UNIVERSITY OF KWAZULU-NATAL

Should the distinction between electronic signatures and advanced electronic signatures be abolished from the Electronic Communications and Transactions Act 25 of 2002?

by

Riona Pillay

211517862

A dissertation submitted in partial fulfilment of the requirements for the degree of

Master of Laws

In the

College of Law and Management Studies

Supervisor: Mr. Lee Swales

30 January 2017

Acknowledgements

I take this opportunity to thank Mr Lee Swales, my supervisor, for his guidance and feedback on my research paper.

I am also thankful to the University of KwaZulu-Natal for allowing me to further my academic career by reading towards a Master of Laws degree.

Declaration

I hereby declare that this research paper constitutes my own work and I have not plagiarised in any manner or form. All academic sources and opinions relied on and/or used in my research paper are acknowledged.

This research paper will be made available for photocopying and for inter-library loan.

_____

Riona Pillay

Turn-it-in Summary

1. The results of the turn-it-in report viewed on the 22nd January 2017 reveal the following:
2. Common words that match other texts are highlighted.
3. The titles of journal articles, case names and legislation used in the dissertation are highlighted.
4. All quotations indicated in single inverted commas are highlighted.
5. There is an overall 26% yellow similarity index.

Table of Contents

1. Chapter 1: Introduction

1.1. Background

The electronic commerce ("E-Commerce") revolution over the past three decades has led to new channels for conclusion of business transactions.[1] The internet is one of the channels on which e-commerce transactions predominantly take place.[2] The benefits of e-commerce include increased choice of goods and services for consumers, business efficiency and reduced paperwork and cost of commercial transactions.[3] However, e-commerce does not present itself without challenges. One of the main concerns of e-commerce is the uncertainty of the identity of the parties to a commercial transaction.[4] Thus, the challenge is to maintain the safe and reliable identity between parties to electronic transactions without interfering with the smooth operation of e-commerce.

The Electronic Communications and Transactions Act 25 of 2002 ("ECTA") is the current South African legislation that regulates electronic communication. It recognises electronic communication as the functional equivalent of paper-based communication.[5] The principle of functional equivalence[6] is one of the underlying principles of e-commerce and has been given effect by ECTA.[7] The principle states that electronic communication will be given the same legal recognition as paper-based communication provided the inherent requirements of the paper-based transactions are satisfied.[8]

Electronic communication is defined by ECTA as 'communication in the form of data messages.'[9] Data messages refer to 'data generated, sent, received or stored by electronic means.'[10] Short message services ("SMSes"), electronic mails ("Email") and

[1] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427; Berman A 'International Divergence: The Keys to Signing on the Digital Line – the cross border recognition of electronic contract signatures' 28 (2001) *Syracuse Journal of International Law and Commerce* 125.
[2] Ibid.
[3] J Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce' (2004) 15(3) *Stellenbosch Law Review Stellenbosch Regstydskrif* 50; Srivastava & Koekemoer (Note 1).
[4] Berman (Note 1).
[5] Coetzee (Note 3).
[6] The principle of functional equivalence is discussed at length in Chapter two at 2.2.
[7] DP Van der Merwe… et al *Information and Communication Technology Law* 2 ed (2016) 156.
[8] S Papadopolous & S Snail *Cyberlaw@SA III: The law of the internet in South Africa* 3 ed (2012) 318.
[9] Section 1 of the Electronic Communications and Transactions Act 25 of 2002.
[10] Ibid.

any other information in electronic form are referred to as data messages and they can be used as formalities in the conclusion of a contract.[11] This was confirmed in the *Jafta case*[12] where the court held that an SMS containing a party's intention to accept an offer of employment constituted electronic communication in terms of ECTA and qualified as a valid acceptance of the offer.[13] In the *Mafika case,*[14] the court held that data messages via SMSes are equivalent to writing.[15] Thus, case law has provided for the application of electronic communication as valid method of transacting.

The functional equivalence of writing in respect of electronic communication is contained in section 12[16] of ECTA. The requirements for writing as a formality for transacting is satisfied if a data message is used and is 'accessible in a manner usable for subsequent reference.'[17] The functional equivalent for a signature is structured in two tiers.[18]

The first tier allows parties to a contract to decide on the form of electronic signature ("e-signature") to be used, provided: the parties themselves require a signature to validate a contract; the 'method used identifies the party to the contract; the method used shows approval of the content of the contract and is reliable and appropriate for the purpose of its use.'[19] Where the parties to a contract require the use of an e-signature, an *ordinary e-signature* defined under section 1 of ECTA will suffice.

The ordinary e-signature is defined by ECTA as 'data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature'.[20] Therefore, any distinct electronic symbol or mark can be used as an electronic signature,[21] provided it is logically associated with data that it is attached to

[11] *Jafta v Ezimvelo KZN Wildlife* 2008 10 BLLR 954 (LC); 2008 JOL 22096 (LC) Paragraph 46.
[12] Ibid.
[13] *Jafta v Ezimvelo KZN Wildlife* 2008 10 BLLR 954 (LC); 2008 JOL 22096 (LC).
[14] *Mafika v The SABC* – Unreported Labour Court Case No. J 700/08.
[15] Ibid.
[16] A requirement in law that a document or information must be in writing is met if the document or information is-
(a) in the form of a data message; and
(b) accessible in a manner usable for subsequent reference.
[17] Ibid.
[18] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal 2808*.
[19] Section 13
(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-
(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.
[20] Section 2 of ECTA.
[21] S Papadopoulos and S Snail *Cyberlaw@sa: The Law of the Internet in South Africa* 3 ed (2012) 49.

and it is intended to be used as a signature. Ordinary e-signatures may take the form of a typed name at the bottom of an email,[22] a scanned version of a handwritten signature,[23] clicking on an 'I accept' icon on webpage[24] and the use of biometrics.[25]

The second tier of e-signatures applies in instances when the *law* requires the use of a signature.[26] This type of e-signature is referred to as an advanced electronic signature ("AES"), which is accredited by the Accreditation Authority of South Africa under section 37 of ECTA. The authority for accreditation is held by the National Department of Communication who may also delegate the authority to other parties.[27]

There are two challenges with the use of an AES. Firstly, the procedure for obtaining an AES is cumbersome, costly and impractical.[28] Secondly, the requirements imposed by ECTA in respect of an AES infringes on the principle of technological neutrality[29] because the requirements to obtain an AES indirectly prescribe the use of *digital signatures*.[30] This will be discussed in the literature review and chapter two of this paper.

The necessity for e-commerce regulation stemmed from the growth of e-commerce transactions taking place over the internet and the uncertainty of legal validity of electronic contracts.[31] This legal uncertainty was shared by consumers and businessmen on a global scale.[32] The United Nations Commission for International Trade Law ("UNCITRAL") had recognised this problem and drafted the Model Law on Electronic Commerce in 1996.[33]

The purpose of the Model Law of 1996 was to serve as a guideline for national legislation to be enacted to promote e-commerce globally. In 2001, an additional

[22] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA).
[23] K Bharvada 'Electronic Signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology* 267.
[24] T Pistorius T 'Click-wrap and web-wrap agreements' (2004) 16(4) *South African Mercantile Law Journal* 568-576.
[25] Bharvada (Note 23).
[26] Section 13 (3) of ECTA.
[27] Section 1 of ECTA.
[28] Eiselen (Note 18).
[29] The principle of technological neutrality is an e-commerce principle that requires legislation to be non-prescriptive of technology. The principle of technological neutrality is discussed at 1.5.4 and at 3.2.2.1
[30] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 430; Berman A 'International Divergence: The Keys to Signing on the Digital Line – the cross border recognition of electronic contract signatures' 28 (2001) *Syracuse Journal of International Law and Commerce* 149.
[31] S Snail 'Electronic Contracts in South Africa – A Comparative Analysis' 2008 (2) *Journal of Information, Law & Technology* can be accessed at http://go.warwick.ac.uk/jilt/2008_2/snail.
[32] DP Van der Merwe… et al *Information and Communication Technology Law* 2 ed (2016) 156.
[33] United Nations Commission on International Trade Law: Model on Electronic Commerce (with guide to enactment, 1996).

model on electronic signatures was drafted based on article 7 of the 1996 Model Law. Article 7 of the 1996 Model Law establishes a presumption that where e-signatures meet the criteria of technical reliability, they will be regarded as functionally equivalent to handwritten signatures.[34] These model laws do not prescribe the type or form of e-signatures to be used and AESes are not mentioned under the model laws. South Africa has adopted most of the model laws' provisions. However, South Africa has followed the approach of the European Council ("EC") in respect of AESes.[35]

In 1999, the EC developed directives governing electronic communication. The concept of the AES is contained in the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures ("EC Directives").[36] According the rules of the European Union, 'if any member states are conducting business transactions with a non-member state, then the non-member state must comply with the provisions of the EC Directive.'[37] South Africa is not a member of the EC but must adhere to the same standards as the EC if transacting with these member states.

The criteria[38] used in the consideration of accreditation of an e-signature violates the principle of technological neutrality.[39] This principle is entrenched under section 2 (1) (f) of ECTA and is contained in UNCITRAL's Model Law on E-Commerce as an underlying principle of e-commerce.[40]

The principle of technological neutrality proposes that law should not discriminate against or favour the use of any particular type of technology.[41] Users of e-commerce

[34] SL Gereda 'The Electronic Communications and Transactions Act' 2006 *Telecommunications Law in South Africa*.
[35] Section 13 (3) read with section 38 of ECTA.
[36] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures.
[37] SL Gereda 'The Electronic Communications and Transactions Act' 2006 *Telecommunications Law in South Africa;* Article 7 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[38] Section 38 (1) (1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate-
(a) is uniquely linked to the user;
(b) is capable of identifying that user;
(c) is created using means that can be maintained under the sole control of that user; and
(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;
(e) is based on the face-to-face identification of the user.
[39] L Swales 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.
[40] Section 2 (1) (f) Promote technology neutrality in the application of legislation to electronic communications and transactions.
[41] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment (2001): Part F.

should decide on the type of technology to be used.[42] Technologically prescriptive law has the potential of stifling the growth and development of e-commerce by restricting newer technologies from being used.[43] Furthermore, it is also possible for technologically prescriptive law to become obsolete as newer and more innovative technologies develop.[44]

In this regard, ECTA contravenes the principle of technological neutrality. ECTA's criteria for accreditation prescribes that e-signatures must be created using cryptography. The e-signature that is produced from cryptography is referred to as a digital signature.[45]

1.2. Statement of Purpose

The purpose of this research paper is to investigate whether South Africa's legal position on e-signature requires amendment.

1.3. Rationale for the Study

The rationale for this study is that South Africa does not seem to adhere to the principle of technological neutrality. The contravention of this principle has the potential of stifling the growth and development of e-commerce in South Africa.[46]

Firstly, the accreditation prescribed by section 13 of ECTA is cumbersome, expensive and impractical.[47] In addition, the South African Accreditation Authority ("SAAA") has only accredited two authentication service providers.[48] The study investigates the possible reasons for this.

Secondly, South Africa's legal position on e-signatures is inconsistent with UNCITRAL's position on e-signatures.[49] This is a concern because UNCITRAL's purpose is to facilitate growth and development of e-commerce and to increase trade

[42] Kamecke, U Korber, T 'Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood' (2008) 331.
[43] Eiselen, S 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2815; Swales, L 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 259.
[44] Swales (Note 43).
[45] L Barofsky 'The European Commission's Directive on Electronic Signature: Technological "Favoritism" towards Digital Signature' (2000) 24(1) *Boston College International and Comparative Law Review* 150.
[46] Swales (Note 43).
[47] Eiselen (Note 43).
[48] SAAA Website accessed at *http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-30-50.html.*
[49] ECTA only adopts UNCITRAL's position on ordinary e-signature.

integration.[50] The guidelines suggested by UNCITRAL is based on the consideration for the interests of developing countries. Furthermore, many technologically advanced countries such as United States and Australia adopt UNCITRAL's approach whereas South Africa partially adopts UNCITRAL's approach.

Thirdly, South Africa's adoption of accreditation of e-signatures differs from the EC Directive. The EC Directive does not require accreditation for validity of e-signatures. The SAAA has accredited only two authentication service providers in the past nine years. This indicates the lack of societal interest in the procedure and the law's irrelevance in this regard.[51]

These issues require further research to investigate the reasons for the South African current position and possible suggestion for reform of the law on e-signatures if it is necessary.

1.4. Research Question

The research paper aims to deal with the question of: whether the distinction between electronic signatures and advanced electronic signatures should be removed from the Electronic Communications and Transactions Act 25 of 2002, in light of technological advancements.

Sub-questions

The research paper aims to answer the main research question by dealing with the following sub-questions:

a) *What is the distinction between the two types of signatures contained in ECTA and the purpose of the distinction in South African law?*
b) *What criticisms can be levelled against AESes and are they valid?*
c) *Why should e-signature law adhere to the principle of technological neutrality?*
d) *Is it necessary for e-signatures to be highly secure and reliable in the manner that ECTA suggests?*

[50] United Nations Commission on International Trade Law Model on Electronic Commerce: Guide to Enactment Part A.
[51] SAAA (Note 46).

e) *Where did the current position of South African law on e- signatures originate from?*
f) *What is the approach to e-signatures in other jurisdictions such as United States, Germany and Australia?*
g) *Is there a need to amend the South African legal position on e-signature law?*
h) *If there is a need to amend the South African legal position on e-signature law, what is an appropriate reform for the position in South Africa?*

1.5. Literature Review

1.5.1. Distinction between the two types of Electronic Signatures

The general functions of a signature are: to identify the signatory; to provide certainty that the signatory is accountable for the signature and to associate the signatory with the information in the document signed by him.[52] As a result of technological advancements, the functions formerly performed by handwritten signatures are now being performed by e-signatures.

ECTA creates a distinction between two types of e-signatures, the ordinary e-signature and the AES.[53] The ordinary e-signature can be used whenever *parties* to an agreement require a signature to validate a contract.[54] However, when the *law* requires a signature, the requirement is met only if an AES is used.[55] The AES is an e-signature that is required to undergo accreditation before obtaining the status of an AES.[56]

AESes are given special evidential advantages, while ordinary e-signatures are not.[57] There is a rebuttable presumption that an AES is a valid signature and a party that disputes the validity of the AES must prove its invalidity. On the other hand, an

[52] Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods (2007)
[53] Section 13.
[54] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2815.
[55] Section 13 (1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.
[56] Section 2 of ECTA.
[57] Srivastava & Koekemoer (Note 1).

ordinary e- signature is not given this advantage, and a party relying on it must prove its validity.[58]

The two-tier approach on e-signatures is criticised to a large extent by academics and legal practitioners. Swales[59] takes the view that ECTA should be reviewed and the concept of AESes removed from the Act. He believes that the AES is contrary to the principle of technological neutrality, is not facilitative of technological development and creates an unnecessary accreditation procedure.[60]

Snail[61] suggests the legislature should abolish the stringent requirements of the AES or make provision for the use of internationally recognised e-signatures, which follow an advanced standard of technology but maintain technological neutrality.[62] This point is relevant because it addresses the challenge with e-signature law. It suggests an internationally harmonised approach to be adopted by countries. However, the suggested approach to e-signature law must be technologically neutral and still provide a high level of security. These two ideas operate in contrast with each other as the current approach to e-signature law demonstrates.

Although the procedure for obtaining the AES is complex and expensive,[63] it provides an additional layer of security to the extent that the accreditation authority is aware of the identity of the[64] authentication service providers. Section 38[65] of ECTA requires the AES to be based on face-to-face recognition of authentication service providers. Thus, the identity of authentication service providers who provide users with e-signature products will be known to the SAAA.[66]

One way of achieving ECTA's primary objective of 'creating legal certainty and confidence in e-commerce'[67] is by ensuring reliability of the use of e-signatures.

[58] Ibid.
[59] Swales, L 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.
[60] Ibid.
[61] Snail, S 'Electronic Contracts in South Africa – A Comparative Analysis' 2008 (2) *Journal of Information, Law & Technology* can be accessed at http://go.warwick.ac.uk/jilt/2008_2/snail.
[62] Ibid.
[63] Eiselen (Note 54).
[64] Swales (Note 57).
[65] Refer to note 36.
[66] Regulation 5 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[66] Regulation 1 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[67] Section 2(1) (e) promote legal certainty and confidence in respect of electronic communications and transaction.

However, the inclusion of a criterion that specifies cryptography to be used in satisfying the requirements of an AES contravenes the principle of technological neutrality.

Barofsky[68] takes the view that accreditation can safeguard technology against fraud and manipulation. He further suggests that using digital signatures based on cryptography provide a degree of security that cannot be provided by ordinary e-signatures.[69] Although the practical implications of the procedure for obtaining an AES is not ideal for growth and development of e-commerce, it does guarantee a higher level of security than an ordinary e-signature. However, societal practice in South Africa reveals that such high levels of security are not being used by parties to commercial transactions.[70]

1.5.2. The Accreditation Process

As mentioned above, where the law requires a signature, the requirement can only be satisfied if an AES is used.[71] In order to obtain the status of an AES, the accreditation authority must accredit an e-signature. The SAAA is held by the minister of the Department of Communication.[72] The SAAA has accredited the South African Post Office ("SAPO") and *Lawtrust*, a privately owned authentication service provider company.[73] According to the SAAA website,[74] there have been no new accreditations since 2007. This creates doubt about the effectiveness and practicality of the accreditation procedure.

The purpose of the accreditation procedure is to ensure the e-signature used is reliable. 'Accreditation is a process whereby an authentication product or service[75] and the authentication product or service provider is recognised by the accreditation authority.'[76] This is done by ensuring the authentication product or service satisfies specific criteria before it can be accredited.

---

[68] A Barofsky 'The European Commission's Directive on Electronic Signature: Technological "Favoritism" towards Digital Signature' (2000) 24(1) *Boston College International and Comparative Law Review* 145-160.
[69] Bharvada K 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology.*
[70] SAAA Website accessed at *http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-30-50.html.*
[71] Section 13(1) of ECTA.
[72] Section 2.
[73] S Papadopoulos and S Snail *Cyberlaw@sa: The Law of the Internet in South Africa* 3 ed (2012) 49.
[74] (*accessed at http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-28-29.html*).
[75]Section 1 of ECTA defines an authentication product or service as "products or services designed to identify the holder of an electronic signature to other persons".
[76] Section 33 of ECTA.

According to section 38 of ECTA, the e-signature must:

> *'uniquely link the e-signature to the user; be capable of identifying the user; create means that can be maintained under the sole control of the user; be linked to the data to which it relates in such a manner that any subsequent change in the data is detectable and based on face-to-face recognition of the user.'*[77]

The applicant in the accreditation process is the provider for authentication products or services. The applicant must follow the procedure set out in the Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations of 2011 ("Accreditation Regulations"). The application form must be hand-delivered to the offices of the SAAA,[78] the prescribed fee of R20 000 must be paid[79] before or at the time of application and all the relevant information must be attached to the application.[80] If any of these requirements are not met, the application for accreditation will not be considered.[81] Eiselen[82] and Swales[83] are opposed to this cumbersome and expensive procedure imposed by ECTA. The accreditation procedure creates unnecessary administration and is very expensive.[84]

Another challenge with ECTA relates to e-signature products which have been used on a global scale and has acquired a good reputation but are not legally valid because they have not been accredited.[85] Examples of these authentication products are *Adobe* and *DocuSign*. ECTA's provisions place an unnecessary burden on these authentication service providers to prove the validity of their product in the event of a dispute.

