations. For this purpose, aspects of commonality, variation and insights into effective approaches are necessary.

2.8 Application of International Theory and Expert Perspectives

In apply the conceptual framework, there is a critical question pertaining to the implications of international theory and expert perspectives – how does commonalties and distinctions in approaches impact South Africa's regulatory effectiveness? While certain authors motivated for the regulations to represent minimum international standards that contribute to interoperability of e-signature technologies and global commerce (Guermazi and Satola, 2003), other authors cautioned national governments about the pressure stemming from existing and emerging information society regimes (Cogburn,2003). Hence, in anticipation of the analysis that follows in Chapter Five, ultimately the issue of effectiveness of e-signature regulation is not a question of absolute conformity but rather whether and to what extent minimum international standards conducive to the nature of global electronic commerce are present.

Ultimately the framework must determine whether electronic signature regulation in South Africa is effective in promoting adoption of electronic signatures as a tool for trust, legal confidence and security in electronic commerce. The outcomes of the interviews and the findings on the developments of South Africa's e-signature regulations, while primarily geared to respond to the conceptual framework above, shall, however, deviate, as it must, to accommodate insights and commentary that add a veil of general qualitative value as is typical of a qualitative case study approach. While Wang suggested uniform law, she cautions that the variation in the different countries of economic and technological conditions make this difficult to achieve (Wang, 2007).

Ultimately, these insights and cautionaries on conformity and harmonisation will also be considered for the conclusions and recommendations produced.

2.9 Summary

The literature reveals certain primary and influencing model frameworks such as the United Nations Commission on International Trade Law (UNCITRAL) Model Laws for Electronic Commerce and E-signatures and the European Union (EU) Directive on E-signatures prepared by the European Commission. Notably, model frameworks and national regulatory approaches acknowledge and agree that e-signatures principally require legal validity to serve their primary function of authenticating and promoting trust in electronic contracts emanating from electronic transactions.

Whilst national (country specific) legislation tends to extract key tenets from at least one of the frameworks, the approaches are notably varied. One author described the comparative e-signature regulatory frameworks of several countries as "divergent and fragmentary" (Wang, 2007). Countries tend to have diverse positions on whether an e-signature is a functional substitute for the hand-written signature and the criteria to establish the functional equivalence. Certain countries have relied on case law for additional guidance whilst other countries have required that the legislation offer the necessary legal certainty. The regulatory approaches reviewed further evidence the establishing of hierarchies of reliance on the various forms of e-signatures. This is evident in emerging definitions and distinctions in law between the *e-signature*, the advanced e-signature and the digital signature.

What emerges, further, is that the manner in which function and form of the e-signature is dealt with has uncovered qualified approaches to the regulation of e-signatures discussed as the *minimalist approach*, *two-prong approach* and *digital signature approach* against which national approaches can be analysed.

Countries have also had varied approaches to the regulation of e-signature products and services and a process of approval for certain e-signatures in the form of certification and accreditation for e-signature products, services and *service providers* is revealed. The approaches to the recognition of foreign e-signatures present a further area of distinction particularly in relation to the ease with which e-signatures accredited in foreign jurisdictions are accepted in the country in question.

The identification of similarities and variation, and the nature and cause thereof, presents an opportunity for comparative analysis and ultimately, an extraction of a conceptual framework for the study of South African e-signature regulations. As

such, this Chapter concludes with a conceptual framework on the tenets for the assessment of the effectiveness of the regulation of e-signature against which South Africa's approaches can be compared and examined in Chapter Five. The Chapter is also interspersed with comment on the challenges associated with regulating e-signatures and recommendations emerging from the literature for effective e-signature regulation.

3 CHAPTER THREE – METHODOLOGY AND RESEARCH DESIGN

3.1 Overview of the Chapter

Chapter One clarified the research question, context and problem statement for e-signature effectiveness in South Africa in Chapter 1. The literature review in the previous chapter provided comparative analysis from research conducted into the UK, Australia and China, as well as model laws from other jurisdictions. We are now in a position to consider an approach to this research and describe the methodology to be used. As such this Chapter posits the research questions, research design and the methodology applied to the research. Analytical, qualitative research approaches with attributes common with the case study method will be discussed. Assumptions that informed the research design are examined.

3.2 Research Questions

3.2.1 Main Research Question

As discussed in Chapter One, South Africa promulgated e-signature regulation as a sub-set of the electronic commerce regulation to advance electronic commerce in South Africa. Chapters One and Two revealed that internationally (i) e-signatures are widely accepted as serving objectives of legal assurance, trust, privacy and security in electronic commerce and (ii) e-signature regulation is enacted to promote the utility of e-signatures to serve such objectives and ultimately, advance electronic commerce. The ECT Act and ancillary Accreditation Regulation being the primary regulatory texts provide prima facie for (i) the legal effect of e-signature methods (ii) distinction between so called e-signatures and advanced e-signatures capable of additional technical authentication of the identity of the holder of the signature (ii) establishing criteria for the accreditation of authentication service providers that authenticate advanced e-signatures and (iii) provisions for the establishment of Accreditation Authority to regulate accredited signature service providers. The above provisions, the manner of application of such provisions, and the resulting regulatory practices constitute the South African e-signature regulatory framework.

The primary research inquiry is the effectiveness of the above regulatory provisions and emanating regulatory approaches for the advancement of electronic commerce. The primary question, hence, with reference to the South African case, is: How effective is the South African e-signature regulatory framework for promoting the adoption and use of e-signatures to advance legal assurance, security, and trust in electronic commerce?

3.2.2 Research Sub Questions

Each of the sub questions should be eligible constituents of the main inquiry of effectiveness of e-signature regulation but provide a meaningful bridge from the inquiries of the conceptual framework to the main research question. Hence, these sub-questions are:

- How effective is South Africa's e-signature legal framework for the promotion of legal confidence in electronic commerce transactions?
- How effective is South Africa's regulation of e-signature products and services to promote trust, information security and user confidence in electronic commerce?
- How effective are South Africa's e-signature regulatory approaches when compared with primary international model laws?
- How effective are South Africa's e-signature regulatory approaches when compared with other country frameworks and approaches?
- How would South Africa be impacted by the continued reliance on the current e-signature regulatory framework and approaches?

3.3 Research Methodology– Qualitative with Case Study Components

3.3.1 Qualitative Study

In order to extract insight on the effectiveness of the regulation under study, both observation of the current regulation and exploration of the effectiveness of the implementation are needed. E-signature regulation intends to promote security, trust and legal confidence associated with electronic commerce hence, further than pure legislative review, or surveys, situational and contextual data is necessary to understand the effectiveness of South Africa's e-signature regulation in association with the regulatory goals. Furthermore, the research question points to several interlaced inquiries represented in the sub-questions, drawing from frames of analysis represented in the conceptual framework, reliant on the perspectives of various experts. The nature of the research method needed to accommodate the researcher's objectives and pursuit of a rich and well considered study.

The qualitative case study approach as defined by several commentators was deemed most suitable. According to Denzin and Lincoln, qualitative studies "implies an emphasis on the qualities of entities and on processes and meanings that are not experimentally examined or measured in terms of quantity, amount, intensity, or frequency" (2000, p.8). This utility in review of processes and meanings as well as Cassell and Symon's assessment of qualitative methods for inquiries on processes, outcomes and experiences promotes the application of the qualitative methods for this study. (Cassell and Symon, 1994, p.1). Inherent in this research and essential to its success is the ability to account for the alignment of outcomes with regulatory intentions, the efficacy of processes imposed by the regulation as understood by the experience of the varied experts interviewed.

Baxter and Jack reflect on the utility of the qualitative case study, more specifically, as a method that promotes and facilitates exploration of the occurrence under study contextually with the reliance on various data sources (Baxter and Jack, 2008). Yin promotes a qualitative case study for explore those situations in which the intervention being evaluated has no clear, single set of outcomes, to answer a question that sought to explain the presumed causal links in real-life interventions that are too complex for the survey or experimental strategies and the explanations would link program implementation with program effects (Yin, 2003). Clearly this research must accommodate various data sources to reflect on substantive regulation and its implementation but what is critical is to ensure that causal associations are made between metrics for effective regulation of e-signatures, the documentary content analysis the experience and perspectives of the experts. The nature of the study further corresponded with Yin's explanation of when the case study is best applied – where the focus of the study pertains to how and why questions and the research intends to reveal the context of the issue under study, as the researcher believes the context will be relevant to the research question (2003). Most importantly, however, the qualitative case study presents an opportunity to consider the data under the sub-issues distinctly and then analysed across the sub-issues which promotes the richness of the analysis and bolsters the understanding of the case in question (Baxter and Jack, 2008). This study is clearly an inter-weaving of various sub-issues to ultimately reflect on the main research inquiry.

3.3.2 Case Study Aspects

Certain case study attributes were selected for the research ultimately due to the method's inherent utilities in (i) assisting with the extraction of the regulation of e-signatures in South Africa as a specific unit of electronic commerce regulation for

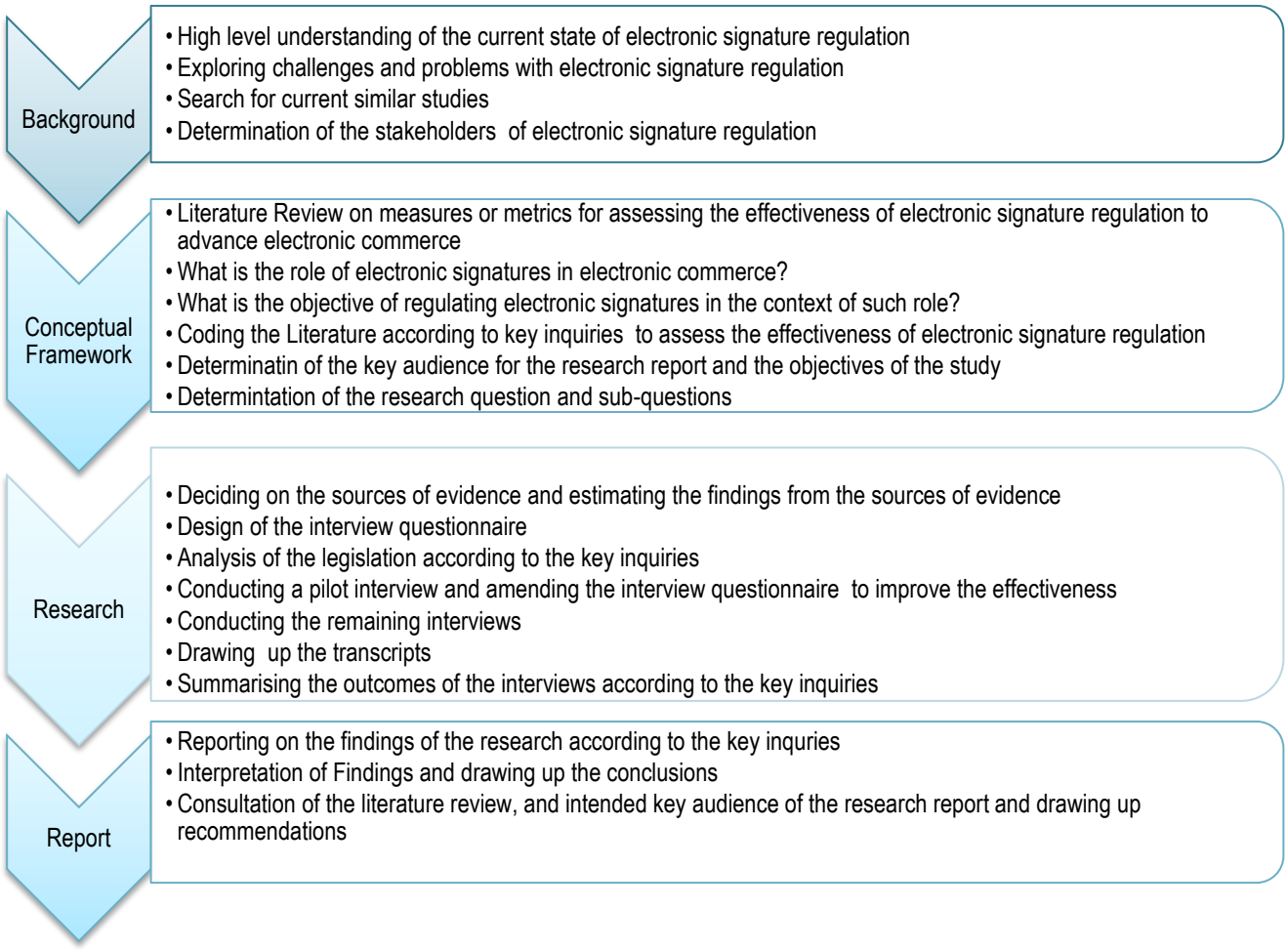
analysis; and (ii) formulation of meaningful appraisal from a variety of interconnected sources of data and research methods. What was deemed necessary and critical was a more in depth study of the effectiveness of particularly, e-signature regulatory approaches as opposed to electronic commerce regulation in general - which specificity of study was lacking in South Africa. This objective correlates with the utilities of case studies described in the literature: defined as: “an intensive analysis of an individual unit stressing developmental factors in relation to the environment” (Merriam-Webster, 2009). Flyvbjerg emphasises that the “demarcation of boundaries” is the key characteristic of a case study (Flyvbjerg, 2011 p301) and using case studies to extract and study a particular aspect is one of the benefits noted by Patton (1987). 301). To assess the effectiveness, legislative sources as well as interviews, review of case law and secondary materials was necessary to promote rich, qualitative inquiry and analysis whilst still accommodating the South African case context for the conclusions. Flyvbjerg directs that amongst the critical characteristics of case study undertakings is the “depth” of the research, the bringing together of several “interrelated events” and the ability to separate research data that is constituent of the case or contextualises the case (2011 p301).

3.4 Research Design

According to Herold, a research design pertains to setting out a plan for the transitioning from the beginning to the end of the research i.e. the initial inquiries to the final conclusions associated with such inquiries (Herold, 2011). Hartley concurred with the need for logical planning and provided that intelligible data collection, analysis and interpretation were necessary for the association of the inquiries with the conclusions (Hartley, 2004).

The following constitutes the logical phasing of the study:

Table 3.1: Phasing of the study



The following Table summarises the approach to the boundary setting and focussed analysis for this study using Yin's research design components recommended for case studies to achieve the logical associations necessary:

Table 3.2: Boundary setting with Yin's research design components

Component	Detail
Propositions	The propositions for the study are extracted from the literature review and are as follows (i) there are defined international e-signature regulatory frameworks and approaches by which to assess the effectiveness of e-signature regulatory frameworks in a particular country (ii) the analysis of e-signature regulation in a particular case or country through comparison with such frameworks and approaches permits conclusions and recommendations on the effectiveness of the country's approach.

Unit of Analysis	It was clear from the conception of the study that the single case of South African e-signature regulation would be studied. Emanating from the literature review, however, was the association of e-signatures and e-signature regulation with advancing electronic commerce interests of the country. With this objective in mind, the analysis was restricted to e-signature regulation as a subset of electronic commerce regulation and the inquiries and the conclusions aligned with such electronic commerce objectives, as opposed to national security or identity management generally for instance. This demarcation instructed the data collection and sources of evidence as well as permitted the general association of the study with other similar studies in other countries. The primary intended audience, e-signature policy makers and regulators further informed the reporting of the conclusions whilst the interests of other stakeholders to the research were notwithstanding, accommodated in the analysis of the findings.
Study Questions	The study main question and sub-questions derived from the literature review as the metrics for the assessment of the effectiveness of e-signature regulation
Logical application of the data to the propositions	A conceptual framework identifying three thematic inquiries and sub-inquiries was developed at the conclusion of the literature review to associate the inquiries for assessing the effectiveness with the data collected and analysed.
Criteria for the interpretation of the findings	The criteria for the interpretation are associated with the propositions of the study, particularly measures for the effectiveness of e-signature regulation and comparison with approaches in key model frameworks and other countries. Several studies of other countries substantiate the use of such propositions. Alternative explanations are further considered for the interpretation of the findings on e-signature regulation in South Africa. Country studies in Australia and China propose alternative explanations for the effectiveness of e-signature regulation extraneous to the framework and approach itself and the application of such alternatives or other revelatory explanations will be reflected on for completeness of the study.

Table adapted from Yin's Case Study Research Design (Yin, 2003, p 21-28)

Herold confirmed that research design not only improves the logical association between research inquiries and conclusions but further forms a means of promoting the quality of the research by promoting the validity of the research by

using certain tests (Herold, 2011). Two of such tests referred to by Herold, “construct validity”, and “external validity” are applied in this study to promote its validity (Herold, 2011, p7-8). Firstly, construct validity or the determination of the appropriate inquiries for the assessment is applied by conducting a literature review of international e-signature regulatory frameworks and the expert approaches to other similar studies in certain foreign countries to reveal the central inquiries for the study. This was particularly relevant to understand the central link between e-signature regulation and the advancement of electronic commerce and in so doing and establish boundaries for the study. The on-going return during the study to the core inquiries for analysis for the development of the research question, sub-research questions, interview questions and analysis of the findings pertains to second test of external validity i.e. the output of the research report is grounded in the accepted theory of effectiveness of e-signature regulation.

3.5 Data Collection and Analysis Methods

As the data collected will be primary legislation, case law and in-depth interviews with stakeholders in e-signature regulation, there are multiple sources from which the data for this study will emanate. According to both Wimmer and Dominick (1997) and Yin (1984) multiple sources of data are a feature of case studies. Wimmer and Dominick suggest that this variety of sources is one of the advantages of the case study method as are the richness of the data; and that the output can reveal explanations of a phenomenon (1997).

3.5.1 Secondary Content Analysis:

The research will include a review of collected materials for the purpose of revealing and understanding the e-signature regulation in South Africa in association with the propositions and conceptual framework. These include: statutes, journal articles, research papers, and policy documents. A more detailed list is in the References. The purpose of such review is the production of findings on the current state of regulation of e-signatures for the analysis in Chapter Five. The secondary content analysis responds to all pillars of the framework but critically, to the issue of effectively regulating the legal validity of e-signatures and the issue of harmonisation and alignment of e-signature regulation in South Africa for effectiveness. Included in the content analysis is comparative analysis of South Africa’s e-signature regulatory approaches with the United Kingdom, Australia, China and model legislation and guidance produced by international organisations such as the United Nations Commission on International Trade Law (UNCITRAL). The frameworks selected for comparison are, in the

researcher's experience as a technology lawyer, a reflection of developed and a developing country approach in the UK and China and representative of a country often consulted for regulatory approaches to technology regulation in South Africa being Australia. De Cruz relates the nature of comparative analysis to include (i) comparison of foreign systems to local systems and produce findings on common and divergent attributes (ii) analysis of different solutions or approaches (iii) investigation of the causal link between systems; and (iv) comparison of the phases or stages of the systems (2005). It is indeed, with such output in mind that such comparative analysis is undertaken. The selection of the data and the proceeding qualitative content analysis is guided as per the research design by the theory and propositions in the conceptual framework, which approach is regarded by Mayring as typical of the qualitative content analysis approach (Mayring, 2002). Glaser and Laudel further refer to type of analysis as composed by an extraction of the pertinent aspects in the text proceeded by the analysis (Glaser & Laudel, 1999). For the analysis, both coding techniques as well as the determination of common themes was necessary. Leedy and Omrod describe the extraction of common themes as core to the data analysis (Leedy & Ormrod, 2005, p. 140). What was necessary in this analysis was to place the themes in the context of the conceptual framework representing pre-identified themes stemming from the literature review in Chapter Two. This process of coding and extraction of categories of examination that was applied to the data analysis is best described by Titscher et al: as "core and central" to the data analysis method (2000, p.58).

3.5.2 Interviews:

This study is not mere documentary analysis of the regulation. Insights and explanations of the approaches to the regulation and the effectiveness of implementation of the regulation is sought. Interviews will be used to reveal the insights and explanations of key persons including the e-signature policy maker, technology lawyers, information security experts and electronic commerce experts. Yin directs that there are a selection of interview types to consider including in-depth interviews, focussed interviews and formal survey interviews (Yin, 2009). For this study, the focussed interview is used i.e. elements of in-depth interviews including requests for the interviewees own opinions and experiences and insights, however, the interview questions and pursued outcomes are guided by the questions associated with a case study protocol developed by the researcher (Yin, 2009). The case study protocol for this study is contained in Annexure A. It is clear in the context of Yin's description of a formal survey that this cannot be applied due to variance in the interviewee backgrounds and context and the requirement for exploratory interviews (Yin, 2009).

Purposive sampling is used to identify the interviewees (respondents). Purposive sampling is a form of non-probability sampling distinguished from probability methods associated with “statistical randomness” of a population (Terre Blanche and Durrheim, 1999, p. 279) and pertains instead to a more deliberate identification of interviewees based on selection criteria ((Leedy and Ormrod, 2005, p. 139). In a study on purposive sampling techniques, issues of bias and dependability of the research relying on purposive sampling to collect interviewee data are raised (Tongco, DC, 2007). This can be countered through careful selection of the interviewees and the need to establish and record key determinants for the selection such as expertise of the interviewees (Snedecor, 1939) or the relevant qualifications (Allen, 1971). Another caution expressed in the literature to promote stakeholder representivity or ensuring adequate representation of vested stakeholder interests (Fraenkel,Wallen, Hyun,1993) This would also assist in the reproducibility of the findings raised by some, as a limitation to purposive sampling (Hones, 1990). It is necessary that the researcher remains cognisant of issues of bias, reliability and competency of the interviewees (Tongco, 2007).

The researcher being a technology lawyer with several year of experience, selected interviewees, being persons in the judgement of the researcher to be aligned with the intended outcomes of the study (Groenewald, 2004, p. 8). The interviewee selection is according to the relevance of their experience and insights on the key inquiries comprising the conceptual frameworks as determined by the researcher and to promote the richness and generalisation of the research as well as being representative of the stakeholder groups for this study. The respondents included at least: one key representative from the Accreditation Authority (Authority /SAAA), being the appointed e-signature certification authority for advanced signatures; and (ii) the Department of Communications (DOC), being the primary e-signature policy maker; information security experts; ICT legal experts; electronic commerce experts. Each of the interviewees had demonstrable knowledge and insights on the areas of inquiry reflected in their qualifications and experience. Collectively, the interviewees were in a position to offer reflections on the multiple areas of inquiry comprising the conceptual framework although it is anticipated that their insights will be deeper or lesser according to the nature of the inquiry and the corresponding area of interest of the interviewee. According to Merriam, this selection of criteria of interviewees can be determined by the researcher (Merriam, 2002, p. 12). The use of purposive sampling for a selection of varied categories of interviewees was further in pursuit of broadening the array of perspectives through (Curtis, Gesler, Smith and Washburn, 2000, p. 1003). This was for the benefit of the relevant insights for the remaining audience, over and above the policy maker, and to evidence the competing requirements of the stakeholders in e-signature regulation. In accordance with the concerns raised in the literature where purposive sampling is used, the researcher will remain cognisant of issues of bias, reliability and

competency of the interviewees through the interviews and use the semi-structured format to specifically probe areas where the above issues are reduced in the opinion of the researcher. Furthermore, the researcher in the analysis of the interview transcripts employs the methods discussed in 3.5.3 below to promote the reliability of the research findings and the overall quality of the research.

