An analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and the SADC region.

ʻMatšepo Regina Kulehile

Thesis Presented for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Private Law

University of Cape Town

August 2017

Supervisor: Professor Debbie Collier
Co-supervisor: Professor Tjakie Naude

TABLE OF CONTENTS

Acronyms

AA: Accreditation Authority
AeS: Advanced Electronic Signature
ASP: Authentication service provider
CA: Certification authority
CISG: United Nations Convention on Contracts for the International Sale of Goods 1980
CPS: Certificate Practice Statement
CROBECO: European Land Registry Association's Cross Border Electronic Conveyancing system
CSP: Certification service provider
CUECIC: UN Convention on the Use of Electronic Communications in International Contracts 2005
DRA: Deeds Registry Act No 12 of 1967
DRR: Deeds Registry Regulations No 52 of 1967
EC: European Commission
ECTA: Electronic Communications and Transactions Act No 25 of 2002
ECT Amendment Bill: Electronic Communications and Transactions Amendment Bill 2012
eIDAS: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for electronic transactions in the internal market.
E-SIGN: Electronic Signatures in Global and National Commerce Act 2000
EU: European Union
GUIDEC: General Usage for International Digitally Ensured Commerce
HIPSSA: Harmonization of the ICT Policies in Sub-Saharan Africa project
ICC: International Chamber of Commerce
ICT: Information and Communications Technology
ISP: Internet Service Provider
ITU: International Telecommunication Union
LAA: Land Administration Authority
LRA: Lesotho Revenue Authority
MLEC: UNCITRAL Model Law on Electronic Commerce 1996
MLES: UNCITRAL Model Law on Electronic Signatures 2001

MVI: Motor Vehicle Import

NCCUSL: National Conference of Commissioners on Uniform State Law

PGP: Pretty Good Privacy

PKI: Public Key Infrastructure

QeS: Qualified electronic signature

RA: Registration Authorities

SAAA: South African Accreditation Authority

SACU: Southern African Customs Union

SADC: Southern African Development Community

SADC ML: SADC Model Law on electronic transactions and electronic commerce 2013

SAPO: South African Post Office Limited

SCD: Secure signature creation device

SeS: Secure electronic signature

SPKI: Simple Public Key Infrastructure

SSCD: Secure signature creation devices

UCC: Uniform Commercial Code 2002

UCITA: Uniform Computer Information Transactions Act 2001

UNCITRAL: United Nations Commission on International Trade Law

UETA: Uniform Electronic Transactions Act 1999

UN: United Nations

UNECA: United Nations Economic Commission for Africa

USA: United States of America

Attachments

Diagram 1 on electronic signatures

Diagram 2 Table of legislative instruments

Recommended draft legislative provisions

Acknowledgements

I wish to express my sincere gratitude to my supervisors, Professor Debbie Collier and Professor Tjakie Naude for their guidance, patience and support in my PhD journey. Their vast knowledge, meticulousness and challenging questions helped broaden the scope of my thesis and make it better. I am grateful for their encouraging words which kept me going even in the most difficult moments. I could not have asked for better mentors for my PhD study.

I would also like to thank legal researchers from The Swedish Law and Informatics Research Institute, Faculty of Law, Stockholm University for their engagement in discussing my ideas and giving input on my thesis. Particular reference is made to Mr. Stanley Greenstein, for facilitating my access to the University research facilities, experts in the field of study and making my research visit in Sweden worthwhile.

I am grateful to my friends and colleagues for the stimulating discussions, advice and support in this PhD journey. Thank you for making my odd moments feel normal and making the experience joyful.

My heartfelt gratitude goes to my family, especially my mother, sister and sister-in-law for their divine support in my PhD journey, for taking care of my family in my absence and bending over backwards for me. Your prayers kept me going to the very end. To my children who endured the void of an absent mother for the period of my study, I thank you for your patience, motivation and love.

Last, but not least, I thank my husband, Moitheri Stephen Kulehile, for his unwavering support in helping me reach my dreams, for believing in me, giving me courage and helping me up when I was knocked down and for showing me that love surpasses all. Without you, it would not have been possible. Words cannot thank you enough, may the good Lord bless you all abundantly.

Above all, I thank God Almighty, through whom all things are possible.

Abstract

Despite the steady growth of electronic commerce (e-commerce), Lesotho and SADC users are uncertain of how to securely sign e-communications practicably. This results in users' lack of confidence in the use of e-commerce. SADC and Lesotho regulatory bodies have developed legal instruments including model laws and bills in an attempt to regulate electronic signatures (e-signatures) in e-commerce to address this problem amongst others. However, it is unclear whether the approach adopted will ensure that the regulatory instruments effectively regulate e-signatures and consequently promote the growth of e-commerce and enhance the socio-economic development of the state.

This study examines what the information and communications technology regulatory principles of functional equivalence and technology neutrality entail, their interpretation by the United Nations Commission on International Trade Law (UNCITRAL), and their appropriateness for effective regulation of e-signatures through conceptual analysis. In particular it examines the UNCITRAL Model Laws on e-commerce, UNCITRAL Model on e-signature and the United Nations Convention on the Use of Electronic Communications in International Contracts.

The study describes the technical operation of different offline and online signatures in order to appreciate how e-signatures should be regulated. Through textual analysis, it examines whether regulatory instruments of Lesotho and SADC correctly apply the theories in a way that will render use of e-signatures practicable and their regulation effective. It also examines initiatives on regulation of e-signatures in South Africa, the United States of America and the European Union.

The study reveals that the purpose of the signature formality is to promote certainty, prevent fraud and provide evidence of a contract despite the form of signature. Although not perfect, functional equivalence and technology neutrality principles render regulation of electronic signatures effective since rules that align with them promote equivalence of legal treatment between offline and online signatures. Consequently, the UNCITRAL's Convention reflects that ordinary e-signatures can meet purposes of the signature formality where appropriate if they observe its functional equivalence criteria. However, the reliability of such electronic signatures is a question of evidence as is the case in offline contracts. Thus, soft laws on electronic evidence must complement the e-signature rules to ensure equivalent legal treatment of signatures.

The study reveals that the Lesotho instruments do not fully align with the regulatory principles whereas the SADC instrument closely aligns with them. To different extents, these instruments do not adequately address the problems of users and may inhibit the growth of e-commerce. It further found that the instruments erroneously exclude certain matters such as wills from e-signature application while they correctly exclude others such as negotiable instruments from e-signature application. Lastly it found that the UNCITRAL convention and the USA instruments provide better models for effective regulation of e-signatures.

By implementing amendments suggested by this study, Lesotho and SADC will address the challenges faced by e-commerce users and make the use of e-signatures feasible for all. Consequently, the instruments will effectively increase the growth of e-commerce and in turn enhance the development of socio economic growth of the SADC region.

CHAPTER ONE: INTRODUCTION

1.1 Study Background

Electronic transactions[1] (e-transactions) concluded through the Internet[2] were introduced in Lesotho in the 21st century and the practice has been gradually escalating. E-transactions are used for the sale and purchase of goods including vehicles, software and textiles, and extend to electronic funds transfers, conclusion of insurance transactions, employment contracts, contracts for services and travel and accommodation bookings.[3] E-transactions are concluded wholly on the Internet (online), or partially online and partially offline.[4] This practice of transacting through electronic means for commercial purposes is called electronic commerce (e-commerce).[5]

Since the Internet is available worldwide, it brings about a myriad of benefits. For instance, it opens access to international markets by the 'fusion of borders that previously existed between… sellers and purchasers, and service providers and clients. All these parties to contracts now meet in virtual shopping malls and virtual boardrooms.'[6] It therefore augments communication, increases the speed and reliability of transactions for business-to-consumers and business-to-business transactions and reduces transaction costs.[7] As a result,

[1] An electronic transaction (e-transaction) is described as a contract or agreement concluded through the use of electronic medium or computer-mediated networks. See the OECD Expert Group on 'Defining and Measuring E-commerce' 2001 available at *http://stats.oecd.org/glossary/detail.asp?ID=758*, accessed on 26 April 2013. The terms e-transaction and e-contract will be used interchangeably in this study.

[2] The Lesotho Electronic Transactions and Electronic Commerce Bill of 2013 defines the Internet in s 2 as 'the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof'. Tana Pistorius in 'Formation of Internet Contracts: An Analysis of the Contractual and Security Issues' (1999) 11 *SA Merc LJ* 282 also defines the Internet as 'a global network of computers all speaking the same language….' The Internet is further described as a set of standards (protocols) which use the same language that makes it possible for computers to pass information from one computer to another, thus forming an international network of computers. See Julien Hofman, David Johnston, Sunny Handa and Charles Morgan (eds) *Cyberlaw: A Guide for South African's Doing Business Online* (1999) 18. It is 'an open network which permits communication without the need for both parties to subscribe to the same closed network.' Chris Reed & John Angel *Computer Law: The Law and Regulation of Information Technology* (2007) 198.

[3] See Mochebele M (ed) *The state of ICT in Key sectors: Business, Education, Health and Tourism Lesotho 2013* 2ed (2015) Lesotho Communications Authority at 11 for more uses of the internet in Lesotho.

[4] Juana Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' (2004) 3 *Stellenbosch Law Review* 501 at 515.

[5] Alan Davidson *The Law of Electronic Commerce* (2009) 1 & 25. Electronic commerce is also defined as 'the act of buying or selling goods or services by means of electronic resources.' (Andrej Savin *EU Internet Law* (2013) 28) and as 'the conduct of commercial activities and transactions by means of computer-based communication and technologies. It generally involves the processing and transmission of digitized information.' (Barry B Sookman *Computer, Internet and electronic commerce terms: Judicial, legislative and technical definitions* (2009) 156).

[6] Pistorius 'Formation of Internet Contracts' op cit note 2 at 282-3.

[7] Mochebelele op cit note 3 at 1.

the Internet has led to the diversification and expansion of businesses,[8] more business efficiency and streamlined commerce.[9] Because of its nature, the Internet has become a forum for the exchange of goods and services for money and thus a platform for a global marketplace.[10]

Due to these benefits, e-commerce can accelerate the economic growth of a state. In fact the World Bank shows that a 10 percent increase in broadband infiltration is likely to result in 1.3 percent in economic growth of a state.[11] This implies that an Information and Communications Technology (ICT)[12] sector's performance is closely linked to the socio-economic growth of a state.[13] To illustrate, the Internet provides employment opportunities and growth 'through investment in innovation and increased competition.'[14] For one, small and medium sized enterprises (SMMEs) in Lesotho can access international markets[15] and market themselves worldwide at minimum costs, and thus carry out business at a regional or international scale. This leads to the expansion of SMMEs, which results in the creation of jobs for Basotho. Although the overall input of e-commerce on Lesotho's economy is not fully recorded, its contribution is reflected by statistics from the Lesotho Revenue Authority (LRA). These indicate a steady increase of Motor Vehicle Import (MVI) Tax collected by LRA from vehicles purchased over the Internet from the non-SACU[16] region within a five year period, from 2005-2010. In 2005, MVI tax collected contributed just 0.056 per cent of Lesotho's Gross Domestic Product (GDP), whereas in 2008, MVI tax contribution increased to 0.19 per cent of GDP, while in 2010 it increased yet again to 0.26 per cent of Lesotho's GDP.[17]

[8] Marilyn Krige 'Using the internet for business purposes' (1998) 1 *Juta's Business Law* 130.
[9] Coetzee op cit note 4 at 501. See also Krige ibid.
[10] Graham JH Smith *Internet Law and Regulation* 4 ed (2007) 773.
[11] Wade Publications CC 'The Lesotho Review: An overview of the Kingdom of Lesotho's economy, Information and Communications Technology' 2015 available at *www.lesothoreview.com,* accessed on 1 May 2017.
[12] ICT is defined as 'technologies that facilitate communication and the processing of information by electronic means, and include everything from radio, satellite, television to telephones, computers and the Internet.' UN-Department of Economic and Social Affairs 2012 cited in Mochebelele op cit note 3 at 1.
[13] Wade Publications op cit note 11.
[14] Savin op cit note 5 at 29.
[15] 'ICT Policy for Lesotho: Policy Measures, Instruments and Initiatives' 2005 available at *http://research.businessonlybusiness.com/matrix.php?Electronic%20transactions%20of%20Lesotho*, accessed on 04 June 2013.
[16] The Southern African Customs Union consists of Botswana, Lesotho, Namibia, South Africa and Swaziland. See the 2002 Southern African Customs Union Agreement available at *www.sacu.int*, accessed on 29 March 2017.
[17] Lesotho Revenue Authority *Report from Performance Analysis and Strategy Management Office* (May 2013).

It is noteworthy that the United Nations Human Development Report declared Sub-Saharan African countries as the least developed region in the world.[18] The global inequality is partly connected to the digital divide between Sub Saharan African countries and other countries in the world.[19] In this regard, digital divide refers to 'the unequal access to and usage of new [Internet] technologies.'[20] This arises from the fact that technology is one of the essentials and basis of material wealth.[21] This study uses Lesotho and the Southern African Development Community (SADC)[22] region as examples of least developed Sub-Saharan African countries that experience challenges in maximising usage of Internet technologies and reflects aspects of how these countries need to address the challenges in order to improve their economic growth.

Lesotho's ICT sector struggles to get good communications infrastructure that enables access to and usage of Internet services. A good ICT infrastructure requires electricity connections, a significant number of computers, mobile phones and the like.[23] In 2013, the Lesotho Communications Authority (LCA)[24] carried out a study to measure the level of ICT infrastructure, access and usage in the business, health, tourism and education sectors across the country.[25] The study found that there was low Internet connectivity across all sectors due to a lack of infrastructure such as a lack of electricity or network coverage and due to high connectivity costs.[26] Further, of the businesses that had computers, 77 percent of them outsourced technical support services, while 17 percent depended on inhouse technical support services.[27] But the number of employees with basic computer skills was high across

[18] Kevin Watkins United Nations Human Development Report 2005 available at *http://hdr.undp.org/sites/default/files/reports/266/hdr05_complete.pdf*, accessed 20 March 2017 221-222.
[19] Christian Fuchs & Eva Horak 'Africa and the digital divide' (2008) 25 *Telematics and Informatics* 99 at 100.
[20] Fuchs et al ibid at 99.
[21] Fuchs et al ibid at 100.
[22] The SADC region consists of 15 countries namely, Lesotho, the Republic of South Africa, Angola, Botswana, Democratic Republic of Congo, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, Swaziland, Tanzania, Zambia and Zimbabwe (SADC 'South African Community Development: Towards a common future' available at *http://www.sadc.int/member-states*, accessed on 13 December 2015).
[23] Wade Publications op cit note 11.
[24] The Lesotho Communications Authority is part of the ICT sector of Lesotho through its mandate to regulate the communications sector. See the Lesotho Communications Authority 'Our mandate' available at *www.lca.org.ls*, accessed on 20 February 2017.
[25] Mochebelele op cit note 3 at 2-3.
[26] Mochebelele op cit note 3 at 10 & 60; See also Phillip Batroff, George Chinea, Thorsten Harstmann, Karl Jonas and Jens Moedeker 'A pilot of a QoS-A ware wireless Back-Haul Network for rural areas' in Radu Popescu-Zeletin, Karl Jonas, Idris A Rai, Roch Glitho and Adolfo Villafiorita (Eds) *e-Infrastructure and e-Services for developing countries* (2011) 98 who found that rural areas tend to lack affordable Internet connectivity access. See more of Mochebelele's report's findings on the presence of computers, presence of network servers amongst entities with computers, employees with basic computer skills, modes of Internet connectivity, wireless Internet connectivity, Internet cafés in the locality, web presence, presence of mobile and fixed phones and presence of facsimile in Lesotho.
[27] Mochebelele op cit note 3 at 16.

the sectors.[28] Apart from these sectors, in 2013 at least 6.4 percent of households had a computer, 4.3 percent had access to the Internet from home while 5 percent of the population used the Internet.[29] Lesotho struggles to get good ICT infrastructure due to, among others, its rugged mountainous landscape, small roads, electricity networks and sparsely populated rural areas which render investment in the infrastructure expensive.[30]

Despite the low ICT infrastructure, low presence of websites and network services, the LCA's study showed a steady increase of Internet connectivity and presence of computers from 2009 to 2013.[31] It also showed a high email presence.[32] It follows that Lesotho and other Sub-Saharan African countries need to harness the opportunities and benefits offered by the Internet and ICT through e-commerce as catalysts for their social and economic development.

1.2 Description of research problem

Although e-commerce presents many possibilities, it is characterised by users' lack of confidence in its e-transactions as a result of, among others the anonymity of Internet users. While contracting online, parties to an e-transaction need to know that the person sitting at a keyboard transacting with them is who they say they are[33] and has authority to act.[34] A party's ability to assent to contracts through electronic means constitutes one of the main concerns in e-transactions so that the parties know they have reached a binding agreement.[35] Consequently, e-commerce users have to adopt a secure means to address these concerns.

An electronic signature (e-signature) is something a user can utilise to prove their identity, verify their authority to act or assent to a contract.[36] It follows that where the law or parties to an e-transaction require a signature, an e-signature will attempt to comply with that requirement. If the requirement of signature is not met, negative consequences may follow. For instance, an agreement may not materialise or a contract may be rendered void.[37] The use

[28] Mochebelele op cit note 3 at 60.
[29] Wade Publications op cit note 11.
[30] Wade Publications op cit note 11.
[31] Mochebelele op cit note 3 at 60 & 81- 89.
[32] Mochebelele op cit note 3 at 60 & 81- 89.
[33] Reed and Angel op cit note 2 at 208.
[34] MHM Schellekens *Electronic Signatures: Authentication Technology from a legal perspective* (2004) 15.
[35] Christopher William Pappas 'Comparative US and EU approaches to e-commerce regulation: Jurisdiction, electronic contracts, electronic signatures and taxation' (2002-2003) 31 *Denver Journal of International Law and Policy* 325 at 340; Reed and Angel op cit note 2 at 208-9.
[36] See Reinhardt Buys & Francis Cronje *Cyberlaw@SA II: The law of the internet in South Africa* 2 ed (2004) 85 & 86; Pistorius 'Formation of Internet Contracts' op cit note 2 at 294-5; Davidson op cit note 5 at 77.
[37] Robert Sharrock *Business Transactions Law* 9 ed (2017) 119. For example, section 5 (1) of the Hire Purchase Act No 27 of 1974 of Lesotho provides that '[n]o agreement shall be of any force or effect unless it is entered into in writing and signed by the buyer and by or on behalf of all other parties to the agreement.'

of e-signatures may therefore increase confidence in e-commerce, ensure the effectiveness of online agreements and enhance the growth of e-commerce.[38]

There are numerous e-signature technologies in existence. These include usernames, passwords, Personal Identification Number (PIN), electronic sound, typed name in an electronic document, clicking on an icon, browsewrap agreements, email signature, digitised signature, contactless identification, biometrics technology and digital signatures based on public key infrastructure (PKI) or based on a pretty good privacy (PGP) web of trust. This study categorises the e-signature technologies into two groups, namely ordinary e-signatures and digital signatures for purposes of analysis. As reflected in Diagram 1 on electronic signatures attached hereto, ordinary e-signatures include all e-signatures except the digital signatures. As part 2.9 below will show, the technologies are differentiated because their security and accessibility levels differ.

The legal system of Lesotho is lagging in regulation of e-commerce despite the growth of e-commerce in the country. The common law of Lesotho is unresponsive to e-commerce due to its paper-based nature and there are few statutes that refer to data messages.[39] This gap in regulation leads to a number of legal uncertainties in e-commerce. For example users are uncertain of which authentication technology they should attach to electronic communication (e-communication) for purposes of signature in their e-transactions; whether the law will recognise future technologies as signature; whether the e-signature attached to an e-communication is that of a signer or has been subjected to undetected manipulation, that is, whether it is reliable; and how to carry out document authentication such as notarisation online. Consequently, e-commerce users have difficulty in knowing how to securely sign e-communication practicably.

These legal uncertainties discourage online users from engaging in e-transactions for lack of confidence in the legality of the e-transactions and the fear of abuse by other users. Users feel the need to be protected against fraud or accusations of impersonation.[40] The challenges further discourage entrepreneurship and foreign investments. Legal uncertainty negatively affects users' trust and confidence which are facilitators of different forms of

[38] Pappas op cit note 35 at 340.
[39] For example, the Criminal Procedure and Evidence (Amendment) Act 2001, Data Protection Act 2011, Communications Act 2011 and Companies Act 2011.
[40] Gavin Jones 'Failings in the Treatment of Electronic Signatures' (2003) 1 *Hertfordshire Law Journal* 101.

trade.[41] Hence the legal uncertainties surrounding the use of e-signature cripple the growth of e-commerce, which will negatively affect economic growth.

1.3 Thesis statement

The thesis of this study is that law reform can reduce the vulnerabilities of contracting parties, foster trust, confidence and legal certainty in the use of e-signatures in e-transactions and increase the desire to engage in e-commerce.[42] A law which indicates when e-signature technologies will be recognised as sufficient to perform the functions of a signature will reduce the fear of contracting with unknown persons online. E-commerce will therefore be boosted if its legal regulation is flexible enough to promote technical innovation but certain enough to inspire trust and confidence in its users from the business section and the public.[43]

Legislation that aims at facilitating the confident use of e-signatures in e-transactions should observe ICT regulation principles in order to be effective in its application. The regulatory principles contemplated in this research study are the technology neutrality principle and the functional equivalence principle. Although the study recognises that these theories are not perfect, they are adopted as guidelines due to their ability to render the use of e-signatures accessible, flexible, trustworthy and economic to the user. Further, for a law to be effective, it should be understood by its subjects and remain stable over time.[44] Since a technology neutral and functionally equivalent law is simple and will not be subject to constant amendments, it can easily be followed by its subjects and can therefore facilitate the use of e-signatures.

Not all Southern African countries have legislative instruments that regulate the technology developments in e-commerce and the interests of their e-commerce users remain under protected.[45] Realising that the SADC countries are faced with unexpected and complex legal challenges on the use of e-communications in e-commerce, SADC developed the Electronic Transactions and Electronic Commerce SADC Model Law (SADC ML) in 2013.[46] The SADC ML is 'a tool that Member States can use to create a more secure legal

[41] Kai H Lim, Kwok Leung, Choon Ling Sia and Matthew K O Lee 'Is eCommerce boundary-less? Effects of Individualism- Collectivism and Uncertainty Avoidance on Internet shopping' (2004) 35 *Journal of International Business Studies* 545 at 546.
[42] Erin Ann O'hara 'Choice of law for internet transactions: the uneasy case for online consumer protection' (2005) 153 *University of Pennsylvania Law Review* 1883 at 1896.
[43] Jones op cit note 40 at 101.
[44] Lon Fuller *The Morality of Law* (1964) at 39, 63 & 79.
[45] These include Swaziland, Namibia, Zimbabwe, Democratic Republic of Congo and Malawi. See part 5.9.4.1 on Bills recently drafted by these countries.
[46] Harmonization of ICT Policies in Sub-Saharan Africa 'Electronic Transactions & Electronic Commerce: SADC Model Law' Preamble ITU 2013.

environment for electronic transactions and e-commerce.'[47] The states can do so by adopting the SADC ML domestically.

Recent developments in this regard occurred in Lesotho in early 2013 when the Ministry of Communications produced a draft Bill on Electronic Transactions and Electronic Commerce (Lesotho Bill).[48] The Lesotho Bill is intended to regulate e-commerce in Lesotho and draws heavily from the SADC ML.

The SADC ML and the Lesotho Bill attempt to respond to a number of legal uncertainties that result from e-commerce transactions, including the use of e-signatures. The instruments introduce two forms of e-signatures, namely an 'electronic signature' and a 'secure electronic signature' (SeS) for signing electronic data. The SADC ML defines an e-signature as data, which includes an electronic sound, symbol or process which is adopted in order to identify a person and indicate their approval or intent towards information in the e-communication to which the e-signature is attached.[49] It further defines a 'secure electronic signature' as a signature which is created and can be verified by application of security procedures that ensure that the electronic signature is unique to the signer, objectively identifies the signatory, was created by the signatory and can only be used under their control, and is linked to the electronic communication in such a way that changes to the communication will be detectable.[50]

It is imperative that the SADC ML and the proposed Lesotho Bill provide effective regulation of e-signatures that will adequately address the fears of e-commerce users and enhance the growth of e-commerce. Law should play a pre-emptive and responsive role in facilitating technical innovations including e-commerce that improve society.[51] Otherwise, an

[47] The Preamble of the SADC ML. SADC recognises that coordination of legislations across its region was also necessary to ensure that different legislations do not obstruct the growth of competitive regional markets. SADC member states that have legislative instruments that regulate e-transactions include South Africa, Zambia, Botswana, Seychelles, Mauritius, Madagascar and Mozambique. It is also noted that member states should use the tool to exploit the stimulant effect of ICT to speed economic integration and economic and social development.

[48] The Lesotho Bill indicates that it is an International Telecommunication Union draft available at *https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2013/Lesotho/Lesotho_E-transactions%20Bill%202nd%20DRAFT%20clean.docx* accessed on 01 December 2014. See also parts 5.3 & 5.4 below.

[49] Section 1 (11) SADC ML; See also s 2 of the Lesotho Bill.

[50] Section 1 (19) SADC ML; See also s 2 of the Lesotho Bill.

[51] Pistorius & Hurter 'Contracting on the Internet: Formation of Contracts, Trade Practices and Online Dispute Resolution' (no date) available at *http://docweb.pwv.gov.za/Ecomm-Debate/myweb/greenpaper/academics/pistorious.html#sdendnote14sym#sdendnote14sym,* as accessed on 20 /12/2006 cited in Deo John Nangela *The Adequacy of the Tanzanian Law on E-commerce and E-contracting: Possible Solutions to be Found in International Models and South African Legislation* (unpublished Doctor of Laws thesis, University of Cape Town, 2011) 2.

inadequate regulatory structure may discourage potential markets.[52] Further, the failure to address the concerns in e-transactions will deny SADC countries the economic opportunities presented by ICT through e-commerce and increase the digital divide between African countries and the rest of the world.[53] The focus of this study is therefore to examine the proposed Lesotho Bill and SADC ML provisions on e-signatures, to assess whether they address the challenges highlighted in the research problem, using the ICT principles identified above, and whether these instruments will provide legal certainty and confidence in e-signature use, thus promoting e-commerce growth.

1.4 Research Question(s)

The question this study addresses is, how can e-signatures in e-commerce be effectively regulated in Lesotho and the SADC region? To investigate this question, it is broken down into sub questions.

a) What do the theories of functional equivalence and technology neutrality entail in the context of e-signatures and the regulation of e-signatures? Chapters three and four of this work address these questions.
b) Do SADC and Lesotho legal instruments on e-signature correctly apply the theories in a way that will render use of e-signatures practicable and their regulation effective? The study covers this question in chapters two and five.
c) Is the SADC and Lesotho instruments' exclusion of wills, negotiable instruments, transfer of immovable property or rights in immovable property transactions, documents of title and indentures from application of an e-signature justifiable in terms of the theories? Chapter six traverses this issue.

1.5 Objective of study and methodology

The objective of the study is to explore the ICT regulatory principles of functional equivalence, technology neutrality and effective law making in the context of the regulation of e-signatures in e-commerce and explore whether the ICT principles are sufficiently reflected within the Lesotho Bill and SADC ML. The aim is to determine whether and how such legal instruments can address concerns raised in the research problem and enhance the

[52] UNCITRAL Secretariat 'Raising Confidence in E-commerce: The Legal Framework' Vienna, Austria available at *http://www.unescap.org/tid/projects/ecom04_s4sorieul.pdf* as accessed on 13 October 2010 cited in Nangela op cit note 51 at 4.
[53] Nangela op cit note 51 at 7.

growth of e-commerce. At the end of the study, a series of proposals are suggested which will provide solutions for the effective regulation of e-signatures. Sections of the Lesotho Bill and SADC Model Law that require revision for the purposes of the functional equivalence and technology neutrality will be pointed out.

The study adopts a descriptive method, coupled with conceptual analysis and textual analysis of legal instruments in order to formulate arguments and opinions in the research. It describes signature technologies used in traditional transactions. Furthermore, it relies on computer science material to describe different e-signatures and authentication technologies and their technical operation. The computer science material is imperative as the research question involves a technical issue - e-signature - which is identified as requiring legal regulation, hence the material will contribute towards the development of legal arguments.

Moreover, the study analyses concepts involved in e-commerce regulation. It clarifies and expounds on the different dimensions of the meanings of functional equivalence, technology neutrality and effective law.