Chapter 3 of the Accreditation Regulations[86] deals with the technological standard and the type of technology the authentication product should be based on.[87] The type of technology prescribed is public key cryptography. Public key cryptography involves

[77] Section 38 of ECTA.
[78] Regulation 8 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[79] Regulation 29 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[80] Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007: Chapter 2.
[81] Ibid.
[82] Eiselen (Note 54).
[83] Swales (Note 59).
[84] Ibid.
[85] Swales (Note 59).
[86] Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007: Chapter 2.
[87] 13(1) A certification service provider whose authentication products and services are on PKI must comply with SANS 21188.

the encryption of electronic messages.[88] The encrypted data messages becomes the signature, which uniquely links the signatory to the message.[89] In order for these messages to be decrypted, one would need to be in possession of a public key or private key. The document is signed with a private key and the recipient of the document will only be able to view the document if he enters the corresponding public key.[90] Public key cryptography is the only known technology that meets the requirements of an AES. Thus, ECTA's provisions on e-signatures are technologically prescriptive.

The accreditation process[91] and the concept of an AES are criticised by authors on the basis that the procedure is inconvenient and the concept violates the principle of technological neutrality. Eiselen[92] describes the procedure as expensive and cumbersome due to the detailed information required by the accreditation authority[93], the requirement of face-to-face recognition[94] and the high costs involved in accrediting authentication products.[95] Swales[96] supports this view and adds that the process is outdated, introduces a layer of administration and unnecessary costs and conflicts with the international best practice.[97]

[88] Ibid.
[89] DP Van der Merwe… et al *Information and Communication Technology Law* 2 ed (2016) 155-156.
[90] Blythe, SE 'Digital Signature law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in e-commerce with enhanced security' (2005) 11(2) *Richmond Journal of Law and Technology* 1-20.
[91] Discussed at length in chapter three of this paper.
[92] Eiselen (Note 54).
[93] Regulation 7 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[94] Section 38 of ECTA.
[95] Regulation 29 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[96] Swales (Note 59).
[97] Ibid.

1.5.3. The Spring Forest Case[98]

The *Spring Forest case*[99] is one of the very few cases dealing with the interpretation of ECTA's provisions.[100] One of the issues discussed in the case is whether an email containing the name of the sender below the message constituted an e-signature.[101] The court confirmed that the type-written name did constitute a signature because it met the functional requirements of a signature.[102]

The case also suggested that courts should be aware that onerous requirements and criteria for accreditation can have a negative effect on electronic transactions.[103] It was decided, where parties have included a non-variation clause in their contract, the type and form of signature required should be decided by the parties alone.[104] The reason for this is the decision to insert the non-variation clause was made by the parties themselves.

The court held further that 'when one has regard to the purpose for which an advanced electronic signature is required it is apparent that it does not apply to the private agreements between these parties.'[105] It must be noted that courts will interpret ECTA in a manner facilitative of e-commerce, which indicates the attitude of South African courts on e-commerce.

1.5.4. Technological Neutrality

South Africa's approach to e-signatures is inconsistent with the internationally recommended approach based on the 1996 Model Law on e-commerce.[106] The 1996 Model Law is technologically neutral and does not prescribe or favour any particular type of technology to be used for an e-signature to be legally recognised. UNCITRAL[107] provides a definition of an e-signature that requires e-signatures to be

[98] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA).
[99] Ibid.
[100] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA) Paragraph 14.
[101] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA) Paragraph 17.
[102] To identify the signatory and show the signatory's assent to the information contained in the document.
[103] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA) Paragraph 22.
[104] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA) Paragraph 20.
[105] Ibid.
[106] United Nations Commission on International Trade Law: Model on Electronic Commerce (1996).
[107] United Nations Commission on International Trade Law Model Law on Electronic Signatures (2001).

'appropriate and reliable for the purposes generated.'[108] In contrast with UNCITRAL, an e-signature in South Africa will only be legally recognised if the e-signature meets the requirements set out in section 38 of ECTA which is prescriptive of the use of cryptography.[109]

ECTA has partially adopted the EC approach by adopting the concept of the AES and accreditation.[110] Thus, the EC Directive is also technologically prescriptive. However, the South African approach to e-signatures is more burdensome than the approach contained in the EC Directive because the latter does not impose compulsory accreditation for legal recognition of an e-signature.[111]

Technological neutrality is entrenched in section 2(1) (f) of ECTA.[112] In the *Ketler case*[113] the court acknowledges the importance of incorporating the principle technological neutrality in ECTA as it facilitates innovative technology.[114] However, ECTA's approach to e-signatures infringes this principle in so far as only cryptography can meet the criteria for an AES.[115]

Technologically neutral regulation is categorised by UNCITRAL[116] as one of three approaches adopted by countries in the regulation of technology.[117] This approach involves minimal regulation and is argued by authors to be advantageous than other types of regulation.[118]

Some of the advantages of technologically neutral law are: it facilitates and fosters innovation of technology;[119] it allows parties to decide on an appropriate technology

[108] Article 2.
[109] DP Van der Merwe… et al *Information and Communication Technology Law* 2 ed (2016) 155-156.
[110] UNCITRAL webpage accessed at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.
[111] Recital 11: Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;
[112] to promote technology neutrality in the application of legislation to electronic communications and transactions.
[113] Ketler Investments CC t/a Ketler Presentations v Internet Service Providers [2014] (2) SA 569 (GSJ).
[114] Ketler Investments CC t/a Ketler Presentations v Internet Service Providers [2014] (2) SA 569 (GSJ) Paragraph 30.
[115] Van der Merwe (Note 109).
[116] United Nations Commission on International Trade Law Model Law on Electronic Signatures (2001) Part F.
[117] Ibid.
[118] C Spyrelli 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) *Journal of Information Law and Technology;* Swales (Note 57); Koger JL 'You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Contemporary Problems* 491-516.
[119] JL Koger 'You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Contemporary Problems* 491-516.

which embraces party autonomy;[120] it prevents law from becoming obsolete[121] and it creates legal certainty and confidence by ensuring the law regulates current societal practice.[122] However, some authors prefer a technologically specific approach because of the risks associated with the internet and electronic devices. These authors take the view that technologically neutral legislation will create legal uncertainty because of its failure to consider the risks of technology.[123] This is discussed at length in chapter three.

UNCITRAL adopts a two-pronged approach to e-signatures.[124] An e-signature will be legally valid if it meets the basic functional requirements of an e-signature[125] and is appropriate and reliable for the purposes that it is generated.[126] This approach is neutral and does not specify any particular type of authentication method to be used. However, Article 6 (3)[127] of UNCITRAL's Model Law on E-Signatures creates a presumption on the reliability of e-signatures.[128] The presumption indirectly favours cryptography but does not make the use cryptography-created e-signatures the only form of e-signatures legally recognised.

In contrast with UNCITRAL,[129] ECTA only legally recognises an AES as a valid e-signature.[130] Any other form of e-signature will not be presumed as valid unless it meets the requirements of an AES or is proved to be valid by a court of law.[131] ECTA's approach is similar to the EC Directive's approach in so far as the concept of an

[120] W, Maxwell M, Bourreau 'Technology neutrality in Internet, telecoms and data protection regulation' 2014 *Hogan Lovells Global Media and Communications Quarterly 19-23.*
[121] Swales (Note 59).
[122] Koger (Note 119).
[123] Koger (Note 119); Stern J 'The Electronic Signatures in Global and National Commerce' (2001) 6 *Berkeley Technology Law Journal* 391-414.
[124] S Mason 'Electronic Signatures in Practice' (2006) 6(2) *Journal of High Tech. Law* 148-164.
[125] Ibid.
[126] Mason (Note 124).
[127] Article 6 (3) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
[128] Eiselen (Note 54).
[129] United Nations Commission on International Trade Law Model Law on Electronic Signatures (2001).
[130] Section 13 (3) of ECTA.
[131] Section 38 (1) of ECTA.

AES.[132] ECTA's prescriptiveness of cryptography is one of the main issues dealt with in the paper.

1.5.5. The Origins of ECTA's provision on Electronic Signatures

ECTA regulates all electronic transactions and communications in South Africa.[133] In respect of e-signatures, South Africa has taken a hybrid approach having adopted provisions from the EC Directive[134] and the United Nations. However, ECTA does add its own requirements in addition to those adopted from UNCITRAL and the EC Directive.[135]

1.5.5.1. United Nations Approach to Electronic Signatures

UNCITRAL was established by the general assembly of the United Nations.[136] The purpose of UNCITRAL is to harmonise and unify laws regarding international trade.[137] In 1996, UNCITRAL drafted a model law on Electronic Commerce[138] ("The 1996 Model Law"). Article 7[139] of the 1996 Model Law was adopted by ECTA.[140] The requirements in article 7 of the 1996 Model Law do not make the distinction between circumstances of law requiring a signature and when parties require a signature.

In 2001, UNCITRAL adopted its Model Law on Electronic Signatures[141] ("The 2001 Model Law"), which was based on article 7 of the 1996 Model Law but should be read in conjunction with the earlier Model Law.[142] Article 6[143] of the 2001 model provide

---

[132] The criteria listed section 38 (1) of ECTA is similar to the content of Article 2 of the EC Directive except for ECTA's additional requirement that the AES must be based on face to face recognition.
[133] Section 4 of ECTA.
[134] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[135] Refer to note 132.
[136] United Nations Commission on International Trade Law: Model on Electronic Commerce (1996): Part A of Guide to enactment.
[137] Ibid.
[138] United Nations Commission on International Trade Law: Model on Electronic Commerce (1996).
[139] (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
[140] Refer to note 107.
[141] United Nations Commission on International Trade Law: Model on Electronic Signatures (2001).
[142] Ibid.
[143] An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

criteria for reliability which are similar to the criteria applied by the accreditation authority under South African law. However, the criteria in article 6 (3) of the 2001 Model Law are presumptions for reliability and are not requirements for legal validity.[144]

1.5.5.2. The European Union's Approach to Electronic Signatures

The EC drafted directives to deal with electronic communications and transactions. The directives are binding on all member states of the EU. One of the directives drafted was the EC Directive on Electronic Signatures.[145] The aim of the EC Directive is to achieve legal uniformity among all member states with regard to e-commerce transactions.[146] Furthermore, the objective of creating uniformity was to maintain a set standard within the EU that would prevent any conflict of laws and allow free flow of cross border transactions.[147]

The EC Directive is one of the regions that makes provision for concepts of accreditation and AESes.[148] An e-signature will only be legally recognised if it meets the criteria of an AES.[149] However, unlike ECTA, it does not require e-signatures to be accredited in order to obtain the status of an AES. E-signatures must meet the requirements set out in article 2.[150] These stringent security requirements can only be met by the use of public key cryptography technology and similar technologies.[151] Blythe[152] takes the view that the EC Directive appears to be technologically neutral but its imposition of the requirements in article 2 indicate its preference for cryptography.[153] Srivastava and Koekemoer[154] adopt a similar view in respect of

[144] Eiselen, S 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.
[145] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[146] Gereda, SL 'The Electronic Communications and Transactions Act' (2006) *Telecommunications Law in South Africa*.
[147] MA Parmentier 'Electronic Signatures' (2000) 6(2) *Columbia Journal of European Law* 251-258.
[148] Article 2 and Recital 11 of the EC Directive.
[149] Ibid.
[150] Article 2
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
[151] Blythe, SE 'Digital Signature law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in e-commerce with enhanced security' (2005) 11(2) *Richmond Journal of Law and Technology* 1-20.
[152] Ibid.
[153] DP Van der Merwe… et al *Information and Communication Technology Law* 2 ed (2016) 155-156.
[154] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446; Berman A 'International Divergence:

ECTA's position. The EC Directive and ECTA only legally recognise e-signatures that are created by cryptography because cryptography is the only known technology that can create an e-signature to satisfy the requirements of article 2[155] of the EC Directive.

Some authors take the view that the EC directive favours public key cryptography technology. The problem is that superior forms of technology may be prevented from entering the market because the law based on the EC directive does not make provision for them.[156] The imposition of specific criteria has the potential of preventing newer technologies from being used even if they provide better security and are more reliable.[157]

1.5.6. A Harmonised approach

Another concern with the South African approach to e-signatures is its failure to harmonise its e-signature provisions with other jurisdictions. As discussed, ECTA requires accreditation to be based on face-to-face recognition.[158] This is not a requirement under the EC Directive. Firstly, the EC Directive does not require accreditation of e-signatures for legal validity.[159] The recitals[160] of the EC Directive make it clear that accreditation is a barrier to e-commerce and operates on a voluntary basis. The EC Directive is technologically specific to the extent it favours the use of cryptography for the creation of a legally recognised e-signature. The implementation of the EC Directive is discussed in chapter four of this paper.

The United States of America ("US") adopted a technologically neutral approach to e-signature regulation. The Electronic Signatures in Global and National Commerce Act ("The E-Sign Act") 2000 operates at a federal level and the Uniform Electronic Transactions Act of 1999 ("UETA") operative at a state level. According to these statutes, any method of e-signature is legally valid provided the requisite intention is present.[161] United States has a far superior technological infrastructure to South

---

The Keys to Signing on the Digital Line – the cross border recognition of electronic contract signatures' 28 (2001) *Syracuse Journal of International Law and Commerce* 125-155.

[155] Refer to note 150.

[156] A Srivastava *Electronic Signatures for B2B Contracting: Evidence from Australia* (2013); Parmentier M 'Legislative Developments' (2000) *Columbian Journal of European Law* 251.

[157] Swales, L 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.

[158] Section 38 (1) (e) of ECTA.

[159] Recital 11 of the EC Directive permits voluntary accreditation.

[160] Ibid.

[161] Kisswani & Al-Bakri 'Regulating the Use of Electronic Signatures Given the Changing Face of Contracts' (2010) 7 *Macquarie Journal of Business Law* 53-65.

Africa[162], adopts a non-prescriptive approach to e-signatures and seems to be functioning smoothly without any amendments. Thus, the minimalist position of the US allowed the law to remain relevant and applicable to current practices evidenced by the US e-signature position not being amended.

South Africa's approach to e-signatures is not completely consistent with EC laws and US laws. The lack of harmonisation can create uncertainties between South Africa and other jurisdictions in respect of international transactions. Developing countries are reliant on international trade for growth and development of their economies and infrastructure. Divergent e-commerce approaches among trading countries will create barriers to trade[163] and will discourage countries from trading with each other due to these inconsistencies.[164]

The EC Directive aims to harmonise e-commerce laws of members for the purpose of allowing the free flow of cross border transactions.[165] This is one way of facilitating e-commerce on a global scale. Harmonisation is important because it promotes further integration of developing countries in international trade which leads to development in many spheres.[166]

South Africa's approach to e-commerce can be improved by the harmonisation of its law with the law of its main trading partners. Furthermore, harmonisation of a technologically neutral approach to e-signatures will improve the state of e-commerce in South Africa by removing barriers to e-commerce without imposing strict security standards for e-signature law. Reform of the law in this manner is discussed further in chapter five of this paper.

[162] Swales (Note 154).
[163] JAE Faria 'E-Commerce and International Legal Harmonization; To Go Beyond Functional Equivalence?' 16 (2004) *South African Mercantile Law Journal* 529-555; Berman A 'International Divergence: The Keys to Signing on the Digital Line – the cross border recognition of electronic contract signatures' 28 (2001) *Syracuse Journal of International Law and Commerce* 125-155 and Boss A 'The Emerging Law of International Commerce' 6(2) (1992) *Temple International and Comparative Law Journal* 293-309
[164] A Boss 'The Emerging Law of International Commerce' 6(2) (1992) *Temple International and Comparative Law Journal* 293-309.
[165] Recital 20 of the EC Directive.
[166] Boss (Note 164).

2. Chapter Two: Electronic Signatures

2.1. Introduction

The evolution of e-commerce has changed the efficiency of business operation.[167] The benefits of e-commerce are evident in the reduction of paper-work and the lowering of transaction costs.[168] Furthermore, transactions take place 'at the click of a button' without restrictions of time and location.[169] This allows for more transactions to take place within a short period of time with immediate responses and without the costs usually involved in cross border transactions.

Nearly two decades ago, e-commerce had not been specifically regulated and concerns about the legal validity of electronic transactions had arisen.[170] Furthermore, the legislation at the time was outdated, inadequate and could not be applied to electronic transactions.[171] This led to legal uncertainty on global level which had prompted UNCITRAL to draft a set of guidelines on e-commerce law to assist national governments around the world to enact harmonised and unified law on e-commerce.[172]

ECTA was enacted to govern e-commerce in South Africa and to a large extent followed the approach suggested by UNCITRAL.[173] ECTA, however departs from UNCITRAL's approach to e-signatures by partially adopting the approach of the European Commission.[174]

This chapter deals specifically with the requirement of e-signatures as a formality for the conclusion of e-contracts in South Africa. It discusses ECTA's contribution to adapting the requirements of the traditional paper-based formality of signatures to the electronic equivalent thereof. This is the essence of the principle of functional

[167] A Srivastava *Electronic Signatures for B2B Contracting: Evidence from Australia* (2013) 21.
[168] Ibid.
[169] Srivastava (Note 167).
[170] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[171] T Pistorius 'From snail mail to e-mail-a South African perspective on the web of conflicting rules on the time of e-contracting' (2006) 39 (2) *Comparative and International Law Journal of Southern Africa* 178.
[172] Ibid.
[173] Discussed under 2.4.
[174] Ibid.

equivalence[175] which was developed by UNCITRAL[176] and has been formerly adopted by and incorporated in ECTA. This principle will be discussed briefly in an attempt to understand e-signature law and its requirements.

The chapter focuses on the South African legal position of e-signatures: the origin of South Africa's approach to e-signatures; the forms of e-signatures and the technological infrastructure required to obtain some of these e-signatures.

2.2. The Principle of Functional Equivalence

Functional equivalence is a key principle of e-commerce and has been incorporated by ECTA in its provisions on 'writing' and 'signature'.[177] The principle of functional equivalence was formulated by UNCITRAL and is contained in the Guide to Enactment.[178] As mentioned earlier, the principle of functional equivalence suggests that electronic communication and transactions should be treated equally to paper-based communications and transactions.[179] Article 15 UNCITRAL's Guide to Enactment[180] states the reason for adopting a functional equivalent approach is to reduce the impediments of paper-based transactions.[181] Where national laws require formalities such as writing,[182] signature[183] and original documents,[184] UNCITRAL

[175] Discussed under 2.2.
[176] United Nations Commission on International Trade Law Model on Electronic Commerce: Guide to Enactment Part E.
accessed at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.*
[177] T Pistorius 'Nobody knows you're a dog: Attribution of data messages' (2002) 13(4) *South African Mercantile Law Journal* 738.
[178] UNCITRAL (Note 176).
[179] Ibid.
[180] UNCITRAL (Note176).
[181] Ibid.
[182] Article 6. Writing
(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.
(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.
[183] Article 7. Signature
(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
[184] Article 8. Original
(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if: (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.
(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

provides the electronic equivalents and the basic criteria to be satisfied for legal validity.

Functional equivalence requires paper-based transactions and electronic transactions to be treated the same.[185] In addition, the principle is based on the idea that the purpose and function of paper-based transactions can be performed electronically having the same effect and consequences as the former.[186] However, this does not mean paper-based documents and electronic documents are regarded as the same. Electronic documents are only a *functional* equivalent of paper-based documents, which means they can provide the same function but are different in form.[187]

Adopting a functional equivalent approach is done in the analysis of the purpose and function of the paper-based communication and finding methods that would serve the same purpose in electronic format. UNCITRAL's model law[188] acknowledges the inherent differences between paper-based communications and electronic communications but ensures the substantive components of the former and the latter achieve the same commercial purpose.[189]

The Guide to enactment attached to the 1996 Model Law discourages national laws from imposing stringent requirements on electronic transaction, which are not required by paper-based transactions.[190] Imposing stringent requirements on electronic transactions would have the effect of stifling e-commerce, which is detrimental to the concept of innovative business. The stringency of standards applied to electronic communications must be in accordance with those applied to paper-based communications.[191] Unfortunately, ECTA's approach to AESes is not consistent with this and applies more stringent requirements than would normally be applied in paper-based transactions.[192] These requirements include the accreditation of e-signatures.