Further detail on the actual interview participants will be provided in Chapter Four. The interview protocol developed, as per Annexure A, provided focus on the key themes to ensure interlacing of the responses in the analysis as well as permitted emphasis on the areas of interest of the stakeholder to contribute to the richness of the study. The researcher did engage in a pilot interview, and following the pilot interview, the interview protocol was streamlined to remove ambiguity in certain questions as well as to amend the background and introduction to interviewees to provide for acquaintance with regulatory terminology and the outcomes of the study.

The following are an indication of questions that will be included in the interviews according to the themes of analysis of the implementation of the regulation:

Table 3.3: Interview themes and questions

Significance of ES Regulation	How would you describe the levels of (i) trust, (ii) security (iii) privacy and (iv) user confidence in electronic commerce (transacting through electronic communications and transactions) in South Africa? What would you describe as the significance of e-signatures on electronic commerce in South Africa? What importance, if any, do you attach to the regulation of e-signatures?
Effectiveness of the Regulation of ES Products and Services	What importance, if any, do you attach to the distinction in the regulation between e-signatures and advanced e-signatures? What importance if any, do you attach to the recognition of foreign accredited signatures as advanced e-signatures?
Effectiveness of the implementation of ES Regulation	What importance, if any, do you attach to the accreditation of e-signatures as advanced e-signatures? Which transactions, if any, would benefit from advanced e-signatures?

	What importance, if any, do you attach to the accreditation of The ASP's signature (product) as an advanced e-signature? What significance, if any, do you attach to the accreditation of The ASP as an authentication service provider? What significance, if any, do you attach to the delay in accreditation of an authentication service provider? What significance, if any, do you attach to a single accredited authentication service provider in the market?
Insights and Recommendations to promote the effectiveness of ES Regulation	What would you say is the key role of the e-signature policy maker (the Department of Communications)? What are your comments on e-signature regulation to date? What impact do you believe effective regulation of e-signatures has on the success of electronic commerce (transacting through electronic communications and transactions)?

Each of the interview questions relate either to a sub-issue in the conceptual framework, provide opportunity for the interviewee to reflect on their experiences on the efficacy of the implementation of the regulation or provide opportunity to contribute recommendations for the policy maker related to stakeholder requirements and interests.

3.5.3 Ensuring the Quality of the Analysis

Yin suggests that construct validity is a common concern associated with case study research and that ensuring variety of sources of data and ensuring a trail of evidence are measures to address this concern (1994). Both of these methods, as discussed above, in the research design, as well as guidelines for the interview and triangulation are also used to promote the validity of the research.

Furthermore, the guidelines provided by Deacon, Pickering, Golding and Murdock (1999) for in-depth interviews are used including refraining from imposing views and requesting the respondent to consider a follow up interview if necessary. This is notwithstanding that a focussed interview is used due to in-depth interview methods being inherently constituent in

focussed interviews (Yin, 2009). The researcher shall use “triangulation” to locate and reveal the understanding of the object under investigation from “different aspects of empirical reality” (Denzin, 1978). In particular, data triangulation through documentary and comparative analysis supplemented by interviews with key stakeholders shall be used to promote the “convergence” (Mathison, 1998, p13) from different data sources within the qualitative methods of this study.

3.6 Summary

As motivated above, the research is inherently a qualitative study with case study aspects and the characteristics of such approaches facilitate the rich and considered research outcomes pursued by the researcher. According to the research design, the research is dependent on the efficacy of two core constituents:

- An international literature review - for the purpose of understanding the components and considerations for effective e-signature regulation and implementation of such regulation as well as to facilitate an extraction of approaches, terminology, concepts and learnings in established e-signature regulatory frameworks that will provide the conceptual framework for the analysis; and
- Adequate research - on current state e-signature regulation and contextual insights of various stakeholders on the effectiveness of the implementation of the regulation with due regard for the components of effective e-signature regulation emerging from the conceptual framework.

The arising interlacing of the conceptual framework, research questions, and data collection during the various phases of the research promotes the quality of the research and the validity is enhanced through for instance the multiple data sources and triangulation of such data to draw out emerging thematic research outcomes. Neuman cautions, however, that this pattern detection is important but must be the platform for the interpretation and translation into meaningful outcomes and conclusions and this is the objective of the reporting phase on the research (1997, p.426). With this in mind, the researcher is cognisant of the background chapter that establishes the importance of e-signature regulation to advancing trust, security and legal confidence in electronic commerce and ultimately that the research must be grounded in a reflection on the outcomes in such context. It is this core pursuit that has informed the methodology as well as the pursuit of adding to the limited body of knowledge on the subject in question.

Having described the methodology and research design in this chapter, Chapter 4 will present the results of the research.

4 CHAPTER FOUR: RESULTS ON REGULATION OF E-SIGNATURES IN SOUTH AFRICA

4.1 Overview of the Chapter

This Chapter comprises the results of the research associated with the queries of the conceptual framework and culminating from application of the research methodology. The results constituted by this Chapter pertain to the manner in which South Africa provides for the requirements of effective e-signature regulation through documentary analysis, on the one hand, and examining South Africa's effectiveness in implementation, through interviews with experts, officials and representatives on the other hand.

Section 4.2 is a detailed examination of the ECT Act and the ES Regulations. This includes how South African legislation provides for the legal validity of e-signatures, distinguishes between forms of e-signatures and regulates foreign e-signatures used in South Africa. The process of accreditation of an e-signature as an AeS as evident in the E-signature Regulations (ES Regulations) will be examined. Section 4.3 examines case law that has a bearing on the e-signature legal system and the import of case law will be set out in this Chapter. Section 4.4 will query several aspects of implementation of the law and the Regulations related to the effectiveness of South Africa's e-signature regulation.

The results are reported according to the sources of evidence: the content of the legislation and regulation, case law that has a bearing on South African law of e-signatures and the outcomes of the interviews with the individual interviewees.

This Chapter concludes with a summary distilling the key results essential to the analysis in Chapter Five.

4.2 Legislative Analysis

4.2.1 Legal Validity of E-signatures in South Africa

4.2.1.1 Functional Equivalence and Valid E-signatures

Chapter Two reveals that whether an e-signature is a functional substitute for the hand-written signature in law, the criteria to establish this functional equivalence and the distinction between forms of valid e-signatures each contribute to the

effectiveness of e-signature regulation. Extrapolating the manner in which South African legislation addresses each of the above is, therefore, essential.

In South Africa, the Electronic Communications and Transactions Act (ECT Act) was enacted in 2002 to facilitate electronic communications and transactions (RSA, 2002, s1). This was achieved by affording electronic communications transactions legal recognition. In so doing it provided for the legal requirements of, for instance, issues of writing, originality, and admissibility of evidence, consumer protection and validity of contracts in the context of electronic communications and transactions (RSA, 2002). Essential to the inquiries of this report, the ECT Act provides for the legal validity of e-signatures by stipulating that "an e-signature is not without legal force and effect merely on the grounds that it is in electronic form" (RSA, 2002, s13). On the issue of functional equivalence for e-signatures, therefore, this provision may be viewed as intending that e-signatures should not be prejudiced merely for their electronic character and are permitted the legal authority of a manuscript signature. This section is, however, conditioned on a preference for a so-called advanced e-signature (AeS) and provides that where any transaction requires a signature by law, and that law does not specify the form of signature, that requirement is only met by the use of an AeS (RSA, 2002, s13(1)).

How then does the ECT Act distinguish between an e-signature and an AeS and its attributes? An e-signature refers to "data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature" (RSA, 2002 s1). An advanced e-signature refers to "an e-signature which results from a process which has been accredited by the Authority as provided for in section 37 of the Act" (RSA, 2002, s1). It emerges that the requirements for an e-signature are primarily concerned with the intention of the sender that certain data be regarded as a signature and that such signature data is adequately associated with the data it serves to certify. An AeS, however, as per the above definition, is constituted by these characteristics as well as accreditation by a certain Authority in terms of an accreditation process. The inference is that the AeS is intended as a higher standard of signature particularly as its validity is dictated by an approval and accreditation process.

E-signatures are further denoted as legally acceptable where a signature is required by the parties for the validity of a transaction but the transacting parties have not specified a form of signature (RSA, 2002, s13). What, however, is the intended application of the AeS? In addition to the abovementioned call in the legislation for an AeS where a signature is required in law, the AeS is to be used in electronic transactions or communications where there is a legal requirement to arrange an electronic certified copy of information, notarise, acknowledge, verify information, affix a seal to information or statements under oath (RSA, 2002, s18, s19). The above cases for application of the AeS suggest that the AeS is preferred

where significant reliance is placed on information such as the certification of information and where legal assurance is crucial in the cases of notarising information or statements under oath. The inference is that the legislation intends that accreditation is the singular variance from an ordinary e-signature, rendering the AeS suitable for such purposes.

In Chapter Two, other country studies of the application of AeS counterparts revealed its utility in securing the evidential weight of electronic information. Section 14 and 15 of the South African ECT Act respectively, provide for the assessment of originality and evidential weight of electronic information (RSA, 2002). Section 14(2), in respect of the adjudication of the integrity of an original electronic document, provides that the integrity is assessed by considering whether the information has remained complete and unaltered except for regular additions in light of the purpose for which the information was generated and having regard to other relevant circumstances (RSA, 2002). Section 15(3) provides that the evidential weight of electronic information is assessed in accordance with the reliability of the manner in which the data message was generated, stored or communicated; the reliability of the manner in which integrity is maintained; the manner in which the originator is identified; and any other factor (RSA, 2002). Albeit that sections 14 and 15 do not directly establish that an AeS may be used to attest the originality or evidential weight of electronic record, the qualities of an AeS may be reviewed to determine its application in this regard.

4.2.1.2 Requirements for Legal Validity

The distinction is made in the ECT Act not only in terms of the applications of the two forms of e-signatures but also in the requirements for their legal validity.

In order to be considered an acceptable e-signature, the signature should represent a reliable method to identify the person and indicate the person's approval of the information. The reliability of the method is to be assessed considering the circumstances at the time the method was used and whether the method is as reliable as appropriate for the purposes for which the information was communicated (RSA, 2002, s13). An AeS (duly accredited) is to be deemed to have been applied properly unless the contrary is proved (RSA, 2002, s13).

This distinction offers the AeS the presumption of validity while other e-signatures rely on the outcomes of the assessment to be undertaken. The implications and effect of these distinctions are discussed in Chapter Five. Clearly, however, the South African legislation is urging the use of an AeS, a higher standard of signature, for cases where greater confidence and assurance is required and offers the user of an AeS the added benefit of placing the onus of disproving its legal validity on the contesting party. At the same time, other e-signatures, while having general acceptance, are in legal terms not valid

for certain transactions and furthermore, their validity requires verification through an assessment of character in relation to the relevant transaction.

Importantly, the Act provides for circumstances where an e-signature (and by inference includes an AeS) is not required for the validity of an electronic transaction between the parties - in such instances, an expression of intent or other statement is not without legal force and effect purely because it is electronic in nature and not evidenced by an e-signature but other manner in which the person's intent or other statement is inferred (RSA, 2002 s 13). This added provision of section 13, in essence establishes a third category of transactions where neither an e-signature nor AeS is necessary for the legal validity of a transaction. In this instance, the assessment is of the intent of the relevant transacting person.

In summary, three categories of transactions emerge from the provisions of the ECT Act, a category of transactions that expressly require an AeS to secure its legal validity, a category of transactions where the e-signature may be used and its validity is subject to the outcome of a prescribed assessment and a third category of transactions where the validity is to be assessed from the intention of the relevant transacting person.

4.2.2 Regulation of E-signature Products, Services and Service Providers

4.2.2.1 Accreditation of Advanced E-signatures

The section above established a distinction in the legal validity of e-signatures per se and the AeS. It was shown that the AeS benefits from a presumption of legal validity owing to its approval through an accreditation process by an Accreditation Authority. The resulting inquiry pertains to the nature of the accreditation provided for.

Chapter 6 of the ECT Act is titled Authentication Service Providers and provisions several aspects of accreditation of the AeS including the (i) the appointment and powers Accreditation Authority (ii) the process of accreditation, (iii) criteria for accreditation (iv) termination or revocation of accreditation and (v) accreditation of foreign products and services (RSA, 2002, s 33-41). The ECT Act further empowers the Minister to make additional regulations (RSA, 2002, s 41). Such legislative provisions and regulations are discussed below to better situate and understand how South Africa regulates AeS products, services and service providers. As discussed above, the regulation of general e-signature products and services is limited to the assessment in the circumstances and the regulation is concentrated on the AeS products and services.

The ECT Act distinguishes three service providers in the context of attesting or verification of electronic communications and transactions and the requirements for accreditation of each: cryptography service providers, certification service

providers (CSPs) and authentication service providers. Cryptography service providers use cryptographic techniques to limit access to electronic information and attest its integrity, authenticity and source (RSA, 2002, s1). CSPs use digital certificates for the authentication of electronic information (RSA, 2002, s1). The AeS is by definition issued by an accredited authentication service provider referred to in section 37 of the ECT Act (RSA, 2002, s1) but no specific authentication technology is prescribed as in the case of cryptography digital certificates service providers. In fact, the legislation and regulations confirm that an AeS service provider can, in technical terms, include a duly accredited CSP and provides additional accreditation requirements where the AeS pertains to a CSP offering digital certificate authentication services (RSA, 2002, RSA, 2007)

The central determinants of the AeS service for validity is accreditation by the Accreditation Authority and compliance with the systems specified (RSA, 2002, s1, s37) as opposed to the technology associated with authentication service. With this in mind, the effectiveness of the legislative provisions on accreditation of the AeS is a significant aspect of this study and key provisions are examined below.

4.2.2.2 Accreditation Authority

Regarding composition of the Accreditation Authority, section 34 of the ECT Act provides that the Director General of the Department of Communications is to act as the Accreditation Authority and following consultation with the Minister, can proceed to appoint employees of the Department as Deputy Accreditation Authorities and officers (RSA, 2002). The South African Accreditation Authority is empowered in the legislation to have oversight of the conduct, systems and operations of an authentication service provider (RSA, 2002, s36). These include powers of sanction and on-going oversight such as powers of suspension, revocation of accreditation and the ability to appoint of an independent auditing firm to assess compliance with the criteria for accreditation and other obligations under the Act.

The Authority is further mandated to maintain a publicly accessible database that includes the details of the accreditations standing or revoked, foreign signature products or services recognised or revoked and other information that may be prescribed in the future (RSA, 2002, s36).

Clearly regulatory oversight and the maintenance of adequate compliance are intended by the legislation as well as transparency with the public of the accredited and recognised authentication products and service providers. As the purpose of this study concerns the effectiveness of the current regulation, several aspects of the efficiencies and experiences with the Authority are queried with the interviewees. Notably, the regulation incorporates regulatory oversight

by the Authority in the form of appointing auditing firms to assess compliance with the criteria for accreditation. This relationship and its efficiencies or inefficiencies are also queried with the interviewees and is reported in this Chapter. The implications will be discussed in the analysis in Chapter Five and Chapter Six.

4.2.2.3 Criteria for Accreditation

Applications for accreditation or "recognition of an authentication product or service by the Accreditation Authority[3]" as an AeS must meet substantive and procedural requirements including the payment of a non-refundable fee on application (RSA, 2002, s37).

The criteria for accreditation are set out in section 38 of the ECT Act and are summarised in the table below. The requirements pertain to the e-signature technology used, the capacity and operations of the applicant service provider including technical requirements of its hardware and software systems and additional requirements for a CSP applicant (RSA, 2002, s38).

[3] Section 33

Table 4.1: Criteria for Accreditation

E-signature Technology	The e-signature to which the authentication products or services relate – • Is uniquely linked to the user • Is capable of identifying the user • Is created using means that can be maintained under the sole control of that user; • Will be linked to the data to which it relates in such a manner that any subsequent change of that data is detectable; • Is based on face-to-face identification of the user.
Authentication Service Provider	The Authority will have regard to the following concerning the authentication service provider – • Its financial and human resources and assets; • The quality of its hardware and software systems; • Procedures for processing of products or services; • The availability of information to third parties relying on the authentication product or service; • The regularity and extent of the audits by an independent body; • Additional factors for certification service providers; • Any other relevant factor which may be prescribed.
Hardware and Software Systems	Such systems shall adhere to at least the following: • Be reasonably secure from intrusion and misuse; • Provide a reasonable level of availability, reliability and correct operation; • Be reasonably suited to performing their intended functions; and • Adhere to generally accepted security procedures.
Certification Service Providers	Where the products or services are to be provided by a CSP, the Authority may stipulate – • The technical and other requirements for the certificates • The requirements for issuing the certificates • The requirements for certification practice statements • The responsibilities of the certification service provider • The liability of the certification service provider

	• The records to be kept and the manner in which and the length of time regarding the retention • The requirements as to adequate certificate suspension and revocation procedures • The requirements as to adequate notification procedures relating to certificate suspension and revocation.

Extracted and summarised from section 38 of the ECT Act

Note. The table above extracts and summarises from section 38 of the ECT Act, the accreditation criteria specified. Notably, additional requirements are prescribed where the accreditation pertains to a CSP whose service entails the use of digital certificates (RSA, 2002, s38).

The legislative provisions above provide the foundation framework for AeS accreditation. The Accreditation Authority is further empowered to impose any further conditions or restrictions necessary (RSA, 2002, s38 (5).From the table above (Table 4.1), however, It is noteworthy that the accreditation pursues several aspects of compliance, ranging from technical requirements to financial and human resources of the applicant service provider. One of the queries for analysis in will be whether the accreditation requirements are too cumbersome.

Associated with compliance with the criteria for accreditation, the accreditation may be suspended or revoked as a consequence of failing to meet the requirements, conditions or restrictions attached to the accreditation and subject to procedural fairness to the service provider (RSA, 2002, s39). Termination of accreditation may additionally be subject to conditions of termination (RSA, 2002, s39) although these are not specified in the legislation.

4.2.2.4 Accreditation Regulations (ES Regulations)

Under section 41 of the ECT Act, the Minister is empowered to pronounce further accreditation regulations (RSA, 2002, s41) over and above the foundation requirements of the ECT Act. In 2007, the then Minister of Communications, issued accreditation regulations (RSA, 2007). The key provisions of the regulations are summarised below. Here again, limited provisions associated with the analysis of the effectiveness of the regulations informed by Chapter Two are considered. These include the nature of the application process; the information security standards being applied and the responsibilities and liability of the AeS service provider.

Table 4.2: Key regulatory provisions

Section	Topic	Summary
6	Application for Accreditation	The application form for accreditation to is to be available on the Authority's website and this completed form, supporting information and the prescribed fee is required. Confidentiality obligations are imposed on the Authority and to be imposed on its appointed (agent) evaluators.
7	Prescribed Information	The application must be supported by: • Where the applicant is a CSP, a copy of the certificate practice statement[4], certificate policy[5] drafted in accordance with the specified standard "X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework" as well as a written undertaking that it can and will comply with the requirements of its certification practice statement and certificate policy. • Declaration of (by way of example): o The products and services resulting in and used to support an e-signature pertaining to the accreditation o Procedures for identification and authentication of the users including face-to-face identification o Manner in which compliance with certain criteria in section 38 will be met; o Manner in which information about the authentication products and services and conditions attached to made available to the public; and o Indications of how the applicant will ensure the availability of the information to third parties relying on the product or service, Details of its operations and outsourced aspects thereof; Audited financial statements for three years; Technical specifications of the software, hardware and information security policies, standards to which it complies;

[4] As per the definitions in section 1 of the Regulations, this refers to the statement issued by the CSP to specify the practices that it employees in generating and issuing certificates

[5] As per the definitions in section 1 of the Regulations, this refers to the named set of rules that indicates the applicability of a certificate to a particular community or class of application or both such community and class, as the case may be, with common security requirements

		Privacy and physical security policy to be implemented by the applicant; Details of human resources, proof of adequate insurance cover to ensure business continuity, a disaster recovery plan; and An audit report pertaining to compliance with the requirements of Chapter 6 of the ECT Act and the accreditation regulations and in the case of a certification service provider whose products and services are based on Public Key Infrastructure, an audit in accordance with "WebTrust".
9	Appointment of Evaluators	The Authority is required to appoint one or more expert independent evaluators to monitor, inspect or evaluate authentication service providers to ensure compliance with the Act and the regulations.
13,14,15	Requirements for CSP Applicants	The requirements include related to Public Key Infrastructure services: Technical requirements including compliance with information security standards such as the SANS 21188 and the ITU X.509 standard for certificates and three factor authentication or a similar level of security; Detailed requirements for the issuing of certificates are specified including in relation the face-to face identification procedures; The documentation to be used to identify and authenticate the relevant e-signature user (subscriber); An agreement with such subscriber must be entered into to ensure the responsibility of the subscriber for the private key and duty to notify the CSP where the key is compromised or stolen; and The practice statement and policy must further describe the provisions governing the conduct of agents or contractors to whom operations have been outsourced as contemplated in the regulations and the private key storage requirements.
16	Duties of subscribers (users) of CSP's AeS	The CSP must ensure that its subscribers comply with the duties specified including provision of accurate information, exercising all reasonable care to retain control of private key.
17	Responsibilities of the CSP	The CSP is required to make certain disclosures in a public database pertaining to the public keys, its certification practice statement and policy etc. and all accredited authentication products or services. The CSP must use trustworthy systems for its services, develop, maintain documented policies and procedures in relation to its entire operational environment, report to the SAAA incidents that may materially affect its trustworthiness, ensure that its personnel are fit and proper

		with the necessary knowledge, technical qualifications and expertise to carry out its duties.
26	Information security requirements	Authentication services providers other than CSPs whose products and services are based on PKI must adhere to the information security principles of SABS/ISO 17799. The abovementioned CSPs must comply with SANS 21188.
19	Liability of the CSP	The liability is in accordance with the certificate practice statement subject to the CSP being unable to exclude liability resulting from gross negligence.
27	Audits and evaluations	The applicant for accreditation must appoint and pay an auditor to audit the application and its authentication products and services resulting in and used to support the e-signature. The auditor can take into account recent audits to reduce audit costs.
29	Fees payable	The application fee is R20, 000 and is non-refundable.

Extracted from the ES Regulations, the relevant sections of the ES Regulations are specified in the table.

As observed above, compliance with international standards, particularly surrounding information security, ensuring adequate operational diligence and regulation of the relationship with the user (subscriber) to the services is called for in the regulations. The regulations make a point of specificity as far as the standards are concerned. As far as operational and customer issues are concerned, it requires explanation of the controls of the applicant himself. The implications of the specificity are discussed with the interviewees and will be analysed in Chapter Five as is the issue of the workability of the remaining compliance requirements. Ultimately, as is observed in Chapter Two, the accreditation requirements are a key determinant of the availability of the AeS in the country. Hence the number of accredited service providers and the experience of the accredited service provider discussed with the interviewees may be an important proxy for ascertaining the effectiveness of the regulations. Other notable aspects of the regulation are that the persons associated with the accreditation extend beyond the Authority and the applicant. Mechanisms for governing the responsibilities of the users and outsourced service providers to the applicant are observed. Furthermore, the role of the evaluators is key to the award of the accreditation. Finally, the ES Regulations again do not prescribe technical requirements where the technology is based on digital certificates (primarily Public Key Infrastructure technologies).