Additionally, the laws the study relies on for textual analysis are drawn from statutes, model laws, guidelines and case law. The study also relies on literature such as textbooks, scholarly articles, reports and proceedings as sources that explain or reflect on the laws. The laws are mainly from Lesotho, the SADC countries and the United Nations Commission on International Trade Law (UNCITRAL). As part of the textual analysis, the study reflects upon laws from South Africa, the European Union (EU), and the United States of America (USA). These jurisdictions have mature legal systems that regulate e-commerce, but adopt different approaches in e-signature regulation.[54] By reflecting on the systems, the study will derive valuable lessons on which is the better approach for e-signature regulation in Lesotho and the SADC region.

1.6 Delineations and limitations

This study is concerned with the regulation of e-signatures in e-transactions concluded over the Internet through computing technology.[55] It deals with e-signature regulation in business-to-consumer, business-to-business and consumer-to-consumer e-commerce. The study does

[54] See part 5.1 below.

[55] According to Dana van der Merwe (ed), Anneliese Roos, Tana Pistorius, Sieg Eiselen & Sanette Nel *Information and Communications Technology Law* 2ed (2016) 7, computing includes the use of computer hardware such as computers, laptops, modern cellular phones which can perform functions of a computer, or any other high technology devices that have computer services such as i-pads. Computing is not limited to computing hardware but also extends to data and information used by such hardware.

not explicitly deal with the concept of electronic government (e-government) although it briefly deals with e-conveyance in the analysis of the transfer of immovable property transactions.

While the writing and signature formality go hand in hand in contract formation, the study does not deal with the writing formality. The study assumes that the written document formality in online transactions is met by an e-communication.[56]

Further, the study limits its scope to investigating the justification of the Lesotho Bill and SADC ML's exclusion of e-signature provisions from wills, negotiable instruments, transfer of immovable property or rights in immovable property transactions, documents of title and indentures. The scope of the study does not extensively investigate the SADC ML and Lesotho Bill's exclusion of other provisions such as writing or time of dispatch and receipt of e-communications from negotiable instruments, wills, transfer of immovable property or rights in immovable property transactions, documents of title and indentures due to time and space constraints. As a result, the conclusions on the legitimacy of the instruments' exclusion of e-signature from application in these matters are tentative, pending further research on the legitimacy of exclusion of the other provisions as they are related to e-signature.

Lastly, the study does not deal with the recognition of foreign secure electronic signatures. This is a comprehensive topic which warrants a thesis in its own right. Therefore dealing with it in this study will only scrape the surface and not do justice to the issue.

1.7 Significance of study

This research study will contribute to knowledge by elucidating the significance of applying the ICT regulation theories of functional equivalence and technology neutrality appropriately as the starting point for the development of online rules for e-signatures in the formation of e-transactions. It will illustrate that the improper understanding and application of the theories can lead to impractical rules. The study will further explicate that a law that applies the theories will align with principles that ensure enactment of effective law. Hence, application

[56] See s 6 (1) of the SADC ML which provides that '[w]here a law requires information to be in writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.' Section 6 (3) gives examples of e-communications contemplated by the SADC ML. See also s 8 (1) of the Lesotho Bill which states that '[w]here a rule of law requires information to be in writing or provides for certain consequences if it is not, an electronic communication satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.'

of the theories leads to an online regulatory system which is certain, meaningful, free of obstacles to electronic commerce and thus effective.

The practical effect of the proposals in this study is that they will create an enabling environment for the use of e-signatures in Lesotho and the SADC region. It is vital for the Lesotho Bill and SADC ML to provide a framework for e-commerce regulation that addresses users' apprehensions in order to facilitate the use of e-signatures by parties to e-transactions. This will protect e-commerce users from abuse by other users, provide legal certainty and promote fair trade. Trust, security and confidence in e-commerce will be facilitated if the use of e-signatures is eased and e-transactions will run more smoothly and efficiently.[57] This will stimulate the growth of e-commerce in the SADC region.[58] The proposals for technology neutral regulation in the research study will promote 'desired innovation and investment in the electronic communications sector.'[59] This will lead to efficient regulation that is responsive to changing market structures.

1.8 Basic outline of thesis

First, the work sets forth the purpose and functions of the signature formality in contracts. It defines traditional signatures and e-signatures and their different forms. It then highlights traditional signature functions that e-signatures can perform and in the process, identifies shortcomings of traditional signatures and e-signature. It also looks into different levels of document authentication and additional measures required for such. A discussion of the concept of signature is imperative for it is the foundation for the legal analysis. The conceptual framework of the study follows. The work explores the functional equivalence and technology neutrality principles of ICT regulation in the context of e-signatures. It further examines how the lawmaker is to design an e-signature law that will be effective in reaching its aim.

Next the study provides an overview of principles of ICT regulation as reflected in international instruments of the UNCITRAL and the International Chamber of Commerce (ICC). It outlines the instruments' proposed regulation of e-signatures in e-commerce and

[57] Schellekens op cit note 34 at 94. This is in line with Lesotho's ICT Policy which aims to '[d]evelop a transparent, stable and effective legal and fiscal operating environment to promote online commercial transactions.' op cit note 15.

[58] E-commerce will flourish due to the lack of fear of legal uncertainty and impracticality currently surrounding the use of e-signatures.

[59] Ilse van der Haar TILEC Discussion Paper *Technology Neutrality; What Does It Entail?* (March 2007) Tilburg University 1 at 24-25.

explores what adequate e-signature regulation would be in the context of contract law and law of evidence.

Subsequently, based on the previous chapters, the work assesses the legal system of Lesotho and the SADC ML on their application of functional equivalence, technology neutral, and their alignment with effective law making principles in addressing challenges in the use of e-signatures. It identifies lacunae existent in the legal systems; and concurrently reflects on the approaches of South Africa, the EU and the USA on regulation of e-signatures. It does so with the objective of identifying effective e-signature regulation and to learn valuable lessons from the respective approaches. It conducts this process with care not to implant rules from the selected jurisdictions into Lesotho's legal system or the SADC Model Law. The study further considers the transactions which the Lesotho Bill and SADC ML exclude from e-signature application. It examines the purpose of signature in these matters and assesses whether e-signature technologies can meet the purposes and functions of signature in these matters. Based on this analysis, the study indicates whether the law can extend e-signature application to these transactions.

Finally, the thesis outlines the findings of the study, makes recommendations in domestic and regional contexts, highlights areas for further research and concludes the study.

CHAPTER TWO: THE FUNCTIONS OF A SIGNATURE AND THE TECHNICAL APPLICATION OF SIGNATURES IN OFFLINE AND ONLINE TRANSACTIONS

2.1 Introduction

E-signatures are increasingly important,[1] and accordingly proper regulation of e-signatures is necessary. This requires an examination of the traditional signature and its functions. The objective of this chapter is therefore to clarify the rationale behind the use of the signature formality. To do so, the chapter looks at the background of the formality of signature, when it is legally required, the definition of the concept of a signature, functions of a signature, different forms of traditional signatures and the basis of their recognition by courts of law.[2] In addition, it considers the hierarchy of document authentication in the offline sphere with the aim to assess how such formalities can be developed in the online sphere. It reflects that the law in the offline sphere focuses on the *effects* of a signature rather than the *form* of signature. The chapter subsequently introduces the concept of e-signature, discusses different forms of e-signature technologies, how they technically operate, how a signer acquires them, considers their practicability and the functions of traditional signature they can perform, if any.

2.2 Background and purpose of the formalities in contract

Formality is an ancient concept which dates back to biblical times. For one, a person had to place their hand under another's thigh to signify that they make an oath to that other.[3] Again, in ancient German customary law, parties signified transfer into a household service by one person handing over a lock of hair to the other.[4] Similarly, parties under medieval English common law symbolised the transfer of land by a grantor handing over a sod and a small tree

[1] Brand New Technologies: Electronic Signatures and Security 'Electronic Signatures – Understanding Technology, Methods and Authentication' 17 May 2011 available at *http://us-cdn.creamermedia.co.za/assets/articles/attachments/34131_brand_new.pdf*, accessed on 12 May 2014.

[2] The study considers Lesotho, South Africa and English case law. South African cases are examined as Proclamation 2B of 1884 states that the law applicable in the Cape of Good Hope (except for statutory law and customary law) should be applicable in Lesotho, which is the common law of the Cape of Good Hope. Although cases of South African courts are not binding on Lesotho, they are highly persuasive. Decisions of courts in England are also referred to, as South African common law is composed of Roman-Dutch law with inroads of English Law, thus English cases have been of assistance in interpretations of South African Law, and hence persuasive on Lesotho law.

[3] See *Genesis* 24 verses 2-3.

[4] Franziska Elizabeth Myburgh *Statutory Formalities in South African Law* (unpublished Doctor of Laws thesis, Stellenbosch University, 2013) 13.

branch to the grantee in the presence of witnesses.[5] In time these practices evolved. Under Canon law a casual agreement was held to be binding, but again people began a regular practice of reducing some agreements to writing.[6] Subsequently, English law compiled the first legislative text that imposed formalities of different kinds for several contracts through the Statute of Frauds of 1677.[7] Formalities are 'requirements relating to the outward, visible form in which the agreement must be cast to create a valid contract.' [8]

The legislature of that time recognized a number of issues resulting in the Statute of Frauds. First, contracts of sale of immovable property were of considerable value and importance. They also had complex conditions attached to them. Consequently parties with interest to the contracts were tempted to engage in fraudulent activities such as making perjured claims.[9] Secondly, the legislature observed that parties to such contracts were considered incompetent witnesses and were not permitted to give evidence in a dispute over their contract.[10] Thirdly jurors decided matters based on their personal knowledge of events.[11] The legislature therefore demanded that such contracts should be reduced to writing and signed.[12]

The Statute of Frauds' objective of imposing formalities of writing and signature was threefold. It was to protect vulnerable parties by guaranteeing trustworthy evidence of terms of a contract with the written contract signed by the parties.[13] This would reduce litigation caused by either abuses of parties to contracts who engaged in fraudulent activities,[14] or by loss of memory on agreed contract terms.[15] The purpose of the formalities was therefore to prevent fraud, promote certainty, and provide evidence of a contract.

Despite the statute's objectives, its poor draftsmanship resulted in more litigation. For example, parties had disputes including claims of non-liability for performance under a

[5] Heather MacNeil 'From the Memory of the Act to the Act Itself. The Evolution of Written Records as Proof of Jural Acts in England, 11th to 17th Century' (2006) 6 *Arch Sci* 313 at 315; Joseph M Perillo 'The Statute of Frauds in Light of the Functions and Dysfunctions of Form' (1974) 43 *Fordham L Rev* 39 at 43.
[6] Myburgh op cit note 4 at 13.
[7] GB Bradfield *Christie's Law of Contract in South Africa* 7ed (2016) 129.
[8] Heinrich Schulze, Roshana Kelbrick & Tukishi Manamela et al *General Principles of Commercial Law* 8 ed (2015) 95; DJ Joubert *General Principles of the Law of Contract* (1987) 154.
[9] Myburgh op cit note 4 at 14.
[10] GHL Fridman 'The Necessity for Writing in Contracts within the Statute of Frauds' (1985) 35 *University of Toronto Law Journal* 43 at 47; Bradfield op cit note 7 at 129.
[11] AWB Simpson *A History of the Common Law of Contract: The Rise of the Action of Assumpsit* (1975) 604; Bradfield op cit note 7 at 129.
[12] See ss 1, 3, 4 & 7 of the Statute of Frauds 1677 Chapter 154.
[13] Michal Hain 'Making Law far away from Kitchen Tables: Imposing Trusts regardless of Formalities' (2014) *Oxford University Undergraduate Law Journal* 55.
[14] Hain ibid at 55.
[15] Bradfield op cit note 7 at 129.

contract after binding themselves orally, simply because it was unclear whether the contract had to be reduced to writing under the Statute of Frauds.[16] However, the courts countered this through several means.[17] For instance, they stated that depending on the surrounding circumstances of each case, where a contract fell within the scope of the statute, but failed to follow the formalities prescribed in the Statute, such contract was not void, but voidable. Nonetheless, English law gradually phased out the Statute of Frauds.

Nevertheless, South Africa adopted similar provisions that imposed formalities.[18] The purpose of the formalities in the South African legal system is to promote certainty, to avert incidents of fraud and malpractices and provide evidence of a contract.[19] But like the English law, parties to a contract have a tendency to misuse the requirement of formalities to escape obligation, by claiming non-compliance with the formalities.[20] This implies that there should be rules that regulate compliance with formalities to determine whether a contract is validly concluded.[21]

The legal system of South Africa is similar to that of Lesotho[22] and Lesotho adopted the concept of formalities in contracts for the same purposes as South Africa.[23] The subsequent section considers when the signature formality plays a role in a contract.

2.3 Signature in the formation of contracts

The general rule is that formalities are not necessary for the formation of a contract under common law,[24] but requirements for the formalities of writing and signature can be exceptions to the rule.[25] A signature obtains legal recognition and effect in conclusion of

[16] Bradfield op cit note 7 at 129
[17] Bradfield op cit note 7 at 129-130.
[18] Bradfield op cit note 7 at 130. Several legislative instruments prescribe that contracts be reduced to writing and signed. For instance, the Alienation of Land Act 68 of 1981; s 6 of the General Law Amendment Act 50 of 1956 on suretyships; s 93 of the National Credit Act 34 of 2005 & s 7 of the Consumer Protection Act 68 of 2008.
[19] Bradfield op cit note 7 at 129; *Exdev (Pty) Ltd v Pekudei Investments (Pty) Ltd* 2011(2) SA 282 (SCA); *Wilken v Kohler* 1913 AD 135 at 142; *Clements v Simpson* 1971 (3) SA 1 (AD). Myburgh op cit note 4 at 16 on the other hand maintains that the legislature of South Africa introduced formalities in pursuit of uniformity of specific contracts.
[20] Myburgh op cit note 4 at 2; *Senekal v Home Sites (Pty) Ltd* 1950 1 SA 139 (W).
[21] Myburgh op cit note 4 at 2.
[22] This is due to Proclamation 2B of 1884.
[23] For example, see the Hire Purchase Act 27 of 1974, s 5 (1) which states that: 'no agreement shall be of any force or effect unless it is entered into in writing and signed personally by the buyer or … other parties to the agreement'. See also the Lesotho Labour Code Order 24 of 1992, s 154 (1) & (2); Companies Act 18 of 2011, s 37; Deeds Registry Act 12 of 1967, s 11; The Partnership Proclamation 1957.
[24] *Goldblatt v Fremantle* 1920 AD 123 at 128; *First National Bank Ltd v Avtjoglou* 2000 (1) SA 989 (C) at 995 E-F; Bradfield op cit note 7 at 123.
[25] *Conradie v Rossouw* 1919 AD 279; Robert Sharrock *Business Transactions Law* 9 ed (2017) 119; Myburgh op cit note 4 at 18.

contracts in two situations. First, where a signature is self-imposed by parties to the contract, and secondly, where the requirement of a signature is prescribed by the law.[26]

Parties to a contract impose the use of a signature in the conclusion of their contract, for one of two reasons: first, they may agree that a contract they wish to conclude will not be valid and binding upon them unless it is reduced to writing and signed by the respective parties.[27] The parties must reach an agreement to this effect. They or the courts cannot just assume or infer the signature requirement from clauses in the contract.[28] Secondly, the parties may agree that their oral contract will be valid and they will be immediately liable upon its conclusion, but require that the contract be reduced to writing and signed for evidential purposes.[29] The formalities of writing and signature here prove the existence of the contract and its terms in case of conflict arising from the contract.[30]

A signature formality also obtains legal recognition where the law requires that parties express their intent to contract by signing the agreement.[31] If parties do not comply with the formality of signature, the contract does not become valid and enforceable.[32]

Failure to comply with the formality of a signature has varied consequences. First, an agreement will be rendered void for lack of signature;[33] secondly, the contract will be invalidated with respect to third parties,[34] third, one of the parties will be liable to a certain penalty of legal disqualification for something they ought to have been entitled to.[35] The subsequent question is therefore, what is a signature?

2.4 Definition of a traditional signature

Scholars and courts have devised several propositions in an attempt to define the concept of a signature. The most common proposition is that a signature is 'the signatory's name, written

[26] Louis F Van Huyssteen & Catherine J Maxwell *Contract Law in South Africa* 3ed (2014) 87 para 159.
[27] Dale Hutchison, Chris-James Pretorius (eds) & Jacques Du Plessis et al *The Law of Contract in South Africa* 2ed (2012) 159; AJ Kerr *The Principles of the Law of Contract* 6 ed (2002) 161- 2; *Marake v National University of Lesotho* [2002] LSLC 10; *Goldblatt* supra note 24 ; *De Bruin v Brink* 1925 OPD 68 at 69.
[28] *Pillay and Another v Shaik and others* [2009] 2 ALL SA 435 (SCA) at par 50.
[29] Van Huyssteen et al op cit note 26 at 88 para 160; Deeksha Bhana, Elsje Bonthuys & Minette Nortje *Student's Guide to the Law of Contract* 3 ed (2013) 114.
[30] Hutchison et al op cite note 27 at 159. Sharrock op cit note 25 at 136.
[31] Hutchison et al op cit note 27 at 159; see note 23 above for statutes that require signature.
[32] Hutchison et al op cite note 27 at 160; See *Mota v Motokoa* [2002] LSHC 7 where the court declared a document that deceased had not signed in terms of s 154 of the Labour Code Order 1992 invalid; *Rockbreakers and Parts (Pty) Ltd v Rolag Property Trading (Pty) Ltd* 2010 (2) SA 400 (SCA); See also note 23 above.
[33] *Wilken* supra note 19; *Pretoria East Builders CC v Basson* 2004 (6) SA 15 (SCA); LF Van Huyssteen, GF Lubbe & MFB Reinecke *Contract General Principles* 5 ed (2016) 166.
[34] Sharrock op cit note 2530 at 119.
[35] Sharrock op cit note 25 at 119.

in his or her own hand, on a paper document'.[36] This definition is rather limited consequently other descriptions of the concept should be explored. The word 'sign' originates from a Latin word 'signum' which is translated into 'mark'.[37] Thus, in *In re Trollip* the court specified that '[t]o sign, as distinguished from writing one's name in full is to make such a mark as will represent the name of the person signing.'[38] In *Harpur v Govindamall*,[39] the court stated that

> 'the words "sign" and "signature", which are not technical or legal terms, must be given their ordinary, popular meaning. … In ordinary usage the word "signature", used without qualification, means signature by name or mark. … the ordinary, popular meaning of the verb "sign" is sign by name or sign by mark'.

Further in *Goodman v Eban* the court stated that 'the essential requirement of signing is affixing in some way, either by pen or pencil or by otherwise impressing upon a document, one's name or "signature" so as to personally authenticate the document.'[40] However, the court in *Putter v Provincial Insurance Co* gave the most comprehensive definition of a signature. It stated that '[a]ny mark made by a person for the purpose of attesting the document, or identifying it as his act, … is his signature thereto'.[41] With these in mind, an outline of functions of a signature in offline contracts follows.

2.5 Functions of a traditional signature

Schellekens identifies at least seven overlapping functions of a signature. These are identification; authentication; authorization; integrity; originality; cautionary function; and attribution.[42] The section discusses each function separately.

[36] Reed 'What is a Signature?' (2000) 3 *The Journal of Information, Law and Technology* available at *http://elj.warwick.ac.uk/jilt/00-3/reed.html*, accessed on 02 May 2014.
[37] *Ex Parte Goldman & Kalmer* 1965 (1) SA 464 at 468; Vivienne Antoinette Lawack-Davids *Aspects of Internet Payment Instruments* (unpublished Doctor of Laws thesis, University of South Africa, 2000) 263.
[38] 12 SC 243 at 246 cited in Bradfield op cit note 7 at 136. See also *Morton v Copeland* (1855) 16 CB 517 at 535; Michael Chissick & Alistair Kelman *Electronic Commerce: Law and Practice* 3 ed (2002) 96; & FR Malan JT Pretorius & SF Du Toit *Malan on Bills of Exchange* 5 ed (2009) 97.
[39] 1993 (4) SA 751 at 756-7.
[40] [1954] 1 ALL ER 763 at 766 and 770.
[41] 1963 (3) SA 145 (W) at 148E.
[42] MHM Schellekens *Electronic Signatures: Authentication Technology from a Legal Perspective* (2004) at 59.

2.5.1 Identification

A signature serves to identify a signer and party to a contract.[43] Identification is defined as 'the determination or verification of which identity belongs to somebody.'[44] It consists of verification that one is who he/she claims to be.[45]

Methods of identification must have at least three properties. That is, the means of identification should be distinctive of the owner; it should point towards the person under investigation; and the person in question must be the only one who can create that means of identification.[46] A handwritten signature is a good example of a means of identification with these properties.[47] Identification is an important aspect to be evidenced by any form of signature.[48] A signature also authenticates a document.

2.5.2 Authentication

Authentication is an act by which the signer declares the document to be genuine.[49] That is, by signing, the signer indicates that the declaration above their signature is a declaration made by them.[50] Consequently, the signature represents the signer's assent to the document[51] and their willingness to be bound by its contents.[52] It follows that a signature is not just a physical act, but is a visible expression of a mental intention of the signer, called the *animus signandi*.[53]

---

[43] O A Orifowomo & J O Agbana ESQ 'Manual signature and electronic signature: significance of forging a functional equivalence in electronic transactions' (2013) 24 *International Company and Commercial Law Review* 357 at 358; Dana van der Merwe, Anneliese Roos & Tana Pistorius et al *Information and Communications Technology Law* 2 ed (2016) 176; Guy Lefebvre 'Electronic Data Interchange and the New Civil Code of Quebec' (1998) *J of Business Law* 300 at 313; Lawack-Davids op cit note 37 at 267.
[44] Schellekens op cit note 42 at 65.
[45] Andrej Savin *EU Internet Law* (2013) 219.
[46] Schellekens op cit note 42 at 65-6.
[47] *Goodman* supra note 40 at 561.
[48] Reed 'What is a Signature' op cit note 3636; Schellekens op cit note 42 at 60.
[49] Orifowomo et al op cit note 43 at 358.
[50] *Sebeko v Sebeko* [2004] LSHC 91.
[51] Bradfield op cit note 7 at 128; Joubert op cit note 8 at 157. See *Chisnall and Chisnall v Sturgeon and Sturgeon* 1993 (2) SA 642 (W) 645A-I; *MAN Truck & Bus (SA) (Pty) Ltd v Dusbus Leasing CC* 2004 (1) SA 454 (W) 478; Eliza Mik 'The Unimportance of being "electronic" or – popular misconceptions about "Internet contracting" ' (2011) 19 *International Journl of Iaw and Information Technology* 324 at 340.
[52] Van Huyssteen et al op cit note 26 at 93 para 172; Juana Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' (2004) 3 *Stellenbosch Law Review* 502 at 513; *Navidas v Essop* 1994 (4) SA 141 (A) 156E.
[53] Schellekens op cit note 42 at 60; *Central Motors (Birmingham) Ltd v PA Wadsworth & Another (Trading as Pensagain)* (1982) 133 NJL 555 Court of Appeal (Civil Division).

Consequently, a signature performs an evidentiary function[54] and a channeling function.[55] The evidentiary function brings certainty to the rights and obligations that flow from the agreement[56] while the channeling function shows that negotiations have graduated into a contract.[57] Moreover, a signature is a symbol of authorisation.

2.5.3 Authorisation

The signature function of authorisation has meaning in at least two contexts. First, it means that a signer has the authority to carry out any legal act that will follow from adopting a declaration.[58] For instance, a director of a company may sign a cheque on behalf of the company if authorised by the company to carry out such a legal act.[59]

Secondly, a signer can use a signature to grant authority to another person.[60] For example, a person can sign a declaration empowering another person to act as their agent.[61]

2.5.4 Integrity

A signature safeguards the integrity of a document. Integrity of a document means that 'the data in a document have not been altered, deleted or supplemented, irrespective of whether this has come about through natural causes or through manipulation.'[62] To verify the integrity of a document, the content of the document at the time it was signed and stored for the first time must be considered, as well as its content at a time it is a subject of investigation.[63]

The general rule is that a contract has to be in complete form before it is signed.[64] A signer's act of signing an incomplete or blank page with the hope that it will be completed later will therefore not suffice.[65] Again, because a signer appends his signature immediately

[54] Myburgh op cit note 4 at 21.
[55] Schellekens op cit note 42 at 61.
[56] Lefebvre op cit note 43 at 313; Reinhardt Buys & Francis Cronjé *Cyberlaw@SA II: The Law of the Internet in South Africa* 2ed (2004) 86; Coetze op cit note 52 at 513
[57] Myburgh op cit note 4 at 21.
[58] Schellekens op cit note 42 at 67.
[59] Havenga & M Havenga (eds), E Hurter, R Kelbrick, E Manamela, T Manamela, H Schulze & P Stoop *General Principles of Commercial Law* 7 ed (2010) 377.
[60] Schellekens op cit note 42 at 68.
[61] Schellekens op cit note 42 at 68; *Construction and Allied Workers Union v Lesotho Brick and Pave and Another (Pty) Ltd* [2011] LSLC 28; *Jurgens v Volkskas Bank* 1993 (1) SA 214 (A) 220F.
[62] Schellekens op cit note 42 at 69.
[63] Schellekens op cit note 42 at 69.
[64] *Van Rooyen v Hume Mellville Motors (Edms) Bpk* 1964 (2) SA 68; Van Huyssteen et al *Contract General Principles* op cit note 33 at 162.
[65] Bhana et al op cit note 29 at 108; See also *Fraser v Viljoen* 2008 (4) SA 106 (SCA) at para 4*; Just Names Properties 11 CC v Fourie* 2008 (1) SA 343 (SCA).

beneath the declaration, it becomes difficult for anything new to be added to the document.[66] Therefore a signature can be a shield against attack on the document's integrity.

2.5.5 Originality

A signature functions as an averment that a signed document is original and not a copy of another.[67] The originality function therefore adds a positive influence on the assessment of the document's evidentiary value.

2.5.6 Cautionary function

A signature also indicates that a signer exercised caution before signing the document.[68] A signer will not immediately attach their signature to a document, instead, the signer is more likely to apply their mind to the contents of the document and consider its legal implications upon signature.[69] Signature thus evidences that the signer applied caution and had informed consent when concluding a transaction.[70]

2.5.7 Attribution function

Furthermore, a signature 'attributes the document to a specific person… .'[71] Attribution refers to whether something results from an act of a particular person, for example whether a signature results from acts of a particular person.[72] Care should be taken not to confuse the concept of authentication with the concept of attribution; the two are different.[73] Attribution is concerned with whether 'an … event may be linked to a person … [and] whether a … message was actually sent by the person who is indicated as its originator.'[74] In the online

[66] Schellekens op cit note 42 at 69.
[67] Van der Merwe et al *Information* op cit note 43 at 176.
[68] Schellekens op cit note 42 at 70; Myburgh op cit note 4 at 21.
[69] *Fourlamel (Pty) Ltd v Maddison* 1977 (1) SA 333 (A) 342-343. The court noted that in contracts of suretyship, the signature requirement draws the attention of the potential surety to the inherent dangers in the suretyship contract before he/she binds himself.
[70] Schellekens op cit note 42 at 71.
[71] Van der Merwe et al *Information* op cit note 43 at 176; Anjanette H Raymond & J Benjamin Lambert in 'Technology, e-commerce and the emerging harmonization: the growing body of international instruments facilitating ecommerce and the continuing need to encourage wide adoption' (2014) 17 *International Trade and Business Law Review* 419 at 432.
[72] Manuel Alba 'Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions' (2014) 47 *Creighton Law Review* 387 at 390-391.
[73] Randolph A Kahn & Dianne J Silverberg 'From Mount Sinai to Cyberspace: Making Good E-business Records' (2001) 57 *Business Lawyer* 431 at 432; Pretorius & Visser (2003) 239 cited in JMC Johnson 'Chapter 8: Consequences of and problems with electronic contracts' 126 available at *reference.sabinet.co.za/webx/access/electronic_journals/medsor/medsor_n37_a9.pdf*, accessed on 24 June 2014.
[74] Johnson op cit note 73 at 124; Tana Pistorius ' "Nobody knows you're a dog": The attribution of data messages' (2002) 14 *SA Merc LJ* 737 at 739; Alba 'Order out of chaos' op cit note 72 at 390 explains that a 'signature shall be attributed to one person if it results from the acts of that person.'

world, attribution deals with whether a certain person can be said to have executed an act performed by a computer. It does not follow that a message authenticated by a signer is automatically attributable to him.[75]

In a similar vein, attribution should not be confused with identification. Whereas attribution in the context of contract deals with whether a signature results from acts of a particular person, identification is concerned with verification that one is who he/she claims to be.

It is evident that the concept of signature is not just a thing, but a process of adducing evidence.[76] It is evidence of the signer's identity and their assent to contents of a document. These functions of signature meet the purposes of formalities, namely to provide evidence of a contract and reduce incidents of fraud and uncertainty in conclusion of contracts. Different types of signatures in the offline world are discussed next.