(3) For the purposes of subparagraph (a) of paragraph (1): (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

[185] Pistorius (Note 177).
[186] UNCITRAL (Note 176).
[187] Ibid.
[188] UNCITRAL (Note 176).
[189] S Papadopolous & S Snail *Cyberlaw@SA III: The law of the internet in South Africa* 3 ed (2012) 318.
[190] UNCITRAL (Note 176).
[191] Ibid.
[192] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.

ECTA incorporates the principle of functional equivalence in many of its provisions;[193] however, the focus of this section will be on functional equivalence of signatures. In order for the principle of functional equivalence to be met the function and purpose of manuscript signature must be identified.[194] The identified purpose and function must be used in determining criteria for legal recognition of the e-signature.[195] Accordingly, the primary purpose and function of a signature will be fulfilled by an e-signature if the 'method used is capable of identifying the signatory, showing his intention to approve the information and if the method was reliable and appropriate for the purposes for which it was used.'[196]

The practical application of this is illustrated in the case of *Spring Forest.*[197] One of the issues in contention was whether the name of a signatory typed out at the bottom of an email constituted a signature of the individual.[198] The court took the view that type-written names fell within the definition of data message because it could be 'generated, sent, received or stored by electronic means.'[199] Furthermore, it satisfied the requirements of an e-signature by identifying the signatory and showing his assent to the information contained in the email.[200] The type-written signature had the effect of authenticating the information contained in the email.[201]

In addition, the court in the case of *S v Miller*[202] clarified that 'functional equivalence of data messages as evidence is necessary to make data messages[203] the functional equivalent of documents.'[204] Therefore, electronic information that meets the functional requirement of data messages can be used as evidence if the paper-based version would qualify as evidence.

---

[193] Sections: 11; 12; 13 and 14.
[194] Pistorius (Note 177).
[195] Ibid.
[196] Section 13 (3) of the Electronic Communications and Transactions Act 25 of 2002.
[197] *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA*).
[198] *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA*) Paragraph 17 of the judgment: "The real dispute is about whether or not the names of the parties at the foot of their emails constituted signature."
[199] Section 1 of ECTA.
[200] Section 13 (3) of ECTA: Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-
(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
(b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.
[201] Ibid.
[202] S v Miller and others [2015] 4 All SA 503 (WCC) at paragraph 52.
[203] In respect of Section 1 of ECTA.
[204] S v Miller and others [2015] 4 All SA 503 (WCC) at paragraph 52.

2.3. The Traditional Manuscript Signature

A signature is defined as a method of showing an intention to authenticate a document.[205] This includes using a mark, symbol or writing the name of the signatory below the information to indicate the signatory's assent to the information.[206] The functions of the traditional manuscript signature have been stated in early case law.

In *Van Vuuren v Van Vuuren,*[207] the court held:

> *'To sign document means to authenticate by that which stands for or is intended to represent the name of the person who is to authenticate. If an illiterate person is to sign, he would put a cross. If a person cannot use his hands as normal due to some disability it will suffice to put the initial, in capital letters, of his name and surname.'*

The above statement outlines the functions of a signature, which are to identify the signatory, to show the acceptance or assent to the terms of a contract and to provide evidence of the existence of the contract. Fagan CJ in the case of *George v Fairmead*[208] stated when a person signs a document he is assenting to the words above his signature. This reemphasises the function of assent of the signature, and provides a guideline about where the signature should be located on the document.

Caney[209] submits that the *form* of signature includes a 'mark, the name and surname of the signatory or the initials of the signatory'.[210] Thus, a signature in any of the aforementioned forms would be legally binding against a person provided he used the mark with intention of assenting to the terms of the document.

Generally, signatures serve different purposes dependant on the document they are affixed to.[211] Mason[212] categorises these purposes as follows: cautionary, channelling, protective and record-keeping. The cautionary function serves as a warning to the signatory to acknowledge the contents of the document and the legal effect of his signature being attached to the document before he signs the document.[213]

---

[205] K Bharvada 'Electronic Signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology* 266.
[206] Ibid.
[207] (1853 - 1856) 2 Searle 116 at 472A.
[208] LR Caney *The Law of Suretyship* (1936).
[209] Ibid.
[210] Caney (Note 208).
[211] S Mason *Electronic Signatures in Law (*2012).
[212] Ibid.
[213] Mason (Note 211).

The protective function serves to protect the receiving party from the signatory denying he has signed the contract.[214] The channelling function shows the point at which the contract has become legal binding and 'reduces risks relating to oral recollections in contracting'.[215] Lastly, the record-keeping function ensures that the document maintained in its original form for use as evidence if the need arises.[216]

Although signatures provide a number of useful functions, it is not mandatory in all instances in South African law. The general position is there are no formalities required for validly concluding a contract.[217] However, parties are reluctant to conclude contracts without these formalities[218] due to the risk that the signatory may deny attaching his signature to the contract which would allow him to escape liability under the validly concluded contract.

2.4. The Legal Position of E-Signatures in South Africa

South Africa follows a two-tiered approach to e-signatures.[219]

Section 13 (3) of ECTA states that

> *'when parties to a contract require a signature the requirement is met if an ordinary e-signature is used, provided a reliable method is used and the method used identifies the party concerned and indicates his approval of the information communicated'.*[220]

The requirements for this section can be satisfied without much effort and gives parties the freedom to decide on the manner in which to validate their agreement. This approach has been adopted by ECTA from Article 7 of UNCITRAL's Model Law on

[214] Ibid.
[215] Mason (Note 211).
[216] Ibid.
[217] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[218] Ibid.
[219] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2814.
[220] Section 13(3) of ECTA.

electronic Commerce of 1996.[221] UNCITRAL's Model Law[222] remains technologically neutral[223] and does not prescribe any particular form of e-signature to be used. [224]

The second type of e-signature under ECTA is the AES. Section 13(1) of ECTA states that:

> *'where the law requires a signature to be used the requirement is only met in relation to a data message if an AES is used.'*[225]

The AES is defined by ECTA as an e-signature that has been accredited by the accreditation authority.[226] Thus, the AES may take the same *form* as an ordinary e-signature but there are other attributes of the AES that the ordinary e-signature falls short of.[227]

The practical distinction between the two types of e-signatures becomes relevant in the event of a dispute. If an AES is used, there is a rebuttable presumption that the signature is valid.[228] However, if an ordinary e-signature is used the party relying on the e-signature must prove its validity. Thus, the AES carries more legal weight than an ordinary e-signature and places the burden of proof on the opposing party to prove its invalidity.

The concept of an AES is not contained in any of the UNCITRAL documents but has been adopted by ECTA from the European Commission's Directive on E-Signatures ('EC Directive').[229] The EC Directive provides member states with a framework of provisions in relation to e-signature laws which member states must include in their

---

[221] Article 7. Signature
(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

[222] United Nations Commission on International Trade Law Model on Electronic Commerce (2001).

[223] Technological Neutrality is discussed at 3.2.2.1.

[224] Eiselen (Note).

[225] Section 13(1) of ECTA.

[226] Section 1 "advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37.

[227] The AES must be accredited in terms of Section 37 of ECTA.

[228] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.

[229] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

national laws.[230] One of the reasons the EC Directive was formulated was to 'facilitate the use and contribute to the legal recognition of e-signatures'.[231] It provides guidelines to its member states of the European Commission on the standards and criteria that e-signatures must adhere to. The concept of the AES is contained in Article 2[232] of the EC Directive and is almost identical to the Section 13 (1) of ECTA in respect of the definition of an AES, except for the requirement of face-to-face recognition,[233] which is not contained in the former. The European Commission acknowledges that accreditation of e-signatures may create an obstacle to e-commerce but includes it in the directive.[234] The EC Directive is discussed at length in chapter 5 of this research paper.

According to ECTA, the AES must be obtained from a process of accreditation.[235] This process involves the 'authentication product or service or the e-signature being formally acknowledged by the accreditation authority.'[236] This gives the recipient of the AES-signed document a sense of security because the product or service that the sender has used is recognised by the government, especially for transactions taking place in distant and unknown locations with an unfamiliar vendor.[237] Furthermore, transacting over the internet lacks the transparency and familiarity that people have when contracting on paper because of the distance between parties and the lack of personal interaction.[238] There is a sense of physical control that provides contractual parties with 'solid' evidence of their transaction. In paper-based transactions, it is also possible for witnesses to be present when terms are being negotiated and assented to. These aspects are lacking when a party contracts over the internet or electronically.

---

[230] A Barofsky 'The European Commission's Directive on Electronic Signature: Technological "Favoritism" towards Digital Signature' (2000) 24(1) *Boston College International and Comparative Law Review* 145-160.

[231] Article 1: The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

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

[233] Section 13(1) (e) of ECTA.

[234] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. (Paragraph 4 of the undertaking).

[235] Section 37 of ECTA.

[236] Section 33 of the Electronic Communications and Transactions Act 25 of 2002.

[237] R Sabett 'Effects of Technology Convergence and Public Key Infrastructure' (1999) 7(2) *University of Baltimore Intellectual Property Law Journal* 143-154.

[238] Ibid.

ECTA also refers to certification service providers[239] who provides a specific authentication service. These certification service providers provide the recipient with a certificate that reveals the credibility of the signature used in the document sent to the recipient. It is also necessary for these certification service providers to be accredited by the accreditation authority. Certification service providers provide AESes in the form of digital signatures.[240]

Although ECTA does not define or specifically mention digital signatures it implies its use by suggesting criteria and requirements that can only be met by the use of cryptography.[241] The type of e-signature that results from cryptography is a digital signature.[242] Cryptography is supported by the technological infrastructure known as the private key infrastructure ('PKI').[243]

The use of the digital signature has the effect of the document being notarised[244] because it involves a trusted third party providing information to the recipient on the legitimacy of the document. Furthermore, use of PKI technology in this manner enables the recipient to detect any alterations to the document.[245] Thus, it can be said that the 'digital signature goes beyond the functional equivalent approach and provides more protection than manuscript signatures'.[246]

It must be emphasised that a digital signature is a *form* of an e-signature but the term cannot be used interchangeably with e-signature even though it falls within the ambit of e-signatures.[247]

In order for the accreditation authority to accredit an authentication service provider or certification service provider, the 'e-signature to which the authentication products relate must: (i) uniquely link the signatory to the e-signature; (ii) be capable of identifying that user; (iii) created using means that can be maintained under the sole

[239] Section 1: "certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with a data message.
[240] A digital signature is a form of e-signature that meets the requirement of an AES. This will be discussed under Heading 2.5.
[241] A Barofsky 'The European Commission's Directive on Electronic Signature: Technological "Favoritism" towards Digital Signature' (2000) 24(1) *Boston College International and Comparative Law Review* 145-160; Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.
[242] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-466.
[243] Van de Merwe (Note 217).
[244] Sabett (Note 237).
[245] Ibid.
[246] S Mason 'Electronic Signatures in Practice' (2006) 6(2) *Journal of High Technology Law* 148-164.
[247] Srivastava and Koekemoer (Note 242).

control of that user; and (iv) be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable; (v) is based on the face-to-face identification of the user.'[248] If the e-signature fails to satisfy these requirements, it will not be accredited.

The application for accreditation must be made by the authentication service provider and must be accompanied by all the relevant documentation pertaining to the 'identity of the authentication service provider, specifications of the product or service, the prescribed fee must be paid[249] and the completed application must be *hand-delivered* to the accreditation authority.'[250] If the applicant is a certification service provider (in addition to the aforementioned requirements), it must provide a 'practice statement and certificate policy that is drafted in accordance with ITU X.509 public key infrastructure and a declaration that it will be able to comply with its policy statement.'[251] These technical concepts will be dealt with in the next chapter. As indicated by the above regulations, the accreditation procedure is complicated, time-consuming, expensive and involves too much effort from authentication service providers.

The concept of the AES and the procedure for obtaining an AES has been criticised to a large extent. Firstly, the procedure for obtaining an AES is complicated, expensive and requires extensive and arguably undue effort by the applicant. This view is raised by Eiselen[252] and Swales.[253] Swales takes the view that the process for obtaining an AES brings with it an 'unnecessary layer of administration and costs.'[254]

It is unreasonable and impractical to expect an internationally used authentication service provider, who has provided secure and reliable authentication services for years, to make an application for accreditation, hand deliver his application to the accreditation authority and to ensure that he meets the requirement of face-to-face recognition. Furthermore, since 2011 only two authentication service providers have

[248] Section 38 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[249] The fee is in the sum of twenty thousand rand for each authentication product or service provided by the authentication service provider. This is in accordance with Regulation 29.
[250] Regulation 7 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[251] Ibid.
[252] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.
[253] L Swales 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.
[254] Ibid.

been accredited.[255] The process has been completely ignored by most authentication service providers and commercial users of e-signatures. In his article, Snail mentions that 'e-signatures would have to be explored and the legislature may have to do away with the stringent requirements of AESes.' [256] This indicates that there was some foresight by academics and practitioners in respect of the non-use of AESes and the difficulties that would be experienced due to the stringent requirements.

The second criticism against ECTA in this context is that its regulations infringe on the e-commerce principle of technological neutrality. Technological neutrality means the law should not regulate the use of technology in a discriminative way.[257] Technology develops continuously and if the law regulates it too stringently then its development would be stifled. This could prevent valuable and innovative methods of practicing commerce from entering the business world. It would be a tremendous loss for society. Furthermore, if South Africa is transacting with the technologically advanced nations, it needs to be conversant with technology.

While ECTA does not directly prescribe the use of digital signatures, the requirements imposed by section 37 prescribes cryptography. This is the only known method that would allow the signatory to maintain control of the contents[258] of the documents and detect any changes[259] to the document.[260] The implication of these requirements is that the only reliable e-signature is the digital signature. Snail[261] argues that biometrics would not meet the requirements of an AES even though it is just as reliable if not more reliable than an AES.[262] The indirect prescription of technology by ECTA needs to be reconsidered.

2.5. Forms of E-Signatures

As mentioned earlier, a person's signature is his way of representing his acceptance of terms or conditions contained in a document. Commercial transactions requiring

[255] According to the Accreditation Authority website that can be accessed at http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-28-29.html.
[256] Snail, S 'Electronic Contracts in South Africa – A Comparative Analysis' 2008 (2) *Journal of Information, Law & Technology* 1-24.
[257] Kamecke U, T Korber 'Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood' (2008) 29(5) *European Competition Law Review* 330-337.
[258] Section 37 (1) (iii) of the Electronic Communications and Transactions Act 25 of 2002.
[259] Section 37 (1) (iv) of the Electronic Communications and Transactions Act 25 of 2002.
[260] A Barofsky 'The European Commission's Directive on Electronic Signature: Technological "Favoritism" towards Digital Signature' (2000) 24(1) *Boston College International and Comparative Law Review* 145-160.
[261]
[262] S Snail 'Electronic Contracts in South Africa – A Comparative Analysis' 2008 (2) *Journal of Information, Law & Technology* 1-24.

formality in the form signatures now take place on an electronic level. Therefore, e-signatures are used to validate or assent to terms of commercial transactions. Various forms of e-signatures have developed, some of which are still in their infancy.

This section of the chapter deals with the different forms of e-signatures and the level of security they provide. A discussion on the different forms of e-signatures is necessary to understand the development in technology in respect of authentication and identification methods and to determine whether the law is abreast with the current e-signature methods.

2.5.1. E-Signatures in General

According to ECTA, 'data is an electronic representation of information.'[263] Section 2 of ECTA defines an e-signature as 'data incorporated in, connected to or logically associated with other data'. Thus, it can be deduced that the e-signature is data used by an individual to assent to terms or conditions. Any symbol, mark or unique attribute of an individual used for the purpose of indicating his intention falls within the definition of an e-signature.[264] This includes digital signatures and biometrics, which are discussed below.

In practice, individuals usually sign documents electronically by placing a scanned version of their signature at the end of the document. This is referred to as a digitised signature and must not be confused with the digital signature.[265] However, both types of signatures are classified as e-signatures because they are either in electronic format or in the form of data. Typing out one's name at the bottom of an email can constitute a signature if it is placed with the requisite intention.[266]

Click-wrap and Web-wrap agreements require authentication in the form of clicking an 'I accept' icon. A Click-wrap agreement takes place over the internet. The terms and conditions of the agreement are available on the webpage and the user is required to view the terms and conditions before accepting them.[267] In order to accept the terms and conditions the user must click on the 'I accept' icon. Once the user clicks on the

[263] Section 1.
[264] *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA*) Paragraph 25.
[265] K Bharvada 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology* 267.
[266] *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA*).
[267] T Pistorius 'Click-wrap and web-wrap agreements' (2004) 16(4) *South African Mercantile Law Journal* 568.

acceptance icon he indicates his assent to the terms and conditions which result in the conclusion of a contract.[268] In a web-wrap agreement, assent to the terms of the website is *presumed* by the continued browsing on the web page.[269]

There are several types of software programs available for computers that enable individuals to formulate their own e-signatures. An example of this type of software includes *Microsoft Word* and *Adobe PDF* which gives the user an option to create an e-signature and attach it to the relevant document.

2.5.2. Biometrics

Biometrics is described as a 'unique behavioural attribute or physical attribute of a person'[270] that can be extracted and stored on a database and can be used to verify the identity of a person.[271] The characteristics of biometrics make it suitable to be used as a signature. These characteristics can identify a person by the uniqueness of his behavioural or physical attribute.

There are two types of biometric systems, namely verification systems and identification systems.[272] Verification systems are more commonly used.[273] A sample of the attribute is taken from an individual for his enrolment on the biometric system.[274] The characteristics of the sample is stored on a database.[275] The sample will also be stored on a template given to the user, usually in the form of a smartcard.[276] The sample is given a reference number or code. The user would usually swipe his smartcard or enter a reference number claiming to represent a certain individual. The system will read the information from the smartcard and will require the user to enter his biometric signature onto the system.[277] The system will compare the live sample of the user with the biometric data stored on the system's database.[278] The system will then verify or deny the identity of the individual.[279]

---

[268] Ibid.
[269] Pistorius (Note).
[270] K Bharvada 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology* 269.
[271] J Ashbourne *Biometrics: Advanced Identity Verification: The Complete Guide* 2ed (2014).
[272] Ibid.
[273] Ashbourne (Note 271).
[274] Ibid.
[275] Ashbourne (Note 271).
[276] Ibid.
[277] Ashbourne (Note 271).
[278] Ibid.
[279] Ashbourne (Note 271).

In a practical situation, a sample for enrolment can be taken from the user using an electronic device. The user can sign on the screen of his tablet using a stylus or manual signature. The geometrics of the signature will be recorded on the system. In the event the user wishes to transact with the party that holds the biometric system, he can verify his identity by using his biometric signature.

Facial recognition, geometrics, iris scan and many other attributes can be used as signatures.[280] Biometrics is one of the most reliable forms of e-signatures that can be used but are not commonly used because they are expensive.[281] Even though biometrics score higher than most other forms of e-signatures in respect of its reliability, it does not prevent situations of duress and undue influence when signing a document.

There has been discussion on including Biometrics as form of an e-signature in ECTA.[282] Submissions have been made to include this form of e-signature due to the high standard of reliability of this type of technology.[283] Although Biometrics is an advanced method of signing, it will not be given the status of an AES because it is not based on cryptography as required by ECTA.[284] This is problematic because the concept of an AES seems to be restricting the type of technology that could promote e-commerce. Furthermore, this kind of restriction conflicts with the principle of technological neutrality, which is one of the objectives of ECTA under section 2 (f).[285]

2.5.3. Digital Signatures

The digital signature is a specific type of e-signature that uses cryptography and public key infrastructure ("PKI") technology. Cryptography is dependent on PKI technology. PKI technology 'creates analogs in the digital world that represents symbols used in real world but with more security mechanisms than the real world.'[286] Cryptography further involves encryption or encoding of data from plain text into cipher text.[287] PKI technology allows for data messages to be encoded in this manner.