4.2.2.5 Regulation of Foreign E-signature Products and Services

The Minister may recognise the accreditation or grant similar recognition to foreign authentication products, services or relevant providers by pronouncement in the government gazette. These will be subject to conditions that may be imposed by the Minister (RSA, 2002, s 40). There are no provisions pertaining to distinct accreditation of foreign authentication products and services. Creating a false perception of accreditation in the case of foreign products, services or service providers is an offence (RSA, 2002, s40(2)).

4.2.2.6 E-signatures in Electronic Government Services

Electronic government services are referred to in the legislation as including government issuing permits, licences, approvals, accepting filing or accepting payment for government services electronically (RSA, 2002, s27).

Section 28 of the ECT Act specifies that where a particular electronic document needs to be signed, the form of signature may be specified by the relevant public body in the government gazette (RSA, 2002) as well as the manner and format in which such e-signature must be attached to, incorporated in or otherwise associated with the document (RSA, 2002, s28). The identity of or the criteria that must be met by any authentication service provider used by the relevant citizen or that the authentication service provider must be a preferred provider may also be specified in the gazette (RSA, 2002, s28(1)). The South African Post Office Limited (SAPO) is defined as the preferred authentication service provider for the purpose of the above section and the Minister may designate any other authentication services provider as a preferred provider on the basis of the relevant obligations of the provider pertaining to the provision of universal access (RSA, 2002, s28(2)).

4.3 Case Law

A search for South African case law providing specifically for the legal validity of e-signatures proved near fruitless and a scarcity in cases that probe or deliberate e-signatures is noted. Three cases were, however, considered relevant and they are discussed below.

4.3.1 Jafta v Ezemvelo Wildlife

The first case is Jafta v Ezemvelo Wildlife[6] (Jafta, 2008). The judgement provided several insights into how the ECT Act is to be interpreted and offers references to key principles for analysis of the impact of the ECT Act on the existing legal system in South Africa. The principles relevant to this study emanating from the Jafta case (Jafta, 2008) are:

- Electronic communication, in view of its nature, urges that regulation – is applied universally applicable principles and in this way internationalised and harmonised for its effectiveness. The judge urged that the international frameworks and relevant foreign law was significant to the application of the ECT Act and to contextualising its intention. Comparison to foreign legal systems was considered a challenge as insufficient depth of understanding, particularly of the socio-economic and political contexts in which they occur, presents a danger of incorrect application. The judgement also notably, drew attention to the objective of the ECT Act being the facilitation of electronic transactions in South Africa conforming to the highest international standards.
- The second firm principle is that the court has to be considered in the application of technical terminology. It must be used deliberately, consistently and in a manner of clarity.
- Thirdly, the law must provide for transferral of concepts such as writing, signature and original with different interpretations. In the context of this study, the judgement's reference and reliance on a Singapore case where the judge developed the common law by finding that the common law does not require handwritten signatures is significant. According to the referred case, a typewritten or printed form of a signature is sufficient even if the sender's name is not typed onto the e-mail. The judge enforced the common law right of the parties to decide on the formalities to apply to electronic contracting is reinforced in the Model Law, the ECT Act and in other foreign laws.
- Finally the judge urged relevant international and foreign law encourage self-regulation. Particularly, the characteristics of international, borderless associated with electronic communications and transactions required rendered it necessary for self-regulation to emerge. Self-regulation was associated with the effectiveness of e-

[6] The legal citation of the case is Jafta v Ezemvelo KZN Wildlife (D204/07) [2008] ZALC 84; [2008] 10 BLLR 954 (LC) ; (2009) 30 ILJ 131 (LC) (1 July 2008)

commerce regulation and ensuring that e-commerce and communication law is current with its actual practices (Jafta, 2008).

Overall, what emerges is the judge's deciphering of electronic commerce law, in the ECT Act, addressing issues of international reference for certainty and predictability and a clear promotion of increased application and reference to the law to facilitate legal effect to electronic communications and transactions. Through clear guidance and endorsement of international references, South Africa is freed from the constraint of limited local case law for precedent on application of the ECT Act. Concurrently, however, in future interpretations of the provisions of the ECT Act, relevant consideration of international cases is referenced as a requisite effort. Furthermore, the judges seeming lack of tolerance for avoidance of legal effect of electronic communications and transactions including the e-signature provisions, adds legal weight to the contents of the ECT Act and denial of claims of ignorance or uncertainty of the legal effect of e-signatures. This being said, as far as the determination of the legal validity of e-signatures, this case means that the provisions of the ECT Act must be interpreted through association with the intention of the UNCITRAL Model Law and with due reference to e-signature case law relevant and consistent with the provisions of the South African ECT Act.

Speaking again to issues of consideration of international and foreign legal systems, Justice O' Regan, equally urged legal professionals to duly consider the lessons of international legal systems both for didactic value and to avoid parochial approaches to interpretation of the law (K, 2005). This urging is particularly relevant for electronic commerce where uncertainty in the application of the law is a factor. In the relevant case, K v Minister of Safety and Security(2005, para 345) the judgement provided that in so doing, "a new optic" on the issue(s) at hand and the approach for resolution by others is valuable (K, 2005, para 345).

Another important case , albeit not on e-signatures specifically but contributing to the application of the e-signature provisions of the ECT Act is the case of Shifren and Others vs SA (1964). Under this case, variation of contracts through informal methods (not hand-written) is not acceptable unless an express agreement by the relevant persons to not abide by the requisite formalities is in place (Shifren 1964). We recall that under the ECT Act, where the parties have not required manuscript signatures the amendment of a contract via electronic means will be valid (RSA, 2002, s13). The abovementioned provision of the ECT Act read with the Shifren case means that parties to an electronic contract that are

varying the terms electronically must first consider any agreement that variation should be in paper form, with a manuscript signature and any other formalities to determine whether the electronic variation is valid.

It is clear from the Jafta case (Jafta, 2008) and the case decided by Justice O' Reagan (K, 2005) that particularly on the electronic commerce legal issues, foreign cases and international approaches relied on by the legislators are important to understand the legislative intent as well as perspective on how to interpret the provisions. Continuing on the issue of particularities of electronic commerce law, one case (Jafta, 2005) urged the legal recognition of electronic equivalents of writing and signature, for instance as determined by the ECT Act. Another case (Shifren 1964) albeit referencing formalities for valid contracting as opposed to the ECT Act directly, ultimately, urges that existing conditions to the law of contracting will need to be applied to electronic contracting and the validity of transactions are limited by the application of such cases as well. Each of the cases, ultimately, expose that the legal validity of e-signatures are not to be assessed from the provisions of the ECT Act alone but contextualised against foreign case law, international approaches and existing case law on surrounding aspects of the law.

4.4 Outcomes of Individual Interviews

4.4.1 Overview of Interviews

The respondents included at least one key representative from the Department of Communications, the primary e-signature policy maker, and The ASP, the accredited AeS service provider, as well as ICT legal experts and electronic commerce experts. Overall, 13 interviewees were interviewed. Further detail on the interview participants is provided in Annexure B. The interview protocol in Annexure A provided focus on the key themes and permits the richness of the study and critically guided the ethics and formalities associated with the interviews.

The interview focus questions for each of the interviews in reality differed or was emphasised based on the aspects of inquiry relevant to the interviewee. The following are the questions that were included in the interviews protocol:

Table 4.3: Interview themes and questions

Significance of E-signature Regulation	How would you describe the levels of (i) trust, (ii) security (iii) privacy and (iv) user confidence in electronic commerce (transacting through electronic communications and transactions) in South Africa? What would you describe as the significance of e-signatures on electronic commerce in South Africa? What importance, if any, do you attach to the regulation of e-signatures?
Effectiveness of the Regulation of E-signature Products and Services	What importance, if any, do you attach to the distinction in the regulation between e-signatures and advanced e-signatures? What importance if any, do you attach to the recognition of foreign accredited signatures as advanced e-signatures?
Effectiveness of the implementation of E-signature Regulation	What importance, if any, do you attach to the accreditation of e-signatures as advanced e-signatures? Which transactions, if any, would benefit from advanced e-signatures? What importance, if any, do you attach to the accreditation of The ASP's signature (product) as an advanced e-signature? What significance, if any, do you attach to the accreditation of The ASP as an authentication service provider? What significance, if any, do you attach to the delay in accreditation of an authentication service provider? What significance, if any, do you attach to a single accredited authentication service provider in the market?
Insights and Recommendations to promote the effectiveness of ES Regulation	What would you say, is the key role of the e-signature policy maker (the Department of Communications)? What are your comments on e-signature regulation to date? What impact do you believe effective regulation of e-signatures has on the success of electronic commerce (transacting through electronic communications and transactions)?

Each of the interview questions relate either to a sub-issue in the conceptual framework, provide opportunity for the interviewee to reflect on their experiences on the efficacy of the implementation of the regulation or provide opportunity to contribute recommendations for the policy maker related to stakeholder requirements and interests.

The researcher did engage in a pilot interview, and following the pilot interview, the interview protocol was streamlined to remove ambiguity in certain questions as well as to amend the background and introduction to interviewees to provide for acquaintance with regulatory terminology and the outcomes of the study. These amendments in approach proved valuable in directing the interviewees' attention to issues pertinent to the study. The selection of interviewees as well as the variation in the number of interviewees per category of interviewee proved successful in securing inputs of particularly legal and regulatory experts and it was uncovered that the electronic commerce experts had similar views, which negated further interviews. Information security experts on the other hand, had conflicting views influenced by the nature of their exposure and interest in e-signatures. In this case, the number of information security experts interviewed proved, again, to be a valuable determination in hindsight.

4.4.2 Summary of Interviews

How would you describe the levels of (i) trust, (ii) security (iii) privacy and (iv) user confidence in electronic commerce (transacting through electronic communications and transactions) in South Africa?

Interviewees' views on trust, security, and privacy and user confidence differed broadly, and are clearly informed through their professional lens and personal experiences of e-commerce. Some observations cut across the spectrum, however, particularly the acknowledgement that despite any concerns around trust, security, privacy, transactions are taking place regardless and growing in both value and number. Similarly, due to the low accessibility of e-commerce currently to most South Africans, there is an obvious inference to low levels of trust and confidence. It is important to unpack each of the issues. An e-commerce expert felt there was trust in a broad sense of e-commerce, but that there was little ability within consumers to distinguish what is trustworthy and what is not. This was echoed by a legal expert, who equally felt that trust was being expressed by consumers in many ways like buying airtime and using websites like Kalahari.net. These two interviewees shared another view when it came to trust and confidence, and it relates to transaction value. They separately

observed that South Africans are reluctant to enter higher value agreements online. The e-commerce expert detailed that in his own company's experience, although they offer the option of paying online to all customers, 80% of transactions and all high-value agreements are paid via bank transfers and contracted traditionally through paper agreements. All other interviews, including senior persons at the DOC and the ASP, described trust in e-commerce in South Africa as weak or low, and primarily due to limited awareness. The ASP representative specifically identified a "false confidence in e-commerce" (INT 10), with the limited awareness resulting in consumers not understanding the potential risks around security and integrity, and quite simple "hoping for the best regarding the privacy and security of their transactions" (INT 10). The DOC senior official focused on government's role toward enabling trust through progress in e-signature adoption, rather than specific observations around current trust levels.

The issue of security through the interviews resulted in an important observation. One the one hand, that South African banks and regulation guidelines around security were both very strong and robust. One legal expert noted our banks for being some of the most innovative in the world around online security. In fact, all non-technical interviewees regarded e-commerce security in South Africa as very strong. However, this was contrasted strongly with the opinions of security and e-commerce experts on the security measures in place within many e-commerce merchants. One went as far as to describe it as "non-existent", lamenting the lack of e-signatures and identification. The DOC official and the ASP representative did not comment on security measures.

Privacy again revealed a common sentiment that users are not really aware of what is happening with their information, and operate on a premise of good intent. An e-commerce expert explained the direct relationship between e-commerce effectiveness and privacy saying that "e-commerce's ability to reach its full potential is directly proportional to the degree to which personal information is used (INT 1) and the user experience is enhanced through the use of personal data. Legal experts were in unison around the state of privacy undergoing a sea change in South Africa as new legislation takes effect and gets implemented, and technical experts were equally collective in their view that personal information was currently being used in ways that people were not aware. The ASP representative described the situation well when he referred to unnecessary and inherent complexity in our privacy approaches in South Africa. "If approached correctly, the market should have access to protective mechanisms; however, complexity detracts from the application of relevant solutions" (INT, 10).

What would you describe as the significance of e-signatures on electronic commerce in South Africa?

In the South African context, interviewees provided the following as areas where e-signatures can provide value to electronic commerce and other electronic transacting processes: (i) securing transactions typically associated with corruption such as tender award processes (ii) banking transactions including the conclusion of home loan transactions and retail banking transactions (ii) judicial procedures including verification of qualities of electronic evidence produced such as date and time stamps and attesting the originality and integrity of such data (iii) increasing the reliability of an electronic transaction, for example email authenticity may be verified through the use of e-signatures; (iv) generally improving the trust and security of electronic transacting processes ; and (v) and limiting identity fraud and other forms of fraud associated with electronic transacting.

The DOC senior official was clear that "South Africans cannot avoid living or transacting in a virtual world" (INT 9) and that electronic transaction processes had a dependency on assurance of the identity of transacting parities which is the primary significance of e-signatures. Secondly, according to the DOC official, advancing the security of electronic transactions particularly through the use of an AeS would grow confidence in electronic transactions for South Africans. As such the DOC's strategic plans place e-signatures as a priority policy and regulatory area.

Several interviewees tended to agree that e-signatures were not broadly adopted and that there was limited awareness of the availability and value of e-signatures. Interviewees pointed to the following issues that limited the extraction of the value of e-signatures: (i) the lack of a "ceremonious" process that is typically associated with traditional manuscript signatures, e-signatures are applied with a mere click of a button (INT 4) (ii) the need for greater investment in e-signatures (iii) the implementation costs of PKI based technologies at large corporations including data storage and IT infrastructure costs being prohibitive (iv) the limited awareness of e-signature value means that full features functionality of e-signature technologies are not being implemented at organisations; (v) general preference in industries such as the banking industry for paper transacting processes; (vi) the availability of other means of verifying data and prevention of the modification of data (v)technical vulnerabilities in certain e-signature technologies that make such signatures (vi)accessibility of e-signatures including only a single issuer of the AeS (vii) limited publicity on e-signature regulation and the Authority that would otherwise permit greater trust in the adoption of the AeS in the market.

Interestingly, one technical expert referred to the availability of competitive technical alternatives to e-signatures including the use of SIM cards to verify the identity of the relevant user and other privacy protection technologies.

What importance, if any, do you attach to the regulation of e-signatures?

The positive implications of regulating e-signatures were characterised by the interviewees, in relation to the value of the provision of technical standards to understand and implement e-signatures that realizes policy intentions, the necessity of applying standards of care and security to identity information handling and use, establishing levels of legal accountability for the various users of identity information particularly in the face of ever increasing commercial applications of personal information and generally promoting the availability of trusted services through accreditation of authentication service providers.

According to the electronic commerce industry expert, the absence of regulation in this area is likely to drive the development of technological innovation in the market, and promote the responsiveness to the needs of the users in the initial stages of market development. However, the market is likely to encounter issues of establishing the necessary barriers to entry for authentication service providers and the implications will be the inability to control the quality of service particularly in relation to the security standards of the authentication service providers which will demote user trust value in e-signatures.

According to an e-signature and information security consultant, legal provision that qualifies the use of e-signatures is necessary to drive market adoption of e-signatures. Furthermore and the business sector in general is reluctant to invest in IT security measures in the absence of standards and approaches imposed by regulation. With this in mind, the expert provided that self-regulation would not be an option due to limited legal consequence.

One interviewee noted that aside from electronic commerce transactions, the AeS has benefits for the public sector and would be a positive measure for proper governance including in the sphere of placing limitations on abuse of electronic systems for unauthorised transactions. In particular, intelligence and defence institutions were regarded by the interviewee as organisations that stood to benefit.

The DOC representative's view on the need for regulation concerned primarily, issues of establishing the legal validity and legal status of e-signatures for predictability, promoting awareness of e-signature applications and outcomes, and affording the market acceptable levels of assurance on e-signatures through the prescribed standards for legal validity. Accordingly, the view was that the absence of standards and determination by the public of what is secure would weaken overall trust in e-signatures. The DOC representative stressed the need for government to recognise the impact of e-signature regulation on foreign investment providing that the regulation has the potential to promote foreign investment.

The current regulation and regulatory approaches were appraised. One of the concerns with the regulation raised by an information security expert was the (i) theoretical nature in the absence of a strict enforcement approach that does not provide the imperative for use of e-signatures. An analogy was drawn to other regulation where industry consultation was not present which in turned resulted in industry "backlash" (INT 5). Industry should have been consulted on the technical standards to be applied as well as the available e-signature technologies, according to the expert.

A legal expert was critical of the "tight regulation" which according to the expert does not give effect to "technological neutrality and non-discrimination of technologies intended by model law approaches (INT 7). As a result, the expert called for changes in the regulatory approach. Recommendations included consideration of an international accreditation approach and improvements in "streamlining" the accreditation processes (INT 7). The UNCITRAL Model Law approach, according to the expert required establishing principles of functional equivalence and technological neutrality and our regulation should be aligned with such approach. The legal expert referred to developments in the UN Convention for consideration. According to the UN Convention a new test or "legal fiction" is applied to e-signatures (INT 7). The traditional approach to regulation of e-signatures was described as a two-tier approach: (i) certain e-signatures are legally valid through evidence of reliability and suitability for purpose and (ii) through a "legal fiction" or "theory" approach , certain e-signatures are valid in relation to mere compliance with the requirements stipulated in legislation and absence of technical verification (INT 7). This two-tier approach with an associated higher level of legal recognition amounts to "discrimination" of e-signature technologies and is problematic in the view of the legal expert (INT 7). This was explained through the example of the costs of accreditation of e-signatures i.e. the verification for a high level of legal validity. Other approaches such as the UN Convention approach could be a move away from the two-tier approach which the legal expert believes to be a positive consideration for South Africa. The legal expert further cautioned that the regulation must be responsive to the local conditions and in South Africa, in the expert's view, South Africa's electronic commerce has not advanced to a stage where "stringent requirements" are called for and such approach may be inhibit to electronic commerce such that consumers may lose confidence in transactions where e-signatures have not been applied (INT 7). In addition to international developments, the legal expert recommended that regional regulatory approaches including the SADC Model Laws and the Draft AU Framework currently being developed should be considered.

The ASP representative provided a noteworthy sentiment "the law is supporting a paradigm shift in electronic commerce which requires awareness and guidance" (INT 10). The interviewee regarded his views on the need to regulate e-signatures as "evolutionary" (INT 10). Initially of the view of an automatic equivalence of e-signatures to paper signatures,

the interviewee did not see a purpose for legal definition of prescription for e-signatures. However, current confusion on the definition, validity and uses of e-signatures amongst industry, the judiciary and perhaps owing to the text of the regulation requires regulatory intervention. The ASP representative called for regulators to align the regulation with the workings of actual e-signatures and established practices.

What importance, if any, do you attach to the distinction between e-signatures and advanced e-signatures?

Interviewees tended to agree that a distinction between e-signatures and advanced e-signatures was necessary. The significance of the distinction was described by the interviewees focused on the need for accreditation and stricter regulation for the AeS. Below are comments of interest:

- An information security expert provided that the higher standards of regulation were required for the AeS due to the legal force and trust associated with it;
- The AeS had an inherent requirement for certification of its security and the accreditation process was necessary to provide for such certification;
- An electronic commerce expert provided that the majority of online transactions did not require the use of an AeS and given that the costs of accreditation and in turn, the costs of the AeS use are high, the distinction permits online transacting parties to decide on the appropriate signature. This view was seconded one of the information security experts relating that certain banks for instance preferred alternative authentication mechanisms and the regulation should always provide for "flexibility and choice" (INT 6). According to this interviewee, in industry "based on the transaction, process and channel, there are different identity verification requirements" being applied (INT 6).
- While an AeS was necessary for contractual processes for instance, where increased legal or security requirements were necessary, however, the requirements for implementation of an AeS were such that it could not be applied to all transactions, the requirement of face to face identification for the issuing of an AeS is an example of such limitation which enforced the need for the distinction.
- The accreditation of an AeS provides for non-repudiation which is not available with all e-signatures which may just provide for confidentiality and integrity. The process of verification of the person's identity face to face is what avails the non-repudiation benefit.

The DOC senior official reflected the views of other interviewees that the distinction was necessary to ensure compliance with the requisite standards by an AeS resulting in a higher level of assurance of users or recipients of such signatures. The concern raised by the senior official of the DOC was that the public was not aware of the distinction. The public should in the opinion of the DOC official deem the assurance attached to an AeS as necessary at certain times and mandatory requirements for the use of an AeS should be understood. Furthermore, the interviewee noted that the courts were not adequately aware of the distinction between the signatures and within the legal industry, there is a preference for paper processes despite the requirements in law for the use of an AeS and even amongst government officials, there was a need for training of the distinctive uses of e-signatures and advanced e-signatures.

What importance, if any, do you attach to the accreditation of e-signatures as advanced e-signatures?

The responses focused on the benefits of an accredited e-signature and its significance for electronic commerce users. Interviewees described the benefits of an accredited AeS as ensuring the appropriate levels of security to the products and services, ensuring that the technology infrastructure is not vulnerable to compromise or abuse, review of the manner in which the accredited provider protects information particularly identity information provided to it, promoting harmonization of SA approaches to the AeS to international approaches. An information security expert noted that the significance of the accreditation is related to the AeS carrying the weight of the handwritten signature.

The availability of an accredited AeS was generally viewed as a positive development for electronic commerce. Interviewees described the benefits for promoting trust, and efficiency with the dependencies on handwritten signatures and courier services for documents transfer being addresses. The corresponding costs benefits of electronic trade were also cited.

According to an interviewee, the “accreditation creates an ecosystem of authority” where the security that the trust hinges on is reviewed by an appropriate authority (INT 1). The annual audit was described as “strengthening the ecosystem” by such interviewee with other interviewees concurring that the annual audit was a positive requirement. According to an information security expert, the annual audit requirement was similar to the conditions of an operating licence and that the requirements for accreditation were similarly incentivised as the provider will lose their “license” for not complying with the letter of the law (INT 5).

A second information security consultant was less complimentary of accreditation describing it as a “checklist exercise” (INT 6) and the accredited service provider remains vulnerable to information security penetration attacks regardless of the

accreditation. This consultant noted other methods of authentication including selecting “notaries” or persons selected by users to make certain validations (INT 6). The validation relies on the relevant user’s requirements and the validator’s knowledge, and the trust placed in elected persons which provide greater control of the validation process.