2.6 Types of traditional signatures

Mason divides traditional signatures into three categories, namely manuscript signatures, impression of a mark and mechanical marks by human action.[77] The section explores the different categories of signatures.

2.6.1 Manuscript signatures

A manuscript signature is defined as 'a pen and paper signature.'[78] There are different types of manuscript signatures and the courts have insisted that they will only be recognised as signature provided there is evidence that the signer used them with an intention to be bound. These manuscript signatures include use of name without a signature,[79] initials,[80] an abbreviated name,[81] a trade name,[82] a partial signature,[83] the use of words that spell out the

[75] Johnson op cit note 73.
[76] Reed 'What is a Signature?' op cit note 36; Myburgh op cit note 4 at 21.
[77] Stephen Mason *Electronic Signatures in Law* 4 ed (2016) 17, 38 & 66.
[78] Louis Van Eeden 'Document security and electronic signatures' (2011) 4 *Enterprise Risk* 19.
[79] *Jhajbhai & others v Master and Ano* 1971 (2) SA 370.
[80] *Ariefdien v Soeker* 1982 (2) SA 570 (C) 578 A-E; *Newell v Tarrant* (2004) WL 741782 para 47; *Selebeng v Hlalele* [2000] LSCA 106.
[81] In *Bartletts de Reya v Byrne* (1983) *The Times* 14 January; (1983) 127 SJ 69, Court of Appeal (Civil Division) cited in note 160 of Mason op cit note 77 at 37, the court stated that an abbreviated name does not invalidate the document but reflects an intention to authenticate just as initials.
[82] Mason op cit note 77 at 32.
[83] Courts of law have accepted a partial signature made by an ill person depending on the circumstances prevailing at the time. If the surrounding circumstances, such as level of illness, indicate the signer's intention to sign a document such as a will, then the incomplete signature is accepted as such (*Re Chalcraft's Goods* [1948] P 222).

signer's relationship with the person he/she is writing to,[84] the use of an identifying phrase,[85] a mark such as a cross,[86] and an assisted mark or signature.[87]

Courts of law have therefore approved manuscript signatures since time immemorial. The next section looks at traditional signatures made through imprinting marks on a document.

2.6.2 Imprint of a mark for signature

Signers have used the imprint of a mark as a signature for centuries. At least five types of marks can apply as signature. For one, courts recognise a seal imprint but emphasise that the intent behind the act of imprinting a seal is the most important determining factor on the admissibility of a seal.[88] The marks further include the finger print;[89] printed name;[90] lithographed name;[91] and a rubber stamp provided it is used with the authority of the person it represents.[92] The courts have thus accepted these symbols as signatures only if the circumstances indicate that the signer used them to signify their intention to adopt a declaration.

2.6.3 Signature through mechanical marks

Signature by mechanical marks may be through a typewritten name, a telegram,[93] telex or facsimile.[94] Courts recognise a typewritten name as a signature if evidence that the name was

---

[84] See *Cook In the Estate of (deceased) Murison v Cook & Another* [1960] 1 ALL ER 689.
[85] *Rhodes v Peterson* [1971] SC 56.
[86] See Bradfield op cit note 7 at 128. See also *Van Niekerk v Smith* 1952 (3) SA 17 at 25; *Harpur* supra note 39 at 760E.
[87] *Matanda v Rex* 1923 AD 435 (B); Mason op cit note 77 at 23-4 & *Van Niekerk* ibid 25.
[88] Sharrock op cit note 2530 at 539; *First National Securities Ltd v Jones* [1978] 2 ALL ER 221, CA at 119 E. Examples of statutes which require a seal in Lesotho are the Lesotho Mines and Minerals Act 4 of 2005, s 11 of the Companies Act 18 of 2011 and Reg 70 (2) of Companies Regulations 2012.
[89] *Sebeko* supra note 50; *Putter* supra note 41; Sharrock op cit note 25 at 123.
[90] In *Sarl v Bourdillon* 140 ER 79 the court held that the printed name of the plaintiff on the first page of an Order book was sufficient to constitute a signature, therefore all entries of orders placed in that book constituted agreements between the person ordering and the Plaintiff. See also *France v Dutton* [1892] 2 QB 208.
[91] *R v Cowper* (1890) 24 QBD 60, 533 cited in Mason op cit note 77 at 52. However, a lithograph has fallen out of use.
[92] *Lesotho Public Motor Transport (Pty) Ltd v Lesotho Bus and Taxi Owners Association* [2015] LSHC 29 ; *Associated Engineers Co Ltd v Goldblatt* 1938 *WLD* 139; *John Barr & Co (Pty) Ltd* 1967 (3) SA 292 (W); Bradfield op cit note 7 at 237; *Macdonald v Sun Life Assurance Company of Canada* 2006 CanLII 41669 (ON SC); Nazzal M Kisswani & Anas A Al-bakri 'Regulating the use of electronic signatures given the changing face of contracts' (2010) 7 *Macquarie J Bus L* 53 at 54.
[93] A telegram is 'a message or communication sent by telegraph' which is subsequently conveyed in printed or written form. Dictionary.com available at *dictionary.reference.com/browse/telegram,* accessed on 03 June 2014. See also *Black's Law Dictionary* Free online legal dictionary 2 ed available at *http://thelawdictionary.org/telegram/,* accessed on 21 March 2017.
[94] Facsimile is defined as 'a method of transmitting over telephone lines an exact copy of a printing…[or] communication sent or received by [a telecopier]' (Garner BA *Black's Law dictionary* 10 ed (2009)).

typed with the authority of the signer and an intention to be bound by the signer is adduced.[95] Courts further recognise a signature made by a telegram clerk through a telegram as the sender's signature. This is since the message sender gives the telegram office clerk authority to write their signature where it forms part of message.[96] Moreover, the courts recognise a sender's signature where it is in a text message sent through telex.[97] The courts also recognise signature on facsimile. They accept it on the basis that it is an exact copy of the original signature.[98]

Courts of law therefore legally recognise all traditional signatures, although they accept some signatures more readily than others. They indicate that the basis for legal recognition of offline signatures is whether a signer affixed a signature to a document with the intention to authenticate the declaration. Without this primary element of authentication, the courts will not accept the purported signature. Consequently, the courts' treatment of traditional signatures demonstrates that the type of signature a signer applies is irrelevant in law; instead function of a signature takes precedence over its form. This said, it is noted that traditional signature may be subject to certain risks.

2.7 Risks of the traditional signature

The different forms of traditional signatures discussed above have a main challenge which is the risk of forgery.[99] In the case of a manuscript signature, the quality of the signature rests in the fact that no two people's handwritings are the same.[100] Therefore forgeries of the manuscript signature are difficult to make.[101] Where a forgery is suspected, the courts may call in handwriting experts to conduct a forensic investigation to verify the authenticity of the signature in question.[102] Where possible, a forgery can be proved without a handwriting

[95] *Ardery v Smith* 35 Ind App 94 73 NE 840 at 841; *Newborne v Sensolid (Great Britain) Ltd* [1954] 1 QB 45; Orifowomo et al op cit note 43 at 357; Mason op cit note 77 at 67-8.
[96] Mason op cit note 77 at 73; *Craib v Crisp* 1984 (3) SA 594 (T).
[97] *Good Challenger Navegante SA v Metalexportimport SA* [2004] 1 Lloyd's Rep 67 at 72. Nonetheless, Reed raises a number of concerns with respect to the authentication function of such a signature. The first concern is that where communication is through telex, identification is of a machine that one communicates through, not the identification of the actual party that sends the message. Secondly, it is possible to manipulate a telex and make it transmit a false identification message. Lastly, where a message is stored by the recipient its contents may be altered. Reed 'What is a Signature?' op cit note 36 at 4.1.
[98] See Canadian case of *Beatty v First Exploration Fund 1987 and Company, Limited Partnership* 25 BCLR 2d 377 (1988) 385. See also *Africa Solar (Pty) Ltd v Divwatt (Pty) Ltd* 2002 (4) SA 681 (SCA) at 706.
[99] See for example *Ntsihlele v Lesotho Bank* [2010] LSLC 32; *Lisenyeho v Mahlomolatoki* [1997] LSHC 16; *R v Rammoneng* [2002] LSCA 110; *Pheko v Mafeteng United Co-Operative Society* [1985] LSCA 119.
[100] Orifowomo et al op cit note 43 at 359.
[101] *Harpur* supra note 39 at 760.
[102] Benjamin Wright 'Eggs in Baskets: Distributing the risks of electronic signatures' (1997) 15 *John Marshall Journal of Computer and Information Law* 189 at 190; *Thamae v Crown* [2005] LSHC 214; Buys op cit note 56

expert. For example, the court can, with help of the person whose signature was allegedly forged or of a witness[103] compare the two signatures to identify any unusual inconsistencies.[104]

Another risk of traditional signature is that text can be squeezed between a statement and a signature in paper documents.[105] However, tests that use ultraviolet, infrared of microscopic inspections can determine whether ink was added or removed from a signed document.

Nonetheless, where any malpractice is suspected in any traditional signature, involved parties can adduce evidence before courts of law to prove that a signer did not intend the legal consequences in the alleged signed documents.[106] These risks can be minimised by certain acts of authentication.

2.8 The hierarchies of offline document authentication procedures

The law sometimes requires different levels of document authentication by competent officers. Document authentication in Lesotho is regulated by common law and statutory law. For example the Authentication of Documents Proclamation[107] and Justices of the Peace and Commissioners of Oaths Proclamation.[108] In terms of the Authentication of Documents Proclamation 'authenticate' with respect to a document means to

> 'certify the authenticity of the signature thereon, the capacity in which the person signing the document has acted, and where appropriate, the identity of the seal or stamp which the document bears'.[109]

Forms of document authentication include notarisation, acknowledgement, verification, to make a statement under oath, certification and use of a seal or stamp.[110] When a notary public notarises a document, he/she verifies the identity of the signer, verifies that the signer understands and attests to what he/she is about to sign, witnesses the signer's

---

at 86; *Makhalane v Minister of Law & Constitutional Affairs* [2013] LSLC 73; *R v Sentle & Another* [1988] LSCA 155 at 25; Brand New Technologies op cit note 1.

[103] *R v Thamae* [2005] LSHC 24.

[104] *Lesotho bank (1999) Limited v Boliba Multipurpose Cooperative Society* C of A (CIV) No 43 of 2011.

[105] *Lesupi & Ano v The Crown* [2012] LSCA; *R v Mahase* [1992] LSHC 51.

[106] *Nedbank Ltd v Mendelow No & Another* 2013 (6) SA 130 (SCA); Alan Davidson *The Law of Electronic Commerce* (2009) 79.

[107] No 2 of 1964 of Lesotho.

[108] No 13 of 1945. The list of statutes that require document authentication is not exhaustive.

[109] Section 2 of the Authentication of Documents Proclamation.

[110] Van der Merwe et al *Information* op cit note 43 at 179.

signature, then signs the document himself/herself as indication that the signer signed in their presence.[111] The notarized document may also contain the impression of a notary's official seal.[112] A notarial seal consists of the notary's full names, the area in which he/she practices, the word 'notary' and an emblem.[113] Documents that require notarization include leases, ante-nuptial contracts, powers of attorney, servitudes, wills and bonds. The purpose of notarization is 'to formally verify that a document or state of affairs exists, to the extent it can be independently verified by a person with a commission to do so.'[114]

Acknowledgement on the other hand is an act where the notary (or administrative officer) affirms that a party admitted, in the notary's presence, that he/she voluntarily signed a document for its stated purpose.[115] Verification is an act where a notary certifies on paper that on a certain date, a person appeared before them and signed their name in the notary's presence. The notary then presents the document that the person signed as evidence of the person's identity. In the case of a statement made under oath, the commissioner of oaths affirms that a declarant understands the contents of a declaration he/she is making and helps them take an oath.[116] The declarant then signs the declaration before the commissioner. The commissioner of oaths indicates below the declarant's signature that the declarant acknowledges the contents of the declaration. He/she then states the date and place of oath taking together with his/her (commissioner) details.[117] But with certification a notary takes a normal photocopy of a document and affirms that it is a true copy of its original.[118] Furthermore, a seal is a design pressed onto wax, or an initial or other design embossed on a

[111] FE van der Merwe *Notarial Practice* (2001) 8 & 16; Sharrock op cit note 25 at 126; Simpson Notaries available at *https://www.simpsonnotaries.com/notarized/*, accessed on 25 November 2015; See also s 5 (4) of the Authentication of Documents Proclamation.
[112] Van Der Merwe *Notarial Practice* op cit note 111 at 10.
[113] Allen West *Conveyancing Practice Guide* 4 ed (2015) 138.
[114] Drukker Solicitors 'Notarisation' available at *http://www.drukker.co.uk/publications/reference/notarisation/#.VlWwFHaDFBc*, accessed on 25 November 2015.
[115] Charles N Faerber 'Being there: the importance of physical presence to the notary' (1997-1998) 31 *John Marshall L Rev* 749 at 751.
[116] They make the declarant utter the words 'I sincerely swear that the contents of this declaration are true, so help me God' (Van der Merwe *Notarial Practice* op cit note 111 at 18-19).
[117] Van der Merwe *Notarial Practice* op cit note 111 at 18-19; see also s 6 of the Commissioners of Oaths Proclamation.
[118] Van der Merwe *Notarial Practice* op cit note 111 at 9.

document to show the document's authenticity.[119] Additionally, a seal safeguards a document's originality.[120]

The Authentication of Documents Proclamation illustrates the differing authentication levels required by law. First, it requires an administrative officer to authenticate a signature on a document with his/her signature, with use of a certificate of authentication optional.[121] A certificate of authentication states the administrative officer's name and capacity, that a particular person signed the document in the administrative officer's presence, that he/she or other witnesses personally knew the signing party and gives the date and place of authentication.[122] Secondly, he/she must authenticate a document from Lesotho for use in Lesotho with a signature and a seal or stamp, or statement that there is no seal. The use of a certificate is still optional.[123] Third, to authenticate a document emanating from Lesotho for use in a foreign country, the administrative officer' must attach to the document an Apostille, his/her signature and a seal or stamp of office.[124] Fourth, for authentication of documents from outside Lesotho for use in Lesotho, the Proclamation alternates between authentication by signature, certificates, seal or stamp depending on where a documents emanates from.[125]

It is noted that the Proclamation does not specify the form of signature sufficient for authentication of documents or signature. It defines 'signature' with respect to a document to 'include execution of a document by any other lawful means'.[126]

Additionally, the Proclamation attaches presumptions to the acts involved in document authentication. For one, it gives a certificate of authentication the presumption that it is attributable to its signer.[127] Further, the Proclamation stipulates that the certificate must be prima facie evidence of the facts it attests.[128] However, these presumptions do not preclude a trier of fact from accepting evidence to the effect that a document was indeed signed by a

[119] Seal Dictionary Definition available at *http://www.yourdictionary.com/seal*, accessed on 16 March 2016. See also Van Der Merwe *Notarial Practice* op cit note 111 at 10; Reg 1 of the Lesotho Companies Regulations 2012 states that a '"company seal" means an official mark of a company, consisting of an embossed impression on paper evidencing the formality of the company's execution of the document and its intention to be bound.'

[120] Karla J Elliott in 'The notarial seal - the last vestige of notaries past' (1998) 31 *The John Marshall L Rev* 903 at 905 & 908, hence its effectiveness against fraud and forgery.

[121] Sections 5 (1) & (3) of the Authentication of Documents Proclamation.

[122] Schedule 1 of the Authentication of Documents Proclamation.

[123] Section 6 of the Authentication of Documents Proclamation.

[124] Sections 9 (2), ss 10 (b), 12, 13 & 15 and the Second Schedule of the Authentication of Documents Proclamation.

[125] Sections 12, 13, 14 & 16 of the Authentication of Documents Proclamation.

[126] Section 2 of the Authentication of Documents Proclamation. It further states that 'sign has an equivalent meaning.'

[127] Section 3 (2) of the Authentication of Documents Proclamation. The certificate should be stamped under the Stamp Duties Proclamation.

[128] Section 3 (3) of the Authentication of Documents Proclamation.

particular party or proving the capacity in which the person acted.[129] Lastly, the Proclamation states that a document that appears to bear a signature of an officer of the Crown together with a seal or stamp of their department shall be presumed to be signed by that person unless the contrary is proved.[130]

While there is no legislative instrument in Lesotho which regulates acquisition of a seal or stamp, in practice, an officer approaches a stamp making supplier with details to be imprinted on the stamp and pays approximately seven hundred rands (R700.00) for it. Hence it is relatively easy to acquire a stamp.

To sum up, an administrative officer's, competent officer's or notary's signature has the same purpose in the acts of document authentication: namely to confirm the identity of parties who signed, [131] certify the genuineness of signatures in a document[132] and to formally verify that a document or state of affairs exists.[133] The seal or stamp serve to authenticate a document and show its originality, while a certificate of authentication is presumed to attribute a document to its signer and to be prima facie evidence of the facts it attests. Authenticated documents have more legal credibility and better chances when tested in court.[134] They therefore deter fraud and forgeries. The hierarchies of document authentication thus seek to achieve the purposes of the signature formality previously discussed.[135]

Having examined traditional signatures, the following section discusses the concept of an e-signature and the corresponding functions of traditional signatures that they can perform.

2.9 The Electronic Signature

Electronic documents and transactions need to be signed just as paper documents do. The effect of an e-signature in an e-transaction needs to be similar to that of a traditional signature in the offline world. This is because it is important to verify that the person sitting at a keyboard is who he/she claims to be, and is authorised to perform the act he/she asserts is authorized to do.[136]

---

[129] Section 3 (4) of the Authentication of Documents Proclamation.
[130] Section 7 of the Authentication of Documents Proclamation.
[131] Faerber op cit note 145 at 762.
[132] West op cit note 143 at 147; Elliott op cit note 120 at 907.
[133] See Drukker Solicitors in note 144 above; Kaata Kartau & Kirsty Saldu 'The purchase and sale of registered immovable property: stages of the registration process carried out by notaries and ensuring the effecting of transactions' (2001) 10 *Juridica* 685.
[134] Van der Merwe et al *Information* op cit note 43 at 122; Investopedia available at *http://www.investopedia.com/terms/n/notarize.asp*, accessed on 26 November 2015.
[135] See part 2.2 above.
[136] Schellekens op cit note 42 at 15.

Researchers have made several attempts to define the concept of an e-signature. For one, an e-signature is defined as 'anything in electronic form that can be used to demonstrate a signing entity intended their signature to have legal effect.'[137] It is also described as 'any symbol, mark or method, accomplished by electronic means, executed by a party with the present intent to be bound by a record or to authenticate a record.'[138] The words 'electronic signature' therefore signify the general concept of a signature which is conveyed by the application of a computer or computer like device.[139]

Scholars make a distinction between signature as a legal term and signature as a technical term in e-communications.[140] Some maintain that signature as a legal term refers to any e-signature technology that can work in place of a manuscript signature in e-transactions and have a legally binding effect,[141] while signature as a technical term refers to a digital signature supported by Public Key Infrastructure (PKI) technology.[142] This distinction gives two different implications on the use of e-signatures.[143] That is, a technical signature ensures integrity and authentication of signed data.[144] Hence it is a technology that provides information security. Mason suggests that authentication in the context of information security has two meanings relevant to e-signatures. First it refers to the verification of the identity of a person and secondly, refers to verification of the origin of a message.[145] Thus some scholars maintain that an e-signature is not a signature per se, but 'just authentication technologies used to confirm the origin of a document.'[146] On the other hand, the legal notion of e-signature attempts to equate an e-signature to a handwritten signature[147] that reflects a

[137] Mason op cit note 77 at 198-199.
[138] Thomas J Smedinghoff 'Analyzing State Digital Signature Legislation' cited in Christopher B Woods 'Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing and Signature Legislation' (1999) 52 *Oklahoma Law Review* 411 at 414; Stephen E Blythe in 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce with Enhanced Security' (2005) 11 *Richmond Journal of Law and Technology* 1 at 3 who defines e- signature as 'any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a writing'.
[139] Mason op cit note 77 at 199.
[140] Christine Kirchberger *Cyberlaw in Sweden* (2011) 272.
[141] Jon Ølnes & Steinar Overbeck Cook *Security and signature requirements for e-tendering systems and services* (16 August 2016) Direktoratet for forvaltning og IKT at 14 & 36.
[142] Ølnes et al ibid at 36.
[143] Kirchberger op cit note 140 at 272; Cecilia Magnusson Sjoberg 'IT Law for IT Professionals' (2013) King's College London Slide 17.
[144] Minyan Wang 'The Impact of Information Technology Development on the Legal concept – A Particular Examination on the Legal concept of "Signatures" ' (2007) 15 *Int'l JL & Info Tech* 253 at 264.
[145] Stephen Mason, Clive Freedman & Sandip Patel 'England and Wales' in Stephen Mason (ed) *Electronic Evidence* 3ed (2012) 327 at 360; Alba op cit note 72 at 390.
[146] Wang 'The Impact of Information Technology' op cit note 178 at 264.
[147] Cecilia Magnusson Sjoberg & Anna Norden 'Managing electronic signatures: Current challenges' 47 *Scandinavian Studies in Law* 79 at 83.

signer's assent to information. However, Sjoberg and Norden argue that different views of e-signature as a legal or technical term cause confusion as users tend to forget that a signature is not just a legal notion but sometimes predominantly serves to safeguard the integrity of a document in e-communication.[148] As a result, they find it prudent to use the term 'e-signature' as a synonym of the digital signature, yet careful to explicitly mention the digital signature where the need arises.[149]

On the contrary, other researchers adopt a broad meaning of technical signature. They maintain that technical signature is 'any action that utilises Information and Communications Technology and is recognised as a signature in a law.'[150] The latter term therefore includes both e-signatures used for the purpose of identification[151] and the digital signature.[152]

Despite the proposed differences between legal and technical signature, this study adopts Sjoberg and Norden's views. It understands that an e-signature is any technology that uses ICT in e-transactions to show a party's assent to information (authentication) and *sometimes* show the integrity of a message.[153] Hence 'e-signature' in this work encompasses all e-signature technologies including the digital signature supported by PKI. Put differently, a digital signature based on PKI is a form of e-signature, but an e-signature may consist of other technologies apart from the digital signatures based on PKI. Amongst these technologies are the username, passwords, electronic sound, typed name in an e-document, clicking on an icon, acceptance through browsewrap agreements, email signature, digitised signature, contactless identification, biometrics technology and digital signature based on a Pretty Good Privacy (PGP) web of trust. Although the digitised signature sounds like the digital signature, the two are different forms of e-signatures. Nonetheless, as reflected in Diagram 1 on electronic signatures attached herein, the study makes a distinction between the other forms of e-signature which it refers to as 'ordinary e-signatures', and the digital signature based on PKI for purposes of analysis.[154] The e-signature technologies are expounded below.

[148] Sjoberg et al ibid.
[149] Sjoberg et al ibid.
[150] Andres Guadamuz & Andrew Rens 'Comparative analysis of copyright assignment and licence formalities for open source contributor agreements' (2013) 10 *SCRIPTed* 207 at 216.
[151] Guadamuz et al ibid at 222.
[152] Guadamuz et al ibid at 229.
[153] My emphasis.
[154] See Diagram 1 on e-signatures annexed hereto.

2.9.1 Usernames, Passwords, PINs and e-Tokens

A username is a name that distinctively identifies a user to a computer system.[155] Most usernames consist of a series of letters and/or numbers and/or symbols.[156] A password accompanies a username. A password is a 'series of characters typed into a computer in order to gain access to the network.'[157] A password therefore consists of a phrase, words or PIN (a Personal Identification Number).[158] When a user inserts their username into a computer system, the computer requires them to verify their identity by entering a password which is known to him/her and the system alone.[159] When the two (username and password) work collectively, a user is said to login to a system. Passwords therefore perform authentication or identification purposes in e-commerce.[160]

However, passwords are susceptible to compromises which can weaken their authentication power. For instance, a user tends to select passwords which are short and easy to remember thus an attacker can effortlessly crack and abuse them.[161] They may also write passwords on a piece of paper that can be easily located by another person and misused.[162] Further, fraudsters can acquire passwords through phishing, dumpster diving and other means.[163] To guard against the weaknesses, a user can use a password together with an electronic token (e-token). An e-token is a hardware mechanism that stores user passwords through either a secure storage device or an active device 'that yields one-time passcodes'.[164] The e-token is placed in either a USB interface,[165] on a smart card or in other alternative technologies.[166]

---

[155] Darrel Ince *Dictionary of the Internet* 3 ed (2013) Online publication, accessed on 18 March 2016.
[156] TechTerms.com available at *http://www.techterms.com/definition/username*, accessed on 18 May 2014
[157] Ince op cit note 155.
[158] Lawrence O'Gorman 'Comparing Passwords, Tokens, and Biometrics for User Authentication' (Dec 2003) 91 *Proceedings of the IEEE* 2021 at 2022 .
[159] Margaret Rouse 'Password' available at *http://searchsecurity.techtarget.com/definition/password*, accessed on 18 May 2014.
[160] BusinessDictionary.com available at *http://www.businessdictionary.com/definition/password.html*, accessed on 18 May 2014.
[161] O'Gorman op cit note 158 at 26 & 30.
[162] See Autralian case *H Sayner and Joblink Plus Limited – re Termination of employment* PR950280 [2004] AIRC 748 (30 July 2004).
[163] Grant Christianson 'Advanced Electronic Signatures' 2012 November *De Rebus*; Kim-Phuong L Vua, Robert W Proctorb, Abhilasha Bhargav-Spantzelb et al 'Improving password security and memorability to protect personal and organisational information' (2007) 65 (8) *International Journal of Human-Computer Studies*.
[164] O'Gorman op cit note 158 at 19-20. At 3 they explain that '[a] passcode is a secret number like a password, except it is machine-generated and machine stored, so it can be longer, more random, and perhaps changing.'
[165] Rose India Technologies Pvt Ltd 'What is an e-Token?' available at *http://www.roseindia.net/whatis/etoken.shtml*, accessed on 18 May 2014.
[166] Russell Coker 'Types of Security Tokens' available on *https://etbe.coker.com.au/2010/03/15/security-tokens/*, accessed on 29 December 2016.

The advantage of usernames and passwords is their inexpensiveness and convenience.[167] The disadvantage of the token is that a user has to always carry it.[168]

2.9.2 Electronic Sound

Software installed into a telephone can capture and make a digital record of the sound of a person speaking over the phone.[169] Some jurisdictions such as the USA recognize assent made by a party to an agreement over the telephone as an e-signature.[170] Use of an electronic sound as a signature is not limited to a telephone but may be made into any software code.[171]

2.9.3 Typing a name into an electronic document

A party's act of typing a name on a screen is considered a signature by numerous jurisdictions. For instance, in a South African case of *Spring Forest Trading v Wilberry*[172] the court held that a typed name at the foot of an email message identifies the email user and authenticates contents of the email.[173] The USA[174] and Australia[175] uphold the same principle as well. The rationale for approving this signature is that current technological developments enable discussions to be held through e-communications, such as an offer and acceptance of employment by email. The content of the e-communications forms an agreement between the parties. Thus the typed names of the parties in an e-communication are a clear indication of an intention to be bound by terms of the agreement, and authenticate information in the documents.[176]

The limitation of a typed name is that it is vulnerable to forgery.[177] An imposter can easily type it into a document.

---

[167] O'Gorman op cit note 158 at 30.
[168] O'Gorman op cit note 158 at 19 & 20.
[169] Mason op cit note 77 at 201.
[170] *Shroyer v New Cingular Wireless Services Inc* 498 F 3d 976.
[171] Mason op cit note 77 at 201.
[172] (725/13) [2014] ZASCA 178 (21 November 2014).
[173] At para 28. See also *Rumarch Investment Holdings (Pty) Ltd v Old Fashioned Fish and Chips (Pty) Ltd* unreported case no 21168/2014 of 25 March 2015 at para 47.
[174] Wilkens v Iowa Insurance Commissioner 457 N W 2d 1 (Iowa Ct App 1990); Shattuck v Klotzbach 2001 Mass Super LEXIS 642 (Super Ct Mass 2001); Dow Chemical Company v General electric 58 UCC Rep Serv 2d (CBC) 74 (E D Mich 2005); Mason op cit note 77 at 223.
[175] *Faulks v Cameron* [2004] NTSC 61.
[176] *Computer Sky Edv v Prime Medical Company Ltd* Tel-Aviv Peace Court unpublished Israeli Civil Case no 29488/04 of 4 August 2004 cited in Mason op cit note 77 at 230. See also Lorna Brazell *Electronic Signatures and Identities Law and Regulation* 2 ed (2008) 81. In *Spring Forest Trading v Wilberry* [2014] ZASCA 178 at 11, Cachalia J stated that courts consider whether a method used identified and authenticated a party and do not look at the form of signature a party applied.
[177] Brazell ibid.