---

[280] K Bharvada 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology* 269.
[281] Ibid.
[282] South African Law Reform Commission: Discussion Paper 131: *The Review of Law of Evidence* (2015).
[283] Ibid.
[284] SALRC (Note 282).
[285] View shared among many authors including: Swales (Note 53); Srivastava (Note 242); Eiselen (Note 53)
[286] R Sabett 'Effects of Technology Convergence and Public Key Infrastructure' (1999) 7(2) *University of Baltimore Intellectual Property Law Journal* 143-154.
[287] DP Van der Merwe … et al *Information Communications Technology Law* 2 ed (2016) 155-156.

In order for a digital signature to be created, a certification authority will create a certificate and issue it to the subscriber. Once the subscriber accepts the certificate, he may create the digital signature by encrypting the message using a private key that he holds.[288] The recipient will receive the signed-encrypted message with the certificate.[289] The public key is available online and is used by the recipient to decrypt the message.[290] The certificate provides the recipient with assurance that the signature has been signed by the sender.[291] The options to create a digital signature and to encrypt a message are available on the internet and the software required is usually purchased and installed onto the user's computer.

The digital signature goes beyond the functional equivalent approach of the traditional signature because it provides evidence relating to the identity of the signatory and can also detect any alterations that have been made to the message.[292]

The process of obtaining a digital signature and encrypting a message is a secure method of concluding a contract and is as easy as clicking the options. However, in South Africa, the matter is complicated due to the requirements involved in obtaining a certificate, which can only be issued by the certification authority. In South Africa, this authority lies with the Department of Communications and there are several requirements that need to be complied with before a certificate is issued to the subscriber.[293]

2.6. Conclusion

ECTA has been drafted with much influence from UNCITRAL and the EC Directive with respect to its provisions on e-signatures and AESes. There has not been much case law dealing with ECTA's provisions on e-signatures.[294] This suggests that ECTA is functioning well as enabling legislation.[295] However, it could be an indication that ECTA's provisions are not sufficiently used. This could be attributed to the cumbersome and expensive nature of the accreditation procedure.

---

[288] Sabett (Note 286).
[289] Ibid.
[290] SE Blythe 'Digital Signature law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in e-commerce with enhanced security' (2005) 11(2) *Richmond Journal of Law and Technology* 1-20.
[291] Sabett (Note 286).
[292] S Mason 'Electronic Signatures in Practice' (2006) 6(2) *Journal of High Technology Law* 148-164.
[293] Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[294] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820
[295] Ibid.

Some of the objects of ECTA are to promote and facilitate e-commerce in South Africa.[296] One of the ways ECTA has attempted to achieve these objects is by adopting a functional equivalent approach to electronic communication and transactions. This means that legal recognition is given to electronic transactions in the same way as paper-based transactions.[297]

There are some concerns regarding ECTA's provisions on e-signatures that will hinder the growth and development of e-commerce.[298] Firstly, ECTA seems to prescribe standards and technology for the use of an AES and this amounts to infringement of the principle technological neutrality.[299] Prescriptive standards could potentially delay the development of e-commerce. Secondly, the procedure for accreditation prescribed by ECTA is impracticable, expensive, involves too much effort on authentication service providers and is prohibitively expensive.[300] This is evidenced by the fact that only two authentication service providers have been accredited since ECTA's enactment.[301] These issues need to be dealt with in order for ECTA to achieve its stated objectives.

[296] Section 2 of ECTA.
[297] T Pistorius 'Nobody knows you're a dog: Attribution of data messages' (2002) 13(4) *South African Mercantile Law Journal* 738.
[298] Eiselen (Note 294).
[299] Ibid.
[300] Eiselen (Note 294).
[301] Ibid.

3. Chapter Three: The South African Accreditation Process and the Principle of Technological Neutrality

3.1. Introduction

ECTA incorporates some of the principles of e-commerce in its provisions.[302] These principles have been adopted from UNCITRAL's Model Law on E-Commerce.[303] The lack of case law regarding suggests that it is functioning smoothly. [304] However, the concerns about ECTA's provisions on e-signatures requires reform.[305]

As discussed in the previous chapter ECTA has adopted a two-pronged approach to e-signatures.[306] The concern lies in the process of obtaining an AES. It has been argued that the process is cumbersome and expensive[307] and conflicts with the fundamental e-commerce principle of technology neutrality.[308]

This chapter discusses the principle of technological neutrality and whether ECTA applies this principle in its provisions. The accreditation process is also discussed in relation to ECTA's objects and principles of e-commerce.

3.2. E-Commerce and the principle of Technological Neutrality

3.2.1. Securing E-Commerce

E-Commerce is an important component of international trade and commerce.[309] It can increase a country's contribution to global trade by the use of innovative methods of transacting that 'reduce paperwork, time and cost' allowing more commercial

[302] The principle of functional equivalence is incorporated in chapter 3 of ECTA; to promote technological neutrality is one the objects of ECTA stated under section 2 (1) (f).
[303] United Nations Commission on International Trade Law Model on Electronic Commerce: Guide to Enactment Part E; Promoting Confidence in Electronic Commerce Legal on International Use of Electronic Authentication and Methods (2007).
[304] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.
[305] SAAA website reveals only two authentication service providers accredited. This indicates AESes are not widely used in South Africa and the law is not consistent with current practice. Secondly, section 13 of ECTA is technologically prescriptive which is inconsistent with the objects of ECTA under section 2 (1) (f).
[306] Eiselen (Note 54)
[307] Ibid.
[308] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.
[309] N Ewelukwa 'Is Africa Ready for E-Commerce – A Critical Appraisal of the Legal Framework for E-Commerce in Africa' (2011) 13 (3) *European Journal of Law Reform* 550-576.

transactions to take place.[310] Increased trade contributes to growth and development, especially in the context of developing and least developed countries.[311]

E-Commerce is also beneficial to consumers and suppliers. Consumers have the advantage of purchasing goods without the issue of unavailability.[312] Furthermore, consumers are exposed to a wide variety of goods and prices of goods can be compared before a purchase is made.[313] This allows consumers to make a more informed choice when purchasing goods. E-Commerce on an international scale also benefits suppliers by enabling their global presence.[314] It also 'encourages better standards, prices and offers a more tailored service to consumers'.[315]

Considering the importance of e-commerce in increasing business and market efficiency and its overall impact on growth and development of economies,[316] it is necessary to ensure that there are no barriers that will reduce the efficiency and momentum of commercial transactions.

E-commerce requires the use of information and communication technology but one of the greatest concerns of its use *is* information security.[317] ECTA's attempt to build confidence and trust in consumers in relation to electronic transactions is setting standards and procedures to ensure the security of user information over the internet.[318] Van der Merwe[319] takes the view that these standards are of great importance in relation to information security.

The accreditation procedure required by section 13(1) of ECTA is one of the procedures prescribed to ensure the integrity and authenticity of electronic

[310] Ibid.
[311] Ewekulwa (Note 309).
[312] ZN Jobodwana 'E-Commerce and M-Commerce in South Africa: Regulatory Challenges' (2009) 4(4) *Journal of International Commercial Law and Technology* 287-298.
[313] Ibid.
[314] Jobodwana (Note 312).
[315] Ibid.
[316] D Ndonga 'E-Commerce in Africa: Challenges and Solutions' (2012) 5 (3) *African Journal of Legal Studies* 243-268.
[317] R Dagada, M Eloff, LM and Venter LM 'Too many laws but very little progress! Is South African highly acclaimed information security legislation redundant?' (2009). Accessed at http://scholar.google.co.za/scholar?hl=en&q=Dagada%2C+R.%2C+Eloff%2C+M.M.+and+Venter%2C+L.M.%2C+2009.+Too+many+laws+but+very+little+progress%21+Is+South+African+highly+acclaimed+information+security+legislation+redundant%3F.&btnG=&as_sdt=1%2C5&as_sdtp=
[318] Coetzee J 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' 2004 15 (3) *Stellenbosch Law Review* 501.
[319] DP Van der Merwe 'A Comparative Overview of the (Sometimes Uneasy) Relationship between Digital Information and Certain Legal Fields in South Africa and Uganda' (2014) 17(1) *Potchefstroom Electronic Law Journal* 296-326.

communication.[320] Furthermore, in order for the criteria of accreditation[321] to be met cryptography[322] must be used as this is the only known technology that can satisfy the criteria.[323] ECTA, therefore, provides the standard or mechanism for PKI cryptography to be used. This standard is referred to as *SANS 21188.* SANS 21188[324] has been adopted by South Africa to assist in the integration of international transactions by unifying and harmonising standards to remove the obstacles to international transactions.[325] SANS 21188 consists of a framework of policy requirements and standards for the use of digital signatures. It also assists with the implementation of PKI technology in respect of digital signatures to ensure the use of PKI is in line with the international best practice.[326] Thus, SANS 21188 complies with international standards and regulations.[327]

Adopting an international standard provides certainty about the level of security measures used in comparison to the global standard. If these standards or similar standards are used by technologically advanced jurisdictions it can assist in building trust amongst users of e-commerce in South Africa.

Another standard that ECTA has adopted is in respect of certificates that are issued by certification providers.[328] This is referred to as the *ITU X509* standard and is the 'most fundamental standard or structure of a digital certificate'.[329] Complying with this standard enables users to verify the certificates and ensure the legitimacy of the certification provider.[330] These standards afford minimum level protection to users and are necessary to improve the confidence in the use of electronic communication.[331]

ECTA attempts to achieve some of its objects: to 'promote legal certainty and confidence in the use of electronic communications',[332] 'to ensure compliance with

[320] S Papadopolous & S Snail *Cyberlaw@SA III: The law of the internet in South Africa* 3 ed (2012).
[321] Section 38 of ECTA.
[322] Refer to heading 2.4.3 under chapter 2.
[323] DP Van der Merwe … et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[324] Regulation 1 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[325] 'Establishing E-Commerce in South Africa: Information from the South African Bureau of Standards' (2006) accessed at *www.ee.co.za/wp.../Establising%20e-commerce%20in%20South%20Africa.pdf.*
[326] Ibid.
[327] Establishing E-Commerce in South Africa: Information from the South African Bureau of Standards' (2006) accessed at *www.ee.co.za/wp.../Establising%20e-commerce%20in%20South%20Africa.pdf*
[328] Regulation 1 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[329] E Gerck 'Overview of Certification Systems: X. 509, PKIX, CA, PGP & SKIP' (2000) 1(3) *The Bell* 8.
[330] Ibid.
[331] R Andrews 'Electronic Commerce: Lessons Learned from the European Legal Model' (2005) 9(2) *Intellectual Property Law Bulletin* 81-94.
[332] Section 2(1) (e) of ECTA.

international technical standards'[333] and 'to remove barriers to e-commerce'.[334] However, ECTA's attempt to achieve its objects has brought about other concerns regarding the *neutrality* of its e-signature provisions.

Technological neutrality is an underlying principle of e-commerce and is relevant when drafting law to regulate technology.[335] There is consensus amongst scholars that ECTA is prescriptive about the use of technology.[336].

3.2.2. Information and Communication Technology Regulation

Regulation can be defined as 'restrictions imposed to control societal behaviour.'[337] The type of regulation that is drafted is dependent on the legislature's goal. In the context of technological regulations, the legislature may seek to influence the behaviour of individuals in respect of: the usage of technology; the 'online and offline equivalence' of technology and the extent to which technology should be used.[338] Generally, the development of society in relation to technology will determine the appropriate legislative approach to be taken.[339]

The principle of technological neutrality is a guiding principle applied in the process of drafting technological regulation.[340] The principle states that 'the law should not favour any particular type of technology neither should it discriminate against any type of technology.'[341] This approach is applied more stringently depending on the developmental needs of the society.

UNCITRAL[342] provides the three approaches to technological neutrality these are: the minimalist approach (technological neutrality); the technologically specific approach and the two-pronged approach.

[333] Section 2(1) (h) of ECTA.
[334] Section 2(1) (d) of ECTA.
[335] United Nations Commission on International Trade Law: Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods (2009).
[336] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[337] BJ Koops 'Should ICT Law be Technology-Neutral' (2006) *IT & Law Series* 77-108.
[338] Ibid.
[339] Koops (Note 337).
[340] C Reed 'Taking sides on technology neutrality' (2007) 4(3) *SCRIPT-ed* 263-284.
[341] U Kamecke, T Korber 'Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood' (2008) 29(5) *European Competition Law Review* 330-337.
[342] United Nations Commission on International Trade Law: Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (2009).

3.2.2.1. The Technologically Neutral Approach ("Minimalist Approach")

The minimalist approach provides the minimum requirements for legal recognition of e-signatures.[343] This approach aims to achieve functional equivalence between e-signatures and manuscript signatures.[344] This approach does not prescribe or suggest any particular type of technology to be used.

UNCITRAL[345] uses a minimalist approach in respect of e-signatures.[346] Article 6 of the 1996 Model Law states that a data message will be given legal recognition as a manuscript signature if a 'method that is appropriate and reliable for the purposes of the transaction is used.' UNCITRAL does not provide any further requirements to satisfy article 6. However, it does provide a set of criteria to establish reliability of the authentication method used. This criteria is similar to the *mandatory* criteria listed in ECTA to obtain an AES but the former does not contain the requirement of face-to-face recognition.

Technologically neutral legislation is conducive to a technologically developing environment and fosters innovation.[347] This means technology can develop without being restricted by outdated law that previously applied to specific technology. Thus, technologically neutral legislation allows the law to remain sustainable and to prevent frequent amendments to the law.[348] Another advantage of this approach is it prevents the delayed response of the law to the development of technology. In other words it prevents the law from becoming meaningless.[349]

Some authors strongly oppose a technological neutral approach to regulation. Greenberg[350] takes the view that technological neutrality is not a favourable approach. The difficulty of this approach is the unpredictability of a developing technological environment.[351] Innovation and development of technology does not occur in a linear manner where the type of change can be foreseen.[352] There is much uncertainty about

[343] Ibid.
[344] UNCITRAL (Note 342).
[345] United Nations Commission on International Trade Law Model on Electronic Signatures with Guide to Enactment (2001).
[346] Koops (Note 337).
[347] C Spyrelli 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) *Journal of Information Law and Technology* accessed at *http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html.*
[348] Koops (Note 337).
[349] Ibid.
[350] B Greenberg 'Rethinking Technological Neutrality' (2016) 100(4) *Minnesota Law Review* 1495-1562.
[351] Ibid.
[352] Greenberg (Note 350).

whether 'technologically neutral law will promote or undermine the law's policy goals.'[353]

Another disadvantage of technologically neutral law is it may bring about an interpretative challenge.[354] The language used in drafting the law may not speak clearly to the advancements in technology.[355] This would result in uncertainty in the application of the law. The *neutral* approach of the e-signature law addresses the functional requirements of e-signatures. Provided the essential requirements of the traditional manuscript signature are satisfied the method used is irrelevant. There is no reason why technologically neutral law would not speak clearly to future developments in e-signature law.

3.2.2.2. The Technologically-Specific Approach

The technologically-specific approach to e-signatures is concerned with providing the highest levels of security to users.[356] This assists by creating confidence and certainty of users of e-signatures.[357] This approach is used in the EC Directive.[358] At the time the EC Directive was drafted, e-commerce was still in its infant stages and the aim of achieving confidence of users of e-commerce was of great importance. Therefore, it is understandable that this approach was part of the EC Directive.[359]

The EC Directive adopted the concept of the AES and sets out the criteria to be satisfied for the e-signature to obtain the AES status. The criteria can only be satisfied if cryptography is used.[360] This provision[361] in the EC directive is technologically-specific because it favours cryptography over other forms technology.[362] Although cryptography is one of the most reliable methods of ensuring authenticity and integrity

[353] Ibid.
[354] Greenberg (Note 350).
[355] Ibid.
[356] United Nations Commission on International Trade Law: Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (2009).
[357] R Andrews 'Electronic Commerce: Lessons Learned From the European Legal Model' (2005) 9(2) *Intellectual Property Law Bulletin* 81-94.
[358] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[359] C Spyrelli 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) *Journal of Information Law and Technology* accessed at *http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html.*
[360] DP Van der Merwe … et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[361] Article 2: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[362] DP Van der Merwe … et al *Information Communications Technology Law* 2 ed (2016) 155-156.

of electronic communications,[363] prescribing this particular type of technology may 'prevent superior and advanced technologies from entering the market.'[364]

Another disadvantage of adopting a technologically-specific approach is in some instances parties do not require such high standards of security for the purposes of their transaction.[365] The party may be relying on the electronic communication for the reasons that it is quick and inexpensive. However, obtaining an AES is costly, time-consuming and involves too much effort which would defeat the purposes for which e-commerce is used.[366]

The common view shared amongst authors is applying a technologically-specific approach in the present technological age would hinder the development of technology because it is not flexible.[367] Reed[368] takes the view that a technologically specific approach can only be adopted if the new technology has entered the market.[369] His view suggests a technologically-specific approach is inappropriate for the present technology used in e-commerce, which has been in existence for almost two decades.

3.2.2.3. The Two-Pronged Approach

The two-pronged approach to e-signatures comprises of two sets of requirements. The first set of requirements are low threshold requirements that e-signatures would need to satisfy for legal recognition.[370] This seeks to achieve a functional equivalent approach to traditional manuscript signatures. [371] The second set of requirements are more stringent.[372] If these requirements are met, the e-signature will obtain the legal status of an AES which is not just legally recognised but also has a higher evidential value.[373]

[363] Koops (Note 337).
[364] UNCITRAL (Note 356).
[365] Ibid.
[366] C Reed 'Taking sides on technology neutrality' (2007) 4(3) *SCRIPT-ed* 263-284.
[367] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820; L Swales 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.
[368] Reed (Note 366).
[369] Ibid.
[370] United Nation Commission on International Trade Law (Note 356).
[371] Ibid.
[372] United Nation Commission on International Trade Law (Note 356).
[373] Ibid.

This approach would be adopted by legislatures who wish to satisfy two regulatory functions. Firstly, it provides flexibility to allow users to choose the type of e-signature that is appropriate for their use.[374] Secondly, the approach provides a more secure environment for electronic transactions to take place.[375] The two-pronged approach strives to achieve legal certainty and security, and at the same time leaves room for development of technology.[376]

'ECTA has seemingly adopted the two-pronged approach to e-signatures.'[377] ECTA's provisions on e-signatures have been adopted from the UNCITRAL model laws[378] and the EC directive.[379] In applying ECTA's provisions, the outcome appears to be technologically specific.

ECTA adopts the functional equivalent approach to e-signatures from UNCITRAL.[380] According to section 13 (3) of ECTA 'when parties to a transaction require an e-signature the requirement is met in relation to a data message if the method used is reliable and appropriate for the purpose of the transaction'.[381] Article 7(1) of UNCITRAL[382] requires the same as in ECTA. However, UNCITRAL's provision applies when the *law* requires a signature whereas ECTA's provision applies when *parties* decide on the use of a signature.

Article 6(3) of UNCITRAL's Model on E-Signatures[383] provides a presumption of the reliability of e-signatures.[384] The criteria listed under article 6 (3) of UNCITRAL essentially refers to a *digital signature* as being presumed to be reliable.[385] This does not mean that UNCITRAL's Model Law on E-Signatures is prescriptive because 'article 6(3) is a presumption not a requirement for validity.'[386]

[374] United Nation Commission on International Trade Law (Note 356).
[375] Ibid.
[376] United Nation Commission on International Trade Law (Note 356).
[377] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.
[378] United Nation Commission on International Trade Law: Model Law on E-Commerce (1996).
[379] Eiselen (Note 53).
[380] Article 7 of United Nation Commission on International Trade Law: Model Law on E-Commerce (1996).
[381] Section 13 (3) of ECTA.
[382] United Nation Commission on International Trade Law (Note 356).
[383] United Nation Commission on International Trade Law: Model Law on Electronic-Signatures (2001).
[384] Article 6 (3) of United Nation Commission on International Trade Law: Model Law on Electronic-Signatures (2001).
[384] United Nation Commission on International Trade Law: Model Law on Electronic-Signatures (2001).
[385] Eiselen (Note 54).
[386] Ibid.