The benefits of accreditation regulation were described by the ASP representative as primarily, advising o the relevant standards for an AeS on which significant reliance is to be placed by the user. According to the interviewee, the accreditation means that the relevant AeS “has been subjected to a process, to audit standards regarding the quality and integrity of the authentication services and process, and to international benchmarks” (INT10), Another interviewee listed the evaluation of an accreditation applicant’s HR procedures including the hiring processes that should ensure proper background checks and the financial viability of the applicant as critical areas of assessment. An information security expert interviewee noted that critical areas for regulation were the process of revocation and termination of “certificates” (INT 4) and the governing of such process. Furthermore this interviewee noted that the industry concern was whether the processes of the accredited service provider were lesser than that of the companies that would be its clients.

Limitations to the accreditation regulation were described the interviewees as including (I) the association with PKI based technology and not being technology neutral, (ii) the regulation refers to outdates international security standards such as ISO 17799, and the current version of the Web Trust standard and was described as “behind the times” (INT 8) which is particularly concerning as the “standards for risk management should change in accordance with technology changes” (INT 8) (iii) that the regulatory intent and requirements for accreditation are not understood, even in the mind of one interviewee, by the DOC, the audit of the controls, approximately 500 can take 3 months.

The significance of the accreditation was described by the DOC senior official as receiving a “government stamp of approval which provides a high level of assurance” (INT 9). The DOC official further noted challenges with the accreditation process including the lack of advertisements and general awareness in the market of the accreditation requirements and benefits or the distinction between the varying levels of trust that can be placed in the accredited signature. This, the interviewee noted was true amongst government agencies as well. Secondly, the challenges associated with the process concurred with other interviewees on the challenge of the extensive requirements as well as describing the costs of accreditation as prohibitive particularly the audit costs, and the annual compliance requirements amounting to further costs. The DOC senior official noted that limited applications were received and where inquiries were received, it was clear that the prospective applicants were unclear of the intent of accreditation. Another issue with the accreditation regulation was described as being too closely associated with particular technologies which in the opinion of the DOC senior official was

"not conducive to innovation" (INT 9). One of the particular difficulties was described as the limitation in the regulation on which auditors may be used. This in essence brought about a lack of competition for the auditing services which resulted in high costs according to the DOC senior official.

According to such DOC official, at this time the "advanced e-signatures are always digital signatures but digital signatures need to be accredited before becoming advanced e-signatures" (INT 9) as the current regulation provides for PKI based technology. The DOC is considering amendments to this approach, however, that would allow the accreditation of technologies that are not PKI based.

The DOC official noted that another applicant was in the process, however, the evaluation was "near completion" (INT 9). This second accreditation would, as described, promote competition particularly in the government sector for AeS service providers.

Which transactions, if any, would benefit from advanced e-signatures?

This question drew another broad range of responses from interviewees, and the common theme was a distinction or set of criteria within currently known transactions that should see advanced e-signatures having an impact. The problem, however, is that there was little consensus on what these criteria should be. One broad factor was around transaction values, and that larger value transactions would benefit from the advanced signatures. Another approach was around the contracting entities, particularly government – and that any dealings with government and business should require advanced signatures. Others felt this applied to when the parties were from different countries or simply that advanced signatures should be required in the place of any contract today where a full written signature is required.

Interestingly, those from legal backgrounds seemed to focus on the smallest set of circumstances that would require accredited signatures in view of the law and perhaps in reference to difficulties in adoption form a legal perspective. Those from technical and business backgrounds focused on opportunities – either from an efficacy point of view in their ability to business faster, or for the sale and use of technology as society moves from written signatures to electronic ones.

Efficiency in dealing with banks and financial institutions and the promotion of e-government services through the use of advanced e-signatures were opportunities identified by most our interviewees. The ASP representative went further to specific that advanced signatures are best suited to documents that may be aggressively disputed. There appeared to be a sense of caution and reality around adoption and use relative to cost, which The ASP representative believes is going to be an obstacle to widespread adoption by the public, despite the potential benefits for e-government services. "There is

government led advanced e-signature adoption in other countries, but in SA, we still do not have a comprehensive e-government strategy, which would drive investment into advanced e-signatures" (INT 10).

What importance, if any, do you attach to the accreditation of The ASP?

Generally, there was significant positive reaction to the ASP's accreditation and confidence was expressed in the ASP itself particularly in relation to the availability of an AeS and the benefits of legal assurance provided by the availability of accredited AeS associated services in the market.

According to the DOC senior official, the ASP "broke dead ground" and in so doing displaced reluctance in the e-signature market attached to the accreditation process and rendered the accreditation process "tangible" (INT 9). Other benefits of the accreditation included, as per the interview response, broader interest in AeS, the SAAA and the accreditation process. The DOC senior official also noted that it benefitted directly through the SAAA growing its experience in accreditation and this is likely, in the view of the representative to deliver efficiencies such as faster accreditation in the future.

The accreditation process was described by the ASP representative as an overall positive experience but not free of challenges. The accreditation requirements encompassed more than 500 "control objectives" (INT 10). This scrutiny was, however, lauded by the ASP representative as necessary. Particularly the requirements of the audit of the ASP's environment may, however, represent a barrier to entry to AeS market entrants, in the ASP interviewee's view. Additionally the interviewee submitted that the reliance placed by the DOC on the audit reports issued as part of the accreditation process represents an area of concerns.

The DOC senior official acknowledged the ASP's investments in the process including financial investments of millions of rands. The DOC interviewee further acknowledged that in accreditation, the ASP's liability for its e-signature services has increased particularly in relation to the nature of the information it held and that information breaches will "significantly damage the company's business case" (INT 9). The ASP interviewee shared the view that information breaches can "end this line of business for the company and the availability of the AeS as the only certified service provider" (INT 10). This liability, as explained by the interviewee requires the ASP to apply the highest level of review of its practices and keep pace with developments and industry guidelines through participation in international forums and developments to manage such liability. In relation to the security standards mandated, the interviewee confirmed that the ASP's standards exceed the requirements of the audited standards.

One interviewee questioned the significance of the accreditation noting that the ASP may have presumptions on user awareness and adoption of the AeS and questioned whether the incentives were present particularly in relation to weak enforcement of the laws that require the use of an AeS. Two information security interviewees cautioned that The ASP will be prone to information security attacks such as hacking and malware vulnerabilities and the service will be targeted by fraudsters and urged consideration of multiple verification mechanisms.

What significance is any do you attach to the delay in accreditation of an authentication service provider?

Interviewees across disciplines and backgrounds concurred that electronic commerce was not brought to a complete halt in the absence of an accredited authentication service provider and the availability of an accredited AeS. Electronic trading over the years ensued. According to the DOC senior official, online transacting should not have been impacted as e-signatures were available and advanced e-signatures impacted transactions where such signatures are required or desired. The demand for accredited e-signatures, the official observed was from foreign companies that were aware of the availability of the benefits of accredited forms of e-signatures in their own countries. Such foreign firms would request and insist on the use of accredited signatures in transactions with South African companies.

Several interviewees reflected on the impact of the delay. According to an electronic commerce industry expert, the delay in accreditation represented an opportunity lost. Earlier availability of an accredited advanced e-signature may have promoted the "speed, efficiency and trust in concluding transactions electronically" (INT 1). IT professionals or "geeks", and banks, were identified as possible early adopters (INT 1).

Legal experts spoke to concerns with the regulatory process. One legal expert queried why the issuing of the accreditation regulations and the accreditation of an authentication service provider was so delayed when provision and regulatory guidance was provided in the ECT Act coming into force in 2002. Another legal expert spoke to possible accreditation cost inhibitors associated with the regulatory approach being the cause of the delay. Furthermore, that the costs to maintain the accreditation status were regarded as prohibitive including the costs of maintenance of the(IT) infrastructure and security standards in accordance with the prescribed standards. These high costs were regarded as having negative implications on the pricing of the service provider's products and services and primarily government or major corporations being able to afford to use advanced e-signatures. One of the legal experts urged government to promote the use of "ordinary e-signatures that develop according to technological standards being developed globally" and in so doing promote the market adopting acceptable standards for ordinary e-signatures which approach would be in line with the UN Convention (INT 7).

An e-signature and information security expert with professional consulting experience in the area revealed that it took approximately 5 years to establish the Authority, the second delay was the promotion of the awareness of the accreditation process by the Authority and that yet another delay is foreseeable i.e. promoting the significance of the accredited signatures being available. A similarly knowledgeable interviewee concurred with the view that the expectation should be of long term adoption. Both of these technical experts made references to best practices in other countries, one being South Korea that has made considerable advances by comparison, the other being Switzerland, opting for other forms of identity certification issued by national government.

What significance, if any, do you attach to a single accredited authentication service provider in the market?

This question drew wide consensus in that having a single accredited service is problematic for the market. The lack of competition would impact pricing, innovation and availability for the better, empowering more consumers and entities to access a signature product.

One interviewee noted in relation to the absence of competition in the market that this was problematic as "competition drives innovation and pricing control"(INT 1) and had negative implications for the service quality that would be provided to the public. The DOC senior official echoed that a monopoly situation was undesirable, stating that "the monopoly may result in the ASP charging fees that do not favour the consumer" (INT 9). However, the DOC official cautioned that pricing should not be evaluated as part of the accreditation process as government should guard against "unduly interfering" (INT 9).

Two interviewees raised the concern that the lack of other providers could be due to there not being a sufficient business opportunity, and if that is the case, there are risks to adoption and use of signatures in a general sense. Security experts were particularly concerned that large companies like banks would not be comfortable with a relatively small player such as the ASP being the sole option for them to pursue advanced signature adoption, and that they would prefer to implement e-signatures themselves in a manner that they trust.

There was expectation and speculation that the South African Post Office (SAPO) would be accredited soon, and that brought both challenges and opportunities. On the one hand, The ASP would have help with educating consumers and encouraging adoption. On the other, one forensics expert was concerned that government entities would immediately use SAPO signatures, as it was a state owned entity, effectively squeezing the ASP out of a significant market.

From perspective of the impact on the Authority, an interesting observation was that of an e-commerce expert who was concerned that a lack of competition would breed complacency and little innovation within the Authority itself, as it would

only have a single authority to audit and compare to best practice. “The Authority has very little to regulate and little opportunity to compare the practices of different entities or apply the regulation more deeply. Such regulator and the provider may develop a relationship that is not an arm’s length relationship” (INT 1).

What importance if any, do you attach to the recognition of foreign accredited signatures as advanced e-signatures?

The responses to the question demonstrated varying views on recognition of foreign accredited signatures and whether accreditation of the foreign signature was necessary versus mere recognition of a foreign accreditation.

The electronic commerce industry expert’s view was businesses trading in foreign countries should follow the laws and regulations of that country. Furthermore, in the expert’s experience, local businesses will require assurance that the foreign e-signature met the local legal requirements for legal validity. Hence local accreditation was necessary.

An information security expert on the other hand, opposed separate accreditation in South Africa where a global standard was applied to the foreign accreditation. This view was linked to the non-repudiation of identities function of accreditation being based on international standards hence where the foreign accreditation process complies with the international standards; the need for accreditation is negated. A fellow information security expert regarded accreditation as the best approach, however, this approach was regarded as unrealistic due to the South African government’s historical reluctance to accept foreign service providers. This expert pointed to an alternative to international accreditation being mutual recognition by countries or “co-operation agreements” but was equally critical of the South African government’s ability to fulfil such co-operation agreements (INT 5). A third information security expert was reluctant about automatic recognition of foreign accreditations providing that this may impede the liability of the relevant signature user as the government would have removed the choice of the user to self-validate.

One legal expert concurred with the international accreditation approach calling for a uniform system of accreditation that in the expert’s view would be of benefit to countries and consumers globally. Another legal expert provided in contrast, that a country’s standards for accreditation are developed to meet local requirements and not necessarily suitable for other countries. Recognition of foreign accreditations hinged, in the view of such expert on the level of compatibility with South African standards and qualified international best practice standards. Regarding full accreditation, this was viewed by the legal interviewee as costly and without real value. An information security expert added to this line of thought by recommending recognition subject to a prior “audit” in relation to duly meeting the accreditation requirements. The issue of

compatibility was expanded by the information security expert as including compatibility with the accreditation process and approach.

The DOC senior official confirmed that the issue with the recognition of foreign accreditations was in fact the compatibility of the standards associated with the foreign accreditation. The DOC interviewee noted that a new ECT Amendment Bill would provide for agreements between governments regarding recognition of the counterpart's signatures. Hence the proposed approach was explained to be to agree at government –to-government level the recognition that is afforded to corresponding accreditations.

The ASP representative cautioned that the identification associated with authentication services, should these be to a foreign service provider, will be contrary to local privacy laws. The representative's view was that the local accreditations are, in line with the company's experience in this area, subject to local scrutiny and offers the benefits of legal certainty in that the legal principles are associated with local laws. Hence a higher level of assurance is offered. The representative urged additional regulation in this area.

What would you say is the key role of the e-signature policy maker (the Department of Communications)?

A legal expert spoke to a fundamental role in ensuring an open channel for electronic commerce that is safe and secure. An electronic commerce expert simply provided that the DOC was charged with blending the best of global best practice and local needs as far as e-signatures are concerned into policy and legislation. According to another interviewee, the DOC should have two primary focus areas: promoting the ease of adoption of e-signatures and ensuring that the regulation promotes that the accredited signatures are as secure as possible. Information security experts in a statement, related to the latter of the focus areas, urged the DOC to ensure enforcement of security standards and conduct continuous "review and updating of the security standards that provide for improved validation and verification mechanisms".

Other interviewees were critical of the DOC's approaches thus far describing the Authority, currently part of the DOC, as a weak regulatory authority questioning whether the DOC would fulfil the need to educate and assist the public on e-signatures and critical of the lack of adequate consultation on the accreditation regulations. The expert had practical concerns such as the impact on organisations who has invested in PKI based implementations of e-signatures that were not accredited and urged the DOC as the policy maker to have an understanding of historical methods of e-signature implementations and stressing the importance of hierarchical categorisation in practical terms of transactions and

associated security requirements prior to regulating in this area. According to the expert "regulating e-signatures without industry and transaction association will result in too many uncertainties" (INT 4).

A legal expert was critical of the recent draft ECT Amendment Bill prepared by the DOC. According to the legal expert the lack of "address of conformance with the (UN) Convention was a disappointment" (INT 7) and a weakness that needed to be addressed and following the approach of the UN Convention regarding e-signatures was likely to deliver the electronic commerce benefits sought. Interviewees agreed that the DOC was required to promote awareness of the benefits of e-signatures and advanced e-signatures, their uses and that advanced e-signatures are available. The ASP noted that it was hopeful of "bolder support" from the DOC (INT 10).

The DOC senior official provided that its role remained the regulation of e-signatures to "create predictability and promote trust and security in electronic transactions" (INT 9). Furthermore, the issue of recognition of foreign accreditations was noted and the DOC official provided that its role including assessment of the compatibility of such signatures. The DOC official noted that the DOC would like to promote the awareness of advanced e-signatures and its benefits.

What are your comments on e-signature regulation to date?

The interviewees were critical of the regulation of e-signatures in the current form and urged review and of the current regulation. Technical experts drew attention to the need for the regulation to respond to developments in fraud technologies, the promotion of skills and industry development to foster growth in market adoption of e-signatures, review of the approach of the accreditation regulations in so far as "3 factor authentication" was concerned was regarded as "not realistic," (INT 10) as well as promoting the knowledge of the Auditors regarding PKI and PKI controls.

The legal experts were critical of the knowledge and information of the accreditation regulations amongst such professionals, and the limited harmonisation with the UN Convention approaches to e-signature regulation.

The DOC senior official tended to echo certain concerns and recommendations providing that the regulations were in need of update and that the draft ECT Amendment Bill was an opportunity for update the regulations. The ASP representative also called for broader review of the ECT Act providing that the limited implementation of certain provisions of the ECT Act was problematic and has negative implications for the remaining provisions and that it remains unclear how the regulatory intent of the ECT Act to promote electronic commerce is realised in practice.

Other issues for review regarding the regulation included for the DOC senior official, consideration of "technology neutral approaches" (INT 9) versus the dependency in the current regulations on PKI based technology. Monitoring and evaluation

of the policies required address in the view of the DOC official and the association between electronic commerce trends and e-signature regulation was an example of an area where this could be applied.

Interestingly, one interviewee spoke to the barrier to adoption of e-signatures as a "human issue" and that the regulation needed to address the "human sentiment of looking into the person's eye, shaking their hand in the presence of witnesses to adequately legitimise the transaction in the opinion of the transacting party" (INT 1).

What impact do you believe the effective regulation of e-signatures has on the success of electronic commerce?

Interviewees spoke to an opportunity to deliver market efficiency. The limited adoption of e-signatures and reliance on traditional methods to complete electronic commerce transactions was referred to as "electronic commerce on crutches" (INT 1).

A legal expert provided that proper regulation promotes proper implementation and integration of e-signatures in electronic commerce and should ultimately promote growth in electronic transactions. Another interviewee held that ineffective regulation impacts e-signature adoption, accreditation and security. The interviewee cautioned that regulation should not be inhibitive and should promote innovation in e-signature technologies and services.

Furthermore the interviewee noted that conflicts and compatibility with other regulation was also a vital assessment.

The DOC official recognised that effective regulation of e-signatures was key to promoting investment, foreign and local in electronic commerce and addresses the reluctance present in the market to use electronic processes of transacting. According to the DOC official, the South African public continue to travel for the purpose of identification of persons or delivery of documents and effective regulation of e-signatures would increase trust in electronic trading promoting cost effective processes, enabling the benefits of economies of scale and other efficiencies. For one information security expert, the central issue of ineffective regulation of e-signatures was the subversion of trust in electronic commerce. Effective regulation particularly effective accreditation regulation, according to the expert, presents the ability to monitor the trust standards implemented by accredited authentication service providers which is necessary promote trust in the use of accredited signatures.

4.5 Summary

The legislative results of this study pertain primarily to the ECT Act and in this regard key provisions of interest to the inquiries of the conceptual framework and the analysis of e-signature regulatory effectiveness. In addition to the ECT Act, provisions of the E-signature Regulations (ES Regulations) are analysed in response to the key inquiries of the conceptual framework. The results included results of South Africa providing for functional equivalence for e-signatures in law and distinguishing between the validity and conditions for validity of e-signatures and the AeS. The accreditation process was analysed to find detailed, multi-pronged requirements for applicants pertaining to technical, operational and security measures that need to be fulfilled to be accredited as a provider of AeS services. The legislative analysis included the result of no recognition for foreign e-signature service providers in South Africa.

The outcomes of the interviews with the policy maker, an accredited e-signature service provider and experts in the fields of law, information security and e-commerce are noted in this chapter with the emphasis on implementation of the legislation and the accreditation regulations in particular. Such insights from the interviews are essential for a real and reflective understanding of the effectiveness of the legislative intent that emerges from the legislative analysis. Interviewees expressed consensus on the significance of e-signatures and effective regulation of e-signatures for electronic commerce benefits. Interviewees spoke to the need for legal assurance, setting of acceptable standards and legal accountability as well as promoting trust in e-signatures as some of the attributes of effective e-signature regulation. Interviewees raised several challenges in their experience with the regulation including the accreditation process requirements and associated inefficiencies and shortfalls in the legislative approach were also noted. Interviewees' recommendations for the policy maker are included in the interview summaries.

The case law findings in this Chapter have an important bearing on the legal conditions that inform the interpretation of the ECT Act and are included on the advice of experts calling for this contextual understanding in the literature. In particular, the case law establishes the courts position on the internationalised nature of electronic commerce law including e-signature law and issues of abiding by other conditions with the use of signatures to conclude contracts from existing laws, each of which issues are relevant to the question of the legal validity of e-signatures.

Hence Chapter Four provides the foundation for the correlative analysis in the chapter following, Chapter Five that will situate the results against the requirements for an effective e-signature regulatory framework and ultimately substantiate conclusions in Chapter Six on overall effectiveness under the sub questions and the main inquiry of this study.

5 CHAPTER 5 - ANALYSIS

5.1 Overview of the Chapter

Chapter Two extracted inquiries and approaches emanating from experts, model frameworks and certain countries to assess the effectiveness of e-signature regulation. The result was the conceptual framework for the study presented in Table 2.2. This framework and its themes are applied in this Chapter to navigate the results into findings on the effectiveness of South Africa's e-signature regulation.

These themes query if and how South African regulation of e-signatures afford legal validity, promote the trustworthiness of e-signatures and apply positive international approaches – and each of these aspects of analysis will include sub-inquiries. This Chapter, as with the topic, is complex and associated with several issues of legal, technical, information security and institutional effectiveness. Discussion on these issues is, however, necessary to give effect to the purpose of the study and adequately respond to the problem statement.

5.2 Legal Validity of E-signatures

5.2.1 Legally Valid Substitution with Handwritten Signatures

The literature review observed that legal acceptance for e-signatures promotes the effectiveness of e-signature regulation. In one study of developing countries the absence of legal validity for e-signatures led to concerns over transactional security and institutional trust (Kshetri, 2006). Other experts confirmed that by affording e-signatures the legal validity necessary for electronic commerce it can be catalytic to its growth (Blythe, 2007, Brazell, 2008). By legal validity we mean, e-signatures are deemed functionally equivalent to hand-written signatures - able to be legally substituted wherever a signature is required in law, giving the law a media neutral character (Low, R, Christensen, S, 2004, Parry et al, 2008). Second to the query of legal validity, a contextual query emerged in the literature: considering the legal functions of signatures in the country concerned, what is the ease with which e-signatures can substitute handwritten signatures (Aalberts and Van Der Hof, 2000)?

To the first query, the South African ECT Act provides that an e-signature has legal force and effect and should not be prejudiced in law, purely because it is in electronic format (RSA, 2002, s13). Thus, a general level of legal acceptance is afforded to e-signatures. Moreover, South African law, in enacting the ECT Act, takes on a media neutral character for the validity of signatures. To the second query, there are several factors to consider to contextualise the parameters of the legal validity including: - the distinction in the legal validity of e-signatures, how the ECT Act interacts with existing laws and any case law that qualifies how the provisions of the ECT Act are applied. These factors are explored in the remaining sections of 5.2.

5.2.2 Distinction in the Legal Validity of E-signatures

Two categories of e-signatures are described, each legally valid for distinct transactions and subject to distinct assessments criteria for their legal validity (RSA, 2002, s13). An advanced e-signature that is associated with a higher standard of trust, security and legal assurance and a second general category, for all e-signatures (RSA, 2002). This distinction may be summarised as follows:

Table 5.1: Distinction between E-signatures in South Africa

	Transactions for which the signature is legally valid	**Criteria for Validity**
E-signature means "data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature"	Transactions where the parties require a signature but have not specified the type of signature	The e-signature must be: – An adequate method to identify the person, – Indicate the person's approval of the information and; – with regard to the context and circumstances, at the time, the method was appropriately reliable for the purpose.
Advanced E-signature (AeS) means "an e-signature which results from a process which	Transactions where a signature is required but the law does not specify the type of signature	The accredited AeS benefits from a presumption of validity subject to it being duly accreditation as set out in the ECT Act, unless

has been accredited by the Authority as provided for in section 37 of the Act" (RSA, 2002, s1)	Transactions associated with legal verification of information integrity or the identity of a person such as electronic notarising, acknowledging, verification, seals or making statements under oath To secure the integrity of electronic information as evidence	the contrary is proven.