2.9.4 Clickwrap agreements

A click on an icon can also authenticate a document. In this case a supplier displays terms and conditions of a contract on their commercial webpage. Any person who wishes to contract with the supplier is to click on an icon that says 'I agree' or 'I accept' to indicate their intent to be bound by the agreement.[178] One cannot proceed to the next stage on the webpage before clicking on this icon.[179] The party's act of clicking the icon thus constitutes authentication of his intention and signifies a signature.[180]

Regrettably, a party's act of clicking on an icon cannot guarantee the signature function of identification.[181] Given security issues surrounding the Internet, a party may experience difficulty to prove that the other party, the buyer for example, is the one who indeed clicked on an icon.[182] Furthermore, steps that a party takes in the process of clicking on an icon do not sufficiently communicate the legal implications of entering into a contract. They therefore fall short of fulfilling the cautionary function of a signature.[183] A supplier can counter these problems by designing a clickwrap agreement that has input boxes that require the clicking party to type in their name, address or email addess.[184] A party's act of typing their name will identify the contractor and caution them that they are about to enter into a contract.

2.9.5 Acceptance through browsewrap agreements

Whether a browsewrap agreement can authenticate a document is debatable. In a browsewrap agreement, a user 'enters into an agreement without giving his unambiguous consent to the terms' of the agreement but by entering the website or using the software. [185] The 'terms and conditions … are posted on a website or web page … usually via a hyperlink on the

[178] Orifowomo et al op cit note 43 at 361; Tana Pistorius 'Click-Wrap and Web-Wrap Agreements' (2004) 16 *SA Merc LJ* 568 at 589; Mason op cit note 77 at 205.
[179] Danielle Kie Hart 'Form & substance in Nancy Kim's *wrap contracts*' (2014-2015) 44 S*outhwestern Law Review* 251 at 252.
[180] Faye Fangfei Wang 'The incorporation of terms into commercial contracts: a reassessment in the digital age' (2015) 2 *Journal of Business Law* 87 at 107; The Law Commission of England and Wales equates the act of clicking on an icon to a manuscript signature conducted with the mark of a cross. Advice from the Law Commission 'Electronic Commerce: Formal Requirements in Commercial Transactions' December 2001 para 3.37 available at *http://lawcommission.justice.gov.uk/docs/Electronic_Commerce_Advice_Paper.pdf*, accessed on 20 October 2014; *Bassano v Toft* [2014] EWHC 377 (QB).
[181] Chissick et al op cit note 38 at 97; Brazell op cit note 176 at 81; David Baumer & JC Poindexter *Cyberlaw and e-commerce* (2002) 76.
[182] Mason op cit note 77 at 208.
[183] Chissick et al op cit note 38 at 97.
[184] Chissick et al op cit note 38 at 97.
[185] Pistorius 'Click-Wrap Agreements' op cit note 178 at 570.

website.'[186] Unlike in clickwrap agreements, a user's assent to the terms is not made a condition to accessing goods, hence perusing the terms of the contract becomes optional. Consequently, the user may not take notice of the terms before use of the website.[187] The user's act of browsing signifies their assent to be bound by terms of that contract, hence their signature to the contract. The argument is that the act of using the website signifies the user's knowledge of the applicable terms, provided that the terms to the contract are noticeable.[188]

Nonetheless, the nature of a browsewrap agreement makes it vulnerable to challenge. Since the user assents to terms by browsing the website and there is no act of self-manifestation required, the contract may not be enforceable due to lack of evidence that the user had actual knowledge of the contract terms. Hence enforceability of a browsewrap agreement will depend on whether a cautious user would have inquired about the terms of the contract. This will depend on the website's design and on whether the hyperlink to the contract terms and conditions is noticeable to a user. [189]

2.9.6 Email signature

An email signature authenticates a document.[190] Email signature refers to either the name in an email address[191] or an email signature block.[192] The information that appears on the 'From' line in an email, which is an email address, clearly indicates who the sender of an email message is and identifies them as the signer of the message. Hence it constitutes signature.[193]

Chissick argues that an email address can be compared to a traditional signature in two ways. Firstly, the signer's act of clicking on the send button is equated to signature of a hard copy document by attachment of a stamp. Secondly, the email address is equated to a letter-head on an offline letter, which indicates who the communication is from.[194]

[186] Hart 'Form & substance' op cit note 179 at 252.
[187] Eliza Mik 'Contracts Governing the Use of Websites' (March 2016) *Singapore Journal of Legal Studies* 70 at 73.
[188] Mason op cit note 77 at 213; Jay Forder & Dan Svantesson *Internet and e-commerce law* (2008) 50; *Edme v Internet Brands Inc* 968 F Supp 2d 519 (2013) 41 Media L Rep 2696.
[189] Mik 'Contracts' op cit note 187 at 73.
[190] Mason op cit note 77 at 269-270.
[191] Mason op cit note 77 at 255.
[192] companySIG.com 'What exactly is an email signature' *http://www.companysig.com/what_is_an_email_signature.php*, accessed on 17 May 2014.
[193] *McGuren v Simpson* [2004] NSWSC 35 para 22; See also *SM Integrated Transware Ltd v Schenker Singapore (Pte) Ltd* [2005] 2 SLR 651 [2005] SGHC 58.
[194] Chissick et al op cit note 38 at 96.

An email signature block on the other hand is a collection of text located at the bottom of an email message. The block consists of the name of a sender and their contact details.[195] The email block is attached to every email a sender sends to their receivers as a form of identification.[196]

The shortcoming of such email footer is that an imposter can easily forge it by copying and pasting it where he/she wants, or they can just type in the contents of the email footer at the end of a message.[197] A fraudster may also use another person's email to defraud others or send defamatory content.[198]

2.9.7 A digitised signature

A digitised signature is a manuscript signature that has been read by a computer and transformed into digital format.[199] A signer may create a digitised signature by either scanning a manuscript signature which will produce a digital image of the hand written signature, or by writing the signature on a special computer input device such as a signature pad.[200] The signer can attach a file consisting of the digitised signature to an electronic document on a computer screen to identify them and to authenticate contents of the document.[201] In such a case, courts may accept the digitised signature as a valid signature.[202]

The drawback of a digitised signature is its susceptibility to forgery.[203] A fraudster can effortlessly copy the digitised signature and paste it on other documents which the signature holder did not intend to sign.[204] Further, it does not guarantee the integrity of a document. A fraudster may alter the contents of a document after a signer has attached a digital signature without trace.

---

[195] companySIG.com op cit note 192.
[196] Kat Neville 'The Art and Science of the Email Signature' available at *http://www.smashingmagazine.com/2010/02/04/the-art-and-science-of-the-email-signature/,* accessed on 17 May 2014.
[197] Emily Maxie 'Digitized Signatures vs. Digital Signatures: A Complete Comparison' 2013 available at *http://www.signix.com/blog/bid/99443/Digitized-Signatures-vs-Digital-Signatures-A-Complete-Comparison,* accessed on the 17 May 2014.
[198] See Australian case of *Tassone v Kirkham* [2014] SADC 134, 2014 WL 3889065.
[199] Office of Management and Budget 'Procedures and Guidance; Implementation of Government Paperwork Elimination Act, 65 Fed Reg 25508-21' (May 2, 2000) in IT LAW.
[200] Orifowomo et al op cit note 43 at 361; Maxie op cit note 197.
[201] Mason op cit note 77 at 287; Brazell op cit note 176 at 81.
[202] See the conflicting views of France and Denmark which do not recognise digitised signatures (Arne Mollin Ottosen 'Case Note Denmark Case Citation U.2006.1341V' (2007) 4 *Digital Evidence and Electronic Signature Law Review* 99) and England which does (Re a debtor (No 2021 of 1995) [1996] 2 All ER 345, Ch D).
[203] Brazell op cit note 176 at 81.
[204] Maxie op cit note 197. See also *Djordje Mitic v Eco Pro Australia Pty Ltd* [2009] AIRC 503 (May 2009).

2.9.8 Contactless Identification

Contactless identification refers to use of cards that consist of a chip with identification information about the card holder. The card need not physically come into contact with a reader for information on it to be utilised. Instead, an antenna mounted in the card transmits the information in the card to the reader by using Radio Frequency Identification (RFID) technology.[205]

The main function of RFID is to automatically identify persons and tagged items in a wireless fashion.[206] Lately, RFID has become a vital link in e-commerce. For instance, it enables fast payment transactions between a consumer and merchant, confirms identity of information seekers and gives such people authority to access the relevant information.[207]

RFID tags are simple, cheap and convenient to use. Additionally, they are unaffected by environmental conditions.[208] These render them an affordable identification device.

2.9.9 Biometrics Technology

A party to a contract can use biometric technology as another form of authentication tool in the conclusion of e-transactions. Biometrics technology refers to 'the technology for measuring and analysing characteristics of a human body',[209] while a biometric refers to 'a feature measured from the human body that is distinguishing enough to be used for user authentication.'[210] A biometric system is therefore a pattern recognition system that identifies a person by comparing his physiological or behavioural attributes (biometrics) to previously determined identities stored as digitised biometric attributes elsewhere.[211]

Biometrics technology in information technology has two main purposes: to recognise a person and/or to verify a person's identity.[212] Verification involves confirming that people

---

[205] 'An introduction to Contactless' available at *http://www.contactless.info/Introduction-to-Contactless.asp,* accessed on the 17 May 2014.

[206] C Mutigwe & F Aghdasi 'Research Trends in RFID Technology' 2007 available at *http://www.stitcs.com/en/rfid/rfidresearchtrends.pdf,* accessed on 29 November 2016.

[207] Smart Card Alliance 'Contactless Smart Chip Technology: The Business Benefits' available at *http://www.smartcardalliance.org/publications-contactless-business-benefits/,* accessed on 20 May 2014 at 1 & 2.

[208] For instance, they work well despite their exposure to water or dirt. Smart Card Alliance ibid at 2.

[209] Schellekens op cit note 42 at 16.

[210] O'Gorman op cit note 158 at 3; Debnath Bhattacharyya, Rahul Ranjan & Farkhod Alisherov A et al 'Biometric Authentication: A Review' (2009) 2 *International Journal of u- and e-Service, Science and Technology* 13 at 14.

[211] Anil Jain, Lin Hong and Sharath Pankanti 'Biometric Identification' (2000) 23 *Communications of the ACM* 91 at 92; Simon Liu & Mark Silverman 'A Practical Guide to Biometric Security Technology' (2001) *IT Pro* 27 at 28; James L Wayman 'Fundamentals of Biometric Authentication Technologies' (2001) *International Journal of Image and Graphics* 93 at 94.

[212] Liu et al op cit note 211 at 29.

are who they say they are by matching their newly captured biometric to their allegedly previously stored biometric template.[213] Recognition involves comparing a newly captured biometric template to all templates stored in a database. Some authors summarise these two purposes as personal identification.[214]

A number of factors will affect the feasibility of the technology's use.[215] For instance, a biometric which is generally possessed by all persons, distinctive to each individual, unalterable, user-friendly[216] and measurable[217] will be practical to use. Peoples' willingness to use a biometric system (acceptance) is also an important factor. For example, if users are afraid their privacy will be threatened, they may not respond well to the biometrics' use.[218] Resource requirements of a biometrics system such as the cost of the equipment, administration and maintenance also affect its feasibility.[219] It follows that a lawmaker is to have insight into these factors so as to assess the practicability of biometrics technology's use in e-commerce.

There are several biometrics available for biometrics technology. Amongst these is the iris. Each iris comprises of a unique and complex pattern consisting of features inclusive of the corona, furrows, rings and filaments.[220] A 'video based image acquisition system' captures the iris pattern and software built into the system creates an iris code.[221] The advantage of an iris recognition biometric system is its speed and accurate results.[222] There is also the retina. The pattern of veins found under the surface of a retina is unique to each individual. A digital image of the vein patterns is photographed and analysed by a coupler. The advantage of a retinal scan is that it cannot be simulated. But the downside is that the retinal scans are expensive, inconvenient to users and require skilled personnel to operate which may be hard to find.[223]

As for finger prints, each individual has a unique pattern of ridges and furrows on a finger. Fingerprints are therefore a good source of personal identification and have been

[213] Wayman op cit note 211 at 93.
[214] Jain et al op cit note 211 at 91.
[215] A Pooe & L Labuschagne 'Factors impacting on the adoption of biometric technology by South African banks: An empirical investigation' (2011) 15 *Southern African Business Review* 119 at 135-6.
[216] Jain et al op cit note 211 at 94.
[217] Jain et al op cit note 211 at 92.
[218] Jain et al op cit note 211 at 92.
[219] Liu et al op cit note 211 at 32; Bhattacharyya et al op cit note 211 at 22; Wayman op cit note 211 at 95.
[220] Bhattacharyya et al op cit note 211 at 17.
[221] Bhattacharyya et al op cit note 211 at 17.
[222] Jain et al op cit note 211 at 97.
[223] Bhattacharyya et al op cit note 211 at 19 & 24.

trusted for centuries.[224] A fingerprint biometric system is affordable. A slight problem is that a subject might have trouble accepting use of the technology as it is associated with criminal investigations.[225] Further there is hand geometry which comprises of an analysis and measurement of a human hand. Either a mechanical or optical scanner capturers hand measurements. This technology is easy to use and inexpensive. However, because of the physical size of a hand, it cannot be used in other applications such as laptops.[226]

Moreover, there is face recognition that can be conducted through creating a facial metric or Eigen faces.[227] The drawback of facial biometrics is that a facial recognition device is external to a normal computer. Thus it is an additional subset of the market for network verification. It is further uncertain whether the face alone can confidently identify a person from a large number of individuals.[228] On the other hand is facial thermogram. The pattern of a vascular system under the skin is distinctive to each individual and therefore constitutes a facial signature of the individual. The infrared camera captures this signature which is called the face thermogram. The advantage of using a face thermogram for personal identification is its user-friendliness and convenience as it does not require contact. Moreover, it cannot be disguised. However, a subject's emotional state or their body temperature may affect the results of a thermogram.[229]

Another biometric is signature verification. This technology analyses the dynamics of making a signature, not the actual signature. It measures the linear features of the signature, together with the speed, direction, pressure, velocity and length of strokes made by the signer in the process of making a signature, and the time spent making the signature. Several applications such as tablets or 'special purpose devices' can capture the dynamics of a signature. The benefits of signature verification are that an imposter cannot forge the signature biometrics.[230]

The voice is also a tool for identification. Vocal recognition technology studies the manner in which one speaks. It analyses the size and dimension of one's vocal bands, mouth, nasal cavity and lips which work together to synthesise a voice and give it a distinct character. The advantage of voice recognition biometrics is that it uses traditional and low-

[224] Jain et al op cit note 211 at 95.
[225] Jain et al op cit note 211 at 93.
[226] Liu et al op cit note 211 at 28.
[227] Tom Wiehl 'Human and computerized facial recognition: comparison and constitutional analysis' (2013) 6 *Northwestern Interdisciplinary Law Review* 95 at 100.
[228] Bhattacharyya et al op cit note 211 at 16; Jain et al op cit note 211 at 95 & Liu et al op cit note 211 at 28.
[229] Jain et al op cit note 211 at 95.
[230] Jain et al op cit note 211 at 97; Bhattacharyya et al op cit note 211 at 20; Liu et al op cit note 211 at 28.

cost hardware such as microphones. It is also a non-invasive technology and thus convenient to the subject. Its disadvantage though, is that voice recognition is susceptible to surrounding noises and is affected by the subject's emotional state.[231]

Other biometric technologies include palm print verification,[232] hand vein geometry,[233] DNA (Deoxyribonucleic acid),[234] ear shape, body odour,[235] keystroke dynamics,[236] fingernail bed,[237] gait and cognitive biometrics.[238]

It is noted that biometrics technology is not perfect, it has its pro and cons. For one, results of their evaluation may be faulty. A biometric technology can reject a valid individual,[239] or accept a fraud.[240] Nonetheless, biometric technologies are difficult to forge,[241] unlike passwords, security codes and so on.

Biometrics used in conjunction with smartcard tokens, which store one's biometric template, are good for e-commerce for verification of the identity of a trading party. Furthermore, a biometric is directly linked to the authenticator and thus ensures that a signer does not reject their signature or act of sending a message.[242] Again, biometrics serve the cautionary function as they involve active participation of the signer such as taking a retinal scan before using it to sign.[243]

Another authentication technology used for signature in e-commerce is a digital signature technology and its discussion follows.

2.9.10 Digital Signature and PKI

To appreciate a digital signature, it is necessary to consider the technical aspects of a cryptography system and how it works as the digital signature applies cryptography.

[231] Jain et al op cit note 211 at 98; Bhattacharyya et al op cit note 211 at 20; Liu et al op cit note 211 at 29.
[232] Palm print verification works like fingerprint verification but the large scanners that accommodate the size of a hand limit the use of the technology (Bhattacharyya et al op cit note 211 at 20).
[233] Hand vein operates like retinal scanning, but it is still undergoing research and not fully operational (Bhattacharyya et al op cit note 211 at 20).
[234] Bhattacharyya et al op cit note 211 at 20.
[235] Body odour can also be captured and turned into a template. But systems which extract the odour are still under development (Bhattacharyya et al op cit note 211 at 20).
[236] Bhattacharyya et al op cit note 211 at 20.
[237] Fingernail bed biometrics technology scans and calculates the space between the dermal structures (channels). The system is developed by the USA Company AIMS (Bhattacharyya et al op cit note 211 at 21).
[238] The most recent development in biometrics is cognitive biometrics. The system looks at the brain responses to specific stimuli and these are linked to a computer catalogue in a 'brain-machine interface' (Bhattacharyya et al op cit note 211 at 15).
[239] This is called a false non-match rate (FNR).
[240] This is called a false match rate (FMR), Jain et al op cit note 211 at 93; O'Gorman op cit note 158 at 11; Bhattacharyya et al op cit note 211 at 23.
[241] Brazell op cit note 176 at 81.
[242] Bhattacharyya et al op cit note 211 at 22; O'Gorman op cit note 158 at 26.
[243] Brazell op cit note 176 at 81.

Cryptography is the art of encrypting and decrypting messages.[244] Encryption involves a process whereby the plain text of a message[245] is scrambled so that it becomes garbled and unreadable. A message breaks down into digit units consisting of 1s and 0s.[246] Encryption then occurs either one digit at a time, or occurs on (groups) blocks of digits.[247] This is done in order to hide the actual content of the message. The garbled message is called ciphertext or a cryptogram.[248] The process of converting the ciphertext back into plaintext which is readable is called decryption.[249] Cryptography is therefore a process which changes a plain message into unreadable hidden form until it is converted into readable form again.[250]

Cryptography requires several instruments. A message sender uses an advanced mathematic algorithm[251] which is referred to as the cipher[252] to encrypt a message. In addition to the algorithm, contemporary cryptography makes use of a key(s).[253] A key consists of a number of values called a keyspace.[254] Cryptography may be symmetric or asymmetric.

2.9.10.1 Symmetric cryptography

In symmetric cryptography parties in communication utilise one key to encrypt and decrypt a message.[255] Parties who wish to communicate must decide on a key to be used for encryption before they commence their communication. The key is only available to the parties to the communication and is unknown to everybody else.[256]

The message receiver decrypts an encrypted message from a sender using the common key he/she holds with the message sender. Successful decryption is strong evidence that the

[244] Schellekens op cit note 42 at 19.
[245] A plaintext message may be 'a stream of binary digits, a text file, a bitmap, a recording of a sound in digital format, audio images of a video or film and any other information formed into digital bits' (Mason op cit note 77 at 295).
[246] Reed 'Old wine in new bottles: Traditional transactions in the internet environment' in *Internet law: Text and materials* 2 ed (2004) 184.
[247] Mason op cit note 77 at 297.
[248] Schellekens op cit note 42 at 20.
[249] Mason op cit note 77 at 295.
[250] Timothy A Wiseman **'**Encryption, Forced Decryption, and the Constitution' (2015) 11 *A Journal of law and policy for the Information Society* 525 at 527.
[251] An algorithm is defined as '[a] documented series of steps which leads to the transformation of some data' (Ince op cit note 155). See for example the RSA algorithm (named after its designers Ron Rivest, Adi Shamir, and Leonard Adleman) and Elliptic curve cryptography, Wiseman op cit note 250 at 533.
[252] Schellekens op cit note 42 at 20.
[253] Wiseman op cit note 250 at 532.
[254] Mason op cit note 77 at 296.
[255] Reed 'Old wine' op cit note 246 at 185; Schellekens op cit note 42 at 20; Mason op cit note 77 at 297.
[256] Reed 'Old wine' ibid; Mason op cit note 77 at 261

message was sent by either of the key holders.[257] However, if decryption through the common key does not lead to a comprehensible message, it is concluded that the message does not come from the sender or the integrity of the message has been compromised.[258] The encryption key is very long, consequently it renders a message secure for it will be difficult to decrypt without the key.[259]

The shortcoming of symmetrical encryption is that while it helps verify the identity of the source of a message such as the computer used to send off the data, it does not verify the identity of the actual sender. This is since a person is not a part of the communication process between the computers.[260] Consequently, it is a good authentication technology for closed groups of users such as banks, where the level of mutual trust is high.[261] Again, with symmetrical encryption there is a single key, which has to transferred/communicated or transported to the receiving party. This is in itself a risk.

2.9.10.2 Asymmetric cryptography

Asymmetric cryptography utilises two different keys, namely the Public Key and a Private Key, to encrypt and decrypt a message. The keys are not identical. The holder of a private key is to keep it a secret while the public key does not have to be kept secret; it may be given to any person or published in a directory on the Internet.[262] Thus, asymmetric encryption is also known as Public Key encryption or Public Key Cryptography. The user may generate a key pair themself, or may ask a third party to generate the pair for them.[263]

In public key encryption, a sender encrypts a message with the receiver's public key, and only the receiver can decrypt the message with their (receiver) private key which is associated to the public key.[264] Alternatively, a sender may encrypt a message with their private key and send it to the receiver, and the receiver will decrypt the message with the sender's public key which is associated with the sender's private key.[265]

Unfortunately to encrypt a complete message with either a public key or private key is computationally expensive and takes long. It is cheaper for a user to subject a smaller string

[257] Reed 'Old wine' op cit note 246 at 185.
[258] Schellekens op cit note 42 at 21.
[259] Mason op cit note 77 at 297; Reed 'Old wine' op cit note 246 at 185.
[260] Mason op cit note 77 at 295.
[261] Mason op cit note 77 at 297.
[262] Schellekens op cit note 42 at 25.
[263] Mason op cit note 77 at 302.
[264] Wiseman op cit note 250 at 533; Lilian Edwards & Charlotte Waelde (eds) *Law and the internet: A framework for electronic commerce* 2ed (2000) 40.
[265] Wiseman op cit note 250 at 533.

to encryption.[266] The Hash function can achieve this effect. [267] It takes a 'variable length input string' such as a message and calculates its 'fixed length input string' which is called the Hash value or Digest. The hash value has a shorter string than an entire message. The slightest change made on a message (the input string) will automatically change the hash value; therefore any interference with the message will be detectable.[268] A one-way hash function is used in cryptography as it is possible to calculate the fixed length input string from the variable input, but it is practically impossible to calculate the variable input string from the fixed length input string. This would practically require more than one million years of calculating. Once the hash value of a message has been calculated, the sender of a message encrypts it with their private key. This encrypted hash value is called the Digital Signature. [269]

The digital signature applies in a particular fashion in e-commerce. After creating a digital signature, A sends the message, together with the digital signature to the receiver, B. Upon receipt of the two, B will first calculate the hash value of the message from A. Subsequent to this, they will decrypt the digital signature with A's public key to get the hash value that was encrypted. B will then compare the two results. If the newly calculated hash value of the message from A is equal to the hash value that was encrypted by A, it means that the digital signature is valid.[270] Applications such as Adobe Reader can verify a digital signature.[271]

The benefits of encryption are fourfold. First, it safeguards the confidentiality of a message.[272] A spy can only see the unintelligible ciphertext in transit, but they cannot decrypt it. Secondly, the effectiveness of encryption as a signature method is that it is computationally impractical to decrypt the encrypted message without a corresponding public key in reasonable time. Therefore it is difficult to forge the digital signature.[273] Thirdly, it assures the integrity of the message as upon decryption the message becomes intelligible. This is proof that the message was not manipulated in transit.[274] Fourth, there is a

[266] Wiseman op cit note 250 at 534.
[267] A hash function is a mathematical process founded on an algorithm that compresses material. Para 40 of Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001).
[268] Schellekens op cit note 42 at 26- 27.
[269] Schellekens op cit note 42 at 26.
[270] Schellekens op cit note 42 at 27; Reed 'Old wine' op cit note 246 at 190.
[271] LawTrust Information Security Solutions 'Our solutions' available at *www.lawtrust.co.za,* accessed on 14 January 2017.
[272] Sharon D Nelson and John W Simek 'Encrypting sensitive emails now a no-brainer' (2016) 41 *Montana Lawyer* 18.
[273] Reed 'Old wine' op cit note 246 at 185.
[274] Schellekens op cit note 42 at 25-26.

presumption that it ensures that authenticity of a message. The fact that the message is decrypted by the necessary key implies that it was sent by a holder of a corresponding key.[275]

There is a drawback to parties' use of a digital signature though. The public key is not a secret and is stored in a public place. Therefore the question is, how does B confirm that the public key is indeed owned by A?[276] Is it possible for an interceptor C, to create a key pair and publish her key as that of A? It is important for the message receiver to verify the identity of the message sender so they confirm who they are contracting with. This drawback can be sorted out through certification of one's public key as elaborated below.

2.9.10.2.1 Verification of a public key through certification – Public Key Infrastructure

Several scholars have attempted to establish an objective link between a public key and its holder.[277] In 1978 Loren Kohnfelder established the concept of certification of a public key.[278] According to Kohnfelder's study, the identity information of an individual or entity together with the key pair information must be digitally signed by the Public File.[279] The signed document is called a certificate of the public key.[280] This certificate will verify ownership of a public key and should be availed to any person who needs it.[281] Over the years, the concept of a public key certificate underwent several improvements. Currently, anybody can sign and issue a public key certificate if they are a trusted third party, trusted intermediary or a trusted service provider.[282] An entity that issues a certificate is called a certification authority (CA).[283]

If one of the communicating parties does not know or trust a CA that signed a public key certificate of the other party, the receiver can ask other CAs they trust to vouch for the

[275] Schellekens op cit note 42 at 25 – 26; Nelson et al 'Encrypting sensitive emails' op cit note 272 at 18.
[276] Mason op cit note 77 at 301.
[277] Whitfield Diffie & Martin E Hellman 'New Directions in Cryptography' (1976) IT-22 *IEEE Transactions on Information Theory* 644; Carl Ellison 'Improvements on Conventional PKI Wisdom' 1st Annual PKI Research Workshop – Proceedings held at NIST in April 2002, 165 available at *www.cs.dartmouth.edu/ ~pki02/,* accessed on 14 June 2014.
[278] LM Kohnfelder *Towards a Practical Public Key Cryptosystem* (unpublished Bachelor of Science thesis, Massachusetts Institute of Technology, 1978) available at *http://groups.csail.mit.edu/cis/theses/kohnfelder-bs.pdf,* accessed on 19 May 2014.
[279] This is 'a central authority trusted by all communicants' (Schellekens op cit note 42 at 28).
[280] Schellekens op cit 42 at 28.
[281] Ellison 'Improvements' op cit note 277 at 165; Chris Sundt 'PKI – Panacea or Silver Bullet?' (2000) 5 *Information Security Technical Report* 53 at 54.
[282] Mason op cit note 77 at 301-302.
[283] Schellekens op cit note 42 at 29.

trustworthiness of the CA in question. This systematic chain of CAs vouching for one another to verify the issued public key certificate is known as a Public Key Infrastructure (PKI).[284]

A person who applies for a public key certificate has to submit a number of documents to a CA. These include their identity documentation,[285] a copy of their public key and evidence that they are a holder of the private key.[286]

The CA also adopts several measures to verify the identity of the applicant. These involve face to face contact with the applicant, use of attestations by authorised persons and so on. When the CA has verified the truth of the contents submitted, it will issue and sign the certificate.

With a public key certificate in hand, A the sender can write a message, calculate its hash value and encrypt the hash value with their private key to get a digital signature. She can then send the message, the digital signature and the public key certificate to B. In this case, A will have sent an authenticated message.[287]

2.9.10.2.2 Trustworthiness of certificate issuing bodies

As previously indicated, an authority issuing key certificates has to be trustworthy for its public key certificates to have value.[288] Trust of an issuing authority could be established through, among others, the use of the Pretty Good Privacy (PGP) web of trust.[289] The PGP system does not need CAs to sign certificates. Instead, a PGP user who is believed to be a reliable introducer certifies another person's public key with PGP software under an

[284] Schellekens op cit note 42 at 30. Public Key infrastructure is also described as a number of protocols that attempt to connect a public key to a legal entity or certain individual and uses trusted third parties to certify the connection. Mason op cit note 77 at 301.