ECTA's provision on e-signatures is argued to be vague and ambiguous because it does not define the meanings of reliable and appropriate.[387] In this instance one would be obliged to consult with the guidelines provided by UNCITRAL.[388] The presumption suggests that an e-signature will be presumed to be reliable if a digital signature is used.[389] The criteria for the presumption suggest a *digital signature* is presumed to be valid.[390] The justification for this is the digital signature is one of the most reliable methods of authentication.[391]

ECTA has adopted the concept of an AES from the EC directive.[392] Article 2[393] of the EC directive is similar to the requirements set out in section 38[394] of ECTA except for the requirement of section 38 (1) (e) which is ECTA's addition to the EC directive provision on AESes. An AES can only be obtained if these requirements are met.[395] ECTA mirrors the EC Directive in relation to AESes and is also prescriptive of technology.[396] ECTA's approach to e-signatures is not widely supported or adopted due to the potential stifling effects on technological development.[397]

3.3. The Accreditation Procedure and Requirements

3.3.1. General

[387] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.
[388] United Nation Commission on International Trade Law: Model Law on Electronic-Signatures (2001).
[389] Srivastava and Koekemoer (Note 387).
[390] Ibid.
[391] Srivastava and Koekemoer (Note 387).
[392] Eiselen (Note 63).
[393] Article 2: 'An advanced electronic signatures means an electronic signature which meets the following requirements:
(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
[394] Section 38 (1) of ECTA: The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate-
(a) is uniquely linked to the user;
(b) is capable of identifying that user;
(c) is created using means that can be maintained under the sole control of that user; and
(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable.
[395] Regulation 5 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007
[396] Snail, S 'Electronic Contracts in South Africa – A Comparative Analysis' 2008 (2) *Journal of Information, Law & Technology* 1-24; DP Van der Merwe … et al *Information Communications Technology Law* 2 ed (2016) 155-156;
[397] C Spyrelli 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) *Journal of Information Law and Technology* accessed at *http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html.*

The principle of technological neutrality has clearly been contravened by ECTA's e-signature provisions.[398] Reed[399] suggests that technological neutrality can be achieved if technology that does not comply with the prescriptive law is modified to comply.[400] The author believes there is no unbreakable barrier that prevents law from being adapted to technological change.[401] While this may be case, ECTA still requires reform in respect of the accreditation procedure.

ECTA's attempt at promoting confidence in the use of electronic communications has been discussed above. In addition to prescribing standards for the use of technology ECTA has also made provision for an accreditation procedure. This procedure is a requirement for obtaining an AES.[402]

An e-signature or authentication product must be accredited to obtain the status of an AES.[403] An authentication service provider's failure to accredit his AES will not grant even the most superior technology the status of an AES. The outcome product of the accreditation procedure is a digital signature which has the status of being advanced and has higher evidential weight than ordinary e-signatures.[404]

Although the outcome of the accreditation procedure is desirable many authors feel the procedure conflicts with ECTA's objective of facilitating e-commerce through the removal of technical barriers.[405] The procedure is contained in ECTA's regulations on accreditation.[406]

The South African Accreditation Authority ('SAAA') lies with the Director General of the Department of Communication and to his employees.[407] The authentication service provider must submit the application to the accreditation authority with all the required documents.[408] Once the SAAA receives the application for accreditation and is satisfied that it is compliant with ECTA and the regulations, it will issue a certificate to the applicant.[409] The certificate provides assurance that the authentication product

[398] Srivastava and Koekemoer (Note 387).
[399] Reed (Note 366).
[400] Ibid.
[401] Reed (Note 366).
[402] Section 13 (3) of ECTA.
[403] S Papadopolous & S Snail *Cyberlaw@SA III: The law of the internet in South Africa* 3 ed (2012) 318.
[404] Srivastava and Koekemoer (Note 387).
[405] Eiselen (Note 54); Swales (Note 59).
[406] Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[407] Section 34 of ECTA.
[408] Regulation 8.
[409] Regulation 10(1)(d)

used to authenticate the document is from a reliable source and confirms the identity of the user of that product.[410]

3.3.2. Criteria for Accreditation

The criteria that must be satisfied in order for the authentication product to be accredited are the e-signature: 'must be uniquely linked to the signatory, must identify the signatory, must be under the sole control of the signatory; must detect any alterations made subsequent to use and the e-signature must be based on face-to-face recognition.'[411]

The intention of the first two requirements under the section are to assure the recipient of the e-signature of the identity and authenticity of the signatory of the document. The second two requirements relate to the integrity of the information contained within the document. This illustrates that the AES goes a step further than the functional equivalent approach and provides measures pertaining to the reliability of the information in the document.[412]

The requirement pertaining to face-to-face recognition allows the SAAA to confirm the identity of the service provider of the e-signature.[413] This serves to provide the SAAA with additional information for consideration before it accredits a product. This requirement is not used by UNCITRAL[414] or the EC directive.[415] Although this requirement will allow for a more informed decision in respect of accreditation, it is extremely unrealistic and impractical. It is unnecessary for an internationally renowned authentication service provider to make an application to the SAAA to accredit their product.[416]

[410] Jøsang and Tran 'Trust management for e-commerce' (2000) *Virtual Banking*.
[411] Section 38(1) (a) – (e) of ECTA.
[412] J Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' 2004 15 (3) *Stellenbosch Law Review* 501-
[413] Jøsang & Tran. 'Trust management for e-commerce' *Virtual Banking* (2000).
[414] United Nation Commission on International Trade Law: Model Law on E-Commerce (1996).
[415] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
[416] Eiselen (Note 54); Swales (59).

3.3.3. Manner of Application

An authentication service provider must obtain an application form for accreditation. This can be obtained from the SAAA website.[417] The Regulations require the form to be completed and *hand delivered* to the SAAA.[418] This seems to be another inconvenient aspect of the process and does not seem facilitative of electronic transactions. Hand delivering a document is time-consuming especially if the applicant's geographical location is not within region of the SAAA.

Some of the information required by the SAAA is a detailed declaration on the specifications and features of the authentication service provider's products.[419] Furthermore, the authentication service provider must pay a fee of R20 000 on each of the authentication products it applies to accredit.[420] One of the benefits of the e-commerce is it reduces costs of transacting. The imposition of a fee is contrary to this benefit of e-commerce and seems unreasonably high for an administration fee.

Another requirement that seems to be unduly burdensome is in respect of audit reports of the authentication service provider. According to regulation 10 (2), 'the authentication service provider must submit an audit report at the time of accreditation and annually thereafter.' The need an audit report annually seems unclear and nonetheless inconvenient.

The regulations do not prescribe time limits for which applications for accreditation will be granted or refused. Thus, it might be misleading to an applicant who wishes to have his product accredited in a matter of days. This could severely delay the smooth flow of e-commerce.[421]

Accreditation is too expensive and involves cumbersome administration.[422] E-Commerce has become prevalent due to its time-saving and cost-saving benefits. The imposition of such unduly burdensome requirements will not nurture the growth and efficiency of e-commerce because they conflict with the essential benefits of e-commerce.

[417] Accessed at *http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-30-50.html.*
[418] Regulation 8.
[419] Regulation 7.
[420] Regulation 29 (1).
[421] Eiselen (Note 54); Swales (Note 59).
[422] Ibid.

Most authentication service-providers have not used the accreditation procedure. This is evidenced by SAAA's website that reveals only two accreditations from the year 2011. This can be attributed to the high costs and complex nature of the procedure.[423] Pappas[424] suggests that lawmakers should avoid undue restriction and unnecessary requirements in their drafting of e-commerce legislation.[425]

Lawmakers should aim to support and enforce e-commerce laws that are predictable, minimalist and simple.[426] The need for security must be balanced with e-commerce facilitation.[427] Based on these considerations, the accreditation procedure must be reviewed to accommodate the consumer's needs for information security in a manner that facilitates e-commerce.

3.4. Conclusion

This chapter focused on some of the major concerns of South Africa's position on e-signatures. ECTA's threshold requirements for validity of e-signatures seems to favour cryptography as the appropriate technology that e-signatures should be based on.[428] This conflicts with the underlying e-commerce principle of technological neutrality.[429] It is understandable that at the time ECTA was drafted it was necessary to provide the highest level of security to users due to the uncertainties of e-commerce, which was in its infancy.[430] However, e-commerce has come a long way since ECTA's enactment and needs to be regulated in a manner that supports its growth and development. The current position is not supportive of this.

The other concern about South Africa's position in respect of e-signatures is the accreditation procedure prescribed by section 13 of ECTA. The procedure imposes unnecessary requirements on authentication service providers and is expensive.[431] The procedure has not been frequently used. Furthermore, the unduly burdensome

[423] Eiselen (Note 54); Swales (Note 59).
[424] C Pappas 'Comparative US and EU Approaches to E-Commerce Regulation' (2002) 31(2) *Denver Journal of International Law and Policy* 325-348.
[425] Ibid.
[426] Pappas (Note 424).
[427] Ibid.
[428] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.
[429] United Nations Commission on International Trade Law: Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (2009).
[430] Ibid.
[431] Eiselen (Note 54); Swales (Note 59).

requirements goes against the inherent advantages of e-commerce, namely, efficiency and cost reduction.[432]

[432] N Ewelukwa 'Is Africa Ready for E-Commerce – A Critical Appraisal of the Legal Framework for E-Commerce in Africa' (2011) 13 (3) *European Journal of Law Reform* 550-576

4. Chapter Four: International and Foreign Legal Framework on E-Signatures: A Comparative Analysis

4.1. Introduction

There is general consensus around the fact that there has been an increase in the use of e-commerce on an international scale.[433] Many jurisdictions, apart from South Africa, have enacted legislation to regulate e-commerce and more specifically e-signatures. The UNCITRAL model laws[434] and the EC Directive[435] on e-signatures have guided many jurisdictions in the manner and form of e-commerce and e-signature regulation, including South Africa. Both these international instruments have been drafted along the same lines with few exceptions regarding certification and accreditation of the authentication products and services.

The chapter considers approaches of other jurisdictions on e-signature law in an attempt to better understand the South African approach and possible reasons for South Africa's divergent approach in specific areas. The chapter briefly discusses the United Nations and the European Union's approach to e-signature law and the differences between the latter and the former. Furthermore, it analyses the approach to e-signatures in the United States, Australia and Germany and discusses the differences and similarities in the legislative approach between the aforementioned countries and South Africa.

The rationale for the comparative analysis is the common roots of the e-signature provisions shared between South Africa and the abovementioned jurisdictions. The EC Directive and Germany adopted similar e-signature provisions, which influenced South Africa's adoption of AESes and accreditation of e-signatures.[436] Secondly, UNCITRAL was heavily relied on by the US and South Africa in so far as the definition and functions of an e-signature but has differed to the extent that US has adopted a

[433] M Parmentier 'Legislative Developments' (2000) *Columbian Journal of European Law* 251.

[434] United Nations Commission on International Trade Law Model on Electronic Commerce: Guide to Enactment Part E accessed at *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.;* United Nations Commission on International Trade Law Model on Electronic Signatures with Guide to Enactment (2001).

[435] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures accessed at *https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf*

[436] Eiselen (Note 54).

technologically-neutral approach.[437] The US is one of the most technologically advanced countries[438] and it useful to consider its approach to e-signatures to identify the methods of regulation, which are conducive to a technologically advanced nation.[439]

Thirdly, Australia's approach to e-signatures is of interest because its law is often compared to South Africa's law. Australia has also undertaken to fully comply with UNCITRAL's approach in respect of e-signatures which is an approach of interest.[440]

4.2. UNCITRAL Model Laws: E-Commerce Model Law (1996) and E-Signature Model Law (2001)

As a result of the increasing electronic transactions taking place in the early 1990's and the legal uncertainty of the status and validity of electronic transactions, UNCITRAL formulated model laws to assist countries in enacting e-commerce legislation to assist countries to establish certainty.[441] One of UNCITRAL's objectives is harmonisation of e-commerce laws for facilitation growth and development of e-commerce.[442] In addition, UNCITRAL acknowledges the importance of the harmonisation of e-commerce laws for development of developing nations by promoting the trade integration of these countries.[443] Trade integration is necessary as it gives developing countries an opportunity to trade competitively.[444]

UNCITRAL formulated the Model Law on E-Commerce and later formulated a Model Law on e-signatures. The former was formulated in1996 with the primary aim of providing legal recognition for electronic contracting.[445] Article 7[446] of the 1996 Model Law on E-Commerce deals with the requirements for validity of electronic signatures

[437] Ibid.
[438] Swales (Note 59).
[439] Barofsky suggests that legislation that 'merely extends legal recognition to electronic signatures can best foster electronic commerce.' The US adopts this approach.
[440] Srivastava and Koekemoer (Note 428); Van der Merwe (Note 398); Swales (Note 59); Pistorius (Note 297).
[441] UNCITRAL (Note 429).
[442] Raymond AH & Lambert JB 'Technology. E-Commerce and Emerging Harmonisation: The Growing Body of International Instruments Facilitating and the Continuing Need to Encourage Wide Adoption' (2014) *International Trade and Business Law Review Journal* 419-441.
[443] Raymond & Lambert (Note 442).
[444] Ibid.
[445] United Nations Commission on International Trade Law Model on Electronic Commerce: Guide to Enactment Part E accessed at *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.*
[446] (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

in law. The provision allows any method to be used provided, the data message identifies the signatory and is reliable and appropriate for the purposes for which it was created.[447] It makes no mention of any type or form of e-signatures.[448] To supplement the 1996 Model Law on E-Commerce UNCITRAL formulated the Model Law on E-Signatures in 2001. This document provides more guidance on e-signatures.

UNCITRAL went further to remedy the situation of international electronic contracting and enacted the Convention on the use of Electronic Communication in International Contracts of 2005 ("the Convention").[449] Australia was one of the first countries to ratify the Convention and has undertaken to maintain all its e-commerce laws with the substantive provisions of UNCITRAL's model laws and the Convention.[450] Australia is one of the subjects of the comparative analysis due to its legislative efforts in the law of information, communications technology.[451] Thus, as a progressive nation it is relevant to understand its position to e-signature law and how it arrived at this position.

UNCITRAL's Model Law on E-Signatures follows a two-tiered approach to e-signatures.[452] This approach means functional equivalence is adopted on two levels. The first tier of functional equivalence suggests any type or form of e-signature may be used to electronically sign a document provided it serves the same function as a handwritten signature.[453] The second tier of functional equivalence deals with the security and reliability of e-signatures. The second tier under article 6 (3) of 2001 UNCITRAL model law provides criteria for reliability of an e-signature. If the criteria under article 6 (3) is satisfied it will be presumed that the e-signature used is equivalent to a handwritten signature in terms of its reliability and not merely its function.[454]

Article 2 of the 2001 model Law provides a definition of the e-signature. According to the definition an e-signature:

[447] SW Braley 'Why Electronic Signatures can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures' (2001) *Law and Business Review of the Americas* 439.
[448] Ibid.
[449] The Convention's provisions on e-signatures has the same effect of UNCITRAL's model laws and for the purpose of the discussion UNCITRAL's model laws and convention will be considered to follow the same approach.
[450]UNCITRAL webpage accessed at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.
[451] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 143.
[452] S Mason *Electronic Signatures in Law* 4ed (2012).
[453] Ibid.
[454] Ibid.

> *"is data in electronic form affixed to or logically associated with a data message and is used to identify the signatory and show his approval of the information contained within the data message."*[455]

This represents the functional equivalence of an e-signature to handwritten signatures.[456] Article 6 (1) of UNCITRAL's Model Law on E-Signatures deals with legal recognition of an e-signature. According to Article 6(1) an e-signature will be 'valid if it is reliable and appropriate for the purpose for which it was generated or communicated in light of all the circumstances.'[457] UNCITRAL's approach is technologically neutral[458] in respect of Article 6 as it does not prescribe any particular type of technology required in order to establish legal validity. However, Article 6 (3) provides a presumption for reliability of an e-signature.[459] The provision states an e-signature will be considered reliable and satisfying the requirements of Article 6 (1) if a certain criteria is met.[460]

The only known technology that can satisfy the criteria is a digital signature which uses PKI cryptography.[461] The provision favours a particular type of technology and is, therefore technology specific. However, the approach of UNCITRAL is different from ECTA because the latter requires the use of specific technology when the law requires an e-signature whilst the former permits the use of any method of electronically signing provided the method is reliable and appropriate for the purposes for which it was created. ECTA requires reform to this extent.

It is suggested that ECTA adopt UNCITRAL's approach to e-signatures which reflects a modern approach to e-signature law and is key to reducing the legal uncertainty of the law in international trade.[462] Australia and the US have adopted UNCITRAL's

---

[455] Article 2 of United Nations Commission on International Trade Law Model on Electronic Signatures with Guide to Enactment (2001).
[456] Discussed in chapter one.
[457] United Nations Commission on International Trade Law Model on Electronic Signatures with Guide to Enactment (2001).
[458] Discussed in chapter 3 under heading 3.2.1.1.
[459] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.
[460] (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
[461] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[462] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 444.

provision through adoption of the Convention.[463] The technologically neutral approach is essential for facilitation of e-commerce and is followed by some of the most technologically progressive nations such as, Australia and the US.[464]

The purpose of presumption in Article 6 (3) of UNCITRAL's model law is to suggest a reliable method but does not make the suggested method compulsory for legal validity. UNCITRAL also makes no mention of an AES and therefore does not prescribe any costly, cumbersome or onerous procedure to ensure reliability of e-signatures. For this reason UNCITRAL's approach is favoured in comparison to the EC Directive.[465]

4.3. Foreign Legal Framework

4.3.1. Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community for electronic signatures ("EC Directive")

South Africa's approach in respect of AESes has been influenced by the approach of the EC Directive.[466] This adoption of this approach in South African law has been criticised largely for its technological specificity and the detrimental effects of prescriptive law on e-commerce.[467]

The EC Directive is a framework that provides guidance to European community[468] on the enactment of e-signature laws.[469] The purpose of the EC Directive is to unify the law of the European Community in order to facilitate cross border e-commerce transactions.[470] Ultimately, the EC Directive gives effect to the treaty establishing the European Union and the common internal market.

[463] Ibid.
[464] Srivastava and Koekemoer (Note 462).
[465] UNCITRAL is adopted by some of the most technologically advanced countries such as the US and Australia.
[466] Eiselen (Note 54).
[467] Ibid.
[468] within the European Union prescribed by the *Treaty establishing the European Community*.
[469] M Siems 'The EU Directive on E-Signatures: A Worldwide Model or a Fruitless attempt to Regulate the Future? (2002) 16(1) *International Review of Law, Computers & Technology* 7-22.
[470] Recital 4: Electronic communication and commerce necessitate ' electronic signatures' and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market; Parmentier (Note 1).

The EC Directive was drafted in consideration of the socio-economic needs and interests of the European Community, specifically.[471] This suggests the provisions of the directive may not operate in other regions as it does in the European Community because it considers the socio-economic dynamics of the European Community.