Note. Table 9 consolidates the ECT Act's distinction between e-signatures and advanced e-signatures in terms of definition, legal transactions for which they are valid signatures and the conditions placed on their validity

The distinction in Table 5.1 is be characterised as a two-tier approach (Brazell, 2008) where both tiers of signatures, the AeS and the general e-signature, constitute legally acceptable signing for *distinct transactions* with *distinct criteria for reliance*. For certain transactions e.g. where a signature is required in law or the signing a statement under oath, only the AeS is to be used and any other form of e-signature will not suffice (RSA, 2002, s13). For other transactions e.g. where parties require a signature to conclude the transaction or for legal communications, any form of e-signature may be used. Additionally, the use of each signature is subject to certain criteria for reliance. The general e-signature, for instance, must adequately identify the person and indicate their approval etc. The AeS must be duly accredited. The accreditation, discussed below, pertains to verification of the technologies and procedures of the service provider to ensure its trustworthiness. In effect whilst 5.2.1 reveals that e-signatures can be used in the place of handwritten signatures, the legal validity is subject to a test of (i) whether the appropriate signature for the transaction has been used; and (ii) whether the e-signature in question meets the criteria for reliance.

Thus the legal provisions are not absolute and the legal validity of a particular transaction calls for conjecture from the user in the circumstances.

The interviewees confirmed that applying this distinction takes away from the ease of substitution and presents uncertainty regarding which signature is the appropriate approval mechanism for the electronic transaction. Several interviewees agreed that the value of the respective e-signatures were not widely understood.

The DOC senior official believed that the public, the legal industry and the courts were not aware of the distinction. Interviewees were also asked which transactions benefit from the use of the AeS to assess the need in practical terms for the distinction. The common theme in the responses was the need for a set of criteria for the use of the AeS but with little consensus on what these criteria should be.

Possible criteria forwarded included:

- transaction values, with a view that larger value transactions would benefit from the advanced signatures;
- contracting entities, legal transactions with government and business should require an AeS (as opposed to consumer to consumer dealings);
- mitigating abuse of public sector electronic systems for unauthorised transactions;
- intelligence and defence processes; and
- documents that may be aggressively disputed in view of its capability to verify the integrity of an electronic document.

Interviewees did however agree that distinguishing the general e-signature from the AeS was a positive measure. According to the interviewees, the additional legal force and trust placed in the AeS relied on for example:

- compliance with technical standards;
- certification of its information security features; and
- verification of the person's identity face to face which mitigates non-repudiation of the transaction by the person.

The senior official of the DOC equally supported the distinction for the securing of higher standards and higher levels of assurance in the AeS.

From the above, the distinctions and definitions supported by the literature as strengthening the legal validity of e-signatures are provided for in the legislation. The effectiveness of the provisions to explain the qualities, and functions of e-signatures appears, however, to be lacking. The support for distinction amongst interviewees is noteworthy, particularly the effect of producing higher standards for the AeS in view of the trust and legal assurance associated with it. The general confusion as to which transactions are suited for such higher standard of e-signature may, however, negate the intended effects of the distinction. This contrast may be characterised as positive legislative intent met with poor outcomes, particularly in view of the limited adoption of electronic and advanced e-signatures revealed by the interviewees in Chapter

Four. The question of whether amending the legislation to provide additional clarity emerges. Public awareness activities amongst a cross section of stakeholders need to be considered by the Authority or the AeS particularly will not reach the desired adoption levels.

The concerning implication of this ineffectiveness is that the electronic commerce benefits of trust, legal assurance and improved security from the regulation are not maximised.

5.2.3 Other Factors impacting the legal validity of e-signatures

The ECT Act takes care to discuss its application in broader transactions. The Act recognises that not all transactions require a signature and permits that an expression of intent to conclude the transaction will suffice in such cases. (RSA, 2002, s13). The Act provides that in the matter of its interpretation, it should not be interpreted to exclude statutory or common law from being applied to or recognising or accommodating the provisions of the Act (RSA, 2002, s 3) or limiting the operation of any law that authorises, prohibits or regulates the use of electronic methods of communication or transaction including requirements for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method (RSA, 2002, s4). The effect is that other requirements in law that will impact the legal validity of e-signatures must be considered when assessing whether an e-signature will be a legally valid substitute for a handwritten signature. Another law may for instance prescribe only handwritten signatures.

Certain laws and transactions are excluded from the ambit of the legislation with the result that agreements for alienation of immovable property, long term lease of immovable property, execution, retention and presentation of a will or codicil or the execution of a bill of exchange are specifically excluded from the application of the ECT Act (RSA, 2002, s4). In such cases an e-signature cannot be substituted for a handwritten signature.

Several barriers to adoption of e-signatures were raised by interviewees that impact perceptions of legal validity. Such barriers to adoption of e-signatures are not associated directly with their legal validity in law but rather a noteworthy perception that e-signatures are not adequately valid as a legal substitute for a handwritten signature. These barriers include:

- the lack of a “ceremonious” process typically associated with traditional manuscript signatures – e-signatures are applied with a mere click of a button (INT 4);
- general preference in industries such as the banking industry for paper transacting processes; and

- perceptions of technical vulnerabilities in certain e-signature technologies that weaken their reliance.

For the policy maker, the effectiveness of the current legislation to promote confidence in e-signatures and their legal validity should be queried further. Furthermore, whether and to what extent the provisions be improved to better articulate the legal validity of e-signatures and instil greater confidence in their legal validity.

5.2.4 South African case law on the legal validity of e-signatures

As discussed in 5.2.1, further to mere assessment of general legal validity, analysis of case law determinations that provide insight on the interpretation of the legislative provisions are essential.

Three distinct cases were considered in Chapter Four in this regard:

- The first case produced several insights on the interpretation of the ECT Act particularly issues of internationalisation of electronic commerce law such as the ECT Act. The court urged that technical terminology must be used deliberately, consistently and in a manner of clarity. It noted that the ECT Act provides for transferral of concepts such as writing, signature and original to electronic interpretations and duly considered. The judge cautioned that the language of electronic communications may appear informal, regarding the contents as not having legal validity and force is erroneous. The judge noted that relevant international and foreign law encourage self-regulation which need to be considered
- The second case pertained to the value of considering and applying foreign lessons and best practice on the adjudication of disputes associated. Justice O' Regan, equally urged legal professionals to duly consider the lessons of international legal systems both for instructive value and to avoid parochial approaches to interpretation of the law (K, 2005). This urging is particularly relevant for electronic commerce where uncertainty in the application of the law is a factor.
- The third case concerns the issue of non-repudiation on which the legal validity of e-signatures and particularly the AeS hinges. The case noted that variation of contracts through informal methods (not hand-written) is not acceptable unless an express agreement by the relevant persons to not abide by the requisite formalities is in place. Under the ECT Act, where the parties have not required manuscript signatures, variation of contracts through electronic methods is valid. However, in line with the judgement of the Jafta case and this case, the variation of transactions through e-signatures will have no force and effect where the

specified formalities are not met and in the instance of a non-variation contractual clause binding on the parties prohibiting variation through non manuscript methods.

From the above cases, principles of interpretation and application for the e-signature validity provisions of the ECT Act emerge, as set out in Table 5.2 below.

Table 5.2: Principles of interpretation of the ECT Act on e-signature validity

Principle	Explanation
Internationalisation	Foreign law and international legal systems must be considered to understand the application of the ECT Act and mitigate narrow approaches to interpretation of the law (including its e-signature provisions). International decisions interpreting similar definitions or the parameters and principles of validity of e-signatures should be consulted.
Terminology clarity and consistency	For legal deliberations, the technical terminology is to be used deliberately, consistently and in a manner of clarity.
Functional equivalence of legal concepts	The ECT Act instructs transferral of concepts such as writing, signature and original in law, with interpretations that accommodate functional equivalence for electronic communications and transactions. Regarding the ECT as informal and not formally conveying legal validity and force to electronic communications and transaction is erroneous.
Consideration of self-Regulation	Particularly for the efficiency of the ECT Act's implementation, the courts should promote self-regulation. This in turn would mean that self-regulation codes and methods of interpreting and implementing provisions of the ECT Act should be considered as relevant.
Accordance with Formalities	For e-signatures to have legal validity in variation of contracts and not attract repudiation, compliance with formalities is requisite and consideration of any other contractual or legally binding provision that prohibits the use of e-signatures in the circumstances.

Note. Table 5.2 summarises legal principles that further contextualise how the provisions of the ECT Act will be regarded by a court of law.

Table 5.2 does not offer legal certainty but instead offers a measure of assurance on how to interpret and apply the ECT Act. With further case law, these principles may fast find obsolescence while new principles emerge. What is important ultimately is that the legal validity of e-signatures is assessed with the inclusion of the approaches by the courts. The tone

of the courts from the cases collectively reveal support for the enabling and globalised nature of electronic commerce - a sea change in law - with the transferral of concepts traditionally associated with transactions concluded on paper. In this area of analysis, the cases do not amend, or in any way diminish the legal validity of e-signatures but promote a considered approach to its use as an approval mechanism for legal assurance in electronic transactions.

5.3 Trustworthy E-signature Services

Analysis of e-signature regulation includes questions on how the regulation addresses (i) reliability and security of the certification service provider (ii) the identity verification procedures of the service provider (ii) procedures for termination and revocation of services of the provider (iii) the liability of the service provider and (iv) the costs associated with e-signature services (Kuechler and Grupe,2003). This indicates that the analysis of e-signature regulation is broad and complex. In this section, several topics of analysis will be used to characterise the effectiveness of South Africa's regulation to promote its trustworthiness. These topics consider the minimum attributes of e-signatures that make it suitable for purpose, the effectiveness of the accreditation procedures, the role of the accreditation authority, the effectiveness of the information security standards specified in the regulation and the liability of accredited service providers.

5.3.1 Essential attributes of e-signature services

E-signature products and services should be regulated to ensure effective delivery of the authentication or verification of the identity of the signatory, evidence of the integrity and accuracy of the relevant information and control against non-repudiation (Mason, 2003, p 20). From this, one can infer that certain minimum attributes of e-signatures must be assured in the regulation for signatures to be effective for their purpose.

Under the ECT Act, the tier of general e-signatures has minimal regulation of attributes prescribing criteria for validity (RSA, 2002, s13) as set out in Table 5.2 above. Such attributes pertain mainly to adequate and reliable methods of identifying the signatory and their approval of the document or transaction in question.

The requirements for an AeS technology (product), service and service provider to be accredited are extensive (RSA 2002, s 38). These are set out in the results of Chapter Four. To understand whether the minimum attributes prescribed in the literature are met for an accredited AeS, the accreditation requirements are compared in Table 5.3 below.

Table 5.3: Requirements for accreditation of the AeS in South Africa

Mason's Key Criteria	Requirements for Accreditation of the AeS in South Africa
Authentication or verification of the identity of the signatory	The e-signature to which the authentication products or services relate shall be, uniquely linked to the user, capable of identifying the user, created using means that can be maintained under the sole control of that user; based on face-to-face identification of the user.
Evidence of the integrity and accuracy of the relevant information	The e-signature to which the authentication products or services relate will be linked to the data to which it relates in such a manner that any subsequent change of that data is detectable. The service provider's systems shall adhere to at least the following: • Be reasonably secure from intrusion and misuse; • Provide a reasonable level of availability, reliability and correct operation; and • Be reasonably suited to performing their intended functions; and • Adhere to generally accepted security procedures.
Control against non-repudiation	The authentication service provider is assessed in relation to for instance, the quality of its hardware and software systems; procedures for processing of products or services; the availability of information to third parties relying on the authentication product or service; the regularity and extent of the audits by an independent body. The records to be kept and the manner in which and the length of time regarding the retention are prescribed for future reference. The requirements as to adequate certificate suspension and revocation procedures are to be met. The requirements as to adequate notification procedures relating to certificate suspension and revocation are to be adhered to.

Note. Table 5.3 associates the requirements for accreditation of the AeS in section 38 of the ECT Act (RSA, 2002) with Mason's specifications of effective accreditation regulation.

With regard to the above Table 5.3, the ECT Act provides for the essential minimum attributes. These criteria include methods of authentication of identities, evidence of integrity of information, due diligence procedures associated with the operations of the applicant service provider and providing safeguards for non-repudiation. Additional mechanisms such as proper records management, periodic audits of compliance, strict control of certificates and notifying persons without delay should they be suspended or revoked further promote the non-repudiation value of the AeS. Moreover, with reference to a query in Chapter Four on the suitability of e-signatures to attest the integrity and originality of electronic documents, the attributes of the AeS set out in Table 5.3 render an AeS is suitable for this purpose. The inference is that the legislators in specifying accreditation requirements intended that minimum criteria be adhered to in the case of the AeS that would promote its utility as a tool for trust, security and legal confidence.

5.3.2 Accreditation Regulation

Termed accreditation regulation, the analysis of accreditation processes, the criteria setting for accreditation and the progress in implementation of accreditation regulations are cumulatively regarded by various authors as important determinants of the effectiveness of e-signature regulation (Parry et al, Cole et al and Low et al). These factors are considered in particular detail in this section.

Chapter Four's documentary analysis revealed that the ECT Act is not the only South African documentary source on accreditation requirements for the AeS. South Africa published further regulations in 2007 (ES Regulations) in accordance with section 41 of the ECT Act, which entitles the Minister of Communication's to pronounce such further regulations. The effect of the regulations, adding to the provisions of the ECT Act, and as discussed in Chapter Four, include declarations and commitments by applicants for accreditation pertaining to actual procedures, technical capabilities and operational safeguards of the applicant entity (RSA, 2007).

The Regulation expands on the requisites of the ECT Act and require the applicant to submit specifications as part of the application including:

- The procedures for identification and authentication of the users including face-to-face identification;
- How the applicant will ensure continued availability of the information to third parties relying on the product or service;

- Technical specifications of the software, hardware and information security policies and standards to which it complies;
- Privacy and physical security policies to be implemented by the applicant;
- Audited financial statements of the entity for three years;
- Human resources related to the AeS products and services; and
- Details of a requisite technical audit in accordance with WebTrust[7] standards (see section 27 of the ES Regulations).

The application requirements are clearly extensive, and likely, preceded by the applicant having implemented significant operational, technical, policy, human resources and other measures at the applicant's organization.

Certain interviewees revealed support for accreditation and the associated requirements in view of the benefits:

- Procuring appropriate levels of security for AeS products and services as a positive development for electronic commerce; even the ASP representative noted that the regulations instruct the relevant standards for an AeS on which significant reliance is placed by the user
- The security afforded to identity information was supported;
- Harmonization with international standards through the regulations was endorsed;
- Promoting the legal force of e-signatures in the AeS;
- The DOC official spoke to the government approval attached to accreditation as promoting higher levels of assurance;
- The ASP representative explained that accreditation means that the AeS has been subjected to a review of the quality and integrity of the authentication services and process, and to international benchmarks.
- Review of the applicants HR procedures including the hiring processes promote proper background checks,
- Assessing the financial viability of the applicant was supported;
- The need for regulation of the process of revocation and termination of certificates was reinforced.

[7] As per the definitions in section 1 of the ES Regulations, WebTrust means the principles and criteria of the WebTrust Program for certification service providers developed by the American Institute of Certified Public Accountants, Inc. and the Canadian Insititute of Chartered Accountants

Conversely, the accreditation process also faced criticism, more notably:

- The process was viewed as a "checklist exercise" (INT 6) with little value in mitigating information security vulnerabilities;
- Standards prescribed were considered outdated which was of particular concern to the interviewees as "standards for risk management should change in accordance with technology changes" (INT 8);
- The regulatory intent and requirements for accreditation are not broadly understood - in the view of one interviewee, even by the DOC itself,
- Poor response in applications - the DOC official noted that limited applications were received and where inquiries were received, it was clear that the prospective applicants were unclear of the purpose of accreditation;
- The audit of the controls required for the AeS service, approximately 500, can take 3 months and constitutes a significant cost;
- Close association with particular technologies was not innovation conducive – the DOC noted that the AeS is currently associated with digital signatures as the current regulation provides for PKI based technology but that the DOC is considering amendments to this approach;
- A specific difficulty is the limitation in the regulation on which auditors may be used resulting in a lack of competition for the auditing services which resulted in high costs according to the DOC senior official;
- According to the DOC official, at this time the, however, that would allow the accreditation of technologies that are not PKI based. High costs associated the use of an AeS were noted by an interviewee which in the mind of the interviewee may, be attributable to the costs of accreditation of the AeS, as per the interviewee.

What emerges quite distinctly is that the accreditation processes as set out in the documents reviewed are extensive and aligned in general with regulation. In implementation, however, it has met with considerable inefficacy. The consolidation of diverse input of various stakeholders reveal varying expectations for the effectiveness of the regulation and accordingly varying frustrations and dissatisfactions with the outcomes in areas including technical robustness, market efficiency and legal assurance. Returning to the purpose of the analysis of this area of e-signature regulation, the failures in securing

effective implementation of accreditation regulation ultimately deters from the availability of AeS products and services and the associated provision of trust, security and legal assurance associated with such form of signature.

5.3.3 Liability of the Accredited Service Providers

The liability of the e-signature providers pertains in general terms to the liability for damages suffered by any person relying on the service or product (certificate) (EU Directive, 2000, and UNCITRAL, 2001 Article 10) particularly for the accuracy or assurance of signature related information or that the signature was not revoked (EU Directive, 2000, art 6).

In South Africa the ES Regulations tends to focus on the accreditation of the CSP of PKI based technologies (RSA, 2007). As a result, the focus is on the CSPs liability. The Regulations address liability by stating that: (i) the apportionment of liability is to be specified in the service providers practice statement to subscribers that sets out processes for generating and issuing certificates in accordance with SANS21188 (ii) with the caveat that the CSP cannot exclude liability resulting from gross negligence (RSA, 2007, s19).

Arguably, effectively regulating the liability of the e-signature service provider can incentivize the service provider to avoid liability through adequate risk mitigation safeguards. It will also promote confidence in the use of the services with the knowledge that the user may be recompensed should the service not be of an adequate standard. The provision in the ES Regulations can be criticised for being scant and affording the service provider too much liberty in the determination of its liability. This would not be conducive to liability avoidance measures by the service provider or growing user confidence.

The EU Directive also spoke to liability associated with diligent revocation procedures (EU Commission, art). The ES regulations require that a certificate be timeously revoked where it is rendered invalid (RSA, 2007, s21). In this area, whilst the Regulations provides for revocation procedures (RSA, 2007, s21) it does not attach specific liability for not applying such procedures in terms of the EU Directive.

The DOC senior official noted that the ASP's liability for its services has increased with the AeS service and that information breaches will "significantly damage the company's business case" (INT 9). The ASP interviewee shared the view that information breaches can "end this line of business for the company and the availability of the AeS as the only certified service provider". This does not bode well for the sustainability of the ASP or the availability of the AeS, each critical to advancing adoption of this form of e-signature that offers heightened legal confidence, trust and security.

Finally, the regulations do not offer guidance on mitigation of liability. As a result, self-informed and varying approaches may result. The ASP representative, for instance noted that the ASP keeps pace with developments and industry guidelines through participation in international forums and developments to manage such liability. Perhaps the Authority has a role to play in offering further guidance.

5.3.4 Analysis of the regulation of information security standards for e-signature products and services

The literature observed that e-signatures play a significant role in:

- the generation of trust in electronic commerce activities (Cogburn, 2003, Dagada, 2009, Kshetri, 2006 Cole, K. Chetty, M. LaRosa, C.Rietta, F. Schmitt, D. Goodman, S, 2008 Low and Christensen, 2004);
- attending to concerns of the identity of the transacting parties (Wang, 2007, Brazell, 2008);
- and the security of the transactions being concluded (Kshetri, 2006, Dagada, 2009).

It is probably with such objectives that e-signature regulation promotes the trustworthiness of e-signature service providers, by mandating acceptable information security standards for an advanced e-signature, duly accredited. Furthermore, 5.2 above explained that the AeS, has a presumption of legal validity as a signature unless the contrary is proven. This presumption, while catalytic to legal confidence in legal transactions, is another reason to ensure the trustworthiness of the AeS and its service provider.

The ECT Act and ES Regulations were examined in detail in Chapter Four for the manner in which such trustworthiness is determined in the South African case. Under the ECT Act, the applicant is required to submit a detailed application that must include the technical features of the e-signature technology, specifications for the supporting hardware and software for the proposed services and particularly the information security policies and procedures. These measures help to ensure the applicant that renders the service trustworthy (RSA, 2002, s38).

Section 26 of the ES Regulations is titled “information security requirements” (RSA, 2007, s26.) Compliance with international standards including SABS/ISO 17799[8] and SANS 21188[9] (RSA, 2007, s26) is specifically mandated. Further to the specific section, the ES Regulations with the focus on certification PKI based services calls for:

[8] See Table of Abbreviations for definition
[9] See Table of Abbreviations for definition

- compliance with the ITU X.509 standard for issuing digital certificates and three factor authentication or a similar level of security is also mandated (RSA, 2007);
- trustworthy systems;
- information security policies and procedures;
- incident management including reporting information security breaches to the Authority;
- ensuring personnel have the appropriate knowledge, technical qualifications in connection with their duties (RSA, 2002, s38);
- face-to face identification procedures and specification of the documentation to identify and authenticate the relevant e-signature user (subscriber); and
- managing risks associated with subscriber conduct and agents or contractors to whom operations have been outsourced through proper agreements (RSA, 2007, s, 13,14, 15).

All applicants must detail the privacy and physical security policies as part of its accreditation process, appoint and pay an auditor to audit compliance with the requirements in the ES Regulations (RSA, 2007, s27). As an added method of assurance, as per Chapter Four, is that the accreditation remains subject to the outcomes of an evaluation of independent experts appointed by the Authority (RSA, 2007, s9)

The above can cumulatively be referred to as the information security requirements.

Notably, the information security requirements are extensive, detailed and specific to certain international standards. The policy maker clearly intended that the accredited service provider sufficiently assures the Authority of adequate information security measures. Notably, strict compliance with specified information security and mitigation of third party risk need to be managed by the accredited service provider. Assurance to the Authority is through audit reports submitted by the applicant and an evaluation instructed by the authority.

Interviewees supported regulation of information security to ensure that AeS service providers apply appropriate standards of care to the information it holds. The reasons were cited as: the absence of security standards will demote user trust value in e-signatures; standards commensurate with the legal force and trust associated must be applied; and ensuring that the technology infrastructure is not vulnerable to compromise or abuse.

Regarding the actual regulation, several concerns were raised and noted in Chapter Four, notably:

- Consultation by the policy maker on the technical standards to be applied and available e-signature technologies was inadequate;
- Security standards such as ISO 17799 and the WebTrust standards relied on were outdated - an interviewee was convinced ASP will be prone to information security attacks such as hacking and malware vulnerabilities despite the standards
- The three factor authentication requirement was unrealistic; and
- Concerns over the knowledge of the Auditors regarding PKI and PKI controls were in need of review to strengthen the outcomes of the audit processes.