[285] 'Electronic Signatures and Infrastructure (ESI): Policy Requirements for certification authorities issuing public key certificates' ETSI TS 102 042 V2.1.1 (2009-05) available at *http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.01.01_60/ts_102042v020101p.pdf*, accessed on 20 October 2014; Mason op cit note 77 at 302 & 310.

[286] Roger Clarke 'The Fundamental Inadequacies of Conventional PKI' Global Co-Operation in the New Millennium, The 9th European Conference on Information Systems, Slovenia, June 27-29, 2001 at 151. For instance, the applicant can sign a message in the presence of the organisation and submit a delivery point of the certificate to the authority.

[287] Schellekens op cit note 42 at 29.

[288] This has proved to be surprisingly difficult to do (John D Gregory 'Legislating Trust' (2014) 12 *Canadian Journal of Law and Technology* 1 at 11).

[289] Schellekens op cit note 42 at 32-33.

assumption of a Web of Trust.[290] However, PGP is an informal exercise with no regulation on which model a web of trust should adopt, hence it is not suitable for professional use.[291] Alternatively, trust in a CA can be verified through an assessment of the practices and procedures it employs in the issuance of certificates and its internal management to ensure that they meet required standards.[292] These include its policies on confirmation of identity of employees in key control and its policy enforcement measures. Further, the 'quality of software, design of the network and management of the security system'[293] of a CA will reflect its trustworthiness on protection of keys from attacks by malicious software or from misuse. The CA may publish its policies on the practices in a Certificate Practice Statement.

Certification authorities within one PKI system adhere to the same practices in issuing public key certificates.[294] The X.509 certificate format and the Simple Public Key Infrastructure (SPKI) certificate format are certification formats in regular use.[295]

2.9.10.2.3 The X.509 certificate format

The X.509 certificate is an International Telecommunications Union (ITU) Recommendation. It describes an outline for public-key certificates and thus standards bodies may use it to plan their application to PKIs.[296] ITU presented it in 1996 and since then it has acquired the status of a standard format for certificates.[297] The X.509 certificate consists of, among others, the version of the certificate format in use (which is X.509); the certificate serial number; the signature algorithm of the certificate issuer; the validity period of the certificate in terms of date and time; the Distinguished Name of the owner of the public key which is universally unique[298] and; the subject public key information which consists of the value of the public

[290] Carl M Ellison 'Establishing identity without certification authorities' paper presented at the 6th USENIX Security Symposium in San Jose 22-25 July 1996 available at *www.usenix.org/publications/library/proceedings/sec96/ellison.html*, accessed on 31 July 2014; Fred Piper and Sean Murphy *Cryptography: A Very Short Introduction* (2002) 104-106.
[291] Schellekens op cit note at 33-34.
[292] Mason op cit note 77 at 316; Schellekens op cit note 42 at 34.
[293] Mason op cit note 77 at 310.
[294] Schellekens op cit note 42 at 34.
[295] See INFOSEC Institute 'Cryptography - An Overview of the Public Key Infrastructure Parameters and Standards' 2017 available at *http://resources.infosecinstitute.com/overview-public-key-infrastructure-parameters-standards/* accessed on 11 July 2017 & Oasis PKI 'PKI Technical Standards' 2006 available at *http://www.oasis-pki.org/resources/techstandards/*, accessed on 11 July 2017 for more PKI standards.
[296] ITU-T Recommendations 'Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks' available at *http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509*, accessed on 05 October 2016.
[297] Since ITU is a United Nations agency that specifically deals with information and communication technologies worldwide, the standard is accepted globally (ITU 'About ITU' available at *http://www.itu.int/en/about/Pages/default.aspx*, accessed on 04 October 2016).
[298] Clarke op cit note 286 at 151; Ellison 'Improvements' op cit note 277 at 165.

key and identifies the algorithm which will be used with it.[299] The X.509 is consequently a complex identification certificate.[300]

2.9.10.2.4 Simple Public Key Infrastructure certificate

An SPKI certificate is a less complicated certificate. It is an authorisation certificate which permits the holder to have access to a certain resource.[301] The holder of an SPKI certificate makes a digitally signed request to a protector of a resource to use the guarded resource. If the protector of the resource verifies the digital signature, it will permit use of the resource. An SPKI certificate holder may use an attribute certificate[302] which consists of his/her identity information with the SPKI certificate to reveal their identity.[303] Having explored the technical operation of a digital signature based on a PKI system, the subsequent section examines challenges faced by a user in the management of a private key.

2.9.10.2.5 Management of the private key and its challenges

A holder of a private key must be cautious of their control of the private key and keep it secure. This is so that they remain the only person in possession of the private key who can rightfully create a digital signature with it. If the private key is compromised in any way, the public key certificate has to be revoked to avoid misuse of the private key that may fall in wrong hands.[304] Hence, the holder of a private key has to adopt measures that will ensure its safety.[305]

The private key holder may use support technologies such as passwords, smart cards, biometric technologies and so on to guard the private key. The assumption is that these technologies will not only ensure that the holder is the only one who can access the private

[299] Schellekens op cit note 42 at 35- 7. The X.509 standard further allows for extensions on the information it contains. For example, it may indicate the purpose for which a key will be used, called the Key usage; or indicate reference to Certificate Policies used by the CA in addition to practise statements. Where a CA cannot issue the extension information in a key certificate for one reason or another, the said information may be issued on an *Attribution Certificate*.
[300] Schellekens op cit note 42 at 37.
[301] Schellekens op cit note 42 at 37.
[302] 'Recommendation … ISO/IEC 9594-8 defines frameworks for attribute certificates' (ITU-T Recommendations op cit note 296).
[303] Schellekens op cit note 42 at 37.
[304] Management of a private key is slightly similar to that of a rubber stamp signature. See note 92 above which shows that a rubber stamp will only represent a signature if it is used with the authority of its holder. Where it is used without such authority, then it will be disregarded by courts.
[305] Mason op cit note 77 at 315.

key,[306] but will also authenticate the sender by verifying that they are the person they claim to be.[307]

Conversely, the use of the private key support technologies is not very effective. To illustrate, where a password guards and provides access to a private key, it means that a person who possesses the password to the private key is the one who attached the digital signature to a message. Regrettably the person who enters the password into a computer is not necessarily the holder of the private key but can be anyone who has access to the password.[308] Furthermore, there is software designed solely for theft of passwords.[309] Social engineering has also proved to be effective in retrieving passwords not intended to be revealed,[310] so is installation of keylogging software on a computer to acquire passwords.[311] These challenges make a password a weak instrument to be used for protecting the private key.[312] They lead to a conclusion that PKI does not necessarily prove the identity of the signer, but that someone in possession of the private key signed a file.[313]

Alternatively, a signer can use a smart card to store a private key. However the challenge with smart cards is that the user communicates with the card through a device controlled by a third party, such as a point of sale terminal, thus they lack control over which exact message they signed.[314] Moreover, a smart card can be misplaced, stolen or hacked.[315] Thus the smartcard is not the best technology to secure a private key.

Moreover, where a user stores or uses a private key in a computer, then such private key may be subject to a number of compromises.[316] For one, a third party can use malicious

[306] Schellekens op cit note 42 at 77- 78.
[307] Mason op cit note 77 at 303.
[308] Mason op cit note 77 at 318. The same problem is experienced in the use of a physical stamp.
[309] Mason op cit note 77 at 324.
[310] In this context, '[s]ocial engineering is the art of manipulating people so they give up confidential information' such as passwords, banking details or tricking one to give access to their computer where malicious software can be implanted. A fraudster may conduct this by, for example, sending a person a friendly email which consists of a link. When the email holder opens the link, their computer gets infected and the fraudster gains access to one's information. (Linda Criddle 'What is social engineering?' available at *https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering*, accessed on 11 Decemer 2017). The system takes advantage of the human's tendency to trust. (Sarah Granger 'Social Engineering Fundamentals, Part I: Hacker Tactics' 2001 available at *https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics*, accessed on 11 December 2017).
[311] Wiseman op cit note 250 at 535-536.
[312] Mason op cit note 77 at 319 .
[313] Sundt op cit note 281 at 60.
[314] Mason op cit note 77 at 158 & 329.
[315] Brand New Technologies op cit note 1.
[316] Mason op cit note 77 at 320-324; Aashish Srivastava 'Electronic Signatures: A brief review of the Literature' 605 at 606 available at *http://dl.acm.org/citation.cfm?id=1151469*, accessed on 28 November 2015; Gregory op cit note 288 at 11 -12.

software to copy the private key[317] or to make the signer attach their signature to documents that are not reflected on their screen, which they have no intention to sign.[318] Hence keys stored in a computer are vulnerable to misuse.

The support technologies that have to protect a private key appear to be vulnerable to misuse when applied individually. It is suggested that a private key holder can best protect the private key by applying two support technologies concurrently. For instance, they may store a private key on a smart card and secure the card with a biometric.[319] Although the technologies have their shortcomings reflected on above, they can complement each other to provide a secure means of protection to a private key. However, it is a challenge for a key holder to exclude others from laying their hands on his/her private key.[320]

It follows that a CA must have an effective system in place to revoke certificates of public keys which are associated with compromised private keys.[321] It should place revoked certificates on a record called a Certification Revocation List available to the public.

The challenges posed on management of the private key cast doubt on a digital signature based on PKI technology's capacity to perform the identification, attribution and authentication functions. The digital signature based on PKI may indicate who signed the document, but this does not necessarily indicate who sent the message.[322] Thus it does not guarantee the attribution function of a signature. The challenges further make it questionable whether the holder of the private key is the one who attached the digital signature, thus whether they assented to a declaration. The technology is therefore not a watertight form of authentication.

The challenges discussed above show that the digital signature based on PKI's performance of traditional signature functions, just as the other e-signature technologies discussed earlier, will depend on evidence and surrounding circumstances in each case. Consequently, 'reliance rests on the quality of the digital evidence that ties a presumed identity to a presumed act.'[323]

The factors raised below will help analyse whether the digital signature based on PKI system is practicable.

---

[317] Clarke op cit note 286 at 153.
[318] Nicholas Bohm in 'Watch what you sign!' (2006) 3 *Digital Evidence & Elec Signature L Rev* 45 at 47 & Clarke op cit note 286 at 153.
[319] Liu et al op cit note 211 at 31; Brazell op cit note 176 at 81.
[320] Richard E Smith *Authentication from Passwords to Public Keys* (2002) 431.
[321] Clarke op cit note 286 at 151; Sundt op cit note 281 at 54.
[322] Sundt op cit note 281 at 58.
[323] Mason op cit note 77 at 319.

2.9.10.2.6 Challenges in use of PKI system

The PKI system has several weaknesses which render its use difficult. First, society accepts that a certificate should be created by a CA which protects its signing keys very strongly. This level of security is obtained by use of 'military grade physical and personnel security, multi-factor authentication of people, multi-person access controls, etc. Such a facility is extremely expensive, so there cannot be many of them [certification authorities].'[324] This means that it is an economic challenge to establish a secure CA.[325]

Secondly, a signer's application for a key certificate is an onerous, expensive and rather impractical process. Apart from the applicant's duty to submit a lot of identification documents to a CA, the applicant has to travel to the vault of the CA to get this application processed. Travelling to a vault can include long distances and travel costs, thus be inconvenient. Alternatively, a CA can issue a key certificate through a Registration Authority's (RA) office which can be closer to applicants. The advantage of using RAs is the reduced costs of travel for applicants, but the challenge is that the CA's private key may be stolen as it is stored on a general purpose computer at the RA.[326]

Thirdly, the measures that a CA engages for identity verification are time consuming, costly and complex. To illustrate, a CA may involve a number of organisations in certifying a key such as an RA which assists it to verify the identity of an applicant through companies with identification databases including that of the applicant such as a bank.[327] Moreover, the numerous organisations increase the number of people who could potentially engage in fraudulent activities during the identity verification exercise, including identity theft.[328] The identity verification process can therefore be complicated.

Fourthly, a PKI system's generation of a key pair and distribution of a key certificate is subject to risk and requires careful management. The key pair might be compromised during electronic transportation to the holder.[329] To avoid this, it is advisable for the CA to physically hand over the certificate to the key holder.[330] But the physical delivery can be difficult to achieve as there are few CAs. Alternatively, the key holder should electronically

[324] Ellison 'Improvements' op cit note a 277 at 166.
[325] See Ellison 'Establishing identity' op cit note 290 for proposed improvements on costs and security involved in this issue.
[326] Ellison 'Improvements' op cit note 277 at 167-8.
[327] Mason op cit note 77 at 311.
[328] Ellison 'Improvements' op cit note 277 at 167.
[329] Carlisle Adams & Steve Lloyd *Understanding PKI: Concepts, Standards, and Deployment Considerations* 2 ed (2002) 92-94; Piper et al op cit note 290 at 109-110.
[330] Law Teacher 'Electronic Signatures Dissertation' available at *http://www.lawteacher.net/free-law-dissertations/electronic-signatures-dissertation.php*, accessed on 17 May 2014.

confirm to the CA, contents of the certificate upon its receipt, which confirmation is signed with a different digital signature.[331] But this will require the applicant to already have the first digital signature hence proving to be a costly exercise. Thus distribution of a key certification poses a challenge.

Fifth, a PKI system has technical and implementation challenges. The 'X.509 standards are long, rich, complex and imprecise'.[332] Because of the complexity of the X.509 certificate, key certificate applicants may require technical advice from technicians to complete the application process. These make the application process and key and certificates management a cumbersome, slow and burdensome exercise to the extent that the objectives of the process are compromised. To make matters worse, there are few people who know about public key encryption technology,[333] which can limit its use.

Again, there is a presumption that use of a PKI system ensures non-rejection of a signature in a contract,[334] but the validity of this is questionable. It is presumed that by use of the digital signature with a public key certificate, the sender of a message is precluded from denying that they signed and sent a message.[335] However, the above discussion on management of the private key and its possible compromise indicates that there is no guarantee that the private key holder is the one who attached it to a document and sent a message. [336]

Difficulties related to use of a PKI system therefore demonstrate that its practicability is a challenge. Owing to the identification of risks and difficulties associated with the PKI system, some authors are troubled by the fact that some legislators consider digital signatures based on PKI of such importance.[337]

It is noted though, that there available measures which can curb some challenges of the PKI system. For instance, the message receiver can verify the genuineness of a signature by

[331] Mason op cit note 77 at 312.
[332] Clarke op cit note 286 at 153 -154.
[333] Mason op cit note 77 at 317.
[334] In the digital sphere, this is also referred to as repudiation. LawTrust states that, '[i]n the context of digital security, non-repudiation refers to the ability to ensure that a party to a contract or communication cannot deny the authenticity of their signature on a document, or the sending of a message that they originated' (LawTrust Information Security Solutions 'eDNA' available at *https://www.lawtrust.co.za/solutions/edna*, accessed on 14 January 2017).
[335] Clarke op cit note 286 at 150. See also Sundt op cit note 281 at 57; Ellison 'Improvements' op cit note 277 at 166.
[336] See part 2.9.10.2.5 above; Mason op cit note 77 at 302-303.
[337] Mason op cit note 77 at 320. For more flaws on PKI, see Don Davis 'Compliance Defects in Public-Key Cryptography' Proceedings of the Usenix Technical Conference (March 10, 1997) available on *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=EBDC2E05F435F95ABB068C453F46F618?doi=10.1.1.195.9905&rep=rep1&type=pdf,* accessed on 22 October 2014; Niels Ferguson, Bruce Schneier and Tadayoshi Kohno *Cryptography Engineering Design Principles and Practical Applications* (2010) ch 19.9.

looking at the information system where a message was sent. They can further use an intrusion detection system to establish whether intruders maliciously attached the signature.[338] Unfortunately though, complex information systems are required for these services and their costs can be onerous.

2.9.11 Alternative online authentication methods

There are other online authentication[339] methods that can show the source of information and preserve its integrity apart from the use of the digital signature and PKI which methods are certain, accessible and economical.[340] However the methods do not indicate a sender's approval of information. The authentication methods simply curb ordinary e-signatures' susceptibility to manipulation and enhance information security. Amongst these authentication methods is the Transport Layer Security (TLS) standard which is a successor of the Secure Socket Layer (SSL) authentication standard.[341] SSL is a widely accepted security standard in Internet websites, email services and is trusted by corporate entities for e-commerce including international financial institutions.[342] TLS is also a cryptographic protocol that secures communication between computer servers. For example, it transmits data between a webserver and a web browser such as a user's laptop in an encrypted form.[343] The servers use symmetric encryption to encrypt the data.[344] TLS therefore protects communication between servers whether signed with an ordinary signature or not. A communication network protected by TSL has the letter 's' added to 'http' in the address line.[345] Microsoft Exchange Server and Gmail[346] are examples of programs that use TLS.[347]

---

[338] Srivastava Aashish 'Legal understanding and issues with electronic signatures – an empirical study of large businesses' (2008) 35 *Rutgers Computer & Technology LJ* 42.

[339] Authentication here refers to the verification of the identity of a person or verification of the origin of a message. See 2.9 above.

[340] Lee Swales 'The regulation of electronic signatures: time for review and amendment' (2015) 132 *SALJ* 257 at 259.

[341] Schellekens op cit note 42 at 44-6.

[342] Swales op cit note 340 at 259; Derek E Bambauer 'Schrodinger's Cybersecurity' (2015) 48 *UC Davis Law Review* 791 at 819.

[343] Nelson et al 'Encrypting sensitive emails' op cit note 272 at 18. Daniel Garrie & Rick Borden 'Encryption for lawyers' (2016) *Business Lawyer Today* 1 at 3; Swales op cit note 340 at 259.

[344] Holly Lynne McKinley 'SSL and TLS: A Beginners Guide' SANS Institute 2003 available at *file:///G:/%C2%A0/corrections%20material/SSL%20and%20TSL.pdf*, accessed on 20 December 2016 at 8; Nelson et al 'Encrypting sensitive emails' op cit note 272; Sharon D Nelson & John W Simek **'**Encryption made easy**:** The basics of keeping your data secure' (2016) *Oregon State Bar Bulletin* 1 at 2.

[345] Tyson J 'How Encryption Works' 2017 available at *http://computer.howstuffworks.com/encryption4.htm*, accessed on 10 January 2017.

[346] Nelson et al 'Encryption made easy' op cit note 344 at 3.

[347] Nelson et al ibid.

Another method of online authentication consists in encryption of email messages which are sent to a receiver through Microsoft Outlook or Zix Corporation. Outlook applies asymmetric encryption. The user acquires a digital ID/certificate from Microsoft Outlook Trust Center by following prompts provided by Outlook on a computer.[348] With Zix Corporation, a user simply clicks on a button to encrypt data and sends it to a receiver through Zix Corporation servers. If the receiver has a TLS server the email message is sent directly to their inbox without any processing.[349] If not, there will be a link to the email message for which the receiver will have to create a password to access and read.[350] Zix Corporation is therefore easy and simple to use[351] as there is no need to know about the mathematics behind encryption or any exchange of keys required. A user simply clicks on an encrypt and send icon.[352] This technology is of great assistance to lawyers in the processing of documents such as deeds of transfer and real estate transactions.[353]

A user may alternatively protect the content of a message by putting it in the form of a password protected attachment attached to an email message. Software such as Adobe Acrobat and Microsoft can provide this level of security. Thus only the attachment is secured instead of the entire body of the email.[354]

Additional authentication methods include XML (Extended/Extensible Markup Language) Digital Signature[355] and XML encryption.[356] XML is a member of the HTML (Hyper Text Markup Language) family. HTML is a display language that converts images, text and videos into a comprehensive webpage which is available for display. It is referred to as a 'language of the web'. In addition to displaying material, XML can name and categorise things in a logical manner.[357] XML is considered to be a future standard with the utmost importance. Particular reference is made to its newly developed form of Secure Assertion Mark-up Language (SAML) standard. The standard has achieved the significant status of an

[348] Nelson et al 'Encrypting sensitive emails' op cit note 272 at 19.
[349] Nelson et al ibid.
[350] Nelson et al ibid; Garrie op cit note 343 at 3.
[351] Nelson et al ibid.
[352] Nelson et al 'Encryption made easy' op cit note 344 at 3; David G Ries and John W Simek 'Encryption made simple for lawyers' (2013) 56 *Res Gestae Indiana Bar Journal* 1 at 6. See also Mimecast and Data Motion which can encrypt email communication on a similar manner.
[353] Nelson et al 'Encrypting sensitive emails' op cit note 272 at 19.
[354] Ries et al op cit note 352 at 6.
[355] Van der Merwe 'How standards (such as XML) accomplish electronic authentication in web services' 2005 *Obiter* 665 at 683.
[356] Dana van der Merwe 'The current legal position regarding digital evidence (and XML as a possible solution)' (2010) 73 *THRHR* 81 at 86.
[357] Van der Merwe 'XML as a possible solution' ibid at 83 & 84. 'Authentication, security, integrity and non-repudiability are essential requirements for XML signatures to be secure' (at 86).

Open standard.[358] It permits parties to make assertions of trust in online transactions using XML language.[359]

Further methods that deal with identity management in e-commerce include the E-sig Method which uses XML language generously.[360] There is also the latest supreme language of the Web, namely Extensible Business Reporting Language (XBRL).[361] This is an XML based language which transmits business and financial data.[362] It enables computers to monitor the acts of other computers, instead of human beings monitoring acts of a computer. The above listed technologies can safe guard e-communication against manipulation in online communications,[363] thus will enhance the element of security, integrity of messages[364] and identity verification.[365]

2.10 Conclusion

The chapter explains that the purposes of formalities in the law of contract are to promote certainty, to curb incidents of fraud and provide evidence of a contract. It defines the signature formality as any mark a signer uses to authenticate a document. It then demonstrates that the signature formality achieves the purposes of formalities through a variety of functions. But two major functions on which all other functions of signature revolve are identification and authentication. It illustrates that since time immemorial, courts of law recognise any mark made by a signer as signature provided it performed these two functions. Therefore function of a signature takes precedence over form in offline contracts. Moreover, it noted the hierarchies of document authentication procedures. The purposes of the procedures are, among others, to formally verify that a signature, document or state of affairs exists. This is conducted by one's signature or attachment of a seal or stamp to the document. Again, traditional signatures can be prone to risks of fraud, but any doubt on a signature application is dealt with by presentation of evidence that proves or disproves a signature.

---

[358] Van der Merwe et al *Information* op cit note 43 at 134.
[359] Schellekens op cit note 42 at 43.
[360] Van der Merwe 'XML as a possible solution' op cit note 356 at 86.
[361] Van der Merwe, et al *Information* op cit note 43 at 178; Dana van der Merwe 'XBRL and the law: legal implications of markup languages' 2011 *THRHR* 418.
[362] Van der Merwe 'XML as a possible solution' op cit note 356 at 87.
[363] Schellekens op cit note 42 at 15 &11.
[364] Dana van der Merwe 'XML as a possible solution' op cit note 356 at 86-7; Van der Merwe et al *Information* op cit note 43 at 137.
[365] Garrie op cit note 343 at 1. In addition to authentication and integrity, they provide privacy and availability (Van der Merwe *Information* op cit note 43 at 134).

The chapter further defines an e-signature as any symbol or process achieved by electronic means used to authenticate a record. It then illustrates different types of e-signature technologies. It expounds on how they operate and shows that their capacity of performing traditional signature functions differ. It demonstrates the benefits of the technologies and discusses their shortcomings which may render the reliability of online signatures challengeable. It then discusses the ease of use of the technologies and illustrates that the digital signature based on PKI is the most difficult e-signature technology to apply. Finally it highlights available online authentication technologies which authenticate e-communication by showing its origin and maintain its integrity. The chapter concludes that it is possible for e-signature technologies to give the same effect or outcome as traditional signatures by meeting the functions of a traditional signature. This is provided their shortcomings are adequately addressed.

The next chapter accordingly discusses the conceptual framework of this study which is founded on principles of ICT regulation. It expounds on how the principles should apply in regulation of e-signatures.

CHAPTER THREE: FUNCTIONAL EQUIVALENCE, TECHNOLOGY NEUTRALITY & EFFECTIVE LAW MAKING IN ICT REGULATION

3.1 Introduction

The conceptual framework of this study derives from three principles regarding the legal regulation of ICT, namely, the principle of Functional Equivalence,[1] Technology Neutrality,[2] and of Effective Law Development.[3] The chapter defines the three principles in the context of law of contract, with particular reference to e-signature regulation in e-commerce. It elucidates the foundations of the principles, and traverses when and how they should apply to the regulation of e-signatures. Justifications for their use are made and their shortcomings explored. Mechanisms are suggested that can complement the principles where necessary such as soft law regulation.

This thesis argues that e-signature regulation must be functionally equivalent, technology neutral,[4] and must clarify the aims of the law to be effective. It maintains that online regulation will meet the principle of equivalence only if its requirements are *practicable*.[5] Thus, it should have an equivalent effect in both legal terms and practicability.[6] The thesis maintains that functionally equivalent online regulation will be effective and promote the use of e-signatures, consequently, functionally equivalent regulation will enhance the growth of e-commerce. The principle of functional equivalence calls for investigation.

3.2 Functional equivalence and the principle of equivalence

The principle of functional equivalence is a component of a basic concept, the principle of equivalence, in legal regulation of ICT which is also termed 'what holds off-line, also holds

[1] Maurice Schellekens 'What holds off-line, also holds on-line?' in Bert-Jaap Koops, Miriam Lips, Corien Prins and Maurice Schellekens (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One-Liners* (2006) 51.
[2] Bert-Jaap Koops 'Should ICT regulation be technology-neutral' in Bert-Jaap Koops, Miriam Lips, Corien Prins and Maurice Schellekens (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One-Liners* (2006) 77.
[3] Chris Reed *Making Laws for Cyberspace* (2012) at 179.
[4] Tana 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 *CILSA* 178 at 211.
[5] My own emphasis.
[6] Reed *Cyberspace* op cit note 3 at 120.

on-line.'[7] The principle of equivalence entails that legislators should not, in regulating online activities, place online activities in a more or less favorable position to that of offline activities. Instead, the same norms that apply in the offline world should apply in the online world.[8] The norms should not be stricter, or less strict, but must strike reconciliation between the two worlds.[9] This concept of 'what holds off-line, also holds on-line' is also known as the 'starting point' in ICT regulation. [10]

3.2.1 The meaning of 'offline' and 'online'

The kind of communication involved in an activity together with the mode of transport of material involved determine whether an activity is offline or online.[11] If transportation of material entails physically moving the subject which carries it, for example, moving a letter from one place to another, then the activity is offline. But if transportation of the material occurs through connected wires or a wireless network, in digital format, it is online.[12] Further, if communication is interactive or reciprocal such as on the Internet, it is online.[13] But if it is not interactive, such as traditional television, it is offline.[14]

However, the recent concept of convergence of technologies has had a negative impact on the latter criteria that distinguishes online and offline. Technological convergence involves marrying the telecommunications sector with the broadcasting sector[15] and computing technology[16] with the aim of controlling the technologies under a single umbrella.[17] For example, in South Africa, all these technologies have been merged by and are controlled by a single statute namely the Electronic Communications Act 36 of 2005.

[7] Schellekens op cit note 1 at 51 & 56. Schellekens and Chris Reed are the leading scholars who explain the essence and meaning of the principle of equivalence. Therefore this part of the chapter relies heavily on their works.

[8] S van der Hof 'The Status of eGovernment in the Netherlands' (2007) 11 *Electronic Journal of Comparative Law* 1 at 13.

[9] Schellekens op cit note 1 at 53. Reed *Cyberspace* op cit note 3 at 106. Tana Pistorius ' "Nobody knows you're a dog": The attribution of data messages' (2002) *SA Merc LJ* 737-738.

[10] The principle of equivalence is applicable in this study as e-signatures are used in e-commerce which forms part of ICT.

[11] Chris Reed 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 *International Journal of Law and Information Technology* 248 at 258.

[12] Schellekens op cit note 1 at 55; Reed 'Online and offline equivalence' op cit note 11 at 258. See also R Bruce Wells 'The fog of cloud computing: fourth amendment issues raised by the blurring of online and offline content' (2009-2010) 12 *Journal of Constitutional Law* 223 at 232-3.

[13] Wells ibid at 234.

[14] Schellekens op cit note 1 at 55.

[15] The broadcasting sector includes radio and television.

[16] Computing technology includes computers, laptops and all smart phones which can do functions of a computer.