The EC Directive follows a similar approach to e-signatures as ECTA. Some authors argue it is technologically specific because it favours asymmetric cryptography.[472] Parmentier[473] postulates that the drafters of the EC Directive intended to restrict the minimum threshold for e-signature technology to PKI technology for ensuring future technologies remain secure. Many authors agree the EC Directive adopts a two-tiered approach to e-signatures.[474] However, the two-tiered approach in the EC Directive only recognises digital signatures as legally valid e-signatures.[475] Other forms of e-signatures are not prohibited from use but the law only recognises AESes. In contrast with UNCITRAL, the functional equivalent approach adopted by the EC Directive requires a higher level of security of e-signatures than UNCITRAL.[476]

The EC Directive defines an electronic signature very broadly which includes a wide variety of authentication and identification methods.[477] Only AESes which satisfy Article 5[478] of the EC Directive are considered to be equivalent to manuscript signatures.[479] The South African approach to e-signatures differ to the extent that an ordinary e-signature is equivalent to a manuscript signature and an AES is equivalent

[471] Recital 2.
[472] A Srivastava *Electronic Signatures for B2B Contracting: Evidence from Australia* (2013); Parmentier M 'Legislative Developments' (2000) *Columbian Journal of European Law* 251.
[473] Parmentier (Note 433).
[474] C Reed 'Taking sides on technology neutrality' (2007) 4(3) *SCRIPT-ed* 263-284; Srivastava A *Electronic Signatures for B2B Contracting: Evidence from Australia* (2013) and Reed C 'Taking sides on technology neutrality' (2007) 4(3) *SCRIPT-ed* 263-284.
[475] S Mason 'Electronic Signatures in Practice' (2006) 6(2) *Journal of High Tech. Law* 148-164.
[476] Stringent requirements imposed for obtaining an AES.
[477] J Schroers, B Van Alsenoy C Cuijpers 'Legal analysis of E-Signature services' (2015).
[478] (1) Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:
(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and
(b) are admissible as evidence in legal proceedings.
2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:
— in electronic form, or
— not based upon a qualified certificate, or
— not based upon a qualified certificate issued by an accredited certification-service-provider, or
— not created by a secure signature-creation device.
[479] SW Braley 'Why Electronic Signatures can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures' (2001) *Law and Business Review of the Americas* 439.

to a notarised manuscript signature.[480] However, the signatory who relies on the e-signature must prove its validity.[481]

Another difference in the approach of ECTA and the EC Directive in respect of e-signatures lies in the procedure for obtaining an AES. While EC Directive and ECTA both include the concept of the AES, in the former legal framework accreditation is not compulsory for legal recognition.[482]

According to the EC Directive, an e-signature will be legally recognised as an equivalent to a handwritten signature if it meets the requirements of a qualified certificate[483] and is created by a secure signature creation device.[484] Unlike the South African approach to e-signatures, obtaining the status of an AES is not dependant on accreditation but rather the criteria set out in the annexures to the EC Directive. This approach is less cumbersome and less expensive than the South African approach because accreditation is voluntary and is not required to be based on face-to-face recognition. This is an indication that the South African approach to AESes has not been carefully considered against the framework of e-commerce because it imposes requirements which are at odds with the development of e-commerce.

Recital 11[485] of the EC Directive permits voluntary accreditation. The rationale behind the voluntariness of accreditation is to allow market forces to develop the best

[480] R Sabett 'Effects of Technology Convergence and Public Key Infrastructure' (1999) 7(2) *University of Baltimore Intellectual Property Law Journal* 143-154.

[481] Eiselen (Note 54).

[482] EC Directive (Note 435); J Schroers , B Van Alsenoy C Cuijpers 'Legal analysis of E-Signature services' (2015).

[483] Annexure 1: Qualified certificates must contain: (a) an indication that the certificate is issued as a qualified certificate; (b) the identification of the certification-service-provider and the State in which it is established; (c) the name of the signatory or a pseudonym, which shall be identified as such; (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; (e) signature-verification data which correspond to signature-creation data under the control of the signatory; (f) an indication of the beginning and end of the period of validity of the certificate; (g) the identity code of the certificate; (h) the advanced electronic signature of the certification-service-provider issuing it; (i) limitations on the scope of use of the certificate, if applicable; and (j) limits on the value of transactions for which the certificate can be used, if applicable.

[484] Annexure 3: Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that: (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured; (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology; (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others. 2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

[485] (11) Voluntary accreditation schemes aiming at an enhanced level of service-provision may offer certification-service providers the appropriate framework for developing further their services towards the levels of trust, security and quality demanded by the evolving market; such schemes should encourage the development of best practice among certification-service-providers; certification-service-providers should be left free to adhere to and benefit from such accreditation schemes;

technological practice, as the principle of technological neutrality advocates.[486] The EC Directive promotes technological neutrality in Recital 4 by acknowledging accreditation to be a barrier to the development of commerce.[487]

The EC Directive was one of the international instruments that has guided ECTA's enactment of AESes. However, the approach in relation to the manner of obtaining an AES differs in ECTA to the extent that ECTA makes accreditation compulsory. Thus, ECTA's approach is more onerous and burdensome on authentication service providers who want their products and services to be legally recognised in a South African court of law. The reason for ECTA's adoption for accreditation is yet to be determined.

4.3.2. United States of America

The United States enacted the 'Electronic Signatures in Global and National Commerce Act ("The E-Sign Act") in 2000. This E-Sign Act operates on a federal level which means that all states must comply with the legislation.[488] The enactment of the E-Sign Act was a response to the immense number of commercial transactions taking place over the internet.[489] There was a serious concern as no laws regulated these electronic transactions.[490] This concern is dealt with by the E-Sign Act as well as the Uniform Electronic Transactions Act of 1999 ("UETA") which is operative at a state level.[491]

The aim of the E-Sign Act is 'to facilitate interstate and foreign e-commerce.'[492] It seeks to achieve its stated aim by providing for legal recognition of 'electronic records, electronic signatures and electronic contracts.'[493] According to this provision, written

[486] Ibid.
[487] Electronic communication and commerce necessitate ' electronic signatures' and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market.
[488] Buckley & Tank 'The Electronic Signatures in Global and National Commerce Act: An Overview' (2001) 20 *Annual Review of Banking Law* 221-241.
[489] Stern J 'The Electronic Signatures in Global and National Commerce' (2001) 6 *Berkeley Technology Law Journal* 391-414.
[490] Ibid.
[491] Buckley & Tank (Note 488).
[492] The Electronic Signature in Global and National Commerce Act (1999).
[493] Section 101(a) (2) of the Electronic Signature in Global and National Commerce Act (1999).

records and contracts are equivalent to the electronic records and contracts. E-Sign Act adopted the minimalist approach to e-signatures.[494]

According to the E-Sign Act an e-signature means 'any electronic sound or process logically associated with a contract or record and executed or adopted by a person with intent to sign the record.'[495] The definition of an e-signature under the E-Sign Act is completely technologically neutral and permits any method of signing provided the requisite intention is present.[496]

UETA was drafted by the National Conference of Commissioners of Uniform State Laws and was enacted around the same time as the E-Sign Act. UETA has similar objects to the E-Sign Act and many provisions of the both acts deal with the same substantive content. An e-signature under UETA is practically the same as it is under the E-Sign Act.[497] Section 7(c) of UETA simply states 'if a law requires a record to be in writing, an electronic record satisfies the law.'[498] The provision is broad and does not prescribe any form of technology for e-signatures.[499]

This approach does not distinguish between different types of e-signatures and legally recognises all types and forms of e-signatures provided the requisite intention to sign the document is present.[500] Furthermore, UETA and E-sign Act do not contain provisions giving additional evidential or legal weight to digital signatures based on cryptography.

Although a technologically specific approach may not align perfectly in a technologically developing world, the technologically-neutral approach adopted by the United States does not present itself without problems. Koger[501] suggests the approach is 'vague and lacks legal guidance.'[502] Stern[503] supports this view and adds that an absolute technologically neutral approach can create an unsafe environment

[494] Kisswani & Al-Bakri 'Regulating the Use of Electronic Signatures Given the Changing Face of Contracts' (2010) 7 *Macquarie Journal of Business Law* 53-65.
[495] Section 106 (5) of the Electronic Signature in Global and National Commerce Act (1999).
[496] Kisswani & Al-Bakri (Note 494).
[497] Section 2 (8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.
[498] Section 7 (c) of the Uniform Electronic Transactions Act (1999).
[499] Van der Merwe DP… et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[500] Kisswani & Al-Bakri (Note 494).
[501] JL Koger 'You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Contemporary Problems* 491-516.
[502] Ibid.
[503] J Stern 'The Electronic Signatures in Global and National Commerce' (2001) 6 *Berkeley Technology Law Journal* 391-414.

for consumers especially when inferior technologies are used. The minimalist approach more likely to induce fraud and interference with data integrity because there are no standards of security imposed in the use of e-signatures to protect user information and their online identity.[504] Furthermore, the lack of standards in the use of e-signatures may frustrate commerce by the United States transacting with countries that impose strict standards, such as the European community.[505] This is further complicated by the fact that the EU and the US are major trading partners.[506]

Another issue with the minimalist approach is evidentiary concern.[507] Under the South African approach in the event of a dispute, regarding the validity of an e-signature there is a rebuttable presumption that an AES is a valid signature.[508] Thus, it is clear the party alleging the AES is invalid must prove this. The US approach, however provides no guidance or presumption and it is the judiciary's responsibility to decide on the authenticity of the e-signature.

The minimalist approach is beneficial to the extent that it can foster innovation prevent law from becoming static.[509] However, there are some major disadvantages of the approach which could also create an obstacle to e-commerce.[510]

4.3.3. Germany

Germany was one of the first countries to enact e-signature legislation.[511] In 1997 the Law for Electronic Signatures ("SigG1997")[512] was enacted and it regulated digital signatures.[513] The SigG1997 was enacted to give legal recognition to e-signatures but only in the form of digital signatures.[514] The focus of SigG1997 is not on legal equivalency of e-signatures and handwritten signatures but rather on the secure use

[504] Koger (Note 501).
[505] Ibid.
[506] Koger (Note 501).
[507] Stern (Note 503) and Koger (Note 501).
[508] Section 13 of Electronic Communications and Transactions Act 25 of 2002.
[509] Koger (Note 501).
[510] Ibid.
[511] Schroers J, Van Alsenoy B Cuijpers C 'Legal analysis of E-Signature services' (2015).
[512] Gesetz zur digitalen signatur (SigG1997).
[513] A Digital signature is a specific form of e-signature that is based on public key cryptography which involves encryption of data messages by the sender and decryption by the recipient. It involves two sets of keys, one of encryption and the other for decryption. The digital signature is an advanced type of e-signature and can perform a number of functions. Digital signatures are discussed at length in chapter two of this paper.
[514] Shroers, Alesnoy & Cuijpers (Note 511).

of digital signatures.[515] Therefore, a technologically specific approach was adopted to overcome the unfamiliarity of the internet at the time.[516]

According to SigG1997, only digital signatures based on a qualified certificate and met the requirements of the Article 23[517] of SigG1997 would be legally equivalent to a handwritten signature.[518] It was the first country within the EU to enact legislation of e-signatures prior to the enactment of the EC Directive.[519]

After the EC Directive had been enacted, SigG1997 had been repealed by the German Electronic Signatures Act of 2001("ESA") to be in line with the EC Directive.[520] One of the most notable changes of the repealed act was the removal of the accreditation procedure for obtaining an AES.[521] Unfortunately, South Africa still maintains this position. Germany abolished the accreditation procedure at a time when e-commerce was still in stages of infancy and thus prevented a potential barrier to e-commerce as suggested by the EC Directive.[522]

The ESA follows a similar approach to e-signatures as ECTA. Section 2(1) of ESA defines an e-signature as 'data in electronic form attached to other electronic data or logically linked to electronic data and used for authentication.'[523] Sections 2(1) and 2(2) of ESA draw a distinction between an AES and a qualified AES. An AES is 'assigned only to one subscriber; capable of being identified as the subscriber; generated using a method under the sole control of the subscriber; and linked to the attached data so that any alteration of the data is detectable.'[524]

A qualified AES means 'an AES which is supported with a qualified certificate and generated with a secure signature creation device.'[525] The difference between an AES and a qualified AES is the latter is supported by a trusted third party which provides assurance that the signature creation device is secure and the user of the e-signature

[515] Barofsky (Note 439).
[516] Ibid.
[517] Same as Article 5 of the EC Directive.
[518] Ibid.
[519] C Bierekoven, P Bazin & Kozolowski 'Electronic Signatures in German, French and Polish Law Perspective' (2004) *Digital Evidence and Electronic Signature Law* 7-13.
[520] Bierekoven (Note 519) and S Blythe 'A Critique of German E-Commerce Law and Recommendations for Improvement' accessed at http://aabri.com/SA12Manuscripts/SA12045.pdf.
[521] Ibid.
[522] Recital 11.
[523] Section 2 (1) German Electronic Signatures Act (2001); Blythe (Note 529)
[524] Section 2 (1) of German Electronic Signatures Act (2001); Blythe (Note 529).
[525] Section 2 (2) of German Electronic Signatures Act (2001); Blythe (Note 529).

is identified.[526] This approach offers more security and reliability than the use of ordinary e-signatures but the prescriptiveness of the legislation may prevent superior and newer technology from entering the market.[527]

Under the old SigG1997, certification service providers had to be accredited by the German Minister of Telecommunications.[528] However the position has changed under ESA as certification service providers are no longer required to be accredited.[529] Accreditation is voluntary in accordance with the EC Directive.[530] Under ECTA, in order for an e-signature to obtain the status of an AES, it must be obtained through accreditation.[531] Consequently, South Africa's approach is relatively stringent in comparison to the German and the EC Directive approach.[532]

The difficulty with the South African approach lies in the accreditation procedure being compulsory for obtaining an AES which is the only legally recognised e-signature. The accreditation procedure has been criticised for hindering e-commerce due to the high cost and the additional time required to obtain an AES.[533]

Bierekoven, Bazin and Kozlowski[534] take the view that an AES offers a far more secure infrastructure than an ordinary e-signature which bears a much greater risk to be forged.[535] Therefore, the evidentiary weight must be distinguished between an ordinary e-signature and an AES. An AES is more than a tool for identification and thus cannot be equated to an ordinary e-signature. Bierekoven, Bazin and Kozlowski[536] support the distinction between the two types of signatures for evidentiary purposes. There has not been any evidence that the distinction has placed an obstacle to e-commerce. However, the divergent approaches of various jurisdictions

[526] A Barofsky 'The European Commission's Directive on Electronic Signatures: Technological "Favouritism" towards digital signatures' (2001) 14 (24) *Boston College International & Comparative Law Review* 145-159.
[527] Ibid.
[528] Sections 3 and 21 of German Electronic Signatures Act (2001); Blythe (Note).
[529] SE Blythe 'Digital Signature law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in e-commerce with enhanced security' (2005) 11(2) *Richmond Journal of Law and Technology* 1-20.
[530] SE Blythe 'Digital Signature law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in e-commerce with enhanced security' (2005) 11(2) *Richmond Journal of Law and Technology* 1-20.
; Recital 11 of the EC Directive; Article 15 of German Electronic Signatures Act (2001); Bierekoven C, Bazin P & Kozolowski 'Electronic Signatures in German, French and Polish Law Perspective' (2004) *Digital Evidence and Electronic Signature Law* 7-13.
[531] Section 13 of Electronic Communications and Transactions Act 25 of 2002.
[532] Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA).
[533] Eiselen (Note 59)
[534] Bierekoven (Note 520)
[535] Ibid.
[536] Bierekoven (Note 520).

may become problematic for growth and development of e-commerce and international trade if the current position remains in place.[537]

The German and US approach to e-signature regulation seem to be extreme in opposite directions. The latter is technologically prescriptive and provides criteria for legal validity of e-signatures whereas the US follows a minimalist approach and contains very little guidance on the use of e-signatures.[538]

4.3.4. Australia

The Australian parliament enacted the Electronic Transactions Act ("ETA") in 1999. ETA follows the minimalist approach to e-signatures.[539] The e-signature provisions of ETA are based on UNCITRAL's Model Law on E-Commerce of 1996.[540] ETA does not provide a definition for e-signatures and there are no prescribed forms or types of signatures mentioned.

Section 10[541] of ETA permits any method to be used to electronically sign a document, provided that the 'method identifies the signatory and indicates his approval of the information.'[542] Furthermore, 'the method used must be appropriate and reliable for the purposes communicated.'[543] UNCITRAL's Model Law on Electronic Commerce requires the same as section 10 of ETA. According to the wording of section 10 of ETA there is no need to verify the information communicated.[544]

---

[537] A Boss 'The Emerging Law of International Electronic Commerce' (1992) 6(2) *Temple International and Comparative Law Journal* 293-309.

[538] JL Koger 'You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Contemporary Problems* 491-516.

[539] Srivastava A *Electronic Signatures for B2B Contracting: Evidence from Australia* (2013).

[540] Ibid.

[541] Section 10 (1) If, under a law of the Commonwealth, the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication if:
a) in all cases—a method is used to identify the person and to indicate the person's approval of the information communicated; and
b) in all cases—having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated; and
c) if the signature is required to be given to a Commonwealth entity, or to a person acting on behalf of a Commonwealth entity, and the entity requires that the method used as mentioned in paragraph (a) be in accordance with particular information technology requirements—the entity's requirement has been met; and
d) if the signature is required to be given to a person who is neither a Commonwealth entity nor a person acting on behalf of a Commonwealth entity—the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned in paragraph (a).

[542] Ibid.

[543] Section 10(1) (b) of the Electronic Transactions Act 1999.

[544] S Christensen & R Low R 'Electronic Signatures and PKI Frameworks in Australia' (2004) 1(2) *The Digital Evidence and Electronic Signature Law Review* 40-43.

Mason highlights the fact that common law jurisdictions focus on the 'form of an object rather than function of the object in its regulation.'[545] The law focused on the appropriateness of the method used and whether the intention of the signatory was present irrespective of how this was done.[546] Thus, it was not necessary to enact complex legislation regulating digital signatures and certification requirements.[547]

Christenson & Low[548] suggest that standards need to be imposed in ETA for transactions where security is critical.[549] This suggested approach is logical because some transactions require more security than others and the current approach by ETA does not sufficiently protect these transactions.

There is no distinction between types of e-signatures or presumptions relating to reliability of e-signatures in ETA. Srivastava's study on the Australian business perception in e-signatures[550] found a very low usage of digital signatures in the Australian business sector.[551] According to the study, some of possible reasons for low usage revealed from the study is attributed to ignorance and lack of understanding of e-signatures.[552] The lack of understanding weakens confidence in the use of e-signatures and more particularly digital signatures.[553]

ETA has undertaken 'to include the substantive provisions of UNCITRAL's Convention to its current provisions.'[554] The provisions on e-signatures will not differ because the Convention's provisions on e-signatures is the same as the model laws.

4.4. The Extent of South Africa's Compliance with UNCITRAL and Foreign Legal Frameworks

South Africa adopted a two-tier approach to e-signatures. The first tier involves the use of an ordinary e-signature and the second tier governs AESes. Each of the two tiers have been adopted from UNCITRAL and the EC Directive.[555] UNCITRAL's 1996

[545] Mason S 'Electronic Signatures in Practice' (2006) 6(2) *Journal of High Tech. Law* 148-164.
[546] Ibid.
[547] Mason (Note 545).
[548] Christensen & Low (Note 544)
[549] Ibid.
[550] A Srivastava 'Businesses' Perception of Electronic Signatures: An Australian Study' 6 (2009) *Digital Evidence and Electronic Signature Law Review* 46-56.
[551] Ibid.
[552] Srivastava (Note 550).
[553] Ibid.
[554] UNCITRAL website accessed at:
http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.
[555] T Pistorius 'Nobody knows you're a dog: Attribution of data messages' (2002) 13(4) *South African Mercantile Law Journal* 738.

Model Law provided for legal recognition of e-signatures if they are reliable and appropriate for their purpose. This has been adopted by ECTA in respect of ordinary e-signatures.[556] The EC Directive played a major role in influencing the adoption of AESes and accreditation of authentication products and services.

South Africa has departed from strictly adhering to the EC Directive by imposing its own requirements in respect of AESes. Firstly, AESes in South African law must be accredited in order to obtain the status of an AES.[557] This is not the case under the EC Directive which only requires specific criteria to be satisfied in order to obtain the status of an AES. A similarity between the ECTA and the EC Directive lies in the functional equivalent approach. ECTA and the EC Directive favours the use of digital signatures through its requirements of a legally recognised e-signature.[558] The critique against infringing the principle of technological neutrality have been discussed in previous chapters.