From the above, it is observed that particularly the current information security standards are regarded as ineffective and outdated, having not kept pace with technology changes. The risk mitigation controls are not equal to the current threats. This exposes the ASP and future accredited service providers to vulnerabilities. In view of the trust placed in an accredited provider, the policy maker must review the information security standards in the ES Regulations. Broader consultation with industry experts were called for by the interviewees and this should be noted by the DOC. This ineffectiveness does not impact the resounding call for information security regulation. Technical safeguards are necessary but soon face obsolescence as technology adapts and changes and new threats emerge. This lesson is particularly true for information security technologies and what is called for, it appears is that the policy maker adopts a robust approach to updating the regulations.

5.3.5 The delay in the accreditation of the ASP

The accreditation process in general is critiqued in 5.3.2 above. This section is focussed on the accreditation specifically of the ASP and associated insights on the effectiveness of the regulation. A particular issue in the problem statement was that of the event timeline for e-signature regulation. The ECT Act was passed in 2002 providing for e-signature legal force and an advanced e-signature, the ES (accreditation) Regulations taking effect in 2007 and the first ASP being accredited in 2012, 10 years after the ECT Act was passed. In this section 5.3.6 an understanding of the impact and possible causes of the delay is pursued.

A particular view amongst certain interviewees was that electronic commerce was not brought to a complete halt with the unavailability of an accredited AeS. According to the DOC official, online transacting should not have been impacted as e-

signatures were available and the availability of the AeS impacted transactions where such signatures are required or desired – the demand was from foreign companies who were of the benefits of accredited forms of e-signatures in their own countries.

Another view was that the delay in accreditation represented an opportunity lost. Earlier availability of an AeS may have promoted the "speed, efficiency and trust in concluding transactions electronically" (INT 1).

Another delay in adoption of AeS was foreseeable according to one interviewee and related to a lack of promoting the understanding of the significance of the AeS. Another interviewee upheld that only long term adoption of the AeS should be expected. Security experts were particularly concerned that large corporations such as banks would not be comfortable with a relatively small player like the ASP being the sole option for them to pursue advanced signature adoption. Banks in particular would prefer to implement e-signatures themselves in a manner that they trust.

Legal experts were concerned that the accreditation regulations were not effective and resulted in the delay of the particular accreditation of the ASP. To this point, the ASP representative spoke to an overall positive experience but noted challenges with certain cumbersome requirements e.g. compliance with more than 500 specific requirements or controls and the extensive audit of the ASP's environment that was necessary. These requirements were noted as possible barriers to further accreditations. The DOC representative, also an official of the Accreditation Authority, acknowledged the significant financial investment of millions of rands by the ASP as an issue, as well as the increase in the ASP's liability for its e-signature services following accreditation. The costs of maintenance of the IT infrastructure and security standards to maintain accreditation were also noted as possible barriers following the ASP experience. Moreover, an interviewee noted that the high costs of accreditation as observed with the ASP accreditation would negatively affect the pricing of AeS services. The result would be that only government and major corporations would find it affordable. One of the legal experts urged government to promote the use of "ordinary e-signatures that develop according to technological standards being developed globally" and in so doing promote the market adopting acceptable standards for ordinary e-signatures - an approach that would be in line with the UN Convention.

The analysis of the impact of the delay presents two alternate realities. Firstly that electronic commerce is not dependent on the availability of an AeS to secure and legally validate transactions. Secondly, South Africa, perhaps unknowingly, has not maximised electronic commerce opportunities as a result of the delayed availability of an AeS. Further study of an empirical nature is needed to prove or disprove either of the realities and is extraneous to the purpose of this study. On the question of effective accreditation regulations, however, what we observe most significantly from the ASP experience is significant

cost and effort investment. This questions the ease of accreditation of other possible AeS providers. The reference to foreseeable further delays is also not encouraging. If long term adoption of AeS in the market is a reasonable outlook, the benefits of added trust, security and legal confidence from the use of the AeS in electronic transactions is hindered. Remembering that South Africa has a two tier approach, the suggestion of a legal expert to promote broader adoption of ordinary e-signatures (not accredited) according to international and market developed standards is indeed interesting.

5.3.6 The effect of a single ASP

Interviewees were asked to comment on the significance, if at all, of a single accredited authentication service provider in the market. This question drew wide consensus in that having a single accredited service is problematic for the AeS market. The lack of competition would negatively impacting pricing and levels of innovation in the AeS service, pricing control and service quality. The DOC senior official echoed that a monopoly situation was undesirable, particularly noting concerns regarding the pricing of the services.

Somewhat off the question at hand, the DOC employee cautioned that pricing should not be evaluated as part of the accreditation process as government should guard against “unduly interfering”.

An interesting observation was that of an e-commerce expert who was concerned that a lack of competition would breed complacency and little innovation within the Authority itself, as it would only have a single provider to govern. This interviewee was further concerned that the regulator and the provider may develop a relationship that is not an arm’s length relationship.

There was also expectation and speculation that the South African Post Office would be accredited shortly, and that brought both challenges and opportunities. On the one hand, the ASP’s efforts to educate consumers on the AeS and encouraging further adoption would be seconded by new accredited service provider. On the other hand, one interviewee was concerned that government entities would immediately use SAPO signatures, as it was a state owned entity, effectively squeezing The ASP out of a significant market. The DOC employee noted that another applicant was in the accreditation process and the evaluation was near completion.

Clearly the lack of competition in the AeS market impedes innovation, service quality and pricing control. This can only be cured by a second accreditation to promote competition and the desired market effects for consumers. Another salient point

of caution is the effect on the Authority – concerns that the Authority's own role may be impeded by only exercising its powers over a single accredited service provider.

5.3.7 Foreign signature service providers

Certain international frameworks and systems provide for the recognition of foreign certificate service providers either in the legislation (Blythe, 2007) or through bilateral or multilateral agreements (EU Directive, 1999, art 7).

The assessment of recognition pertains to legal provision for equivalent legal validity to foreign providers, subject to the foreign provider meeting specified requirements (EU Directive, 1999).

In the UK, The Electronic Communications Act does not provide for recognition of foreign certificates or certification service providers (Brazell, 2008). In China, legal recognition of foreign e-signature certificates issued by CSPs outside China is provisioned. This is conditioned on a relevant agreement, a principle of reciprocity, between China and the country in question.

In South Africa, both the case law (Jafta, 2008) and legislative documentary analysis (ECT Act, 2002) revealed that the Minister may recognise the accreditation (or similar form of recognition) granted to authentication products, services or service provider by pronouncement in the government gazette, subject to conditions that many be imposed by the Minister (RSA, 2002, s 40). There are no provisions pertaining to distinct accreditation of foreign authentication products and services. The conditions for recognition are equally absent. South Africa does not provide for agreements between South Africa and other countries on the issue of recognition of each other's accredited e-signatures. This tends to place South Africa at odds with the EU Directive of 1999 and with a fellow developing country, China.

Interviewees were queried on the importance if any of the recognition of foreign accredited signatures in South Africa. The electronic commerce expert's view was to meet the legal requirements of the country of trade, which necessitated local accreditation rather than recognition of the foreign accreditation. Another legal expert provided, in contrast, that a country's standards for accreditation are developed to meet local requirements and not necessarily suitable for other countries. Recognition of foreign accreditations hinged, in the view of the expert, on the level of compatibility of the foreign accreditation with South African and international best practice standards. Full accreditation was viewed by the legal interviewee as costly and without real value.

Interviewees also provided recommendations for the approach to foreign accredited signatures. As a general recommendation, an interviewee submitted that global accreditation standards should be investigated - accreditation based on international standards would negate accreditations in each country. A legal interviewee supported this approach calling for a "uniform system" of accreditation that in the expert's view would be of benefit to countries and consumers globally. An information security expert added to this line of thought by recommending recognition where a global standard is applicable but subject to a prior assessment of compatibility of the global accreditation process and approach. The DOC senior official confirmed that the issue with the recognition of foreign accreditations was in fact the compatibility of the standards associated with the foreign accreditation.

An alternative to international accreditation was forwarded in the form of mutual recognition by countries or "co-operation agreements" but the interviewee concerned was critical of the South African government's ability to fulfil such co-operation agreements.

The DOC senior official noted that the new ECT Amendment Bill provided for agreements between governments regarding recognition of the counterpart's signatures. Hence the proposed approach was explained to be to agree at government –to-government level the recognition that is afforded to corresponding accreditations. The ASP representative cautioned that recognition of foreign accreditations may result in conflicts with other laws such as privacy laws. Local accredited service providers' practices would be generally more compatible with the broader laws in South Africa.

The issue of regulation of foreign e-signatures is a curious case. From the above, as early as 2002, provision was made in the ECT Act for the Minister to pass regulations on the recognition of foreign signatures. Such regulations were never passed and approaches are today still being debated. This holds true while other jurisdictions have developed this area of their regulation. An approach of mutual recognition is noted by the DOC senior official as the possible way forward. Other sections of this analysis revealed a less than ideal market for accredited signatures. High cost, poor service and quality signatures will only weaken the legal confidence, security and trust in e-signatures for approval of electronic transactions. The case of Jafta (Jafta, 2008) also urged consideration of the global and internationalised nature of electronic commerce. On this issue, this urging is particularly relevant. South Africa appears to be behind the times as far as regulatory effectiveness in the domain of foreign signatures is concerned.

5.3.8 Oversight of E-signature Products and Services

According to Kuechler and Grupe, the implementation issues of (digital) signatures in any jurisdiction are constituted not only by technical issues but extend to challenges with the legal authority and regulatory bodies (2003).

In South Africa the Director General of the Department of Communications acts as the Accreditation Authority in respect of the accreditation of the AeS (RSA, 2002, s34). This Accreditation Authority's powers and duties discussed in Chapter Four include: oversight of the conduct, systems and operations of an authentication service provider; powers of revocation or suspension of an accredited service provider, powers to appoint an independent auditing firm to conduct periodic compliance audits on the service provider; maintaining a publicly accessible database of accredited products and services and recognising foreign signature products or services (RSA, 2002, s36).

According to an interviewee, the "accreditation creates an ecosystem of authority" where the security that the trust hinges on is reviewed by an appropriate authority. The DOC senior official described the role of the Authority as the regulation of e-signatures to "create predictability and promote trust and security in electronic transactions".

According to other interviewees:

- the Authority should create an open channel for electronic commerce that is safe and secure,
- blend the best of global best practice and local needs as far as e-signatures are concerned into policy and legislation;
- the DOC as policy maker and Authority should have two primary focus areas: promoting the ease of adoption of e-signatures and ensuring that the regulation promotes that the accredited signatures are as secure as possible;
- the Authority should ensure enforcement of security standards and conduct continuous "review and updating of the security standards that provide for improved validation and verification mechanisms".

Other interviewees were critical of the DOC's approaches thus far describing the Authority as weak, questioning whether the DOC would fulfil the need to educate and assist the public on e-signatures and critical of the lack of adequate consultation on the accreditation regulations

A legal expert was critical of the recent draft ECT Amendment Bill prepared by the DOC. According to the legal expert the lack of "address of conformance with the (UN) Convention was a disappointment" and a weakness that needed to be addressed and following the approach of the UN Convention regarding e-signatures was likely to deliver the electronic

commerce benefits sought. Interviewees agreed that the DOC was required to promote awareness of the benefits of e-signatures and advanced e-signatures, their uses and that advanced e-signatures are available. The ASP representative noted that it was hopeful of "bolder support" from the DOC.

The role of the DOC is clearly multi-faceted as a policy maker and an Accreditation Authority. This is rendered even more challenging with the diversity of the accreditation authority roles including public awareness on e-signature products and services, regulatory oversight roles, and extensive assessment of accreditation applications. As a policy maker too, the interviewees called for increased consultation and improved consultation of best practice technical standards and regulatory guidance available. This positions the role of the DOC as far as e-signature regulation is concerned as quite a dynamic role. Institutional challenges of the DOC where not assessed in detail but what is apparent from the limited study is that the DOC will need to review its current capability to deliver on this multi-faceted, dynamic and no doubt, challenging role. There is a clear association between the effectiveness of the policy maker and Accreditation Authority in delivering e-signatures that will promote and advance trust, security and legal confidence in electronic commerce.

5.4 Harmonisation of Approaches to Regulation of E-signatures

5.4.1 How do South Africa's approaches to e-signature regulation compare with international models and frameworks

The UNCITRAL Model Law on Electronic Commerce provided a general legal framework for electronic commerce including general legal constructs for the legal effect of e-signatures (UNCITRAL, 1996). To be harmonised with the UNCITRAL Model Law, South Africa would need to align with predominantly Article 7 of the UNCITRAL Model Law. Provisioning that functional equivalence of e-signatures to paper signatures requires meeting prescribed conditions (UNCITRAL, 1996, art 7). Brazell reinforced that this provision would enable the equivalence of the e-signature to the paper signature as the aspects of identity of the person, association of the information with the person and indication of intent to sign was present. Brazell noted this approach as a technology neutral approach, not aligned with any specific technology. (Brazell, 2008).

In accordance with the discussion in 5.2.1 above which has no cause for repetition in this section, South Africa's regulation of e-signatures is aligned with the UNCITRAL Model Law on Electronic Commerce and its associations with effective e-signature legal validity.

The second key international framework considered in Chapter Four, was the UNCITRAL Model Law on E-signatures taking effect in 2001. This model law provided definition for an e-signature and certificate. Furthermore, supplementary to the UNCITRAL Electronic Commerce Model Law, this model law re-emphasised the issue of reliability of the e-signature and offers a reliability test (UNCITRAL, 2001). Brazell noted this subsequent approach as restrictive, with an inclination to public key infrastructure technologies, but ultimately providing a two-tier approach for signatures that automatically meet the reliability requirements that will need to assess on a case by case basis. Blythe viewed the approach to rather be a preservation of the first technology neutral approach and an introduction of standards for e-signature technologies. As far as trustworthiness is concerned, Article 10 of the Model Law on E-signatures provided several inquiries to regulate the trustworthiness of the service provider of CSP. To be harmonised with the UNCITRAL Model Law would mean that over and above the mere provision of legal validity, distinction between e-signatures of varying reliability would need to be evidenced as well as the presence of reliability standards. Moreover, the regulation of the trustworthiness of the CSP would need to be evidenced concurrent with requirements of this Model Law.

An extensive analysis of the distinctions in the South African regulation for e-signatures and advanced e-signatures is contained in 5.3 above, with the resulting provision over and above the requirements of the 1996 UNCITRAL Model Law for distinction between the forms of e-signatures and their level of reliance. The assessment of the reliability of both e-signatures and the AeS were also specified in Table 5.2. The accompanying analysis revealed that in implementing the legislative provisions, several challenges in understanding the value and application of these forms of e-signatures are observed in the market, albeit that minimum reliance requirement(s) are prescribed. While this does not take away from the harmonisation with the UNITRAL Model Law on E-signatures, this reveals that such alignment in and of itself does not equate to effective regulation.

The third international framework is the EU E-signatures Directive of 1999. Comparatively, a firm distinction between an e-signature and a so called advanced e-signature is noted (European Commission, 1999 art 5). An e-signature per se that is associated with the information and serves as a method of authentication of a person's identity retains legal force and effect (European Commission, 1999 art 5). An advanced e-signature is an e-signature but is based on a qualified certificate or electronic attestation of the signature and identity verification of the person and subject to meeting additional security requirements including creation by a signature creation device, signature verification data, indications of the CSP and the period of validity and unique identifiers of the certificate (European Commission, 1999). Brazell provided that standardised certificates are available that meet the requirements (Brazell, 2008). Furthermore, the Directive instructs EU member

states to provide for the admissibility of e-signatures as evidence. Harmonisation with the EU Directive, would, therefore, entail clear definition between an e-signature and an advanced e-signature, as well as a certificate and qualified certificate, reference to standards of security and improved trustworthiness concurrent with the EU Directive approach and provision for the evidentiary admissibility of e-signatures. Forder noted this approach as a two-tier approach (2010). Further commentary on the effectiveness of the approach is noted in the literature review and is revisited in the conclusion. For the purposes of alignment, the extensive discussion in 5.2 reveals the highest alignment of the South African approach with the EU Directive. This may be chronologically influenced with the Directive issued in 1999 providing the policy makers time for consideration for the ECT Act promulgated in 2002. Again the analysis of 5.2.2 specifically will attest to the detailed alignment in even the accreditation approach to advanced e-signatures, the requirements for incorporation of international standards and the emphasis on security requirements. The analysis of South Africa's e-signature legislative provisions and ensuing regulatory approach reveals a harmonisation with particularly the EU Signatures Directive of 1999.

The alignment is further evident in the two-tier approach evidenced in South Africa, in that the legislation and regulations provide for an e-signature and an advanced e-signature, and a greater reliability in so far as trust and security is concerned for the advanced e-signature – which is subjected to various requirements to enable this improved reliability. Winn noted, however, that the approach could be an accommodation of various EU government technology neutral and technology specific approaches, as well as a demand for substantive regulation versus calls for self-regulation (2007). Winn noted that market adoption of AeS in the EU countries has remained low which is synonymous with the application of this approach in South Africa. Evans noted a review of the approach to address changes in regulatory demands of electronic commerce and that issues of regional co-operation and improving the effectiveness of the security requirements need to be considered as consumer and business confidence in electronic transactions were still at low levels (Evans, 2011). This realisation of lack of effectiveness of the current e-signature regulatory approach and the review process has important implications for South Africa. Furthermore, the context of accommodation of various EU country demands reveals a complex and compromising approach between technology neutral and specific as well as between substantive regulation and self-regulation. This has not produced the levels of adoption of AeS desired or the trust and security pursued, and as such requires further consideration.

5.4.2 How does South Africa's approaches to e-signature regulation compare with foreign country approaches?

The literature considered regulatory developments in UK, Australia and China. The motivation for the country selection is addressed in Chapter 2 and included ensuring that a developed and developing country is considered and a country that is often consulted for regulatory precedent in electronic commerce regulation. What emerged is that each of the countries offered regulation of (i) the advanced signature (ii) regulation of the products and services associated and (iii) regulation of the certification service provider. This is commensurate with the key aspects of regulation in South Africa.

Furthermore, regulation in the countries tended to include a primary law that governed the legal validity of e-signatures and supplementary regulations that governed the certification service providers of advanced e-signature products and services. In South African, the ECT Act is supported by the ES Regulations which again finds compatibility with the countries.

In so far as the effectiveness of the country's regulations, and comparison with South Africa, the following salient observations are made:

UK

- The UK legislation provides a definition of an e-signature did not distinguish the forms of e-signatures and was referred to as minimalist by Brazell (2008). The subsequent Regulations, however, provided for the distinction defining an AeS in a manner inclined towards the EU Directive on E-signatures.
- The UK has an industry led regulatory authority for CSPs despite provision for government to have the authoritative function, attributable according to Brazell to a lapse in the time afforded to appropriate such scheme by the government (5 years) (Brazell, 2008).
- Foreign CSPs are not recognised in the legislation;
- Case law in the UK has substantiated the application of rule framework of the legislation thereby promoting its relevance.

South Africa comparatively has similar distinctions and definitions of the tiers of e-signatures and provision for reliability standards together with the notation of CSP regulation. South Africa does not have self-regulation of e-signatures hence this is a point of discord. In South Africa too, particularly the Jaffa case, (2008), the case promoting the credibility of the ECT Act which is true to the value of case law in the UK.

Australia

- The Australian legislation similarly provided definitions of an e-signature and catered for its functional equivalence in law to handwritten signatures
- The law defined an AeS and conditions of reliance on the AeS (Brazell, 2008) but by Forder as being inadequate in its criticised for the reliance on self-regulation (Forder, 2010).
- A dependency on case law was noted on parties producing evidence to attest to conformance with the reliability conditions – which shortcomings render the legislation inadequate (Forder, 2010).

South Africa's approaches finds strong correlation with Australia in the definitions of forms of signatures, reliability standards and CSP regulation. At this stage, there are no dependencies on court determinations as in Australia but as noted in section 5.2, case law must be considered in the interpretation of the South Africa's ECT Act provisions on e-signatures.

China

- China's e-signature legislation (i) grants e-signatures legal validity equivalent to the handwritten signature (ii) provides the processes surrounding the use of e-signatures and (iii) providing for the rights and responsibilities of various parties including the parties to an electronic transaction (Blythe, 2007, Brazell, 2008).
- Srivastava assessed the definition of the AeS in the legislation aligned again with the EU Directive providing that while such reliable e-signatures may refer in practicality primarily to digital signatures, there is a rationale for not using the term digital signatures - a reluctance inhibit the use of other signature technologies and limit outdating of the legislation in the face of new technologies (2005).
- A challenge raised is that it is unclear which transactions would require a certified signature (Srivastava, 2005). This approach was supported by another expert as affording the Chinese public the autonomy to select the appropriate e-signature technology that meets the reliability requirement and the autonomy to decide whether to use an e-signature at all (Wang, 2007).
- Significant regulatory standards were established for CSPs including competent human resources, financial sustainability, and the imposition of security standards

- Legal recognition of foreign e-signature certificates issued by CSPs outside China following approval after a relevant agreement or where there is a principle of reciprocity of recognition
- Uniquely, three conditions in which an end user signatory shall be liable for damages where the signatory is aware that e-signature creation data (private key in case of digital signatures) has been descrambled or may have been descrambled but fails to inform the relevant parties in a timely manner and fails to stop its usage, failure to provide accurate information when applying to the CSP and commission of a fault resulting in loss to parties relying the signature or to the CSP.
- Research that queried the efficacy of law reform for positive electronic commerce outcomes concluded "dim prospects" (Winn and Song, 2007, page). Winn and Song asserted that Chinese businesses would benefit from legislation that accounts for unique Chinese conditions rather than transplantation of foreign approaches. The primary criticism concerned the promotion of a technology that is not broadly used, and while the law intended to be technology neutral it actually leaned heavily toward a single technology (Winn and Song, 2007).

South Africa's regulatory approach to e-signatures as well as the challenges with the regulation bears a striking resemblance the Chinese case. The primary variations are in the approaches to recognition of foreign signatures and the end user liability provisions. South Africa neither has a mechanism for the recognition of foreign signatures nor does the law set out end user liability provisions as in China. The outcome of the research of efficacy of the Chinese approach is relevant in South Africa too. Firstly, South Africa should avoid mere transplantation of foreign approaches that impede market efficiency. Secondly, South Africa too intends technology neutrality but leans too heavily to certification services based on PKI technologies. The result may be technologies that are not suitably adopted for the benefits of the AeS to be realised. The implications of this strong lenience must be further explored.

Table 5.4: Comparison of SA regulatory approaches to e-signatures

	Definition of E-signature and Functional Equivalence provisions	**Definition of AeS and conditions of reliance**	**Defined CSP (AeS Service Provider) Regulation**
UK	Yes	Yes	Yes (defined regulation and self-regulation

			through Tscheme)
Australia	Yes	Yes	No (self-regulation through Gatekeeper)
China	Yes	Yes	Yes (defined regulation, self-regulation unclear)
South Africa	Yes	Yes	Yes (defined regulation, no self-regulation)

Note. Table 5.4 compares South Africa's approaches to e-signature regulations in key effectiveness areas with the UK, Australia and China.

5.4.3 Is South Africa's approach to e-signature regulation aligned with developments in regulatory approaches that advance electronic commerce?