[17] Dana van der Merwe, Anneliese Roos & Tana Pistorius et al (eds) *Information and Communications Technology Law* 2 ed (2016) 6-7; Ilse van der Haar 'Technology Neutrality; What Does It Entail?' March 2007 TILEC Discussion Paper Tilburg University at 3.

Convergence has therefore rendered the criteria of communication blurry and increasingly difficult to apply.[18] With this in mind, the section below reflects on the origin of the principle of equivalence.

3.2.2 Origins of the principle of equivalence

From the beginning of the online world (also referred to as the Internet in this study), its users who were mainly academics, believed that there was no need for regulation of Internet activities.[19] Around the 1990s, commercial Internet service providers (ISP) availed the Internet to the public. The public subsequently used the Internet for commercial activities. But Internet users maintained that netiquette[20] was sufficient to regulate activities of users of the Internet, making law and policy intruders in their sacred Cyberspace.[21] They argued that the law had no place on the Internet.[22]

Internet users of that time further contended that application of the law to the Internet could only cause trouble. Evidence of this was reflected in the cases of *Stratton Oakmont v Prodigy*[23] and *Cubby Inc v CompuServe Inc*[24] which issued different decisions regarding service providers. In *Cubby*, the District Court of Southern New York held that a service provider is not liable for material posted by its users as it is not a publisher but an electronic library. But in *Prodigy*, the New York Supreme Court rejected Prodigy's argument that they should not be held liable for the defamatory material as they were simply distributors of the material. It held that Prodigy was a publisher of the material as it exercised editorial functions to regulate some of the posted material, hence it was liable for defamation.[25]

The decision in *Prodigy* left online service providers confused as to how to conduct themselves. They were uncertain as to whether they had to screen material from their users and risk liability for defamation, or whether they should refrain from any attempts to screen

[18] Van der Merwe et al *Information* ibid; Van der Haar ibid at 3.
[19] Schellekens op cit note 1 at 51.
[20] These are rules of polite or correct behavior between people using the Internet. AS Hornby, *Oxford Advanced Learner's Dictionary of Current English*, 7 ed (2005).
[21] Richard Hill 'The internet, its governance, and the multi-stakeholder model' (2014) 16 *Info* 16 at 19; Hana Weijers *Made in Africa: A discussion on the role of law in absorptive capacity in African software industries* (2014) 66; Schellekens op cit note 1 at 51.
[22] John Perry Barrow 'Declaration of Independence of Cyberspace' 09 February 1996 Davos, Switzerland, available at *https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration,* accessed on 03 May 2014; See also Andrej Savin *EU Internet Law* (2013) 8.
[23] 1995 WL 323710 (NY Sup Ct 1995) United States of America (USA).
[24] 776 F Supp 135 (SDNY 1991) USA.
[25] Martin Samson 'Stratton Oakmont, Inc. et al. v. Prodigy Services Company, et al' Internet Library of Law and court Decisions available at *http://www.internetlibrary.com/cases/lib_case80.cfm,* accessed on 10 December 2013.

the material and risk their user placing offensive material online.[26] It was for fear of this kind of confusion that the online community resisted interference of the law in online activities.

Despite Internet users' fears of legal regulation of the Internet, reality showed that they did not feel obliged to follow the law.[27] They started prejudicing other people through their online activities. For instance, they were free to make unauthorized use of copyright material, such as music, to the prejudice of copyright holders. In reaction to this disobedience of the law, governments indicated that the online world is part of the offline world and has to be legally regulated.[28]

Governments stated that netiquette is not sufficient for control of online activities. Netiquette's insufficiency was mainly caused by the fact that its rules were subject to a number of interpretations and its enforcement mechanisms were not strong enough to regulate the Internet.[29] Governments therefore devised the starting point for regulation of the Internet, namely 'what holds off-line, also holds on-line' (the principle of equivalence).[30]

The principle of equivalence made its first public appearance in 1997 at the Bonn Ministerial Conference Declaration.[31] European ministers in the Conference made a joint declaration on global information networks and proclaimed that 'Ministers stress that the general legal frameworks should be applied on-line as they are off-line.'[32] Since then, the principle of equivalence has made its way into policy documents and is increasingly recognized by a growing number of law makers.[33] Elucidation of the meaning of this principle is therefore necessary.

---

[26] Alek Felstiner 'Grappling with online work: lessons from cyberlaw' (2011-2012) 56 *Saint Louis University Law Journal* 209 at 220; Traverse Legal Attorneys and Advisors 'After Stratton Oakmont v. Prodigy: Section 230 of the Communications Decency Act Provides Blanket Immunity For Interactive Computer Service Providers' 2008 available on *http://tcattorney.typepad.com/digital_millennium_copyri/2008/07/after-stratton.html*, accessed on the 10 December 2013.

[27] Schellekens op cit note 1 at 52-3.

[28] Dutch policy document titled 'Legislation for the Electronic Highways' (1998) cited in Schellekens op cit note 1 at 53.

[29] Schellekens op cit note 1 at 53.

[30] Schellekens op cit note 1 at 53.

[31] Reed 'Online and Offline Equivalence' op cit note 11 at 248.

[32] Principle 22; Conference held on the 6-8 July 1997, available on *http://europa.eu.int/ISPO/bonn/Min_declaration/i_finalen.html* cited in Reed *Cyberspace* op cit note 3 at 106.

[33] Reed *Cyberspace* op cit note 3 at 106. See for example, the G8 Okinawa Charter on the Global Information Society of 2000 where a declaration was made to 'Promote consumer trust in the electronic market place consistent with OECD Guidelines and provide equivalent consumer protection in the on-line world as in the offline world…' (Knowledge-Based Society and Role of Global Mapping, Conference Global Mapping G8 Okinawa, Okinawa Charter on Global Information Society available on *http://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html*, accessed on 10 December 2013).

3.2.3 The meaning of the principle of equivalence

The principle of equivalence in ICT regulation has at least four meanings.[34] First, the statement implies that the Internet is not above the law, but subject to legal regulation like the entire society;[35] secondly, it is a method that helps find a rule for an online situation. It seeks to discover an offline rule that can work as a model for rules in online situations.[36] Thirdly, it is a substantive guideline used to create rules for online situations; and fourthly it is a policy statement. That is, a familiar legal background must be created online for the purpose of achieving extra-legal online policy objectives. The policy statement sets out norms which will guide online users in their activities.[37] Among these, the meaning that is particularly pertinent to this study is where the principle works as a substantive guideline.

The law-maker can use the principle of equivalence as a guideline in two ways.[38] They can use it to apply an existing offline rule to an online situation. This is referred to as *equivalence of form*. Alternatively, they can use it to formulate a new law for an online situation, which is referred to as *functional equivalence*.[39]

3.2.3.1 Equivalence of form

In equivalence of form, 'if off-line and on-line cases are equivalent, they must be dealt with similarly',[40] consequently a particular rule which deals best with a situation offline will apply to regulate an equivalent situation online.[41] Equivalence of form is illustrated with the case of a bookshop and an ISP. Rules on liability of a bookshop for defamatory content in books it distributes will apply to an ISP as both are distributors of material without editorial control of distributed content.[42]

To determine whether situations are equivalent, the court must first identify an offline rule that will be applicable to an online situation.[43] The rule may be applicable directly or analogously. Subsequently, they should ask the question whether for purposes of the identified rule, the offline situation addressed by the rule is equivalent to the online situation

[34] Schellekens op cit note 1 at 56.
[35] Schellekens op cit note 1 at 53.
[36] Schellekens op cit note 1 at 56. See the cases of *Cubby v CompuServe* supra note 24 and *Stratton Oakmont v Prodigy* supra note 23 above.
[37] Schellekens op cit note 1 at 56; Reed 'Online and offline equivalence' op cit note 11 at 253.
[38] Reed *Cyberspace* op cit note 3 at 107-108.
[39] Reed *Cyberspace* op cit note 3 at 107; Reed 'Online and Offline Equivalence' op cit note 11 at 250.
[40] Schellekens op cit note 1 at 56.
[41] Hill op cit note 21 at 19; Reed 'Online and offline equivalence' op cit note 11 at 250.
[42] Reed *Cyberspace* op cit note 3 at 107; Reed 'Online and offline equivalence' op cit note 11 at 251; Schellekens op cit note 1 at 67.
[43] Schellekens op cit note 1 at 66.

at hand. The court's or lawmaker's interpretation of the rule and its rationale will guide them towards the answer to this question.[44] Schellekens lists three methods that can be used to intepret the rule. First, does the language of a rule in question subsume the online situation? For example, is an e-signature a signature? Secondly, are the goals to be met offline and online comparable? Thirdly, are the underlying legal principes comparable? If for instance, the lawmaker views a rule as a result of a balance between interests, values and principles in an offline situation, and that balance is valid online, they will consider the situations as equivalent.[45]

Equivalence of form differs with the principle of equivalence used as a method but the difference is superficial. Where the principle is used as a method, the lawmaker seeks to find an offline rule they can use as a template for law on online situations.[46] But with equivalence of form, it is determined whether online and offline situations are equivalent so that an offline rule can be reused online. However the methods converge in their application.[47]

3.2.3.2 Functional equivalence

The fact that a rule's balance of interests and values offline is valid in an online situation does not imply that the offline rule will automatically apply to an online situation without any difficulty. It may occur that the offline rule is framed in a technology dependant manner or there are particular features which render the rule ineffectual online. In such a case the lawmaker may reconstruct the offline rule or develop a new rule altogether, but such rule should be based on the underlying offline norm.[48]

Where a lawmaker needs to develop a new rule, it could be said the offline and online situations are inequivalent.[49] That is, offline and online situations are not equivalent when

[44] Schellekens op cit note 1 at 66; LL Ramokanate 'The Lesotho electronic transactions and electronic commerce bill: will it replace the common law of contract as we know it?' (2015) 22 *Lesotho Law Journal* 117 at 129.
[45] Schellekens op cit note 1 at 66; Luca G Castellani 'Related international instruments and organizations: an assessment of the Convention on the limitation period in the international sale of goods through case law' (2013) 58 *Villanova Law Review* 645.
[46] Schellekens op cit note 1 at 66 & 56.
[47] Schellekens op cit note 1 at 72.
[48] Schellekens op cit note 1 at 66; José Angelo Estrella Faria 'e-Commerce and International Legal Harmonization: Time To Go Beyond Functional Equivalence?' (2004) 16 *SA Merc LJ* 529 at 531; A Brooke Overby 'UNCITRAL model law on electronic commerce: will cyberlaw be uniform? An introduction to the UNCITRAL model law on electronic commerce' (1999) 7 *Tulane Journal of International and Comparative Law* 219 at 227.
[49] Schellekens op cit note 1 at 57; Julien Hofman 'Electronic evidence in criminal cases' (2006) *SACJ* 257 at 260.

carrying out a certain activity. The lawmaker must therefore treat the situations 'differently to the extent of their inequivalence.'[50]

Consequently, the new rule should give the same level of protection or same effect for online users as the level of protection or effect given by a rule to an offline user when carrying out the activity.[51] Because both offline and online activities will have an equivalent result, this is referred to as '[f]unctional [e]quivalent legal treatment of an activity.'[52]

The functional equivalence principle should guide regulation of signature in online activities for a number of reasons: the definition of signature subsumes the concept of e-signature;[53] legal principles underlying the requirement of signature offline, for example authentication, are comparable to those in online situations;[54] the goals to be met by the law's requirement of signature offline, such as to provide evidence of contract, are comparable to goals of signature online.[55] Thus the law's balance of interests and values by the signature requirement offline is valid online. Nevertheless, since e-signature technologies differ from traditional signature in form and application,[56] the offline rules on signature are ineffective online. The law maker must develop new law for regulation of e-signature based on the underlying norm of the offline rule.[57] Such new law must ensure that signatures have the same effect online as they do offline. In effect, 'equivalence guides the law maker as to the principles of law which should apply to cyberspace activities and thus shapes the substantive rules of any law.'[58]

Nonetheless, there are situations where the offline and online situations are completely inequivalent because a rule's balances of interests, values and principles offline are invalid online, and the basic offline norm becomes invalid when applied online.[59] For example, the

[50] T Pistorius 'Developing countries and copyright in the information age: The Functional Equivalent Implementation of the WCT' (2006) 2 *PER* 1 at 17; Schellekens op cit note 1 at 57; Lee Swales 'The regulation of electronic signatures: time for review and amendment' (2015) 132 *SALJ* 257 at 258. For example, functional equivalence notes that e-communication is not an equivalent to a paper document due to the differences in their nature and the functions they can perform, yet the offline norm will still apply to the data message.
[51] Immaculada Barral Vihials 'Electronic mass procurement by means of "web technology": basic options in its regulation' (2013-2014) 20 *ILSA Journal of International & Comparative Law* 373 at 396; Carys J Craig 'Technological Neutrality: Recalibrating Copyright in the Information Age' (2016) 17 *Theoretical Inquiries L* 601 at 609; Elizabeth Macdonald 'Dispatching the dispatch rule? The postal rule, email, revocation and implied terms' (2013) 19 *European Journal of Current Legal Issues* 1 at 4; Schellekens op cit note 1 at 56-7 & 70.
[52] Reed *Cyberspace* op cit note 3 at 108.
[53] See parts 2.4 & 2.9 above.
[54] Pistorius 'Nobody knows you're a dog' op cit note 9 at 738; See parts 2.5 & 2.9 above.
[55] See part 2.2 above.
[56] See parts 2.6 & 2.9 above.
[57] Farisa Tasneem 'Electronic Contracts and Cloud Computing' (2014) 9 *Journal of International Commercial Law and Technology* 105 at 112.
[58] Reed *Cyberspace* op cit note 3 at 107.
[59] Schellekens op cit note 1 at 69.

opt out rule balances interests of an offline mail receiver by protecting them from an influx of spam mail while maintaining the retailer's marketing rights. But it fails to protect an online user from receiving an influx of spam while the retailer manitains its right to market online. In such situations, either the principle of equivalence becomes irrelevant in the matter or a lawmaker may need to formulate a new rule for the online situation to realise the rationale of an offline norm, if still valid online.[60]

3.2.3.2.1 The practicability element of functional equivalence

A regulator can only achieve functional equivalence in e-commerce regulation if the new online rule is equivalent to the offline rule in both legal terms and *its practicability.* Equivalence of legal effect between online and offline rules which exists in the legal terminology of the online rule is not sufficient on its own. Instead, the rule must concern itself with the feasibility of its requirements in practice.[61] That is, the requirements of the regulation should be attainable by it subjects. Hence,

> 'the obligations imposed on the subject of the rules should be broadly equivalent in burden once allowance has been made for the differences between the online and offline versions of the activity.' [62]

If a rule does not concern with the practicability of its compliance, then functional equivalence will be compromised or not achieved.[63]

A number of factors may affect the practicability of an online rule for regulation of e-signatures.[64] These include costs a rule's subjects incur to comply with it;[65] changes it brings to the manner of interaction of contracting parties from when they contract offline to when contracting online, for example their involvement of a third party to conclude an e-transaction;[66] and the need for legal and technical advice to comply with the rule.[67] Thus an online rule must demand activities which are doable and not too burdensome for it to be functionally equivalent. Since functional equivalence is an integral part of the principle of

[60] Schellekens op cit note 1 at 69-70; Reed 'Online and offline equivalence' op cit note 11 at 254-5 & 264.
[61] Reed *Cyberspace* op cit note 3 at 120.
[62] Reed *Cyberspace* op cit note 3 at 108; Reed 'Online and offline equivalence' op cit note 11 at 269.
[63] Reed *Cyberspace* op cit note 3 at 120.
[64] Reed *Cyberspace* op cit note 3 at 120.
[65] Pistorius 'Developing countries'op cit note 50 at 16; Reed *Cyberspace* op cit note 3 at 120.
[66] Reed *Cyberspace* op cit note 3 at 120.
[67] Reed *Cyberspace* op cit note 3 at 120.

equivalence, the rationale for adoption of the principle of equivalence in ICT regulation follows.

3.2.4 The rationale behind the principle of equivalence in ICT regulation

Several aspects motivate the use of the principle of equivalence in ICT regulation, particularly in the law of contract. First, it is not advisable to have two sets of rules applicable to a single activity, with one set regulating the activity carried out online, and another set regulating the same activity offline.[68] This can confuse users as they will need to consult differing rules every time they switch from working offline to online.[69] Application of the principle of equivalence will not require a change of mindset when activities are conducted offline and online.[70] Further, many people already find it challenging to understand rules regulating offline activities and it is unrealistic to expect them to know and understand a new set of rules that regulate online activities.[71] Separate laws could also be a source of more legal disputes because they will have their challengeable loopholes. Yet it is advisable to keep the possibility of new disputes to a minimum. Use of the same rules offline and online can improve a legal system as new disputes will be subsumed under existing law.[72] Once more, the development of law is evolutionary and not revolutionary in nature,[73] thus sudden changes of establishing a new legal system for online activities might be problematic.[74]

Secondly, the lawmaker's reference to old law gives proposed online law authority and acceptability. Methods of reasoning by use of similarity of cases and arguments on a contrary position help drive the acceptability of new laws. This can only be possible if reference to existing law is made. The principle of equivalence therefore assists in the making of new online rules based on offline rationale and proposed adaptations of existing law to online situations acceptable.[75]

Thirdly, application of the principle of equivalence gives meaning to online rules. If a rule prescribes behavior expected of online users and the rule is derived from the offline

[68] Schellekens op cit note 1 at 57; Eliza Mik 'The Unimportance of being "electronic" or – popular misconceptions about "Internet contracting" ' (2011) 19 *International Journl of Iaw and Information Technology* 324 at 326; L Lessig 'The Path of Cyberlaw' (1995) 104 *Yale LJ* 17 at 17-18.
[69] Reed *Cyberspace* op cit note 3 at 108.
[70] Reed 'Online and offline equivalence' op cit note 11 at 253.
[71] Reed *Cyberspace* op cit note 3 at 108.
[72] Schellekens op cit note 1 at 57 & 58.
[73] Schellekens op cit note 1 at 65.
[74] Thomas J Smedinghoff 'The Legal Challenges of Implementing Electronic Transactions' (2008) 41 *Uniform Commercial Code Law Journal* 3 at 10.
[75] Hill op cit note 21 at 18; Schellekens op cit note 1 at 59.

norm that is accepted by the community as meaningful, the rule introduced online will be accepted and recognized as meaningful by the online community.[76]

It is challenging to draft an online rule which is a functional equivalent of an offline rule and to direct the lawmaker with regard to the desired result and what interests to balance. Without this, '[n]on-application of the starting point entails the risk of a legal vacuum.'[77] Since functional equivalence is part of the principle of equivalence, the rationale discussed above applies equally to it. It follows that the content of a new online regulation which will help a lawmaker develop a functionally equivalent rule needs to be determined.

3.2.5 Content of a functionally equivalent rule

A rule will achieve equivalence of application if it addresses a performer's state of mind or the consequence of a performer's conduct,[78] not the method used by a performer in undertaking their conduct. The different focal points of regulation are addressed below.

3.2.5.1 Rules that address the mental state or consequence of a performer's behavior

Offline rules that address a performer's state of mind at the time of action do not need to undergo alterations to enable them to have an equivalent effect to an online activity. This is because the state of mind of a person who carries out a certain activity offline does not change when they do the same activity online.[79] For example, a party who signs to conclude a contract both offline or online does so to indicate their assent to the contract. Thus, an online regulation on use of e-signatures will have an equivalent effect to offline rules if directed to the user's mental state.

Likewise, a regulation that addresses consequences of peoples' conduct does not need to change to apply online. If the law provides that when one commits an act offline a certain consequence must follow, it will not be difficult for the lawmaker to develop a law that ensures the same consequence online.[80] For example, an offline regulation that requires that traders must be identifiable[81] can be easily transposed to the online world by demanding that online traders must provide their address and contact details on their websites to ensure that they are identifiable.

---

[76] Reed *Cyberspace* op cit note 3 at 108.
[77] Schellekens op cit note 1 at 58.
[78] Reed *Cyberspace* op cit note 3 at 109.
[79] Reed 'Online and offline equivalence' op cit note 11 at 270.
[80] Reed *Cyberspace* op cit note 3 at 110.
[81] Section 79 of Consumer Protection Act 68 of 2008 of South Africa.

3.2.5.2 Rules that address means of conduct of persons

The situation is different where a rule focuses on the way conduct is carried out. In this case, two factors make it difficult for the regulation to achieve equivalence; first, when an activity is conducted online, the technology may inspire a user to do the activity in novel ways which induce him to stop duplicating all characteristics of the act when conducted offline.[82] Features of the online sphere which are not present offline encourage this. Reed uses the example of a magazine publisher. If they publish material in their offline magazine without the consent of the owner of the material, they will be liable for copyright infringement. However, if they publish their magazine online, technology can enable them to engage in unauthorised linking and give their website users access to other websites through links on their webpage. It will be debatable whether the publisher infringed copyright as they do not engage in unauthorised copying or communicating the material to the public. Consequently, applying the online rule focusing on means used to engage in copyright infringement may encounter difficulties.[83] These novel ways were not anticipated by offline rules and it may be a challenge to transpose such offline rules to the online activities.

The second factor that makes it difficult for a rule focusing on means of conduct to achieve equivalence is that conduct carried out online is done in such a different fashion from offline that the application and outcome of rules become difficult to evaluate and compare.[84] As a result transferring the rationale of an offline norm onto online becomes difficult. For example, the law of defamation focuses on the act of publishing information about another; which is behavior of an actor.[85] If this rule is transposed to the online world and grants online hosts immunity from defamatory liability for material they distributed similar to offline distributers, online distributers will be favored by the regulation. This is because technologies they use in the distribution of material sometimes allow them to see content of the distributed material before distribution, yet they maintain immunity. But offline distributers lose their immunity once they know of the defamatory nature of the content before distribution. The different ways of publishing information online therefore make it difficult to achieve equivalence of legal treatment. This difficulty would not be encountered if the rule focused on the effect of the actor's behavior which is reputational damage.[86] As will be reflected later, a similar difficulty will be encountered if a rule focuses on methods of applying e-signatures.

[82] Reed *Cyberspace* op cit note 3 at 111; Reed 'Online and offline equivalence' op cit note 11 at 258.
[83] Reed 'Online and offline equivalence' op cit note 11 at 112.
[84] Reed *Cyberspace* op cit note 3 at 110.
[85] *Khumalo & others v Holomisa* 2002 (5) SA 401 at 413-4.

Although the principle of equivalence provides a starting point for making regulations for online activities, it still has drawbacks.

3.2.6 Limitations of the principle of functional equivalence

First, the lawmaker may find it difficult to achieve equivalence in the development of rules for online activities as offline rules that form the basis for formulating a new online rule can carry unstated assumptions. The unstated assumptions may in fact be untrue in the online world, thus render the offline law an improper base to begin development of the online law.[87] To illustrate, the lawmaker may assume that a law balances certain interests and protects them from impairment, whereas the law is actually framed in terms of behavior. For instance, an offline copyright law protects rights of a copyright holder by prohibiting unauthorised commercial copying of their material, but exempts private copying from the rule because it occurs at a low harmless rate. However, online technology enables private copying to occur easily and at high rates to the copyright holder's prejudice. The assumption that exempting private copying does not harm a copyright holder then proves untrue online.[88] The unstated assumption consequently makes it difficult for the lawmaker to achieve equivalence using the offline rule as a starting point.

To illustrate further, lawmakers may assume that a handwritten signature is analogous to a digital signature based on PKI and believe that it can substitute the handwritten signature in e-commerce, yet this is false. For one, a handwritten signature is strongly bound to its maker.[89] That is, there is direct association between the signer as an owner of the signature and the signing process.[90] This implies that the signer has to be physically present to sign a document,[91] they are aware of the document they are going to sign and the signature will be difficult to forge without detection. Thus the manner in which a signer signs offline positively affects the authenticity and cautionary function of the signature. A digital signature based on PKI on the other hand is weakly bound to its maker. The bond depends on the signer's ability to keep their private key secret and safe from others.[92] The implication here is that a thing such as a computer or certain software, attaches the signature; the signer does not need to be present. Consequently, the signer's ability to attach their signature only to a document they

[87] Reed *Cyberspace* op cit note 3 at 112.
[88] Reed *Cyberspace* op cit note 3 at 113.
[89] Nicholas Bohm 'Watch what you sign!' (2006) 3 *Digital Evidence & Elec Signature L Rev* 45.
[90] Lorna Brazell *Electronic Signatures and Identities Law and Regulation* 2 ed (2008) at 81.
[91] Chris Reed 'Old wine in new bottles: Traditional transactions in the internet environment' in *Internet law: Text and materials* 2 ed (2004) 192.
[92] See part 2.9.10.2.5 above.

are aware of or intends to sign is affected.[93] The way a signer attaches the digital signature based on PKI online therefore negatively affects the authentication and cautionary function of their signature.

Another unstated assumption is that the law tends to categorise actors into different groups and deal with them according to those categories by making a different set of rules for each category.[94] Offline categorization may become problematic as online actors may fall into many of these categories at the same time, thus making it difficult for the lawmaker to know which set of rules to apply to the online activity.[95] An example can be seen in the attempt to regulate search engines. For one there is the *infrastructure* argument that puts search engines in the category of public services and proposes that they be regulated as such, while there is the *content* argument which fits search engines into freedom of expression promoters like newspapers and argues they should be regulated as such.[96] Otherwise, online actors may break down the distinct categories and merge them into one.[97] When this occurs, the lawmaker has the tendency to fit an online actor into an improper category and develop a new law for the online actor basing himself on the faulty premise. This will lead to an improper law. In order to avoid confusion, the lawmaker must remove the categorization applicable offline to appropriately suit the online situation.[98] Alternatively 'the law [should be] reformed on the basis of accurate assumptions.'[99]

A second drawback of the functional equivalence principle is that it does not give a regulator an opportunity to assess a situation afresh and draft a new law altogether without relying on an offline rule.[100] However, as previously indicated, this *de novo* assessment of the law runs the risk of operating in a legal vacuum with no direction in the development of online law.[101] Hence the regulator's reference to an existing offline rule is an advantage, not a drawback.

[93] In essence a handwritten signature connects a person to a document while a digital signature connects device to a document (Ugo Bechini 'Bread and donkey for breakfast: How IT law false friends can confound lawmakers: An Italian tale about digital signatures' (2009) 6 *Digital Evidence and Electronic Signature Law Review* 80).
[94] Reed 'Online and offline equivalence' op cit note 11 at 264.
[95] Urs Gasser 'Regulating Search engines: Taking Stock and Looking ahead' (2005-2006) 8 *Yale LJ & Tech* 201 at 221-2.
[96] John D Saba Jr 'Internet Property Rights: e-Trespass' (2001-2002) 33 *St Mary's LJ* 367 at 377.
[97] Reed *Cyberspace* op cit note 3 at 114.
[98] Reed *Cyberspace* op cit note 3 at 118.
[99] Reed *Cyberspace* op cit note 3 at 109.
[100] Reed *Cyberspace* op cit note 3 at 115.
[101] Schellekens op cit note 1 at 63.

Thirdly, critics argue that functional equivalence may not be the best method of determining reasonableness in technology regulation.[102] Functional equivalence focuses on functions of technology to regulate it but this is not ideal. They state that technology artefacts are multidimensional. They matter for more reasons than their functions such as their language, architecture or their development methods.[103] Thus the lawmaker could address technology regulation from other angles.[104] Even so, it is contended that this argument relates to different kinds of laws excluding e-commerce. E-commerce regulation concerns the function of a signature in enabling e-commerce.[105] Consequently, in e-commerce regulation 'function is more important than the technology's essence'.[106] Again, there is a danger in regulating online activities based on technological artifacts – this may lead to a technology specific regulation.[107] Hence the argument does not hold in e-commerce regulation.

Furthermore, opponents to the theory argue that functional equivalence is insufficient for facilitation of e-commerce as it only works one way.[108] It only tries to create 'an electronic equivalent of a real-world concept' such as writing. But facilitation of e-commerce may require 'finding of a real-world equivalent of a concept that exists only in the "electronic world" ' such as hypertext.[109] This criticism requires new research into whether it is at all necessary to create offline equivalents of online activities and the rationale behind doing so.