Another departure of ECTA is by the imposition of face-to-face recognition as a requirement for granting of an accreditation application.[559] The EC Directive does not require this. The purpose of face-to-face recognition is to verify the identity of the authentication service provider.[560] Although this provides greater security, it also involves more time and effort of the authentication service provider. This is could slow down the operation of e-commerce. It is suggested that South Africa adopt a harmonised approach to e-signature law based on the guidelines provided by UNCITRAL.[561]

4.5. Conclusion

The analysis undertaken in this chapter reveals the different approaches to e-signature law. Boss[562] emphasises the importance of harmonisation of the law on e-commerce on an international scale.[563] Growth and development of economies can be improved

[556] Eiselen (54).
[557] Section 2 of ECTA on the definition of an AES.
[558] According to Article 5 of EC Directive only a qualified AES is legally recognised. 'Qualified' in this context means certified by a trusted third party. The physical form of a qualified AES is a digital signature which is implied by the requirements imposed. Only cryptography based digital signatures can satisfy the requirements of an AES.
[559] Section 38 (1) (e);
[560] Koger (Note 538).
[561] UNCITRAL (Note 566).
[562] A Boss 'The Emerging Law of International and Electronic Commerce' (1992) 6 *Temple International and Comparative Law Journal* 293-309.
[563] Ibid.

if commercial transactions flow smoothly on an international scale.[564] Harmonised law on e-commerce can substantially contribute to the free flow of international trade.[565] Thus, there needs to uniformity of the law in respect of e-commerce. An appropriate approach to e-signature law amongst all countries is a relevant point of departure.

South Africa's approach to e-signature contains elements of both international instruments but seems to add further security requirements than those suggested in the EC Directive and UNCITRAL.[566] Firstly, an e-signature will not obtain the status of an AES if it does not meet the requirements set out in section 38 of ECTA. The criteria set out includes an extra requirement that the e-signature must be based on face-to-face recognition. This requirement seems to complicate the process. It attempts to add more security as the signatory's identity can be verified.[567] Secondly, the EC Directive does not make accreditation of e-signatures compulsory in order for them to be legally recognised.

It is clear that AESes in the form of digital signatures with attached certificates issued by trusted third parties is the most reliable and secure method of electronically signing documents.[568] However, in consideration of the South African approach[569] to obtaining an AES, the question that arises is whether such a high security requirement and reliability afforded by the AES is necessary and practical in our society. This will be discussed in Chapter 5 of this paper.

[564] Boss (Note 562).
[565] Ibid.
[566] UNCITRAL website accessed at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.
[567] Bechini U & Gassen D 'A New Approach to Improving Interoperability of Electronic Signatures in Cross-Border Legal Transactions' (2008-2009) 17 (3) 703-720.
[568] Blythe (Note 530); Bierekoven (Note 520).
[569] The complex and expensive accreditation procedure.

5. Chapter Five: Synthesis and Suggestion

5.1. Introduction

The previous chapters of this paper discussed the current South African approach to e-signatures, the underlying principles of e-commerce and how they influence e-signature law. The paper also highlighted the concerns of the current South African position and provided a comparative analysis of the position with some of the most technologically advanced countries.

South Africa's legislative approach on e-signatures has been largely influenced by UNCITRAL's model laws and the EC Directives. However, South Africa has also incorporated some of its own requirements for the legal validity of e-signatures.[570] The concept of the AES is a reflection of the EC Directive but ECTA goes a step further by imposing compulsory accreditation for obtaining an AES.[571] The EC Directive only imposes requirements to be satisfied and only refers to voluntary accreditation.

ECTA and the EC Directive both adopt a technologically-specific approach to e-signatures because only a digital signature can meet the requirements of an AES.[572] Technologically-specific legislation has been criticised by many authors and remains a concern due to its detrimental effects on the growth and development of e-commerce in South Africa. Furthermore, the accreditation procedure formulated by the South African legislature has been criticised for its potential hindrance to e-commerce by slowing down the pace of e-commerce transactions and imposing high costs on authentication service providers.[573]

This chapter provides a summary of the main arguments in favour of and against the South African position and highlights the stronger viewpoint amongst academics. Furthermore, the chapter provides some suggestions to improve the current e-signature law positon in South Africa. These suggestions include harmonisation of the e-signature law with UNCITRAL and removing the obstacles to growth and development of e-commerce that prevail in law.

[570] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.
[571] Section 13 read with section 38 of the Electronic Communications and Transactions Act 25 of 2002.
[572] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 155-156.
[573] Eiselen (Note 1); L Swales 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.

5.2. Synthesis

The various types of e-signatures have been explored in chapter two. Digital signatures are found to be the most superior form of e-signatures available in the market.[574] The digital signature is a type of e-signature that is dependent on a specific type of technology referred to as cryptography.[575] Cryptography allows the content of messages to be encoded and disguised, which permits only the intended recipient to view the contents thereof.[576]

Cryptography involves the use of keys, which may be in the form of pin codes, passwords or user pin or identity number.[577] One of the keys is used to encode or disguise the message whilst the other is used to decode or decrypt the message.[578] The sender of the electronic document will hold the encrypting key and the decrypting key will be held by the recipient thereof.[579] The encrypting and decrypting keys can be generated by computer software.[580]

Thus, if a sender wants to send a document to another attaching his digital signature to the document he would usually use the software on his computer to encrypt the contents of the document and send it to the recipient email.[581] The email address or typed name within the document of the sender fulfils the identification function of a signature. The recipient will only be able to view the contents of the document if the he enters in his key which will usually be in the form of a password or pin code.[582]

The distinguishing features of the digital signature that sets it apart from ordinary e-signatures are the encrypting function and the ability to reveal any alterations that have been made to an electronic document.[583] The digital signature satisfies the functions of identifying the signatory and showing his assent to the contents of the document.[584] It goes further than manuscript signatures by maintaining the integrity and

[574] K Bharvada 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology.*
[575] S Mason *Electronic Signatures in Law* 4ed (2012); Digital signatures are also discussed in Chapter Two of this paper.
[576] Ibid.
[577] Mason (Note 575).
[578] Ibid.
[579] Mason (Note 575).
[580] Ibid.
[581] Mason (Note 575).
[582] Ibid.
[583] Mason (Note 575).
[584] Van Vuuren v Van Vuuren (1853 - 1856) 2 Searle 116 at 472A sets out the functions of a manuscript signature.

confidentiality of the document.[585] However, the digital signature does not come without risks.

One of the glaring risks with this type of e-signature is the possibility of the decrypting or encrypting key being stolen or misplaced and being used by an imposter.[586] The digital signature cannot guarantee the person using it is the signatory because it binds software and not the person.[587] This indicates that there is no risk-free method of electronically signing a document. The risk of a decryption key being misplaced or stolen prompted ECTA to adopt face-to-face recognition as one of its requirements for obtaining an AES. Face-to-face recognition allows SAAA to verify the identity of the authentication service provider.[588]

Digital signatures are relevant to the discussion because the South African approach to e-signatures prescribes this form of e-signature to be used for the purposes of the law. As previously discussed, ECTA does not specifically mention digital signatures but the requirements it imposes can only satisfied if a digital signature based on cryptography is used.

ECTA is technologically specific because it does not recognise an ordinary e-signature as valid for the purposes of the law.[589] Only an AES will be sufficient to satisfy ECTA's requirements for validity.[590] The status of an AES can only be obtained by the process of accreditation whereby the South African Accreditation Authority ("SAAA") will confirm that the e-signature meets the requirements of an AES.[591] The only type of e-signature that can meet these requirements is the digital signature that uses cryptography.[592]

The questions that arise are whether the South African approach to e-signatures creates a safe and reliable environment for use of e-commerce by consumers and businesses and whether the approach is conducive to growth and development of e-commerce.

[585] Srivastava A *Electronic Signatures for B2B Contracts: Evidence from Australia* (2013).
[586] Mason (Note 575).
[587] Ibid.
[588] Kisswani & Al-Bakri 'Regulating the Use of Electronic Signatures Given the Changing Face of Contracts' (2010) 7 *Macquarie Journal of Business Law* 53-65.
[589] Section 13 (1) of Electronic Communications and Transactions Act 25 of 2002.
[590] Ibid.
[591] Section 38 of Electronic Communications and Transactions Act 25 of 2002.
[592] DP Van der Merwe… et al *Information Communications Technology Law* 2 ed (2016) 155-156.

In response to the first question, the South African approach in theory prescribes a reliable and safe manner of transacting through e-commerce.[593] However, in practice the accreditation procedure has hardly been used. The SAAA website reveals that only two authentication service providers have been accredited since the year 2011.[594] Possible reasons for this is the cumbersome and expensive procedure is society's emphasis on efficiency of e-commerce rather than security of e-commerce.[595]

According to a European Commission, report on the operation of the EC Directive[596] there had also been a low usage of AESes.[597] This could be attributed to the lack of knowledge of an AES which led to uncertainty and low usage.[598] South Africa has adopted the concept of the AES, which is similar to the EC Directives approach, and thus the reaction by society to the introduction of technologically specific law will be along similar lines.

Stern[599] suggests that businessmen are more likely to embrace technologically neutral approaches to e-signatures that are free from hindrances of specific technology and would rather use methods that allow them to construct their own e-commerce practices.[600] Elsonbaty[601] and Norton[602] also take the view that digital signatures would not attract consumers or businessmen.[603] Accordingly, businesses and consumers will generally not use methods that are time-consuming and expensive even if they provide extra security than the usual practices because it would defeat the purpose of e-commerce, which would lead to counter productivity[604]. A possible justification is e-commerce saves time and money. Users of e-commerce do not want to lose these benefits.[605]

---

[593] Pistorius (Note 555).
[594] SAAA website accessed at *http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-30-50.html.*
[595] Boss (Note 562).
[596] Commission of the European Communities, Report on the operation of Directive 2999/93i1C on a Community framework for electronic signatures accessed at http://ec.europa.eufnformation-society/eeuropel 2oio/docslingle.info-space/comelectronicsign atures report-en.pdf.
[597] Ibid.
[598] Kisswani & Al-Bakri (Note 588).
[599] J Stern 'The Electronic Signatures in Global and National Commerce' (2001) 6 *Berkeley Technology Law Journal* 391-414.
[600] Ibid.
[601] EM Elsonbaty 'The Electronic Signature Law: Between Creating the Future and the Future of Creation' 2 (2005) *Digital Evidence and Electronic Signature Law Review* 45-60.
[602] Elsonbaty (Note Noet 601); Norton WK 'Enforcing Simple Electronic Signatures in an International Context' 9 (2012) *Digital Evidence and Electronic Signature Law Review* 74-78.
[603] Ibid.
[604] Elsonbaty (Note 601).
[605] Eiselen (Note); Coetzee J 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' 2004 15 (3) *Stellenbosch Law Review*'

The above discussion leads further to an enquiry about whether e-signatures are required to be reliable. Gregory[606] takes the view that the *form* of the signature should not determine the reliability of the signature.[607] Common law does not require manuscript signatures to be reliable and the approach to e-signatures should also not require the signature to be 'reliable and appropriate for the purpose the signature was generated'[608] as required by section 13 (3) of ECTA. Gregory argues that e-signatures should only be required to fulfil the function of manuscript signatures, which in his view is to link the signatory to the information contained in the document.[609] The intention of the signatory is indicated by the context in which he signed the document.[610] Furthermore, he concludes that ensuring reliability of an e-signature should be the responsibility of the parties to the transaction and not be imposed by the law.[611]

This approach embraces technological neutrality gives parties freedom to decide on the type of e-signature that will be appropriate for its use. This is relevant because not all transactions require the same level of security.[612] Thus, whether an e-signature is required to be reliable should be dependent on the needs and interests of consumers and users of e-signatures. In applying Gregory's view[613] to the South African society's interest indicated by number of accreditations[614] it is resoundingly clear the South African society does not require such high levels of security for electronically signing documents.

The second question deals with whether the South African approach to e-signatures as set out in ECTA is conducive to the growth and development of e-commerce. ECTA is technologically specific in respect of e-signatures in instances where the law requires a signature.[615]

At the time of ECTA's enactment e-commerce was still in its infancy. Endeshaw[616] suggests the correct approach in enacting e-commerce law is to allow for e-commerce

[606] Gregory J 'Must E-Signatures be Reliable' 10 (2013) *Digital Evidence and Electronic Signature Law Review* 67-70.
[607] Ibid.
[608] Gregory (Note 606).
[609] Ibid.
[610] Gregory (Note 606).
[611] Ibid.
[612] Gregory (Note 606).
[613] Ibid.
[614] SAAA Website (Note 594).
[615] Mason (Note 575), Srivastava (Note 550) and Swales (Note 59).
[616] Endeshaw A 'The Proper Law for E-Commerce' 7 (1) (1998) *Information and Communications Technology Law* 5-13.

practices to be explored by society and only once the risks of e-commerce have been identified should appropriate law be enacted.[617] This is important because it prevents law from regulating e-commerce in a manner that leads to law to becoming obsolete.[618] Furthermore, the inconsistency between the law and practice will lend itself to uncertainty in e-commerce and this could create obstacles in the path of e-commerce and would prevent growth and development of e-commerce.[619]

Another aspect of technological prescription that is required to be addressed is the law's prescription of digital signatures. It is noted that digital signatures are one of the most reliable e-signatures available.[620] However, use of this form of e-signature also has disadvantages. One of the disadvantages of prescribing one type of technology is hackers and fraudsters will only be focused on unravelling digital signatures.[621] The identity of the transacting parties are as secure as their encryption or decryption keys. Hackers will be aware of this and will formulate ways of intercepting the system to access the keys.

Another argument against the prescription of digital signatures is that its use has been misdirected to be used in day to day business transactions. One of the earliest users of digital signatures was civil law notaries in Europe.[622] Due to large amounts of data gathered in notaries' offices, provision had been made for electronic data transmissions of paper-based documents into electronic documents.[623] Thus, documents could only be notarised by the use of technology that could guarantee the integrity of the document.[624] Therefore, digital signatures met the functional requirement of a notary's signature which guarantees the integrity of the document. It is understandable and acceptable that digital signatures are used in such an environment. However, not all transactions and communications require such a high level of security and reliability. Therefore, law should not prescribe this type of technology for use in all transactions.

---

[617] Endeshaw (Note 616). The author mentions law reacting to change is the usual manner of development and should be endorsed.
[618] Stern (Note 599).
[619] Endeshaw (Note 616).
[620] Bharvada K 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology.*
[621] Stern (Note 599).
[622] Bechini U & Gassen D 'Á New Approach to Improving Interoperability of Electronic Signatures in Cross Border Legal Transactions' 17(3) 2008-2009 *Michigan State Journal of International Law* 703-720.
[623] Ibid.
[624] Bechini & Gassen (Note 622).

5.3. Suggestion

From the above discussion, most authors do not approve of a technologically specific approach e-signature regulation.[625] In addition, it has been argued that the law has become outdated in relation to the requirement of accreditation of e-signatures.[626] Support for this argument is on the basis that the accreditation procedure has not been used for several years.[627]

Furthermore, the comparative analysis in chapter four reveals that some of the most technologically advanced countries in the world refrain from imposing compulsory accreditation.[628] Recital 4[629] of the EC Directive also acknowledges accreditation to be a barrier to e-commerce. Thus, the South African approach to e-signatures is in need of reform. The accreditation procedure by its very nature is likely to slow down the fast moving pace of e-commerce due to the detailed information it requires from the authentication service providers, the requirements of face-to-face recognition and hand delivery of application documents.

The requirements created by the South African legislation also affect the status of internationally recognised authentication products and services, such as digital signatures provided by Adobe. An e-signature provided by Adobe, which is one of the most popular software used internationally, would not qualify as an AES in South Africa. Thus, a user of an Adobe e-signature is required to prove it reliability in the event of a dispute on the validity of the e-signature.

The first suggestion submitted is that South Africa should harmonise its e-signature law to be fully compliant with UNCITRAL's Model Laws and the Convention on E-Commerce[630] and E-Signatures.[631] Eiselen[632] supports this view. The effect of this

[625] Gregory (Note 606); Stern (Note 599); Eiselen (Note 54); Swales (Note 59); Endeshaw (Note 615).
[626] (Note 24;25 and 26)
[627] Swales (Note 59); Eiselen (Note 54).
[628] Germany; United States and Australia.
[629] Electronic communication and commerce necessitate ' electronic signatures' and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic signatures will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market;
[630] United Nations Commission on International Trade Law Model on Electronic Commerce with Guide to Enactment (1996).
[631] United Nations Commission on International Trade Law Model on Electronic Signatures with Guide to Enactment (2001).
[632] Boss (Note 6562

reform would be ECTA legally recognising ordinary e-signatures[633] and abolishing the concept of an AES.[634] ECTA should adopt the presumption on reliability based on Article 6(3)[635] of UNCITRAL's Model Law on E-Signatures.[636] This approach would facilitate growth and development of e-commerce as stated under section 2 of ECTA by removing barriers to e-commerce.[637] It will also prevent the law from becoming obsolete.[638] Faria,[639] Berman[640] and Boss[641] suggest conflicting national e-commerce legislation creates a barrier to trade because the diverging approaches to e-commerce discourages countries from trading with each other.[642] Harmonising the law would encourage more international trade and contribute to growth and development of economies in the world.[643]

UNCITRAL was formulated for the purposes of harmonisation and unification of the domestic legislation. The recitals of UNCITRAL's Model Law on E-Signatures acknowledges harmonisation as being crucial to international trade integration.[644] UNCITRAL[645] was formulated in consideration of differences among developing countries, developed countries, civil law and common law jurisdictions and the different legal culture.[646] UNCITRAL's model laws are unlike EC Directives, which only consider harmonisation of the European countries for greater benefit of e-commerce within European Community.[647] For the above reasons, UNCITRAL's model laws should be adopted by South Africa to allow for streamlined and free flowing e-commerce transactions.[648] This would assist in increasing international trade and e-commerce transactions.

[633] Forms of ordinary electronic signatures discussed in Chapter 2.
[634] To be in accordance with section 7 of UNCITRAL Model Law in E-Commerce (1996).
[635] Article 6 (3) of UNCITRAL Model Law on E-Signatures (2001).
[636] Eiselen (Note 54).
[637] Ibid.
[638] Stern (Note 599).
[639] JAE Faria 'E-Commerce and International Legal Harmonization; To Go Beyond Functional Equivalence?' 16 (2004) *South African Mercantile Law Journal* 529-555.
[640] A Berman 'International Divergence: The Keys to Signing on the Digital Line – the cross border recognition of electronic contract signatures' 28 (2001) *Syracuse Journal of International Law and Commerce* 125-155.
[641] A Boss 'The Emerging Law of International Commerce' 6(2) (1992) *Temple International and Comparative Law Journal* 293-309.
[642] Ibid.
[643] Ewelukwa N 'Is Africa Ready for E-Commerce – A Critical Appraisal of the Legal Framework for E-Commerce in Africa' (2011) 13 (3) *European Journal of Law Reform* 550-576
[644] UNCITRAL (Note 631).
[645] UNCITRAL (Note 630).
[646] Boss (Note 641).
[647] Andrews R 'Electronic Commerce: Lessons Learned from the European Legal Model' (2005) 9(2) *Intellectual Property Law Bulletin* 81-94.
[648] Boss (Note 641).

5.4. Conclusion

South Africa's approach to e-signature laws require reform because its current position does not provide opportunities for growth and development of e-commerce.[649] Furthermore, the South African society does not require accreditation and the law remains obsolete to the extent that it requires accreditation.[650]

Harmonisation with UNCITRAL's approach to e-signatures has been suggested as a possible reform measure. The instrument has been designed and formulated for the purpose of harmonisation.[651] It aims to create unified and harmonised law for global benefit through increased international trade which leads to economic growth and development.[652]

[649] Discussion in Note 56 to 59.
[650] Ibid.
[651] Boss (Note 641).
[652] UNCITRAL (Note 630).