In chronological terms, as discussed above, the e-signature regulatory approach evolved from affording legal validity of e-signatures as a functional equivalent to hand written signatures, to providing a distinction between forms of e-signatures with conditions of reliability of signatures to a complete two-tier approach with significant provisions for accreditation of so-called advanced e-signatures. Detailed provisions for regulation of certification service providers have also emerged including providing for the liability of CSPs and recognition for foreign e-signatures.

South Africa, with the enactment of the ECT Act and the ES Regulations provided for many of the documented requirements for improving legal validity, trust and security associated with electronic commerce through a detailed approach to regulation of e-signatures that has at least, kept pace with the UNCITRAL and EU model frameworks. The challenge is that certain approaches that South Africa relies such as the EU Directive on are currently under review (Evans, 2011) or are not effective (Winn, 2007) and South Africa will be forced in the near future to review the extent to which it accommodates developments associated with the outcomes of such review.

A typology of approaches emerged from the literature review, chronologically and descriptively for establishing and promoting the legal validity, trust and security of e-signatures and in so doing, electronic commerce. This includes:

a digital signature approach that is technology specific requiring the use digital signature technologies for validity and reliance,

a two prong approach providing reliance criteria specific to certain tiers of e-signatures but catering for alternative e-signature technologies that meet specified criteria offering varying legal validity, trust and security

a minimalist approach with a less restrictive description of the functions of e-signatures, and reliance criteria designed to be applied to various technologies that meet legal validity, trust and security requirements (Aalberts and Van Der Hof, 2000). Smedinghoff and Bro promoted the notion of technology neutral terminology to facilitate the myriad means of attesting that would be associated with e-signatures (1999). Refraining from naming any specific authentication method or technology, in the ECT Act, South African legislators appear to have endorsed the technology neutral at least in the ECT Act.

While South Africa intended a minimalist, technology neutral approach, in effect, however, with the lenience in the ES Regulations on particular certification signatures has followed two-prong approach. This is clear from the definitions of e-signatures and advanced e-signatures in the ECT Act. South Africa further provides evidentiary presumption to advanced e-signatures subject to change by consensus by the relevant transacting parties which is a further indicator according to Smedinghoff and Bro (1999).

The digital signature approach would grant only digital signatures based on particular encryption methods, asymmetric cryptographic signatures and third party verification requirements to be a substitute to handwritten signatures Menzel and Schweighoffer (1999) and this is not the case in South Africa.

The legal experts were critical of the limited harmonisation with the UN Convention approaches to e-signature regulation. A legal expert was critical of the “tight regulation” which according to the expert does not give effect to technological neutrality and non-discrimination of technologies intended by model law approaches. As a result, the expert called for changes in the regulatory approach. The traditional approach to regulation of e-signatures was described as a two-tier approach: (i) certain e-signatures are legally valid through evidence of reliability and suitability for purpose and (ii) through a “legal fiction” or “theory” approach, certain e-signatures are valid in relation to mere compliance with the requirements stipulated in legislation and absence of technical verification. This two-tier approach with an associated higher level of legal recognition amounts to “discrimination” of e-signature technologies and is problematic in the view of the legal expert. This was explained through the example of the costs of accreditation of e-signatures i.e. the verification for a high level of legal validity. The UN Convention approach is a move away from the two-tier approach that the legal expert believes to be a positive consideration for South Africa. The legal expert further cautioned that the regulation must be responsive to the local conditions and in South Africa, in the expert’s view, South Africa’s electronic commerce has not advanced to a stage where “stringent requirements” are called for and such approach may be inhibit to electronic commerce such that consumers may lose confidence in transactions where e-signatures have not been applied. Other interviewees recommended consideration of technology neutral approaches versus the dependency in the current regulations on PKI based technology.

The DOC senior official agreed that the regulations were in need of update and that the draft ECT Amendment Bill was an opportunity for update the regulations. The ASP representative also called for broader review of the ECT Act providing that the limited implementation of certain provisions of the ECT Act was problematic and has negative implications for the remaining provisions and that it remains unclear how the regulatory intent of the ECT Act to promote electronic commerce is realised in practice. Monitoring and evaluation of the policies required address in the view of the DOC senior official and the association between electronic commerce trends and e-signature regulation was an example of an area where this could be applied.

Ultimately, the considerable harmonisation with approaches such as the EU approach does not equate to effectiveness. The two-tier approach is perhaps no longer effective for South Africa. There is a serious concern in the misalignment between the technology neutral approach intended by the legislator and the prevailing near technology specific approach with the regulated preference for specific technologies. In the context, of adoption of e-signatures that promote legal confidence, security and trust, improvements in the approach that permit lower costs of the service, legal acceptance of technologies emerge as important considerations. This resonates with the view of Winn (2007) on the review of China's regulation – for developing countries increased attention to market efficiency is necessary.

5.5 Summary

There are several insights emerging from Chapter. Equal legal validity to handwritten signatures is offered to e-signatures in the ECT Act. Two categories of e-signatures are defined and distinguished according to the transactions for which they are legally valid and their respective criteria for validity. Ultimately, South African legislation offers a two-tiered, in the ECT Act to the legal validity of e-signatures.

Regarding the regulation of e-signatures, the minimum attributes of the AeS were appraised for suitability. The accreditation provisions contained in the ECT Act and the subordinate regulations of 2007 corresponds with the requirements specified in certain international frameworks, particularly the EU Directive including adequate regulation particularly of technical methods deployed by the CSP for issuing or revoking a certificate, verification of the identity of the user, ensuring that experienced, knowledgeable persons are employed, maintenance of sufficient financial resources for its functions and obligations, the trustworthiness of its systems (EU Directive) . Other aspects surrounding the accreditation including the

oversight role of the Authority, the information security standards and the liability of an accredited service provider were discussed. In particular, the accreditation of the single accredited service provider, the ASP was analysed.

Analysis of country comparative approaches further reveal alignment and commonality in certain areas with particular deviations on for instance, the regulation of accreditation of foreign signatures.

While several positive measures were observed in the legislation and the ES Regulations, the analysis of the interviews provided a contrasting view of the effectiveness of the e-signature regulation in South Africa. Accreditation procedures and standards are commended but challenges with the understanding of the distinction between the signatures and their application are noted. The accreditation processes are challenged for issues such as technology bias towards PKI based technologies, outdated standards that render an accreditation service provider vulnerable to information security breaches, high costs of accreditation, unrealistic requirements pertaining to authentication methods etc. A legal expert was particularly critical that the accreditation approaches had not kept pace with international model law developments which South Africa should have considered. Delays in establishing the Accreditation Authority were concerning as were criticisms of the effectiveness in delivering public awareness of the accreditation regulations issued in 2007 and only a single accredited service provider.

Ultimately, South Africa's regulatory approaches and framework are being assessed for their ability to deliver adoption of e-signatures as a trust, security and legal confidence instrument to advance electronic commerce. The implications of the contrast in documentary analysis and practical outcomes, particularly for policy makers are considered in Chapter Six. Chapter Six will conclude on the basis of the analysis in this Chapter, on the effective and ineffective attributes of South Africa's regulation in response to the research questions.

6 CHAPTER SIX – CONCLUSIONS

Chapter One, at the outset, spoke to the assessment of regulatory effectiveness in the context of achievement of intended goals, objectives and results and in particular policy goals associated with the regulation. Effective regulation is further associated with establishing the key factors that will promote or inhibit the success of the regulation. In the context of the effectiveness of e-signature regulation, the conceptual framework of Chapter Two suggests that the regulatory framework needs to firstly, be effective in securing a level of legal validity in electronic signatures that would promote their value as an adequate approval mechanism in legal transactions and promote legal confidence in electronic commerce. Secondly, the attributes and standards of electronic signatures would need to be regulated to enhance their trustworthiness and thirdly, appropriate information security needs to be in place to promote user confidence in their ability to attest valid electronic transactions.

Likewise, regarding the significance of the study in this report, Chapter One noted (i) the critical role that electronic signatures play in addressing issues of legal confidence, trust and security in electronic commerce; and (ii) the role of electronic signature regulation in promoting electronic signature availability and suitability in order that these three issues are indeed addressed.

The regulatory framework, that was under study, is constituted by legislation in the form of the ECT Act, regulations passed in 2007, case law that has provided guidance on the application of the legal framework in the ECT Act and ancillary regulatory mechanisms investigated and discussed in Chapter Four. Returning to the problems that were the basis for the research, ultimately, several inefficiencies pointed to possible inefficiencies in securing the abovementioned outcomes associated with effective e-signature regulation.

An analytical qualitative case study of electronic signature regulation in South Africa was pursued. Firstly an understanding of the regulatory approach was necessary. This emerged through an extensive extraction of information from multiple sources and often complex legal provisions and considerations. This framework was used to analyse the current regulation through the creation of optics for the analysis and comparison with model frameworks and other country approaches. The other objective in the research was to understand what the effects and outcomes of the approaches. For this, interviews with a range of stakeholders were pursued. The analysis of Chapter Five is again an extensive accumulation of findings from multiple sources on several frames of analysis. Perhaps the one regret, in this regard, was a conceptual framework

that was too ambitious with often too many considerations for a conclusive finding. Albeit introduced as measures to maintain the quality of the work through ensuring a range of data and queries - a less ambitious set of sources and areas of analysis may have been pursued.

A spectrum of meaningful and worthwhile findings has, however, emerged, no doubt of value to the intended stakeholders of this research. The research as set out in Chapter One pursues the analysis of electronic signature regulation in broad terms and the analysis of the regulation of the AeS as a category and form of e-signature regulation. What was not initially anticipated was the emerging emphasis on the regulation of the AeS in particular as an area of various inefficiencies. This emerged from participants in the interviews and in the documentary analysis. As a result many of findings of the previous chapter and conclusions of this chapter pertain to the regulation of the AeS.

Returning to the conclusions pursued in this Chapter, only the most significant of conclusions, in the opinion of the researcher are set out herein. These are associated with key areas of the desired effectiveness of the electronic signature regulation in South Africa and respond to the research question and sub-questions.

6.1 How effective is the electronic signature legal framework for the promotion of legal confidence in electronic commerce transactions?

6.1.1 Effective Legal Validity

The legal validity of electronic signatures as substitutes or functional equivalents for handwritten signatures establishes an approval framework that promotes legal confidence in electronic commerce transactions (Brazell, 2008). The analysis in Chapter Five, uncovered, in general terms, that the ECT Act (i) provides for electronic signatures to be a functional equivalent to handwritten signatures in law; and (ii) renders South African law media neutral as far as the legal validity of signatures are concerned. This is an area of general effectiveness.

Significantly, however, the Act makes an important distinction in the legal validity between a general tier of electronic signatures and an advanced electronic signature (AeS). Legally, the AeS benefits from a rebuttable presumption of reliability and is preferred for certain transactions where a higher level of legal assurance is necessary. This presumption is arguably intended to promote higher levels of legal confidence in electronic transactions concluded using the AeS, which are associated with an accreditation of the technologies, procedures and operations to render them sufficiently trustworthy.

Electronic signatures, in general, remain legally valid for other transactions, their validity being subject to whether it is an adequate method for authenticating the identity of a person and their approval of information.

The sum effect is distinction between tiers of electronic signatures, each valid for different categories of transactions and each subject to certain criteria for their validity. While the distinction in the legislation is generally supported by model frameworks and experts interviewed, a complexity has also resulted; which signature to use for which transaction and does the signature legally valid according to the relevant criteria? Interviewees revealed confusion in the market with a general lack of understanding, particularly around when an AeS is required for a legally valid electronic transaction. A related preference in the market for paper transacting processes for higher value transactions was also noted by interviewees. Accordingly, the complexity in the distinction between these two tiers has resulted in confusion regarding the function and legal validity of electronic signatures. This complexity deters from the effectiveness of a legal framework to provide in electronic signatures an approval framework that would promote legal confidence in electronic commerce.

6.1.1.1 Recommendation – Consider Legislative Amendment

The extent to which the barriers to legal confidence can be cured by amendments to the legislation that clarify the distinction in legal standing and intended utility of electronic signatures in general and the AeS should be considered.

6.1.2 Ease of Substitution of Electronic Signatures – Case Law Perspectives

Case law results were used to understand how electronic signatures would be received in the ordinary legal system. The cause for such analysis was to gain insights into the ease of substitution of an electronic signature for a handwritten one in the broader legal system, interpreting the perspectives of court judgements. Principles of interpretation of the relevant electronic signature provisions of the ECT Act emerged that would have appeal with the legal fraternity. These principles emphasised, for example, the importance of considering foreign law, international systems and international lessons learnt in the area to understand the intent of the law, the need to accommodate formalities and any prohibitions in law that have a legal bearing for the legal validity of the electronic signature in the circumstances.

From the case law, there were no challenges cited with the interpretation of the ECT Act or the substitution of an electronic signature for a handwritten signature - only calls to promote alignment and consistency with international and domestic legal formalities and approaches. From the case law considered, transferral and substitution of a requirement in law for a signature should be readily applied to include an electronic signature (subject to the considerations). This broader legal

framework is encouraging, if not effective for advancing confidence in the legal validity of electronic commerce transactions concluded with electronic signatures.

6.2 How effective is South Africa's regulation of electronic signature products and services to promote trust and information security in electronic commerce?

The accredited AeS as per the legal framework described in this paper is intended to be a preferred, trusted security mechanism for electronic commerce transactions. The regulation promotes the AeS serving this function through regulated standards for information security and trustworthiness of the products, services and service provider of the AeS via an accreditation process. Accordingly, the analysis in this area tended to focus on the AeS, including the attributes of trustworthiness, the effectiveness of information security standards, the efficacy of the accreditation process.

6.2.1 Partially Effective Regulations

The ECT Act and ES Regulations, in documentary terms, accounted for several provisions that would theoretically promote electronic signatures to roles in delivering trust, information security and user confidence in electronic commerce. Areas of effectiveness included prescribing international best practice standards for information security, several levels of assurance, audit requirements, independent evaluation requirements and extensive specifications of operational vigor including assessment of the financial and human resources of the applicant. The above requirements point to the intention to ensure adequate security standards and trust in electronic signatures, which in turn would promote their utility as a trust and security mechanism of electronic commerce transactions.

Effectiveness in certain areas was met with shortcomings in other areas. Compared with other countries and model frameworks, the findings revealed shortcomings in for instance, limited prescribed liability of the AeS service provider, no prescribed liability provisions for the actual signatories, and regulations that tended to focus on the accreditation PKI based signatures almost entirely. The lack of adequate liability provisions would likely have the effect of demoting user confidence in the AeS and electronic commerce transactions where the AeS is the trust and security mechanism.

6.2.2 Ineffective Regulatory Outcomes for Trust and Information Security Standards

Interviewees, each with distinct backgrounds and interests in the subject, noted distinct frustrations with the regulatory outcomes. Concerning AeS regulation:

- Market efficiency shortfalls in a single accredited service provider, the lack of competition in the AeS market with speculation of poor quality of services and limited technical innovation in the future;
- Delayed, costly and cumbersome accreditation processes for the ASP resulting in a single accreditation and foreseeable barriers to accreditation for future applicants for accreditation;
- Limited public awareness of the functions and benefits of the AeS that limit adoption of the AeS; and
- The failure to provide technology standards that are current and robust to the standards of trust required for electronic signature products and services, particularly in the case of information security standards that were inadequate; and
- Market inefficiencies, accreditation process pitfalls, and limited understanding of the benefits of the AeS reveal poor regulatory outcomes for regulation that sought to produce, as a primary objective, the availability of the AeS to advance trust and security levels for electronic commerce.

Outdated standards equally frustrate the utility of the AeS as an information security tool. This was of particular concern for information security experts who cautioned that reliance on the current standards would render the ASP vulnerable to information security attacks with the prescribed information security standards not being equal to current fraud technologies. Furthermore, as a trusted service provider, the ASP is a target for information security attacks, inferring that a more dynamic and robust approach to information security standards should be taken.

Active consultation with information security experts perhaps through the establishment of a committee by the Authority to assess the currency and adequacy of the information security standards is recommended.

The regulatory intentions are not met with effective outcomes in this area.

6.2.3 Auditor Appointments and Knowledge

Little competition amongst auditors that audit applicants' conformance with accreditation requirements bolster the costs of accreditation and ultimately deter applicants. A broader panel of auditors needs to be established to promote competition amongst auditors and arguably, lower the costs of the service. The availability of the AeS as an electronic signature with a

higher legal standing and higher standards of information security and trustworthiness is negated by high costs of accreditation.

Limited knowledge on the part of the auditors of electronic signature technologies and regulatory processes also emerged. This limitation may be addressed through improved specification of the qualifications and experience of the auditors. This would improve the quality of the audit and arguably, align the AeS products and services more closely with the standards set by the Authority.

6.3 How effective are South Africa's electronic signature regulatory approaches when compared with primary international model laws?

6.3.1 Close Alignment with EU Directive but Ineffective Approaches

Firstly it should be noted that South Africa's approaches corresponds to a large degree with minimum characteristics of electronic signature regulation specified in international model frameworks. An alignment in the detail, particularly in accreditation regulatory approaches, is noted visavis the EU Directive.

In this area, however, a particular insight is the tension between harmonised approaches and effective approaches. What are the implications of South Africa's alignment to model frameworks? Does this render the South African approach effective? As set out in Chapter Five, experts have criticised the EU Directive approach as a compromise between various EU government's respective technology neutral and technology specific approaches, as well as a demand for substantive regulation versus calls for self-regulation. South Africa, in pursuing alignment with the EU Directive, followed a complex approach constituted by a web of compromises between various country approaches. Even in the EU, such approaches have not produced the levels of adoption of AeS or the trust and security pursued (Evans, 2011). Should the levels of adoption in be associated with the regulatory approaches, this does not bode well for South African electronic signature adoption levels.

Hence, the pursuit of harmonisation alone with model frameworks, however well received, is insufficient to yield effectiveness. Each framework carries a context that must be understood to determine the influences for the framework and any resulting inefficiencies. While the case of Jafta vs. Ezemvelo KZN Wildlife (Jafta, 2008) emphasised harmonised

regulatory approaches for electronic commerce, the challenges of not being availed to the context of other international approaches was noted. While the judgement provided that such challenges are limited for electronic commerce regulation due to the equality of conditions, what clearly emerges is that the variation of the context between the EU Directive as a regional Directive and South Africa's requirements for a national and localised approach is a critical understanding. Perhaps the broader insight is that electronic signature regulatory approaches should not be homogenous. Mere transposing of model frameworks in South Africa without adequate consideration for workability in the South African context should be avoided. As far as technology and applications are concerned, electronic commerce is global in nature. One can argue that this calls for harmonised regulatory approaches that promote regulatory certainty. Such efficiency must be balanced against market efficiency which has been the resulting ineffectiveness in this area.

6.4 How effective are South Africa's electronic signature regulatory approaches when compared with other country frameworks and approaches?

Each of the countries, UK, China and Australia, offered regulation of (i) the distinction of an advanced signature or higher standard of signature (ii) detailed regulation of the products and services associated and (iii) regulation of the certification service provider. These were largely aligned with the South African approach. Furthermore, regulation in the countries tended to include a primary law that governed the legal validity of electronic signatures and supplementary regulations that governed the certification service providers of advanced electronic signature products and services. Conformity again, in South Africa is noted.

South African regulation on comparison deviated in the following areas:

- The UK and Australia have self-regulatory bodies for the issuance of accreditations of the more secure signature equivalent;
- Legal recognition of foreign electronic signature certificates issued by service providers accredited outside China is catered for; and
- End user signatory liability is provisioned in the Chinese accreditation regulations.

Equally noteworthy is that in China, there is a preference for a specific electronic signature, the digital signature as an advanced electronic signature. The terminology in the legislation, however, is technology neutral. The rationale for not

using the term digital signatures is a reluctance to inhibit the use of other signature technologies and limit problems associated with the legislation becoming outdated. This contradiction of technology specific in practicality and technology neutral in the text of the regulations is also the case in South Africa. China's rationale might influence continued technology neutrality in the regulations for the reasons specified.

In China the difference between 2 tiers of signatures is also unclear as well as which transactions would require a certified signature and this was criticised by one expert in the literature.

This approach was, however, supported by another expert as affording the Chinese public the autonomy to select the appropriate electronic signature technology that meets the reliability requirement and the autonomy to decide whether to use an electronic signature. This issue is highlighted in this study as a critical one. For the policymakers deliberating on this issue, the expert perspective on the Chinese experience may be of value.

In summary, South African regulation compares well to other countries as far as the fundamentals are concerned. Other countries tend to have progressed in for instance, developing approaches to self-regulation foreign signature approaches, and the determination of liability of the signatory. In such areas, by pure failure to deal with such topics in any meaningful way, South Africa is less dynamic, if not, less effective.

6.5 How would South Africa be impacted by the continued reliance on the current electronic signature regulatory framework and approaches?

Clearly from the conclusive remarks made in this chapter so far, there are areas of weakness - the completeness of the content of legislation and the Regulations as well as several challenges with implementation of the regulations to produce the intended outcomes. Particularly, the availability of a suitable electronic signature that is an effective facility for trust, information security and legal confidence in electronic commerce transactions is frustrated in the current approach. Continued reliance on the current frameworks will not aid this effectiveness. Several of the important areas of assessment are discussed above but two broad areas of ineffectiveness emerge as critical considerations for the policy maker for improving future effectiveness.

Firstly, the significance of the accreditation and the AeS service should be rationalised. A study in China revealed the Chinese population of e-commerce users as having a preference for selecting their own technology. A legal expert in South Africa further noted regulatory options that provide added legal weight to the general category of electronic signatures. Presumptions in South Africa on user awareness and demand for the AeS need to be assessed. Related to this inquiry is then whether the incentives for offering AeS products and services exist and are sufficient, particularly in view of weak enforcement of the laws that require the use of an AeS. What is necessary in a future study is a renewed rationalisation of the regulation considering market trends in electronic signature adoption in South Africa and regulatory approaches that foster electronic commerce markets. Even the DOC senior official indicated that this was necessary.

The second critical area is to clarify the role and duties of the Authority. It appears thus far to be an administrator of accreditation processes and enforcer of compliance with regulation, rather than servicing education and advocacy around the benefits of electronic signatures and encouraging their adoption. Significant challenges distinguishing the role of the Authority from the DOC is observed amongst interviewees and in the experience of the interview conducted with the DOC. This is largely because the Authority currently resides within the DOC. Even the duty to ensure closer and broader consultation with industry, particularly on issues on information security standards, was strongly forwarded by information security interviewees. Formations of committees, and dynamic engagement, communications and awareness were called for and these duties need to be ascribed to a relevant stakeholder in electronic signature regulatory outcomes.

6.6 How effective is the South African electronic signature regulatory framework for promoting the adoption and use of electronic signatures to advance legal assurance, security, and trust in electronic commerce?

The final task is to answer the primary research question. I shall do this in two parts. The first issue is efficacy of the e-signature regulatory framework to promote the adoption and use of electronic signatures. The conclusions point to early attempts to establish an enabling legal framework in the ECT Act of 2002, to provide e-signatures a legal validity that would promote its use as a substitute to handwritten signatures. This implied an expectation that the enabling legal environment

would support the adoption of electronic signatures. This intent was, however, frustrated by confusing definitions, distinctions in tiers of electronic signatures and their criteria for validity. The findings point to low adoption levels of electronic signatures, preferences for handwritten signatures and paper transactions and possibly disincentivised electronic signature service providers as a result of such market outlook.