Moreover, Mik contends that the functional equivalence principle forces the lawmaker to redefine an offline concept in order to find its electronic functional equivalent and this can be misleading.[110] In redefining a concept, the lawmaker ends up giving the concept features it does not have when applied offline. She illustrates this with the 'redefinition' of signature in an online sphere. She argues that an e-signature is required to identify a party, yet a traditional signature applied offline is barely legible and is not required to identify a signer. However, it is maintained that this contention is flawed. A traditional

[102] See Marcelo Thompson 'The neutralization of harmony: the problem of technological neutrality, east and west' (2012) 18 *Boston University Journal of Science & Technology Law* 303 at 312.
[103] Thompson ibid at 312.
[104] Thompson ibid at 313.
[105] Birnhack M 'Reverse engineering informational privacy law' (2013) 15 *Yale Journal of Law and Technology* 24 at 47.
[106] Birnhack ibid at 47; The situation is different with copyright where the law focuses on technology itself (Greenberg BA 'Rethinking Technology Neutrality' (2016) 100 *Minnesota Law Review* 1495 at 1544 & 1547).
[107] Thompson op cit note 102 at 314.
[108] Eliza Mik 'Evaluating the Impact of the UN Convention on the Use of Electronic Communications in International Contracts on Domestic Contract Law--The Singapore Example' (2010) 28 *Chinese (Taiwan) Yearbook of International Law and Affairs* 43 at 50.
[109] Mik 'UN Convention' ibid at 50.
[110] Mik 'UN Convention' ibid at 49.

signature is defined as any mark that is used to identify a signer and show their intention.[111] Hence redefining signature for an online purpose does not necessarily give it features it does not have offline.

Nonetheless, it is conceded that some of the criticisms raised against the functional equivalence principle are real and ought to be guarded against when creating laws for e-signatures. Reference is made to unstated assumptions buried in an offline rule. The lawmaker ought to reveal the assumptions and explore them before deciding on using a particular offline norm for an online situation. Although this study and other legislative instruments rely on the principle of functional equivalence, there is not much academic writings that explain or criticize it.[112]

3.2.7 Summary

It is maintained that a lawmaker should develop a new rule for e-signatures in e-commerce, which rule should have a similar effect or level of protection to that provided by an offline rule. Most importantly, the rule should be feasible in practice. Lastly, the content of a new rule should target the mental state of actors and consequences of actors' conduct, not the behavior of actors or means through which conduct is carried out. The following section discusses the principle of technology neutrality in e-signature regulation.

3.3 Technology neutrality

3.3.1 Introduction

Technology Neutrality is 'a key principle for internet policy.'[113] It first emerged around 1986 in the USA where it was used to express the objectives of the USA Electronic Communications Privacy Act.[114] The USA Framework for Global Electronic Commerce (1997) subsequently espoused the concept and stated that online regulation should be technology neutral.[115] The European Commission also adopted technology neutrality during

[111] See parts 2.4 & 2.5 above.
[112] Gustaf Johnssén 'Time, space, and documents – Principles for e-government regulation' (2006) Proceedings of the 39th Hawaii International Conference on System Sciences at 2.
[113] Winston J Maxwell & Marc Bourreau 'Technology neutrality in internet, telecoms and data protection regulation' (2015) 21 *Computer and Telecommunications Law Review* 1; OECD 'OECD Council Recommendation on Principles for Internet Policy Making' 13 December 2011 at 6 available at *https://www.oecd.org/internet/ieconomy/49258588.pdf*, accessed on 26 November 2016.
[114] John R Kresse 'Privacy of Conversations over Cordless and Cellular Telephones: Federal Protection under the Electronic Communications Privacy Act of 1986' (1987) 9 *Geo Mason UL Rev* 335.
[115] 'Framework for Global Electronic Commerce' 1 July 1997 available at *http://www.ecommerce.gov/framewrk.htm*, accessed on 6 March 2014.

the review of its telecommunications regulation. The concept attracted more attention during the European Commission's discussions of the 1997 Convergence Green Paper where it supported arguments for convergence.[116] Technology neutrality subsequently formed the basis of several legislative instruments and policies on ICT regulation in the EU[117] and USA. Nonetheless, the instruments that refer to the principle of technology neutrality did not adequately explain its meaning. Subsequently Bert-Jaap Koops clarified the concept of technology neutrality,[118] and many rely on his definition.[119] Consequently, this section draws heavily on the writings of Koops.

This section explores the denotation and purposes of technology neutrality in ICT regulation, with particular reference to the e-signature. The limitations of technology neutrality are investigated and possible means through which these limitations may be countered are explored.

3.3.2 Definition of 'technology' in technology neutral

The word 'technology' carries different meanings depending on the context in which it is used. Technology in ICT regulation refers to the specific types of 'technologies that store, transmit and/or process information and communication…in particular electronic data-processing technologies.'[120] The meaning of technology neutrality follows.

3.3.3 Meaning of technology neutral regulation

The principle of technology neutrality in regulation has three meanings. First it refers to the purposes of online regulation; second, it communicates the consequences of regulation that a lawmaker should avoid, and third, it explicates the principles necessary in legal drafting of ICT regulation.[121] These meanings are interrelated and are explained below.

---

[116] Van der Haar op cit note 17 at 3; Van der Merwe et al *Information* op cit note 17 at 6-7.

[117] For example, the Amended Proposal for a European Parliament and Council Directive on a common framework for electronic signatures COM (99) 195 final available at *http://aei.pitt.edu/13384/1/13384.pdf*, accessed on 25 November 2016; Proposal for a decision of the European Parliament and of the Council on establishing a multi annual Community programme on promoting safer use of the Internet and new online technologies COM (2004) 91 final availbable at *http://library.certh.gr/libfiles/PDF/PAPYR-1205-EU-PROPOSAL-SAFER-INTERNET-COM-2004-91-PP37-EN-acte_en.pdf*, accessed on 25 November 2016; See also the 2002 EC Electronic communications framework cited in Van der Haar op cit note 17 at 3.

[118] Koops 'Should ICT regulation be neutral-technology' op cit note 2.

[119] Reed *Cyberspace* op cit note 3 at 191; Ulrich Kamecke & Torsten Korber 'Technological neutrality in the EC regulatory framework for electronic communications: a good principle widely misunderstood' (2008) 29 *European Competition Law Review* 330 are examples of these.

[120] Koops note 2 at 79.

[121] Koops note 2 at 83.

3.3.3.1 The purposes of online regulation

Koops maintains that online regulation should regulate the effects of peoples' behaviour in society, not the mechanisms used to accomplish such effects. It should also promote the principle of equivalence between offline and online transactions.

3.3.3.1.1 Regulation of effects in society

Technology neutral regulation controls the effects of peoples' behaviour in society,[122] the means of accomplishing the effect are irrelevant and often unregulated.[123] This implies that ICT regulation should not be concerned with which technology (means) is used to achieve a particular outcome.[124] For instance, where parties have to sign an e-transaction, regulation should not be concerned with which e-signature technology they employ to sign the e-transaction. Rather it should be concerned with the fact that parties sign primarily to express their assent to contents of the contract. Such e-signature regulation will be technology neutral.[125]

Technology neutrality also implies that functions of different technologies may be regulated. The functions of a technology will indicate the uses that the technology can be put to, which uses will help determine whether an effect aimed at by regulation may or may not be achieved by the technology.[126] Again, regulation may be outlined in terms of its values.[127]

3.3.3.1.2 Promotion of equivalence between offline and online transactions

Technology neutrality also serves to achieve or compliment the principle of equivalence. It maintains that if regulation aims to control effects of behaviour instead of means of achieving the effect, it will lead to equivalence between the offline and online worlds.[128] This is because the regulator desires a similar goal in both the online and offline worlds. As a result, whether the sphere employed to achieve the goal is electronic or not is irrelevant.[129] Thus, a technology neutral regulation will primarily require an e-signature to authenticate a

[122] Koops note 2 at 83; Maxwell et al op cit note 113 at 1.
[123] Koops note 2 at 83. John D Gregory 'Legislating Trust' (2014) 12 *Canadian Journal of Law and Technology* 1 at 7.
[124] Patrice Wylly 'Evaluating the costs of technology neutrality in light of the importance of social network influences and bandwagon effects for innovation diffusion' (2015) 23 *NYU Environmental Law Journal* 300 at 302.
[125] Koops note 2 at 83.
[126] Thompson op cit note 102 at 309-11
[127] Thompson op cit note 102 at 307.
[128] Koops op cit note 2 at 85. See also Reed *Cyberspace* op cit note 3 at 191.
[129] Maxwell et al op cit note 113 at 2.

document, that way the effect of the e-signature online will be similar to the effect of signature offline, hence promotion of equivalence.

Several legal instruments support technology neutrality's implication of offline and online equivalence.[130] The second meaning of technology neutrality relates to consequence of regulation.

3.3.3.2 The outcome of regulation

The principle of technology neutrality emphasises two negative consequences that a regulation should avoid. First, regulation should not have the effect of discriminating between technologies, and secondly, regulation should not hamper the development of new technologies.[131]

3.3.3.2.1 Non-discrimination between technologies

Technology neutrality signifies that regulation 'should neither require nor assume a particular technology.'[132] Put differently, regulation should not discriminate between technologies that have the same effect nor should it prescribe or impose the use of a certain technology to the exclusion of others.[133] It is argued that the fact that regulation should not 'impose' technology means that the market, not the state, should determine the success or failure of technologies, while 'discriminate' implies that regulation should not directly or indirectly differentiate between technologies without good justification.[134] It is only where technologies have 'effects or functions that differ in a legally relevant way' that differentiation between technologies will be appropriate in the circumstances.[135] The principle of technology neutrality therefore upholds the norm of non-discrimination of technologies.

---

[130] Office of the e-Envoy 'United Kingdom e-Policy Principles' Principle 5 available at *http://webarchive.nationalarchives.gov.uk/20040722012351/e-government.cabinetoffice.gov.uk/assetRoot/04/00/60/79/04006079.pdf*, accessed on 10 March 2014; Dutch policy memorandum on Legislation for the Electronic Highways 1998 cited in Koops note 2 at 77; Electronic Transactions Act 162 of 1999 (Cth) of the Commonwealth of Autralia, s 10; Anupam Chander *The electronic silk road: how the web binds the world together in commerce* (2013) 562.

[131] Koops op cit note 2 at 85-6.

[132] Reed *Cyberspace* op cit note 3 at 191; Birnhack op cit note 105 at 36; Wylly op cit note 124 at 302 & 307; The European Commission 'Towards a new framework for Electronic Communications infrastructure and associated services' The 1999 Communications Review COM (1999) 539 available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24216*, accessed on 25 November 2016.

[133] Luca G Castellani 'The role of UNCITRAL texts in promoting a harmonized legal framework for cross-border mobile payments' (2013) 8 *Washington Journal of Law, Technology & Arts* 265 at 269; Nazzal M Kisswani & Anas A Al-bakri 'Regulating the use of electronic signatures given the changing face of contracts' (2010) 7 *Macquarie J Bus L* 53 at 58.

[134] Kamecke et al op cit note 119 at 331.

[135] Koops op cit note 2 at 85at 86

Proponents of non-discrimination of technology reveal that the idea of non-discrimination was to a large extent influenced by the idea of technological convergence.[136] A neutral regulation system became necessary to regulate activities that took place across the technology sectors and to enable free competition between the technologies. A regulation which illustrates the non-discriminatory and non-prescriptive approach of technology neutrality is a regulation which sanctions any format of e-signature technology in e-commerce matters.

3.3.3.2.2 Regulation not to impede future development of technology

The principle of technology neutrality maintains that the lawmaker must frame regulation in a fashion that permits innovation of new technologies.[137] If regulation regulates only a specific technology, it may discourage innovators from creating technologies that are not recognised by the law.[138] Consequently, such regulation will cripple technological development. Additionally, technology neutrality makes recommendations on legislative drafting.

3.3.3.3 Methods employed in drafting legislation

As indicated earlier, technology neutrality sets out methods for the drafting of ICT legislation maintaining that ICT legislation should be sustainable and transparent.

3.3.3.3.1 Sustainability of legislation

The technology neutrality principle recognises that technology develops at a fast rate; novel technologies are produced every day and succeed each other at an alarming rate.[139] These technologies develop faster than laws.[140] Accordingly, e-signature legislation must be drafted

[136] See Van der Haar op cit note 17 at 3-4; Kamecke et al op cit note 119 at 330; Maxwell et al op cit note 113 at 2.
[137] Van der Haar op cit note 17 at 8 & 24; Castellani 'The role of UNCITRAL texts' op cit note 133 at 269; Reed *Cyberspace* op cit note 3 at 192; Maxwell et al op cit note 113 at 2; Greenberg op cit note 106 at 1521; Koops op cit note 2 at 86.
[138] Mireille Hildebrandt 'Legal protection by design: objections and refutations' (2011) 5 *Legisprudence* 223 at 237; Birnhack op cit note 105 at 43; Wylly op cit note 124 at 312.
[139] Lyria Bennett Moses 'Understanding Legal Responses to Technological Change: The example of *In Vitro* Fertilization' 2004-2005 *Minnesota Journal of Law, Science and Technology* 505 at 513.
[140] Lynne M Thomas 'Abandoned Frozen Embryos and Texas Law of Abandoned Personal Property: Should There Be a Connection' (1997-1998) 29 *St Mary's LJ* 255 at 25; Micheal D Kirby 'Medical Technology and New Frontiers of Family Law' (1987) 1 *Australian Journal of Family Law* 196 at 212; Moses 'Legal Responses' op cit note 139 at 515-516.

in such a way that it will be able to withstand and incorporate such technology developments without the need for amendment.[141] It must be flexible[142] and dynamic.[143]

3.3.3.3.2 Regulation to be transparent

Technology neutrality further maintains that the lawmaker must draft a regulatory instrument with less technological detail. This is so that it becomes accessible to the lay person who needs to conform with it, hence its transparency.[144] For instance, a regulation that deals with e-signatures must be drafted in technology neutral terms because an e-transaction can be concluded by any Internet user; it is not used by technology specialists alone. Having explored the meanings of technology neutral regulation, a discussion of its advantages follows.

3.3.4 Benefits of technology neutral legislation

Technology neutral legislation has several benefits. It decreases the risk of a law being obsolete due to technological developments, thus the law will not quickly lose meaning and power to its applicants in the near future. It is also economical in nature; it does not require constant amendments and hence saves costs, resources and time of the legislature spent on amending laws.[145]

Moreover, technology neutral legislation permits technological developments. Accordingly it increases market investments in new technologies.[146] Again, since it encourages market driven technologies, innovators can easily find 'better, cheaper and more effective solutions' which will help users reach policy goals at less costs.[147]

The technology neutrality principle further helps ICT regulation to achieve one of its objectives – to facilitate the growth of e-commerce. It does so by reducing unnecessary government participation in the regulation of e-signatures. Thus it forbids government to set

[141] Koops op cit note 2 at 88; Hildebrandt op cit note 138 at 237; Birnhack op cit note 105 at 36; Ernesto U Savona (ed) in *Crime and Technology New Frontiers for Regulation, Law Enforcement and Research* (2004) 43.
[142] Birnhack op cit note 105 at 38-39.
[143] Van der Haar op cit note 17 at 24; Yana Welinder 'Facing real-time identification in mobile apps & wearable computers' (2013-2014) 30 *Santa Clara High Tech LJ* 89 at 125; Koops op cit note 2 at 88-9.
[144] Koops op cit note 2 at 90.
[145] Reed *Cyberspace* op cit note 3 at 202.
[146] Van der Haar op cit note 17 at 23; Aalberts AA & Van der Hof S 'Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication' (2000) 7 *EDI L Rev* 1 at 9.
[147] Wylly op cit note 124 at 312 & 302.

up numerous rules that a law subject has to comply with to use e-signatures.[148] Hence, it renders e-signatures use in e-commerce more accessible to the online user. It promotes equivalent treatment of offline and online users as well, enabling a party to switch from an offline transaction to an online one without difficulty. This signifies that it promotes party autonomy in the conclusion of contracts.

Additionally, technology neutral regulation is effective. Its subjects understand its simple language and can comply with it with ease.[149] Lastly, it promotes harmonisation in different jurisdictions where they have to deal with certain issues simultaneously.[150] For instance, it would be a challenge where parties from different states wished to contract but each state prescribed different e-signature technologies. Nonetheless, technology neutrality has its limitations.

3.3.5 Challenges faced by technology neutral regulation

First, some authors allege that technology neutral regulation's aim of regulating unforeseen technologies is problematic. They maintain that the effect of the regulation may bring about unwanted ramifications and subsequently discourage technology innovation.[151] However, Reed disputes this and reveals that even though there are some 'future-proof' ICT regulations which became redundant in the past, that was not caused by their failure to incorporate new technology developments. Instead, the redundancy was caused by radical changes to business models supporting use of the technologies.[152]

Secondly, adversaries of the principle aver that the exercise of drafting technology neutral legislation requires the use of neutral language and this is impractical. They argue that the language of the legislature has to clearly speak to prospective technologies and this cannot be done in technology neutral legislation.[153] Conversely, proponents of the principle argue that technology neutral language can be achieved by employing phrases such as 'any means of communication' or 'any signature that is in electronic form is legally recognised'.[154]

---

[148] Spyrelli Christina 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) 2 *The Journal of Information, Law and Technology (JILT)* available at *http:/www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2.spyrelli/*, accessed on 16 January 2014.
[149] Wylly op cit note 124 at 312.
[150] Birnhack op cit note 105 at 44.
[151] Daniel J Gervais 'Towards a New Core International Copyright Norm: The Reverse Three-Step Test' (2005) 9 *Marquette Intellectual Property Law Review* 1.
[152] Reed *Cyberspace* op cit note 3 at 200. As a result, he affirms that a technology neutral regulation can provide a sufficient degree of sustainability if other legislation facets are in place.
[153] Moses 'Legal Responses' op cit note 139139 at 578.
[154] Roger Brownsword 'Regulating Human Genetics: New Dilemmas for a New Millennium' (2004) 12 *Medical Law Rev* 14 at 31.

Such open language ensures that potential technologies will be linked to the regulation when it is given a literal interpretation.[155] Hence technology neutral terminology is practicable. Rather, soft law in the form of guidelines may address prospective e-signature technologies when the need arises.

Thirdly, opponents of the principle argue that it may be risky for the lawmaker to regulate a technology before its effects are evident and appreciated. If the lawmaker drafts a law before they comprehend how the technology is used and discover consequences of its use, such legislation will be oblivious to difficulties it needs to deal with. Consequently it may not manage to deal with the technology developments.[156] Thus the best law is a reactive one which waits for consequences before regulating them, not proactive law required by the principle of technology neutrality.[157]

By contrast, scholars dispute the allegation that regulation should be reactive. They argue that the question of when the legislature should intervene to regulate technology is not fixed.[158] Whereas it might be advantageous for the legislature to wait until the perils and advantages of the technology are known before intervention, the delay in regulating may result in irreversible harm that could have been prevented had regulation been proactive.[159] An alternative could be to create ways that will augment the chances of regulation being up to date. The technology neutrality principle falls in this option.[160] For instance, a rule which gives a broad definition of an e-signature will be up to date with upcoming authentication technologies.

It is acknowledged that despite the viability of drafting legislation in technology neutral terms, it is still a challenging exercise.[161] This is because of the limited degree to which the lawmaker envisages future use of the technology and understands how it will work.[162] The Convention on Cybercrime is an example of an instrument which updated the definition of traffic data without appreciating the way different technologies collect different forms of data.[163]

---

[155] Brownsword ibid at 31.
[156] Reed *Cyberspace* op cit note 3 at 202.
[157] Greenberg op cit note 106 at 1526.
[158] Ron Westrum *Technologies and Society: The Shaping of People and Things* (1991) at 13 cited in note 424 of Moses 'Legal Responses' op cit note 139 at 580.
[159] Westrum ibid.
[160] Moses 'Legal Responses' op cit note 139 at 580.
[161] Reed *Cyberspace* op cit note 3 at 201.
[162] Reed *Cyberspace* op cit note 3 at 201; Escudero-Pascual A & Hosein I 'The Hazards of Technology neutral Policy: Questioning Lawful Access to Traffic Data' (2004) 47 *Communications of the ACM* 77 at 77 - 8.
[163] 185 of 2001 Art 1 (d).

Again, there is a concern that the lawmaker may tend to abstract too much from technology in an effort to be technology neutral. They may end up with a law that is non-representational of technology, is vague[164] and senseless.[165]

Since the risk of legislation abstracting from technology is evident, the lawmaker can guard against it when drafting regulation. They must ensure that formulation of a rule is in parity with the main goal of regulating.[166] This will minimise the chances of a rule abstracting too much from the technology it ought to regulate. In fact other scholars defend the use of vague language in regulation. They explain that the legislature intends for regulation to cover unforeseen conduct. When new conduct arises, the regulation will be interpreted to determine whether it includes the new conduct or not. Consequently, technology neutral regulation adapts legal concepts to socially desirable results.[167]

Further, some scholars contend that technology neutral regulation disregards the fact that some e-signatures are more secure than others. For instance, the mark 'X' signed on an e-document does not have the same level of security as a digital signature based on PKI.[168] It is contended that this criticism misses the point of technology neutrality. Emphasis under this principle is the achievement of a certain legal effect in society, such as authentication by signature, not the technologies used to achieve the effect.[169] The market on the other hand takes care of security and reliability issues of an e-signature.[170] If the law dwells with the latter issues, it will not be sustainable.

Moreover, some authors allege that the principle of technology neutrality produces legal uncertainty.[171] Uncertainty may be caused when new activities do not fit into current legal structures and thus their legal consequences are unclear.[172]

In fact the quandary of legal uncertainty is all-encompassing. It has been declared that 'it will never be possible to determine the precise meaning of all legal rules so as to be able to

[164] Moses LB 'Recurring Dilemmas: The Law's Race to Keep up with Technological Change' (2007) *University of New South Wales Faculty of Law Research Series* Paper 21, 1 available at *http://law.bepress.com/unswwps-flrps/art21*, accessed on 21 February 2014 at 23; Thompson op cit note 102 at 307.
[165] Escudero-Pascual et al op cit note 162 at 77-82; Koops op cit note 2 at 88-9.
[166] Moses 'Recurring Dilemmas' op cit note 164164 at 59 & 66.
[167] HLA Hart *Jhering's Heaven of Concepts and Modern Analytic Jurisprudence, in Essays in Jurisprudence and Philosophy* (1983) 269-270 cited in note 88 of Moses 'Recurring Dilemmas' op cit note 164 at 24.
[168] Blythe E Stephen 'Lithuania's Electronic Signature Law: Promoting the Growth of Secure E-commerce Transactions' (2007) 8 *Barry Law Review* 23 at 32.
[169] See part 3.3.3.1.1 above.
[170] Mason S *Electronic Signatures in Law* 4ed (2016) 158.
[171] Van der Haar op cit note 17 at 24; James X Dempsey 'Creating the Legal Framework for ICT Development: The Example of E-Signature Legislation in Emerging Market Economies' (2003) 1 (2) *Information Technologies & International Development* 39 at 50.
[172] See Moses 'Legal Responses' op cit note 139 at 528; Aalberts et al op cit note 146 at 7.

answer all legal questions unequivocally.'[173] In other words, technology does not bring uncertainty in law, but comes into an already uncertain legal sphere. Technology aggravates an already existent problem by bringing up new questions which cannot be answered, or by exposing concealed ambiguity in the law.[174] Either courts of law[175] or legislation can resolve upcoming legal uncertainty where necessary, thus uncertainty is not an impediment to creating technology neutral regulation.[176] Nonetheless, the costs of developing technology neutral legislation should be weighed against the cost of judicial proceedings.[177]

Furthermore, scholars contend that technology neutral e-signature regulation does not provide a 'reliable security infrastructure.'[178] Accordingly, people may be discouraged to use e-commerce since insecure e-signatures may make e-communication susceptible to fraud or message interference while there are no legally acceptable security procedures.[179] Consequently, they propose that a technology specific regulation is required to give a reliable security structure to e-signatures and promote the use of e-commerce.

Nevertheless, it is counter argued that e-commerce users are free to select an e-signature that will fulfil their contractual needs. If there is no need for tight security in their e-communications, they may decide to use less secure e-signatures. As previously indicated, technology neutrality promotes party autonomy.[180] Additionally, chapter five shows that laws of evidence help prove the reliability of e-signatures where fraud or manipulation is suspected. Hence technology neutral regulation is not a deterrent to the use of e-commerce.

Lastly, critics argue that regulation may take place under a false pretence that it is technology neutral, yet it is not.[181] Although the law maker desires to design a technology neutral regulation, they inevitably design the legislation with existing technologies in mind.[182] However, where the regulation subsequently inadvertently discriminates against new technologies due to the inbuilt structure,[183] the courts can apply an interpretative methodology of reverse engineering the law to establish any technological assumptions of the

[173] Moses 'Legal Responses' op cit note 139 at 528.
[174] Moses 'Legal Responses' op cit note 139 at 528.
[175] Moses 'Recurring Dilemmas' op cit note 164 at 72.
[176] Moses 'Legal Responses' op cit note 139 at 605; Moses 'Recurring Dilemmas' op cit note 164 at 66.
[177] Moses 'Legal Responses' op cit note 139 at 606. Wylly op cit note 124 at 350.
[178] Christopher Kuner 'German Consumer Association Denounces EU Draft Digital Signature Directive' 1998 at *http://www.kuner.com/data/sig/verbrauc.htm,* accessed on 20 February 2014.
[179] Amelia H Boss 'Searching for Security in the Law of Electronic Commerce' (1999) 23 *Nova Law Review* 585 at 617.
[180] Aalberts et al op cit note 146 at 39.
[181] Greenberg op cit note 106 at 1543.
[182] Greenberg op cit note 106 at 1527; Birnhack op cit note 105 at 28.
[183] Greenberg op cit note 106 at 1544; Birnhack op cit note 105 at 28.

law.[184] This method will help with the understanding of the law and its better application to future technologies.[185]

3.3.6 Soft law as a complement to e-signature regulation

Soft law can complement e-signature regulation where necessary.[186] It can guide e-commerce users on how to apply appropriate e-signature technologies in their e-transactions and how to prove their reliability in proceedings. Whereas hard law denotes legal obligations which are officially binding and enforceable,[187] soft laws consist of obligations or 'norms that are deliberately non-binding in character but still have legal relevance'[188] and practical effects. Consequently, soft law is characterized with words like 'should' instead of 'shall'.[189] Although the obligations in a soft law are 'not directly enforceable',[190] a state that adopts them expresses commitment and an honest obligation to observe them.[191] Soft law instruments are in the form of guidelines, recommendations, codes of conduct and so on.[192]

Soft law has a number of benefits. First, it can elaborate on sections of hard laws.[193] For example, a soft law can explain e-signature technologies and encourage use of certain e-signature technology for specific matters. Secondly, it offers flexibility of law implementation[194] by filling in cracks that reflect in hard law caused by unforeseen future conditions.[195] Thirdly, soft law can easily adjust to fast technology changes in the ICT field[196] as it is more informal and cost effectively negotiated than hard laws.[197] Again, soft law

[184] Birnhack op cit note 105 at 53 & 55.
[185] Birnhack op cit note 105 at 55.
[186] John J Kirton & Michael J Trebilcock (eds) *Hard Choices, Soft Law: Voluntary Standards in Global Trade, Environment and Social Governance* (2004) 31; Gregory C Shaffer and Mark A Pollack 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance' (2010) 94 *Minnesota Law Review* 706 at 725.
[187] Shaffer et al ibid at 707; Jovan Kurbalija 'Internet Governance and International Law' at 113 available on *http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf*, accessed on 12 November 2014.
[188] Jon Birger Skjærseth, Olav Schram Stokke & Jørgen Wettestad 'Soft Law, Hard Law, and Effective Implementation of International Environmental Norms' at 104 available at *http://www.fni.no/doc&pdf/JBS-OSS-JW-GEP-2006-3.pdf*, accessed on 11 November 2014; Kenneth W Abbott & Duncan Snidal 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421 at 421-2; David M Trubek, Patrick Cottrell & Mark Nance Legal Studies Research Paper Series No 1002 *"Soft Law," "Hard Law," and European Integration: Toward a Theory of Hybridity* (2005) University of Wisconsin Law School 1.
[189] Kurbalija op cit note 187 at 113.
[190] USLegal.com 'Soft Law & Legal Definition' available at *http://definitions.uslegal.com/s/soft-law/*, accessed on 11 November 2014.
[191] Kurbalija op cit note 187 at 113.
[192] USLegal.com op cit note 190.
[193] Shaffer et al op cit note 186 at 708-9.
[194] Abbott et al op cit note 188 at 445; Skjærseth et al op cit note 188 at 118.
[195] Shaffer et al op cit note 186 at 722.
[196] Kurbalija op cit note 187 at 114.
[197] Shaffer et al op cit note 186 at 719; Trubek et al op cit note 188 at 28.

enables states to manage situations of uncertainty with its flexibility and allows them to 'learn over time'.[198] In other words, soft laws enable processes of persuasion and acquisition of knowledge in situations of uncertainty.[199] This way, it affords guidance in the application of the law.[200]

Further, soft law helps 'states deal with the domestic political and economic consequences' of adopting a law.[201] Its non-binding nature allows states to observe the soft law to the best of their ability considering their socio-economic settings. Soft law therefore encourages progressive development[202] and increases the effectiveness of a law on the ground.[203] For these reasons, soft law can complement a technology neutral hard law for e-signature regulation by generating knowledge, building trust and creating non-binding standards of conduct,[204] consequently achieving the purpose of regulation. The Electronic Signatures Guideline for the Law Society of South Africa is a case in point.[205] It is an instrument to assist lawyers understand e-signatures and their regulation and thus use them correctly.