6. Chapter 6: Conclusion - Should the distinction between electronic signatures and advanced electronic signatures be abolished from the Electronic Communications and Transactions Act 25 of 2002?

6.1. Summary of Findings

The development of e-commerce has vastly increased the number of business transactions, market efficiency and business opportunities.[653] It has increased choice for consumers by providing access to goods and services over the internet.[654] E-Commerce has also made commercial transactions convenient for consumers and businessmen by saving time, cost and effort of entering into transactions.[655] This can be attributed to the instantaneous operation over the internet.

During the last two decades, directives, model laws and legislation were adopted and enacted to regulate e-commerce to ensure its growth and development in a secure environment.[656] E-signatures as a formality for contracting, is one of the areas of e-commerce receiving considerable attention. The concern is the divergent approaches of e-signature law adopted by countries.

Chapter two and chapter three of this paper discusses the various approaches to e-signature regulation in contrast to South Africa's approach to e-signature law. E-signatures in South Africa are only *legally* recognised if an AES is used.[657] An AES can only be obtained if the e-signature undergoes accreditation.[658] Furthermore, an accreditation application will only be granted if specific requirements are met.[659] Many authors[660] suggest that only digital signatures based on cryptography meets the prescribed requirements.[661] Thus, ECTA technologically favours cryptography,

[653] Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.
[654] Ibid.
[655] Coetzee J 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' 2004 15 (3) *Stellenbosch Law Review* 501-521.
[656] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures; United Nations Commission on International Trade Law Model on Electronic Commerce (1996); United Nations Commission on International Trade Law Model on Electronic Signatures (2001).
[657] Section 13 (1) of the Electronic Communications and Transactions Act 25 of 2002.
[658] Section 37 (1) of ECTA.
[659] Section 38 (1) of ECTA.
[660] Van der Merwe DP… et al *Information Communications Technology Law* 2 ed (2016) 155-156; Srivastava (Note 1);
[661] Ibid.

infringing one of the most fundamental principles of e-commerce, namely technological neutrality.[662]

The infringement of technological neutrality has detrimental effects to growth and development of e-commerce.[663] It was found that regulation in favour of a particular type of technology has the potential of preventing newer and more innovative technologies from entering the market.[664] This may defeat the strongly desired benefits of e-commerce, namely saving time and cost in commercial transacting.[665]

Moreover, technologically specific legislation may lead to e-signature law becoming obsolete.[666] This would result in amendments to the law in order to align it to societal practice. Amendments take a considerable period of time to become operative. The period between its operation and societal practice would lead to confusion about the legally valid position and this would lead to uncertainty. Uncertainty in the legal position could potentially delay the fast-moving operation of e-commerce.

South Africa's approach to e-signatures not only infringes on the principle of technological neutrality but it is also inconsistent with ECTA's objective of facilitating e-commerce by removing barriers to growth and development of e-commerce.[667] The accreditation procedure required for obtaining an AES was found to be extremely cumbersome and expensive.[668] The purpose of the procedure is to provide for trusted third parties to certify the reliability of the authentication service providers.[669] This procedure contributes to ECTA's objective of ensuring growth and development of e-commerce in a secure environment. However, there are negative aspects about the procedure.

Firstly, the accreditation procedure requires submission of detailed information and documentation relating to the products and services of authentication service providers including financial statements.[670] Secondly, the application for accreditation

[662] Srivastava and Koekemoer (Note 1); Swales, L 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.
[663] United Nations Commission on International Trade Law: Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (2009).
[664] Swales (Note 10); UNCITRAL (Note 11).
[665] J Stern 'The Electronic Signatures in Global and National Commerce' (2001) 6 *Berkeley Technology Law Journal* 391-414.
[666] Ibid.
[667] Section 2 states its objectives.
[668] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2804-2820.
[669] Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.
[670] Chapter 2 of Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations 2007.

must be hand delivered to the SAAA.[671] Thirdly, a substantial fee of R 20 000 for each authentication product must be paid. Furthermore, the authentication service providers need to verify their identity at the offices of the SAAA.[672]

Although these aspects of the procedure provide additional security and reliability in the use of e-signatures as opposed to the ordinary e-signatures, the practicality of the accreditation procedure is questioned.[673] Only two accreditations have been granted since the operation of ECTA's accreditation regulations.[674] The reasons for the low accreditation rate may be attributed to ignorance of the law,[675] unwillingness to change current business practices[676] and the cost, time and effort involved in the accreditation procedure.[677] It is also relevant to mention that the distinction between the two types of e-signatures only become necessary when there is a dispute. As it stands there has not been much case law on the validity of e-signatures. This implies that there is no practical necessity for an AES.

The number of granted accreditations indicates the lack of societal interest in the procedure.[678] This suggests society does not require such high-level security and reliability of e-signatures at the expense of the immense effort, time and cost involved in obtaining an AES. Thus, the law should be amended in accordance with the current societal practice.

The comparative analysis[679] among the United States, Germany and Australia indicates the approach to e-signatures in relation to the needs of society. Germany was one of the first countries to adopt the technologically-specific law on e-signatures requiring accreditation of authentication service providers.[680] After the adoption of the EC Directive, Germany was required to amend its legislation to be consistent with the EC Directive. One of the amendments was the change from a technologically-specific

[671] Ibid.
[672] Accreditation Regulations (Note 18).
[673] K Bharvada 'Electronic signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology*.
[674] SAAA Website accessed at *http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-30-50.html.*
[675] Elsonbaty EM 'The Electronic Signature Law: Between Creating the Future and the Future of Creation' 2 (2005) *Digital Evidence and Electronic Signature Law Review* 45-60; Norton WK 'Enforcing Simple Electronic Signatures in an International Context' 9 (2012) *Digital Evidence and Electronic Signature Law Review* 74-78.
[676] Stern (Note).
[677] Elsonbaty (Note); Norton (Note).
[678] This is relevant in so far as the law develops in relation to the societal change in morals, belief and behaviour. This is discussed by BJ Koops (BJ Koops 'Should ICT Law be Technology-Neutral' (2006) *IT & Law Series* 77-108).
[679] Contained in chapter four of this paper.
[680] Schroers J, Van Alsenoy B Cuijpers C 'Legal analysis of E-Signature services' (2015).

approach to the two-tiered approach.[681] Furthermore, voluntary accreditation replaced compulsory accreditation.[682] The rationale behind the removal of compulsory accreditation is attributed to the stifling effect of the procedure as acknowledged by the EC Directive.[683]

The EC Directive aims to achieve harmonisation of laws within the European Union and does not place emphasis on international trade among non-members of the European Union. Reports[684] on the operation of the EC Directive indicate the slow adoption of AESes. Thus, the European Union shares a common problem with South Africa in relation to the slow implementation of AESes.

The United States and Australia follow a technologically-neutral approach to e-signatures and both countries have adopted their e-signature law from UNCITRAL.[685] The advantage of the minimalist approach is the law does not need to be amended in accordance with technological development.[686] This was demonstrated by the United States and Australia.[687] Technologically-neutral law can be applied to any type of technology due to its flexibility and adaptive nature.[688] This is one of the most advantageous aspects of technologically-neutral law.[689] In addition, the adoption of technologically-neutral law prevents legal uncertainty which promotes public confidence and increases the use of e-commerce.[690]

---

[681] Bierekoven (Note 66) and Blythe S 'A Critique of German E-Commerce Law and Recommendations for Improvement' accessed at http://aabri.com/SA12Manuscripts/SA12045.pdf.

[682] Recital 11 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[683] Ibid.

[684] Commission of the European Communities, Report on the operation of Directive 2999/93i1C on a Community framework for electronic signatures (Brussels, 15-3.2oo6, COM(2oo6) 120 final) http://ec.europa.eufnform ation-society/eeuropel 2oio/docslingle.info-space/co melectronicsign atures report-en.pdf.

[685] T Pistorius 'Nobody knows you're a dog: Attribution of data messages' (2002) 13(4) *South African Mercantile Law Journal* 737-747.

[686] Koops (Note 337).

[687] Australia and United States have not amended their legal position on e-signatures. Both jurisdictions adopted a technologically neutral approach and have maintained this position.

[688] Spyrelli C 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) *Journal of Information Law and Technology* accessed at *http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html.*

[689] Ibid.

[690] Endeshaw A 'The Proper Law for E-Commerce' 7 (1) (1998) *Information and Communications Technology Law* 5-13.

6.2. Should the distinction between Ordinary e-signatures and AESes be abolished from ECTA?

In consideration of the above findings, it is suggested that the distinction between ordinary e-signatures and AESes be abolished.[691] Thus, ECTA should comprise only of ordinary e-signatures and adopt a presumption on reliability based on Article 6 (3) of UNCITRAL's Model Law on E-Signatures.[692] A *presumption* on reliability that favours cryptography, as opposed to a *legal requirement* that favours cryptography, is a sensible approach. The approach gives parties discretionary power to decide on the appropriate measure of security to be used in their transactions. Furthermore, a presumption on reliability prevents instances of insecurity that may arise if parties are unsure of safe methods of signing electronically.

The above approach is consistent with the principle of technological-neutrality because it does not prescribe a particular type of technology to be used for purposes of law. E-Commerce principles was formulated to facilitate the growth and development of e-commerce.[693] The importance of adhering to these principles has immense benefits for international trade and development of countries.

Maintaining a common international standard for e-commerce transactions lowers barriers to e-commerce and allows for the free flow of e-commerce, which results in more international trade among countries. Increased international trade leads to growth and development of developing economies and the global economy. The central purpose of UNCITRAL is trade-harmonisation and unification of laws to increase the free flow of trade.[694] Adhering to suggestions and guidelines provided by UNCITRAL would be in the best interests of the South African economy due to UNCITRAL's consideration of the improvement of developing countries.

[691] Eiselen (Note 54).
[692] Ibid.
[693] United Nations Commission on International Trade Law Model on Electronic Commerce (1996); United Nations Commission on International Trade Law Model on Electronic Signatures (2001).
[694] Ibid.

7. **References**

Primary Sources

South African Legislation

1. Electronic Communications and Transactions Act 25 of 2002

   s 13
   s 38 (1)

2. Electronic Communications and Transactions Act 25 of 2002: Accreditation Regulations of 2007.

   Regulation 7
   Regulation 8
   Regulation 29 (1)

Case Law

1. Jafta v Ezimvelo KZN Wildlife 2008 10 BLLR 954 (LC); 2008 JOL 22096 (LC).

2. Mafika v The SABC – Unreported Labour Court Case No. J 700/08.

3. Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash and another (2015) JOL 32555 (SCA).

4. S v Miller and others [2015] 4 All SA 503 (WCC).

5. Van Vuuren v Van Vuuren (1853 - 1856) 2 Searle.

International Legal Framework

1. United Nations Commission on International Trade Law: Model on Electronic Commerce (1996).

2. United Nations Commission on International Trade Law: Model on Electronic Signatures (2001).

3. United Nations Commission on International Trade Law: Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods (2009).

Foreign Legal Framework

1. Australia: Electronic Transactions Act (1999).
2. European Union: European Union Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community.
3. Germany: Gesetz zur digitalen signatur (1997).
4. United States of America: Electronic Signatures in Global and National Commerce Act (2000); Uniform Electronic Transactions Act (1999).

Secondary Sources

Books

1. Ashbourne, J Biometrics: *Advanced Identity Verification: The Complete Guide* 2ed: Springer, (2014).
2. Caney, LR *The Law of Suretyship,* (1936).
3. Van der Merwe, DP… et al *Information and Communication Technology Law* 2 ed: Lexis Nexis, (2016).
4. Mason, S *Electronic Signatures in Law* 4ed London: Institute of the Advanced Legal Studies for the SAS Humanities Digital Signatures Library, (2012).
5. S Papadopoulos and S Snail *Cyberlaw@sa: The Law of the Internet in South Africa* 3 ed Pretoria: Van Schaik Publishers (2012).
6. Srivastava, A *Electronic Signatures for B2B Contracting: Evidence from Australia:* Springer, (2013).

Journal Articles

1. Ali, R 'Technological Neutrality' (2009) 14(2) *Lex Electronica* 1-15.
2. Andrews R 'Electronic Commerce: Lessons Learned from the European Legal Model' (2005) 9(2) *Intellectual Property Law Bulletin* 81-94.
3. Barofsky, A 'The European Commission's Directive on Electronic Signature: Technological "Favoritism" towards Digital Signature' (2000) 24(1) *Boston College International and Comparative Law Review* 145-160.
4. Bechini U & Gassen D 'A New Approach to Improving Interoperability of Electronic Signatures in Cross-Border Legal Transactions' (2008-2009) 17 (3) 703-720.

5. Berman A 'International Divergence: The Keys to Signing on the Digital Line – the cross border recognition of electronic contract signatures' 28 (2001) *Syracuse Journal of International Law and Commerce* 125-155.

6. Bharvada K 'Electronic Signatures, Biometrics and PKI in the UK' (2002) 16(3) *International Review of Law, Computers and Technology* 265-275.

7. Bierekoven C, Bazin P & Kozolowski 'Electronic Signatures in German, French and Polish Law Perspective' (2004) *Digital Evidence and Electronic Signature Law* 7-13.

8. Blythe, SE 'Digital Signature law of the United Nations, European Union, United Kingdom and the United States: Promotion of Growth in e-commerce with enhanced security' (2005) 11(2) *Richmond Journal of Law and Technology* 1-20.

9. Boss A 'The Emerging Law of International Electronic Commerce' (1992) 6(2) *Temple International and Comparative Law Journal* 293-309.

10. Braley SW 'Why Electronic Signatures can Increase Electronic Transactions and the Need for Laws Governing Electronic Signatures' (2001) *Law and Business Review of the Americas* 417-444 .

11. Buckley & Tank 'The Electronic Signatures in Global and National Commerce Act: An Overview' (2001) 20 *Annual Review of Banking Law* 221-241.

12. Coetzee, J 'The Electronic Communications and Transactions Act 25 of 2002: facilitating electronic commerce' (2004) 15(3) *Stellenbosch Law Review Stellenbosch Regstydskrif* 501-521.

13. Christensen S & Low R 'Electronic Signatures and PKI Frameworks in Australia' (2004) 1(2) *The Digital Evidence and Electronic Signature Law Review* 40-43

14. Eiselen, S 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2805-2820.

15. Elsonbaty EM 'The Electronic Signature Law: Between Creating the Future and the Future of Creation' 2 (2005) *Digital Evidence and Electronic Signature Law Review* 45-60.

16. Endeshaw A 'The Proper Law for E-Commerce' 7 (1) (1998) *Information and Communications Technology Law* 5-13.

17. Ewelukwa N 'Is Africa Ready for E-Commerce – A Critical Appraisal of the Legal Framework for E-Commerce in Africa' (2011) 13 (3*) European Journal of Law Reform* 550-576.

18. Faria JAE 'E-Commerce and International Legal Harmonization; To Go Beyond Functional Equivalence?' 16 (2004) *South African Mercantile Law Journal* 529-555.

19. Gerck, E 'Overview of Certification Systems: X. 509, PKIX, CA, PGP & SKIP' (2000) 1(3) *The Bell* 8.

20. Gereda, SL 'The Electronic Communications and Transactions Act' 2006 *Telecommunications Law in South Africa* 262-294.

21. Gregory J 'Must E-Signatures be Reliable' 10 (2013) *Digital Evidence and Electronic Signature Law Review* 67-70.

22. Jobodwana ZN 'E-Commerce and M-Commerce in South Africa: Regulatory Challenges' (2009) 4(4) *Journal of International Commercial Law and Technology* 287-298.

23. Jøsang and Tran 'Trust management for e-commerce' (2000) *Virtual Banking*.

24. Kisswani & Al-Bakri 'Regulating the Use of Electronic Signatures Given the Changing Face of Contracts' (2010) 7 *Macquarie Journal of Business Law* 53-65.

25. Koger JL 'You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Contemporary Problems* 491-516.

26. Koops BJ 'Should ICT Law be Technology-Neutral' (2006) *IT & Law Series* 77-108.

27. Mason S 'Electronic Signatures in Practice' (2006) 6(2) *Journal of High Technology Law* 148-164.

28. Maxwell W Bourreau M 'Technology neutrality in Internet, telecoms and data protection regulation' 2014 *Hogan Lovells Global Media and Communications Quarterly* 19-23.

29. Ndonga D 'E-Commerce in Africa: Challenges and Solutions' (2012) 5 (3) *African Journal of Legal Studies* 243-268.

30. Norton WK 'Enforcing Simple Electronic Signatures in an International Context' 9 (2012) *Digital Evidence and Electronic Signature Law Review* 74-78.

31. Pappas C 'Comparative US and EU Approaches to E-Commerce Regulation' (2002) 31(2) *Denver Journal of International Law and Policy* 325-348.

32. Parmentier, MA 'Electronic Signatures' (2000) 6(2) *Columbia Journal of European Law* 251-258.

33. Pistorius T 'Click-wrap and web-wrap agreements' (2004) 16(4) *South African Mercantile Law Journal* 568-576.

34. Pistorius T 'From snail mail to e-mail-a South African perspective on the web of conflicting rules on the time of e-contracting' (2006) 39 (2) *Comparative and International Law Journal of Southern Africa* 178-213.

35. Pistorius T 'Nobody knows you're a dog: Attribution of data messages' (2002) 13(4) *South African Mercantile Law Journal* 737-747.

36. Raymond AH & Lambert JB 'Technology. E-Commerce and Emerging Harmonisation: The Growing Body of International Instruments Facilitating and the

Continuing Need to Encourage Wide Adoption' (2014) *International Trade and Business Law Review Journal* 419-441.

37. Reed C'Taking sides on technology neutrality' (2007) 4(3) *SCRIPT-ed* 263-284.

38. Sabett R 'Effects of Technology Convergence and Public Key Infrastructure' (1999) 7(2) *University of Baltimore Intellectual Property Law Journal* 143-154.

39. Snail, S 'Electronic Contracts in South Africa – A Comparative Analysis' 2008 (2) *Journal of Information, Law & Technology* 1-24.

40. Srivastava and Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' 2013 21 (3) *African Journal of International and Comparative Law* 427-446.

41. Srivastava A 'Businesses' Perception of Electronic Signatures: An Australian Study' 6 (2009) *Digital Evidence and Electronic Signature Law Review* 46-56.

42. Stern J 'The Electronic Signatures in Global and National Commerce' (2001) 6 *Berkeley Technology Law Journal 391-414.*

43. Swales, L 'The Regulation of electronic signatures: time for review and amendment' (2015) 132(2) *South African Law Journal* 257-270.

44. Van der Merwe DP 'A Comparative Overview of the (Sometimes Uneasy) Relationship between Digital Information and Certain Legal Fields in South Africa and Uganda' (2014) 17(1) *Potchefsroom Electronic Law Journal* 296-326.

Law Commission Papers

South African Law Reform Commission *The Review of Law of Evidence* (Discussion Paper 131, Project 126) Pretoria: SALRC (2015).

Websites

1. Kamecke, U Korber, T 'Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood' (2008) available at https://www.uni-goettingen.de/.../Kamecke-Koerber_ECLR08_29(5)_33.

2. Schroers J, Van Alsenoy B Cuijpers C 'Legal analysis of E-Signature services' (2015) available on

   http://www.futureid.eu/data/deliverables/year3/Public/FutureID_D33.06_WP33_v1.0_Legal_analysis_eSign_service.pdf.

3. South African Accreditation Authority website available at http://www.saaa.gov.za/index.php/accreditation/2013-12-04-09-30-50.html.

4. Spyrelli C 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach towards Electronic Authentication' (2002) *Journal of Information Law and Technology* available at http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html.

5. United Nations Commission on International Trade Law: Status available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html.