The second area pertains to how effective the regulation has been in advancing legal assurance, security and trust in electronic commerce. In the ECT Act of 2002, a more secure tier of e-signature was introduced as the advanced electronic signature which is subject to accreditation as a tool for heightened levels of legal assurance, security and trust in electronic commerce. These intentions were supported by a presumption of legal validity in the ECT Act, extensive specifications of trust and security standards and assessment of the prospective service provider's operations, in the regulations. It is here that curious and significant delays were observed: five years between the passing of the Act and the ancillary regulations and a further five years for the accreditation of the first AeS service provider in 2012. During this period of delay, South Africa was not availed of the AeS and on this fact alone, the regulatory framework was not effective in delivering its intended tool for added trust, security and legal confidence in electronic transactions. There were other challenges too, as discussed above, outdated information security standards inadequate to emerging security vulnerabilities: auditors appointed to audit compliance with the regulatory requirements were not suitably knowledgeable, no regulatory consideration to possible recognition of foreign signatures accredited in other countries. Recognised foreign signatures may have served the purpose of the AeS. The regulation clearly has not delivered the higher levels of trust, information security and legal confidence in electronic commerce.

In conclusion, the *content* of the regulatory framework is, associated, in peripheral terms, with the objectives of promoting legal assurance, security and trust in electronic commerce. This holds true in the analysis of the ECT Act provisions that deal with the general category of e-signatures and the AeS specifically and the ES Regulations which deals, in the main with regulation of the accreditation of the specific form of AeS. The regulatory framework has, however, not been effective in actually delivering on such intended outcomes. The technical standards in the ES Regulations appear to be outdated. The regulation of e-signatures in general and specifically the AeS, in many instances, have not kept pace with expert recommendations or country developments. Even in the alignment with model frameworks, challenges with the particular model of choice were detected. The regulatory frameworks as a result are ineffective and in need of review. The regulation of e-signatures appears to be a subject of neglect in South Africa and concurrently lacks that certain kind of dynamic approach called for, particularly for ICT regulation. Moreover, this ineffectiveness suggests a negative impact for advancing

electronic commerce opportunities and a vibrant information economy in South Africa, suggested in Chapter one, as having a dependency on the effective regulation of e-signatures.

6.7 Limitations of the Study

The limitations of this research study are that the scope did not encompass the analysis of the adoption e-signature technologies, electronic commerce market analysis or economic conditions influencing the regulatory outcomes. Rather the focus was an analysis of the regulatory approaches to e-signatures in South Africa. As such, questions for future studies may be concerned with actual levels of e-signature technology adoption in various markets and relational analysis of the impact of the regulation on e-commerce market effects. Future studies may further consider any presiding economic and socio-economic conditions that have influenced the variations in South Africa's regulatory approaches.

REFERENCES

Allen, H.B. (1971). Principles of informant selection. *American Speech.* Vol 46:47-51.

Aalberts, B. P., & Van Der Hof, S. (2000). Digital signature blindness analysis of legislative approaches to electronic authentication. EDI L. Rev., 7, 1.

American Bar Association. (2001). Digital Signature GuidelinesTutorial, Retrieved 16 February 2013 from http://www.abanet.org/scitech/ ec/isc/dsg-tutorial.html.

Arias, M. (n.d) Electronic Signatures in U.K. Retrieved 7 September 2012 from http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=2082

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and Methods. Retrieved 16 February 2013 from http://www.nova.edu/ssss/QR/QR13-4/baxter.pdf

Brent Flyvbjerg, 2011, "Case Study," in Norman K. Denzin and Yvonna S. Lincoln, eds., *The Sage Handbook of Qualitative Research*, 4th Edition (Thousand Oaks, CA: Sage, 2011), Chapter 17, pp. 301-316

Berthon, P. Pitt, L. Cyr,D. Campbell, C (2008). E-Readiness and Trust: Macro and Micro Dualities for E-Commerce in a Global Environment. *International Marketing Review*. Vol. 25(6) (2008). Retrieved 16 February 2013 from http://www.diannecyr.com/berthon_pitt_cyr_campbell2008.pdf

Blythe, S (2005). Digital Signature Law of the United Nations, European Union, United Kingdom and United Stats: Promotion of Growth in E-Commerce with Enhanced Security. *Richmond Journal of Law & Technology*. Volume XI, Issue 2. (2005). Retrieved from http://law.richmond.edu/jolt/v11i2/article6.pdf.

Blythe, S (2007). China's new e-signature law and certification authority regulations: a catalyst for dramatic future growth of e-commerce. *Chicago-Kent Journal of Intellectual Property* (2007)

Blythe, S (2007). Lithuania's E-signature Law: Promoting the growth of secure e-commerce transactions. *Barry Law Review*. Vol 8. (2007) pp. 23 – 42.

Brazell, L. (2008). *E-signatures and identities: Law and regulation*. Sweet & Maxwell/Thomson Reuters. London (2008).

Bundschuh-Rieseneder, F. (2008). Good Governance: Characteristics, Methods and the Austrian Examples. *Transylvanian Review of Administrative Sciences*. Vol 24E (2008) pp 26-52

Cassell, C., & Symon, G. (1994). Qualitative research in work contexts. *Qualitative methods and analysis in organizational research: A practical guide* London: Sage, 1-13.

Cogburn, D.L (2003). Governing global information and communications policy: Emergent regime formation and the impact on Africa. *Telecommunications Policy* 27 (2003). pp 135 – 153

Cole, K. Chetty, M. LaRosa, C.Rietta, F. Schmitt, D. Goodman, S (2008). Cybersecurity in Africa: An Assessment. Sam Nunn School of International Affairs Georgia Institute of Technology, 2008

Curtis, S., Gesler, W., Smith, G., & Washburn, S. (2000). Approaches to sampling and case selection in qualitative research: examples in the geography of health. *Social Science & Medicine*, 50, 1001-1014.

D' Andrade (2005). Is the pen mightier than the e-signature? –Retrieved 13 February 2013 from http://www.derebus.org.za/nxt/gateway.dll/bsxha/uei9/7okka/eqkka/svbua

Dagada, R. Eloff, MM. Venter, LM (2009). Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant? Proceedings of the 8th Annual ISSA Conference, 6 -8 July 2009, University of Johannesburg's School of Tourism and Hospitality facility, Auckland Park, Johannesburg, Gauteng, South Africa. Available at: http://hdl.handle.net/10500/2660

Denzin, N. and Y. Lincoln (1994). *Handbook of Qualitative Research in Education: A Qualitative Approach*. Jossey Bass Publishers. California.

EU Commission (2000) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.2000. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML last accessed on 16 February 2013

Evans, B, (2011). EU Review of e-signature Laws. Retrieved 6 April 2012 from http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/9178-EU-review-of-e-sig-laws.htm, Forder, J (2010), The Inadequate Legislative Response to E-signatures. *Computer Law and Security Review* 26 (4) pp. 418 - 426

Fraenkel, J. R., Wallen, N. E., & Hyun, H. H. (1993). How to design and evaluate research in education.

Groenewald, T. (2004). A Phenomenological Research Design Illustrated. *International Journal of Qualitative Methods , 3* (1).

Guermazi, B. Satola. D. (2005). Creating the right enabling environment of ICT. Robert Schware (eds). E-Development – From Excitement to Effectiveness. Washington, DC, The World Bank

Hartley, J. (2004). Case study research. Essential guide to qualitative methods in organizational research, 323-333.

Herold, M (n.d) Case Study Research: design and implementation for novice researchers. The Qualitative Report, 13(4), 544-559.

Hones, M.J. (1990). Reproducibility as a methodological imperative in experimental research. Proceedings of the Biennial Meeting of the Philosophy of Science Association. Vol 1, 585-599

ITWeb (2012) LAWtrust makes history as the first accredited SA provider of advanced electronic signatures. Retrieved on 19 May from http://www.itweb.co.za/index.php?option=com_content&view=article&id=52874

Jafta v Ezemvelo KZN Wildlife (2008) ZALC 84 Retrieved from Lexis Nexis Database

K v Minister of Safety and Security (2005) (9) BLLR 835 (CC) Retrieved from Lexis Nexis Database

Kshetri, N (2006). Barriers to e-commerce and competitive business models in developing countries: A case study. *Electronic Commerce Research and Applications* 6 (2007). pp 443 - 542

Kuechler, W., & Grupe, F. H. (2003). Digital signatures: A business view. *Information Systems Management*, 20(1), 19-28.

Leedy, P. D., & Ormrod J, E. (2005). *Practical Research Planning and Design* (8 ed.). Pearson Education International.

Low, R. Christensen, S (2004) E-signatures and PKI Frameworks in Australia. *The Digital Evidence Journal, incorporating the e-Signature Law Journal* 1(2):pp. 56-59.

Lupi, P., Manenti, F., Sciala, A., & Varin, C. (2011). On the assessment of regulators' efficiency: an application to European telecommunications. *info*, *13*(1), 61-73.

Makaya, G. (2001). The Determinants of Regulatory Effectiveness in Liberalised Markets: Developing Country Experiences. Conference Paper, Trade and Industrial Policy Strategies (TIPS), Johannesburg, 2001

Mason, S. (2002). Electronic Signatures—Evidence: The Evidential Issues Relating To Electronic Signatures, Part 1. *Computer Law & Security Review*, 18(3), 175-180.

Menzel, T., & Schweighofer, E. (1999). The Austrian Signature Act. Implementation of the EC Directive proposal in an Austrian Signature Act. DuD, 23 (9).

Merriam, S. B. (2002). Introduction to Qualitative Research. In Merriam, S. B. (Ed.), *Qualitative research in practice: examples for discussion and analysis* 1st edition (pp. 1-17). San Francisco: Jossey-Bass

Merriam-Webster Online Dictionary. (2009). Case Study.Retrieved 16 February 2013 from http://www.merriam-webster.com/dictionary/case%20study

Miller, J. (n.d.). Promoting Electronic Commerce in South Africa: Ten Academic Perspectives. Retrieved 16 February 2013 from http://www.ecomm-debate.co.za

Neuman, W. L. (1997). *Social Research Methods Qualitative and Qualitative and Quantitative Approaches* (3 ed.). Boston, United States of America: Allyn and Bacon.

Outlaw, (2008). Electronic Signatures - FAQs. Retrieved 13 February, 2013 from http://www.out-law.com/page-443Parry, G.C. James-Moore, M. Graves, A.P. Altinok, O (2008). Legal aspects of e-signatures. University of Bath School of Management Working Paper Series (2008).

Perry, S. (2012). E-Signatures Finally Go Legit. Brainstorm Magazine, May 2012, pp 18-21

RSA (1999) Discussion Paper on Electronic Commerce Policy, Republic of South Africa, Pretoria, available online at http://www.polity.org.za/html/govdocs/discuss/ecomm.html

RSA (2002) Electronic Communications and Transactions Act, No 25 of 2002, Republic of South Africa, Pretoria, available online at http://www.internet.org.za/ect_act.html

RSA. (2002). Electronic Communications and Transaction Act. Section 71. Pretoria, Republic of South Africa Government Printers, August 2002.

SALRC (South African Law Reform Commission). (2010) Issue Paper on Electronic Evidence Law, Republic of South Africa, Pretoria

Scorecard, E. R. (2005). Regulatory Scorecard–Report on the relative effectiveness of the regulatory frameworks for electronic communications in Austria. Belgium, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Italy, the Netherlands, Poland, Portugal, Spain, Sweden and the United Kingdom, 1st December.

Shifren and Others vs SA Sentrale Ko-op Graan Maatskappy Bpk (1964) SA 1964 (2) 343 (O) Retrieved from Lexis Nexis Database

Smedinghoff, T. J., & Bro, R. H. (1998). Moving with change: electronic signature legislation as a vehicle for advancing e-commerce. J. Marshall J. Computer & Info. L., 17, 723.

Snail, S. (2008) 'Electronic Contracts in South Africa – A Comparative Analysis', *Journal of Information, Law & Technology (JILT)* Vol. 2 (2008) Available at <http://go.warwick.ac.uk/jilt/2008_2/snail>

Snedecor, G.W. (1939). Design of sampling experiments in the social sciences. *Journal of Farm Economics* Vol 21, 846-855.

Spyrelli, C, 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication', *The Journal of Information, Law and Technology (JILT)* 2002(2) Retrieved from <http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html>. New citation as at 1/1/04: <http:/www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/>.

Srivastava, A. (2005). No Rice, No Wife to Cook: An Analysis of the E-signatures Law of China. *International Journal of Law and Information Technology*. Vol 13, No. 3 (2005) Oxford University Press

Terre Blanche, M., & Durrheim, K. (1999). *Research in Practice: Applied Methods for the Social Sciences.* Cape Town: University of Cape Town Press.

Tongco, DC (2007). Purposive Sampling as a Tool for Informant Selection. Ethnobotany Research & Applications. Vol 5, 147-158. (2007). University of Hawaii. Retrieved from http://scholarspace.manoa.hawaii.edu/bitstream/handle/10125/227/i1547-3465-05-147.pdf?sequence=4

UN (1996) UNCITRAL Model Law on Electronic Commerce (1996) with additional article 5 bis as adopted in 1998 and Guide to Enactment, United Nations, Geneva

UNCITRAL (2001). Uniform Rules on Electronic signatures with guide to enactment .United Nations Commission on International Trade Laws. Available at: <http://www.uncitral.org/english/sessions/wg_ec/wp-86.pdf>, last accessed on 22 January 2013

UNCITRAL. (1996). Model Law on Electronic Commerce. United Nations Commission on International Trade Laws. Available at: <http://www.uncitral.org> last accessed on 22 January 2013.

Wang, M (2006). The Impact of Information Technology Development on the Legal Concept – A Particular Examination on the Legal concept of 'Signatures'. *International Journal of Law and Information Technology* Vol. 15 No. 3 (2006).

Wang, M (2007). Do the regulations on e-signatures facilitate electronic commerce? A critical review. *Computer Law and Security Report* Vol. 23 (2007), pp 32 -41

Warden, S.C. Motjolopane, I.M (2007). E-Commerce Adoption Factors: Supporting Cases from South Africa. Information Resources Management Conference. Vancouver, Canada (2007)

Waverman, L., & Koutroumpis, P. (2011). Benchmarking telecoms regulation–the telecommunications regulatory governance index (TRGI). *Telecommunications Policy*, *35*(5), 450-468.

Wimmer, RD and Dominick, J (1997). Mass Media Research: An Introduction. Belmont, MA: Wadsworth.

Winn, J.K (2010). Electronic Commerce Law: Direct Regulation, Co-Regulation and Self-Regulation. University of Washington School of Law CRID 30th Anniversary Conference (2010)

Yin, R (1984). Case Study Research: Design and Methods. Sage Publication, California.

Yin, R. (2009). Case Study Research: design and methods.4-th edition, Sage Publishing. 2009.

Yin, R. . (2003). *Case study research: Design and methods* (3rd ed.). Thousand Oaks, CA: Sage.

Yin, R.(1994). Case study research: Design and methods (2nd ed.). Sage Publishing, Beverly Hills, CA.

Annexure A – Interview Protocol

Information Sheet:

Masters Research Report: An analysis of electronic signature regulation in South Africa

Dear Key Participant

You are invited to take part in this research study. Before you decide whether or not to take part, it is important for you to understand why the research is being done and what it will involve. Please read the following information carefully.

Background & Overview of the study

This study is being conducted by Prialoshni Chetty in partial fulfilment of the requirements for a Masters of Management in ICT Policy and Regulation at the Graduate School of Public and Development Management at the University of the Witwatersrand.

The study investigates the effectiveness of electronic signature regulation in South Africa.

In 2002, South Africa enacted electronic commerce regulation to promote electronic commerce. In view of the critical role that electronic signatures play in addressing issues of trust, identity and security in electronic commerce, provisions for the promotion of the use of electronic signatures in electronic commerce were included. These included (i) distinction between so called electronic signatures and advanced electronic signatures capable of additional technical authentication of the identity of the holder of the signature (ii) establishing criteria for the accreditation of authentication service providers and (iii) provision for the establishment of Accreditation Authority to regulate accredited signature service providers.

Notwithstanding the emergence of the regulatory framework in South Africa in 2002, the first advanced signature service provider was only accredited in 2012. The reasons for the delay, the challenges associated with accreditation and the effectiveness of the accreditation regulations is unclear. Moreover, whilst several studies reveal an analysis of electronic signature regulatory approaches in other countries, such a study is absent in South Africa. Issues of trust, identity and security continue to afflict electronic commerce. This study is an analytical and qualitative case study of electronic signature regulation in South Africa.

The primary objective is to compare the electronic signature regulatory framework and approach to counterparts in other jurisdictions and produce findings on the effectiveness of South Africa's electronic signature regulatory frameworks. In addition, this study shall produce recommendations, as relevant, for improving the effectiveness of electronic signature regulatory frameworks in South Africa. In view of the significance of electronic commerce on South Africa's socio-economic goals, more especially, the goal of pursuing a knowledge economy, pursuing pervasive use of electronic signatures to curb barriers to adoption of electronic commerce through effective electronic signature regulation is essential.

The organisation and funding of the research

Prialoshni Chetty is a private student and the study is not being funded.

Deciding whether to participate

Taking part in the research is entirely voluntary. If you do decide to take part you will be given this information sheet to keep and be asked to sign a consent form. If you decide to take part you are still free to withdraw at any time and without giving a reason.

There are no risks in participating in this interview although you may be inconvenienced by taking time out of your busy schedule to be interviewed. There will be no direct monetary benefit to you for your participation. However, the study may have several beneficial outcomes. In particular, it will further our understanding of the topic and contribute to the knowledge in the field.

Confidentiality

Any personal information collected about you will be kept strictly confidential. Identifiers will be removed from the data when the research findings are consolidated into a report and will not be included in any subsequent publications. The anonymised data generated in the course of the research will be kept securely in paper or electronic form for a period of five years after the completion of a research project. It may be used for further research and analysis.

Research Ethics

If you have concerns about the research, its risks and benefits or about your rights as a research participant in this study, you may contact Luci Abrahams, see contact details below.

Contact for Further Information

Please contact the below for any further information you require pertaining to the study.

Supervisor details	**Student details**

Charley Lewis Senior Lecturer, LINK Centre Degree Convenor, MM(ICTPR) Mobile: + 27 83-539-5242 Email: Charley.Lewis@wits.ac.za	Pria Chetty Student, LINK Centre Degree, MMICTPR Mobile: +27 83-384-4543 Email: pria.chetty@za.pwc.com

Thank you for taking time to read the information sheet.

Consent Form:

Masters Research Report: An analysis of electronic signature regulation in South Africa

Please initial box

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask questions. ☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving reason. ☐
3. I understand that the researcher will not identify me by name in any reports using information obtained from this interview, and that my confidentiality as a participant in this study will remain secure. ☐

Please tick box Yes No

4. I agree to the interview being audio recorded. ☐ ☐

5 I agree to the use of anonymised quotes in publications. ☐ ☐

6. I agree that my data gathered in this study may be stored (after it has been anonymised) in a specialist data centre and may be used for future research. ☐ ☐

_____ _____ _____

Name of Participant Date Signature

_____ _____ _____

Name of Researcher Date Signature

The following semi-structured interview questions were used for the interview:

1. How would you describe the levels of (i) trust, (ii) security (iii) privacy and (iv) user confidence in electronic commerce (transacting through electronic communications and transactions) in South Africa?
2. What would you describe as the significance of electronic signatures on electronic commerce in South Africa?
3. What importance, if any, do you attach to the regulation of electronic signatures?
4. What importance, if any, do you attach to the distinction between electronic signatures and advanced electronic signatures?
5. What importance, if any, do you attach to the accreditation of electronic signatures as advanced electronic signatures?
6. Which transactions, if any, would benefit from advanced electronic signatures?
7. What importance, if any, do you attach to the accreditation of The ASP's signature (product) as an advanced electronic signature?
8. What significance, if any, do you attach to the accreditation of The ASP as an authentication service provider?
9. What significance, if any, do you attach to the delay in accreditation of an authentication service provider?
10. What significance, if any, do you attach to a single accredited authentication service provider in the market?

11. What importance if any, do you attach to the recognition of foreign accredited signatures as advanced electronic signatures?
12. What would you say, is the key role of the electronic signature policy maker (the Department of Communications)?
13. What are your comments on electronic signature regulation to date?
14. What impact do you believe effective regulation of electronic signatures has on the success of electronic commerce (transacting through electronic communications and transactions)?

ANNEXURE B: INTERVIEWEES

REF.	Particulars
INT 1	*Electronic Commerce Industry Expert:* Was on Executive Committee of Digital Media and Marketing Association for 2 years Headed a web technology business for 10 years and enabled electronic commerce for many customers in South Africa and abroad. Interest in topic because efficient and accessible electronic commerce is key to unlocking economic potential and opportunity and identity and trust is critical to electronic commerce.
INT 2	*Electronic Commerce Technology Expert:* Software engineer and project manager responsible for multiple electronic commerce implementations for various corporations
INT 3	*Electronic Commerce Legal Professional:* Electronic commerce and internet law legal professional
INT 4	Information Security and E-signature Technology Expert: Security Product manager for an IT distribution company. IT security for industry professional 10 years. Exposure to multiple security technologies. Implemented PKI at major organisation. Engage with The ASP on an on-going basis.
INT 5	*Information Security and E-signature Technology Expert*: Working in forensics and digital signatures, Involved in setting up of the original post office trust centre, providing technical advice to DOC in early 2000's Executive in the Information Security Group (South Africa)
INT 6	*Information Security and Privacy Consultant and Expert:* Information Security industry consultant to large financial institutions and other corporate clients delivering information security and privacy services
INT 7	*Electronic Commerce Legal Expert:* Practising Attorney, specialising in ICT/ internet law related matters. Executive member of the Law Society E-Law committee.

INT 8	*Information Security and Privacy Expert:* Information security consultant with several years of experience corporate clients delivering information security and privacy services. Member of the audit team that assisted the current accredited signature service provider review and improve its business processes to meet the compliance criteria for accreditation. Member of the International Association of Privacy Professionals and Information Security Group (South Africa)
INT 9	Senior official at the DOC and the Accreditation Authority
INT 10	Representative of the Accredited Authentication Service Provider, the ASP: Senior Representative at the ASP, background is in engineering specialising in cryptography. Regarded in the industry as an e-signature solutions authority and policy authority.
INT 11	*Legal Expert:* Technology lawyer with particular experience in research in electronic identity regulation. Prior experience in media and online communications industries. Contributor to industry publication on aspects of ICT regulation impacting media industries
INT 12	*Legal Expert:* Technology lawyer with a Masters degree in public international law experience in drafting contracts for online products and services providers as well as research on technology regulation Speaker at conferences and seminars on IP, electronic records management, electronic commerce law Published articles in online news portals on ICT law and consumer protection law
INT 13	*ICT Law and Policy Expert:* Lecturer in ICT Law Law and Policy Advisor to several countries Author or several articles and book chapters on ICT law topics Speaker at local and international conferences