3.3.7 Summary

According to the technology neutral principle, a new online rule must focus on outcome not means of signature, give equivalent legal treatment between offline and online transactions, do not discriminate between e-signature technologies, enable new technology development and be sustainable. Additionally, the lawmaker may develop soft laws to guide e-commerce users on the use of current and new e-signature technologies for different situations.

To complement the technology neutrality principle, the lawmaker must develop effective e-signature regulation.

---

[198] Shaffer et al op cit note 186 at 719; Trubek et al op cit note 188 at 28.
[199] Shaffer et al op cit note 186 at 721 & 724.
[200] Christine Chinkin 'Normative Development in the International Legal System' in Dinah Shelton (ed) *Commitment and compliance: the role of non-binding norms in the international legal system* (2003) 21 at 30–31.
[201] Abbott et al op cit note 188 at 445; Trubek et al op cit note 188 at 28.
[202] Kurbalija op cit note 187 at 113-4.
[203] Shaffer et al op cit note 186 at 720-1.
[204] Trubek et al op cit note 188 at 29.
[205] Mark Heyink 'Electronic signatures for South African Law Firms Guidelines' 2014 Law Society of South Africa; See also the American Bar Association *Digital signature guidelines* (1996).

3.4 Effective laws for e-signature regulation

State regulation plays an important role in society.[206] It sets up market relations, and protects markets from fragmentation.[207] Thus state regulation controls the market; an uncontrolled market may not reach anticipated results in line with public interests.[208] State regulation of e-commerce aims to facilitate e-commerce through, amongst others, legal recognition of electronic authentication technologies.[209] The authentication technologies are to instil trust and legal confidence in e-commerce.[210] It follows that state regulation in this case aims to provide effective frameworks that will enable e-commerce to work, the growth of which will be in the public interest.

Regulation is effective if it achieves its social aims.[211] It will achieve its aims if it provides for achievement of policy goals based on clear objectives.[212] The ease of compliance with the regulation, availability of enforcement options and involved costs also impact on its effectiveness.[213]

Whereas subjects of an effective law accept its authority, an ineffective law that fails to achieve its aims loses its authority and is not accepted by its subjects.[214] It is therefore important for an online law to be effective in order to maintain authority over cyberspace actors and subject their conduct to its rules.

In this regard, Lon Fuller's principles of morality of law provide parameters for a lawmaker to produce effective law.[215] These are referred to as principles of effectiveness and provide guidance on the procedural steps that a lawmaker is to observe in the formation of law. Additionally, there are methods that test the effectiveness of substantive law content.[216]

---

[206] Robert Baldwin, Martin Cave & Martin Lodge *Understanding Regulation: Theory, Strategy, and Practice* 2ed (2012) 15; Koops note 2 at 81.
[207] Tony Prosser 'Regulation and Social Solidarity' (2006) 33 *Journal of Law and Society* 364 at 382.
[208] Baldwin et al op cit note 206 at 15.
[209] Section 3 (d) of the Lesotho E-transactions and E-commerce Bill- ITU First Draft on Objectives of the Act.
[210] Pria Chetty *An analysis of electronic signature regulation in South Africa* (Master of Management Research Report, University of Witwatersrand, 2013) at 8.
[211] Reed *Cyberspace* op cit note 3 at 179. See also Baldwin et al op cit note 206 at 30.
[212] Gertrude Makaya 'The Determinants of Regulatory Effectiveness in Liberalised Markets: Developing Country Experiences' (2001) Annual Forum, Trade and Industry Policy Strategies, Johannesburg at 5; Friederike Bundschuh-Rieseneder 'Good Governance: Characteristics, Methods and the Austrian Examples' (2008) 24E *Transylvanian Review of Administrative Sciences* 26 at 29.
[213] Diver CS 'The Optimal Precision of Administrative Rules' in Robert Baldwin, Colin Scott & Christopher Hood (eds) *A Reader on Regulation* (1998) 220 at 225-6.
[214] Reed *Cyberspace* op cit note 3 at 179-180.
[215] Lon Fuller *The Morality of Law* (1964).
[216] Reed *Cyberspace* op cit note 3 at 182.

3.4.1 Fuller's principles of effectiveness

There are eight indispensable features that should be present in every legal system to ensure that laws serve their purpose and are thus effective.[217] That is, there must be rules; which must be promulgated; the rules should be prospective and not retroactive; they must be clear and concise so that they are understood by their subjects; they should not be contradictory in nature; they must not demand the impossible from their subjects; they must be stable over time; and there must be congruence between the law and official actions.[218] These represent the minimum internal morality of law.[219] Of these features, two are relevant to this study, namely that rules must be understandable by their subjects; and that laws should be stable over time.[220]

3.4.1.1 Rules to be understandable by their subjects

Rules need to be comprehensible to their subjects. If rules are incomprehensible to subjects who have to comply with them, they tend to lose meaning and lack force.[221] Different factors render a law incomprehensible and subsequently meaningless. These include, in the context of ICT regulation, precise descriptions of the law and over-complexity of the law as illustrated below.[222]

3.4.1.1.1 Precision in law

For a lawmaker to ensure that a law succeeds in effecting its purpose, they are to use language that explicitly expresses their intention.[223] The lawmaker is thus tempted to draft a law with detailed precision in an attempt to avoid ambiguousness in the law and the desire to achieve certainty.[224] However, precision in law making, while advantageous in some regulatory fields, is not necessarily effective in ICT regulation.

[217] Fuller op cit note 215 at 39 & 47-91.
[218] Fuller ibid.
[219] Reed *Cyberspace* op cit note 3 at 180.
[220] Fuller op cit note 215 at 39, 63 & 79.
[221] Rolf H Weber 'Proliferation of "Internet Governance" ' 1 September 2014 GigaNet – Annual Symposium 1 available at *http://ssrn.com.abstract=2809847*, accessed on 21January 2015 at 8.
[222] Reed *Cyberspace* op cit note 3 at 129 & 181.
[223] Diver et al op cit note 213 at 220.
[224] Chris Reed 'How To Make Bad Law: Lessons from the computing and communications sector' Research Paper 40/2010 Part 2 Queen Mary University of London, School of Law Legal Studies at 1 available at *http://ssrn.com/abstract=1538527*, accessed on 15 January 2014; Reed *Cyberspace* op cit note 3 at 130 & 141.

Although a precise law indicates what the actor must do to comply with it, it does not explain why the actor should engage in those specific activities. Consequently, the norm of the law is lost in the detail of the law.[225]

Clarifying the normative effect of the law becomes helpful where it is uncertain whether the detailed law applies to a new technology. In such a case, an actor will comply with the spirit of the law. The lawmaker's failure to elucidate the normative effect of the rule in its detailed wording will require the actor to secure the assistance of legal experts, without which, they will remain perplexed by the rule, find it meaningless and eventually lose respect for it. [226]

Again, laws characterized by precision may debilitate the normative effect of an online law.[227] For one, a detailed law may be ignored by its subjects by avoiding the activity it encourages. Consequently, such a failed law will make the authority of its lawmaker questionable and laws developed by that lawmaker might be disregarded by the community. Further, law subjects may find precise laws to be meaningless and decide to disobey them where they believe that the law's demands are not directed towards the achievement of its aims.

The elements of precise laws which make it beneficial are its transparency, accessibility and congruence.[228] Transparency implies the lawmaker's use of well-defined words which are generally recognized by the regulated community.[229] It thus provides certainty, prevents official arbitrariness, and increases the rate of compliance with the rule.[230] Conflicts may be reduced and their resolution outcome is predictable.[231] An accessible rule on the other hand is applicable to situations without extreme effort.[232] Lastly, congruence implies that the substantive content of the rule should produce anticipated behavior.[233]

Despite the clear elements of precision, the lawmaker faces a challenge of putting the elements into practice when drafting a rule.[234] The elements are difficult to measure in

[225] Reed *Cyberspace* op cit note 3 at 134.
[226] Reed *Cyberspace* op cit note 3 at 134.
[227] Reed 'How To Make Bad Law' op cit note 224 at 1; Reed *Cyberspace* op cit note 3 at 130.
[228] Diver op cit note 213 at 219.
[229] Diver op cit note 213 at 219; HLA Hart *The Concept of Law* (1961) 121; Fuller op cit note 215 at 63-5.
[230] Diver op cit note 213 at 224-225; Duncan Kennedy 'Form and Substance in Private Law Adjudication' (1976) 89 *Havr L Rev* 1685 at 1687-8; Jerry L Mashaw 'Administrative Due Process: The Quest for a Dignitary Theory' (1981) 61 *Boston University Law Review* 885 at 901-2.
[231] Diver op cit note 213 at 226.
[232] Diver op cit note 213 at 220; Laurence H Tribe 'Perspectives on *Bakke*: Equal Protection, Procedural Fairness, or Structural Justice?' (1979) 92 *Harvard Law Review* 864 at 869-70.
[233] Joseph Tussman & Jacobus tenBroek 'The Equal Protection of the Laws' (1949) 37 *California Law Review* 341 at 346-49; Diver op cit note 213 at 220.
[234] Diver op cit note 213 at 221.

practice and trade-offs are effected between them to achieve the correct level of precision. But the lawmaker struggles to find the appropriate degree of precision for the rule which guarantees that the rule will achieve its purpose.[235] This results in ineffective laws.

In the context of e-signature regulation, it is proposed that,

> '[T]hese defects can be cured by abandoning the search for certainty. In its place we should substitute a method of lawmaking which requires the law's subjects to make their own qualitative assessments as to whether they were meeting the obligations imposed on them. This will not only make the law more easily understandable by those to whom it applies, but it will also increase the normative effect of computer and communications law.'[236]

Related to this, a rule's comprehensibility may be affected by its level of complexity.

3.4.1.1.2 Over complex law

Sometimes the lawmaker clarifies what seem to be ambiguities in the law and attempts to formulate it with precision but ends up with the opposite result of over complexity.[237] The lawmaker conducts the clarifications by constructing additional 'provisions' to the main legislative instrument. Eventually, a law will have too many provisions and end up being so complicated that it will only be understood by legal experts and not by its subjects. This poses a problem as the subjects have to seek legal advice from legal experts to explain the law to them so that they can comply with it. Without legal advice, the law will remain a conundrum to its subjects and end up failing to achieve its aim.[238]

It follows that laws which regulate e-signatures should not be too precise or over complex due to the risk of meaninglessness, and subsequent ineffectiveness. In addition, effectiveness requires stability of a law.

3.4.1.2 A law should be stable over time.

One of Fuller's principles of effectiveness holds that a law should be stable over time. A law should not be subject to a stream of amendments. This will render compliance with the law difficult.[239] If an e-commerce law is precise and detailed in nature, it will require amendments

[235] Diver op cit note 213 at 221-224.
[236] Reed 'How To Make Bad Law' op cit note 224 at 1.
[237] Reed *Cyberspace* op cit note 3 at 130.
[238] Reed *Cyberspace* op cit note 3 at 129-130.
[239] Fuller op cit note 215 at 38 & 79.

as soon as technology changes.[240] Changes in the law will impose a duty on its subject to adapt their actions and thus obstruct efforts to comply. Eventually, it loses authority over its subjects and will not achieve its social aim.[241]

Whereas Fuller's principles of effectiveness are directed towards procedures of a law's drafting, it is also important to test whether the substantive content of law achieves its aims, and is thus effective.

3.4.2 Testing the effectiveness of law's content

A law's capacity to attract participants and retain membership is a measure of its effectiveness. If membership of the law fades away, it is a sign that the law's authority is diminished.[242]

Behavioural choices of actors who partake in a law together with choices of those not partaking in a law help assess a law's quality. The behavioural choices of participants include their compliance with the law, evasion of the law or attempts to rebel against it.[243] Behavioural choices of those outside the law include attempts to join the legal system, to team up with it, alternatively, efforts to fight it.[244] Data reflecting these behavioural trends will determine the law's effectiveness. For example, if participants in e-signature law avoid using the digital signature based on PKI as prescribed by law, whilst non participants fight the statute by lobbying for its amendment, it is a sign that the law does not achieve its aims and is regarded as ineffective.[245]

Additionally, a law's effectiveness may be measured by its legitimacy. Legitimacy is a relative concept that consists of five components, namely political, legal, cultural, operational and internal rationality.[246] Political rationality implies that a law is a tool that serves to achieve political reformative objectives. Therefore, it must be as simple as possible to achieve the objectives with ease.[247] Further, a law is legally rational if it is less detailed, stable and provides predictability.[248] But cultural rationality connotes that a law must be accepted by its subjects from a moral, ethical, and religious point of view. It should not

[240] Reed *Cyberspace* op cit note 3 at 181.
[241] Reed *Cyberspace* op cit note 3 at 181.
[242] Reed *Cyberspace* op cit note 3 at 183.
[243] Schmidt A 'Radbruch in Cyberspace: About Law-system Quality and ICT Innovation' (2009) 2 *Masaryk University Journal of Law and Technology* 195 at 208.
[244] Schmidt ibid.
[245] Reed *Cyberspace* op cit note 3 at 183-4.
[246] Peter Wahlgren 'The Legitimacy Sphere: Between Law, Culture, Politics and Enforceability' (1999-2015) 56 *Scandinavian Studies in Law* 427 at 428.
[247] OECD *Guiding Principles for Regulatory Quality and Performance* (2005) 3; Wahlgren ibid at 431.
[248] Wahlgren ibid at 433-4.

conflict with its subjects' traditional customs.[249] Put differently, a law should be 'understandable, in accordance with the public sense of fairness'.[250] To achieve this, the law maker must obtain inputs of interested parties through public consultations during the law making process to ensure its acceptance.[251] Moreover, a law is functionally rational if it can achieve its objectives efficiently at minimal costs, has a clear underlying purpose and can adjust to different situations in several parts of society.[252] Lastly, the language of a law must be transparent and coherent, and it must be systematically integrated into an existing legal system to be internally rational.[253] Without these elements, a law's effectiveness is limited.

3.5 Conclusion

This chapter explores the principle of functional equivalence which maintains as follows:

- where an offline version of an activity is inequivalent to its online version, the lawmaker must develop a new rule for the online activity which gives an online activity the same level of protection or effect as a rule for the offline activity;
- the new online rule should be equivalent in both legal terms and practicability;
- a functionally equivalent rule should address the mental state of the actor or the effects of their conduct, not the conduct an actor engages in to reach a certain outcome.

The chapter further explores the principle of technology neutrality in online regulation. It maintains that:

- a law should regulate the effects of a person's conduct instead of the means they use to achieve the effects;
- the law should complement online and offline equivalence;
- it should not impose a technology or discriminate between technologies;
- it should encourage the development of new technologies;
- it must sustain technology developments.

[249] Ibid 434.
[250] Ibid.
[251] OECD 'APEC–OECD Integrated Checklist on Regulatory Reform' at 17 available at *www.oecd.org/dataoecd/41/9/34989455.pdf,* accessed on 4 January 2018.
[252] OECD op cit note 247; Wahlgren op cit note 246 at 436-7.
[253] Wahlgren ibid 438.

The chapter illustrates that soft law can complement e-signature law to help it achieve its objectives.

Moreover, the chapter elaborates on the need for and how a lawmaker should draft an effective law. It explains that:

- an effective law achieves its aims;
- it must be comprehended by its subjects and stable over time;
- a law's effectiveness is assessed by its capacity to attract and maintain participants, and the extent of its legitimacy.

If Lesotho and SADC e-signature instruments adequately observe these principles, the instruments will enhance the growth of e-commerce with ease. With this in mind, an examination of international legal instruments on regulation of e-commerce follows.

CHAPTER FOUR: INTERNATIONAL INITIATIVES ON REGULATION OF E-SIGNATURES

4.1 Introduction

In recognition of the rapid growth of e-commerce, international organisations acknowledged the need to draft rules and guidance for the use of e-commerce.[1] Due to the international nature of e-commerce, the rules of one state inevitably impacted on those of another.[2] This called for a harmonisation of e-commerce regulation and the United Nations (UN) and the International Chamber of Commerce (ICC), among others, responded to these issues. The United Nations Commission on International Trade Law (UNCITRAL), a body of the UN, developed two model laws and one convention on e-commerce. These are the UNCITRAL Model Law on Electronic Commerce (MLEC),[3] the UNCITRAL Model Law on Electronic Signatures (MLES)[4] and the UN Convention on the Use of Electronic Communications in International Contracts (CUECIC).[5] These instruments provide guidance, and serve as instruments that states can use to draft their national legislation.[6] The ICC also developed non-binding guidelines called the General Usage for International Digitally Ensured Commerce (GUIDEC version I and II). These are the international instruments discussed in this chapter.

This chapter considers the guiding principles adopted by UNCITRAL on the regulation or facilitation of e-signatures. It examines how UNCITRAL interprets application of the principles through its instruments. The study further highlights assumptions made by UNCITRAL on the facilitation of e-commerce. It points out that the MLEC together with CUECIC provide guidance on the application of the principles of functional equivalence and

[1] Alan Davidson *The Law of Electronic Commerce* (2009) 330.
[2] Ibid.
[3] United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998' 1999 available at *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*, accessed on 17 September 2015.
[4] United Nations 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001' 2002 available at *https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf*, accessed on 17 September 2015.
[5] United Nations 'United Nations Convention on the Use of Electronic Communications in International Contracts' 2007 available at *http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf*, accessed on 18 September 2015.
[6] Stephen Mason *in Law* 4 ed (2016) 95.

technology neutrality on e-signature regulation. These instruments give an online user equal treatment to an offline user as they do not place a heavy burden on the online user for the adoption and use of e-signatures. They also do not discriminate between technologies. The MLES, on the other hand, imposes a heavy burden on an online user contrary to the functional equivalence principle, and is both technology neutral and technology specific.

4.2 United Nations Commission on International Trade Law (UNCITRAL)

The UN General Assembly established UNCITRAL in 1966. [7] It is the main legal body of the UN through which the UN can actively manage international trade issues.[8] Its mandate is to progressively harmonise and unite international trade law in the interests of developing countries and to remove impediments to trade caused either by insufficiencies or inconsistencies in national legislation on trade.[9] It thus drafts legal texts to promote this mandate through its different working groups.[10] It also provides assistance to nations in reviewing their legal instruments or drafting of new pieces of legislation to put UNCITRAL texts into effect.[11] The working group on e-commerce drafted the three instruments mentioned above.

4.3 UNCITRAL Model Law on Electronic Commerce (MLEC)

4.3.1 Purpose and objectives of the MLEC

UNCITRAL developed the MLEC in response to a number of factors. First, the communication legislation passed in several countries was considered either inadequate or outdated because it did not anticipate the use of e-commerce. Secondly, existing legislation restricted the use of non-paper communication by, for instance, prescribing the use of 'written', 'signed' or 'original' documents. Thirdly, while these laws covered some aspects of e-commerce, they did not deal with it in its entirety. This led to uncertainty as to the legality and validity of information presented differently from that on paper.[12] Fourthly, the inadequate national legislation and their different approaches to governance of the new forms

[7] General Assembly Resolution 51/162 of 16 December 1996; Davidson op cit note 1 at 331.
[8] United Nations Commission on International Trade Law 'A Guide to UNCITRAL: Basic facts about the United Nations Commission on International Trade Law' 2013 at 1 available on *http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf*, accessed on 19 August 2015 (A Guide to UNCITRAL); Davidson op cit note 1 at 331.
[9] A Guide to UNCITRAL ibid; Davidson op cit note 1 at 331.
[10] A Guide to UNCITRAL ibid, for instance, the Working Group on Electronic Commerce and Working Group on the International Sale of Goods; Davidson op cit note 1 at 331.
[11] A Guide to UNCITRAL ibid; Davidson op cit note 1 at 331.
[12] Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) [within the MLEC] (Guide to MLEC) para 3.

of communication created obstacles to international trade.[13] UNCITRAL therefore adopted the MLEC on 12 June 1996.[14] It was subsequently adopted by the UN General Assembly on 16 December 1996.[15]

The MLEC has several aims. Amongst these are its intention to offer national legislators a set of internationally acceptable rules relating to e-commerce; to demonstrate how legal obstacles such as requirements for 'writing', 'signed' and 'original' may be removed and how to develop a safer legal environment for e-commerce.[16] The UN General Assembly was convinced that the development of a model law that facilitates the use of e-commerce and is suitable for states with differing economic, social and legal systems, can contribute to harmonious relations between the economic associations of different states.[17]

Accordingly, the objectives of the MLEC include enabling and facilitating e-commerce.[18] It aims to encourage economic development and promote effectiveness in international trade.[19] Its role is to assist states in the enhancement of their existing legislation or the formulation of new legislation that deals with the use of non-paper based methods of communication.[20] UNCITRAL therefore recommended that states which enact or revise their laws must reflect on the MLEC for purposes of uniformity, in regulation of non-paper based communication methods.[21]

4.3.2 Guiding principles of the MLEC

The MLEC was the first legislative text to adopt the underlying principles of functional equivalence and technology neutrality.[22]

4.3.2.1 The Functional-equivalent approach

UNCITRAL based the MLEC on the realisation that legal requirements that prescribe the use of paper based documents create the core obstacle to growth of a modern means of

[13] Para 4 of Guide to MLEC ibid.
[14] 'UNCITRAL Model law on Electronic commerce (1996): Text – Guide to enactment status' available at *www.uncitral.org*, accessed on 23 September 2016.
[15] General Assembly Resolution 51/162 of 16 December 1996.
[16] Para 2 & 5 of Guide to MLEC op cit note 12; Mason *Electronic Signatures* op cit note 6 at 95-6.
[17] Para 4 of General Assembly Resolution 51/162 of 16 December 1996.
[18] José Angelo Estrella Faria 'e-Commerce and International Legal Harmonization: Time To Go Beyond Functional Equivalence?' (2004) 16 *SA Merc LJ* 529 at 530-531.
[19] Para 6 of Guide to MLEC op cit note12.
[20] General Assembly Resolution 51/162 of 16 December 1996.
[21] General Assembly Resolution 51/162 of 16 December 1996; Tana Pistorius 'From snail mail to e-mail – a South African perspective on the web of conflicting rules on the time of e-contracting' (2006) XXXIX *CILSA* 178 at 180.
[22] 'UNCITRAL Model law on Electronic commerce (1996): Text – Guide to enactment status' op cit note 14.

communication.[23] It pointed out that the MLEC should allow states to adjust their national legislation to accommodate improvements in communication technology pertinent to trade law.[24] In so doing, it recommended that they should not discard paper based requirements or disrupt the legal concepts that motivate them.[25] It has also acknowledged that the development of new laws may be necessary in some cases to ensure the fulfilment of the writing requirement.[26] The MLEC is therefore modelled on the 'functional equivalent approach'.[27]

The functional equivalent approach in the MLEC is to analyse 'the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.'[28] UNCITRAL gives examples of functions performed by a paper document, namely, to provide that it would be legible by all; that it would remain unaltered over time and to allow for the authentication of data by means of a signature. It notes that an electronic record can provide a level of security similar to that of paper in respect of these functions, and may provide greater speed and reliability, particularly with regard to identifying a source and content of data, provided certain technical and legal requirements are met.[29]

In addition, the MLEC warns of negative effects to be avoided when the functional equivalence approach is applied. It notes that states' application of this approach should not result in imposing on online users stricter standards of security and related costs than that found in a paper based sphere.[30] Hence it advocates that a functionally equivalent rule should be practicable as reflected in chapter three.[31]

The MLEC recognises that a data message alone is not equivalent to a paper document.[32] The two are different in nature, thus a data message cannot perform all possible

[23] Para 15 of Guide to MLEC op cit note12; Eiselen S 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17 *PER/PELJ* 2805 at 2807.
[24] Faria 'e-Commerce' op cit note 18 at 531.
[25] Para 15 of Guide to MLEC op cit note 12; See part 2.2 above.
[26] Para 15 of Guide to MLEC op cit note 12.
[27] Faria 'e-Commerce' op cit note 18 at 531; Para 16 of Guide to MLEC op cit note 12; see part 3.2.3.2 above.
[28] Para 16 of Guide to MLEC op cit note 12; See part 3.2.3.2 above; LL Ramokanate 'The Lesotho electronic transactions and electronic commerce bill: will it replace the common law of contract as we know it?' (2015) 22 *Lesotho Law Journal* 117 at 129; Brian C Pidcock 'Cross-border fraud: Bridging global protection disparity through international cooperative efforts' (2008-2009) 17 *Currents International Trade LJ* 78 at 82; Tana Pistorius ' "Nobody knows you're a dog": The attribution of data messages' (2002) *SA Merc LJ* 737 at 738.
[29] Para 16 of Guide to MLEC op cit note 12.
[30] Para 16 of Guide to MLEC op cit note 12; T Pistorius 'Developing countries and copyright in the information age: The Functional Equivalent Implementation of the WCT' (2006) 9 *PER/PELJ* 149/197 at 164/197.
[31] See part 3.2.3.2.1 above.
[32] Julien Hofman 'Electronic evidence in criminal cases' (2006) *SACJ* 257 at 260.

functions of a paper document,[33] and vice versa.[34] Hence it assumes a flexible approach of functional equivalence.[35] It further noted the hierarchy of form requirements in paper based documents and their differing levels of reliability, inalterability and traceability. For example, the requirement of 'writing' is not to be confused with stricter requirements of 'signed writing', 'legally authenticated act' or 'signed original'.[36]

The MLEC seeks to identify primary functions of paper based form requirements, and then create criteria, which if satisfied by a data message, will allow it to enjoy a similar level of legal recognition as paper documents which perform a similar function.[37] It should not be misunderstood as trying to describe 'a computer-based equivalent to any kind of paper document.'[38] The MLEC adopts the functional approach principle in relation to 'writing', 'signature' and 'original' requirements.[39] The second underlying principle of the MLEC is media neutrality.

4.3.2.2 Media neutrality as technology neutrality

The concept of 'media neutrality' is described as the opposite of a statement by Marshall McLuhan and Quentin Fiore that 'the medium is the message'.[40] This statement proposes that effects accomplished by means or methods of communication of a message are more significant than effects of the message itself.[41] The authors illustrate this by comparing a message transmitted through a handwritten document to one transmitted through the Internet and television. They argue that because the message transmitted by the latter means reaches more people, it will be more influential or have more effect than the message transmitted by a hand written document. Therefore, the effect of the message does not depend on the message itself, but on the medium of transmission.[42]

---

[33] Para 17 of Guide to MLEC op cit note 12.
[34] Farisa Tasneem 'Electronic Contracts and Cloud Computing' (2014) 9 *Journal of International Commercial Law and Technology* 105 at 112; Mason *Electronic Signatures* op cit note 6 at 96.
[35] See part 3.2.3.2 above.
[36] Para 17 of Guide to MLEC op cit note 12; See part 2.8 above.
[37] Para 18 of Guide to MLEC op cit note 12; Luca G Castellani 'The role of UNCITRAL texts in promoting a harmonized legal framework for cross-border mobile payments' (2013) 8 *Washington Journal of Law, Technology & Arts* 265 at 269; C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' 2015 *TSAR* 461 at 464; A Brooke Overby 'UNCITRAL model law on electronic commerce: will cyberlaw be uniform? An introduction to the UNCITRAL model law on electronic commerce' (1999) 7 *Tulane Journal of International and Comparative Law* 219 at 222; See part 3.2.3.2 above.
[38] Para 18 of Guide to MLEC op cit note 12.
[39] Articles 6, 7 & 8 of the MLEC.
[40] Marshall McLuhan & Quentin Fiore *The Medium is the Message* (1967) 8.
[41] Huei-ju Tsai 'Media neutrality in the digital era: a study of the peer-to-peer file sharing issues' (2005) 5 *Chicago-Kent Journal of Intellectual Property* 46 at 52.
[42] Tsai ibid at 52.

On the other hand, media neutrality states that 'an idea is independent of the media in which it gets placed.'[43] The media in media neutrality varies from physical storage media such as books, electric storage media like computer disks, to systems of communication or entertainment like the broadcast media and modes of expression in the digital world.[44] For example, in copyright law, media neutrality means that a copyright owner should enjoy the same rights notwithstanding the analogue or digital medium in which their work is presented.[45]

The media neutrality approach covers messages in current and future mediums.[46] Accordingly, it encourages more creativity and improves the growth of science and technology development.[47] Its purpose is to shape flexible laws that will accommodate new technology without the need for amendment in future.[48]

The MLEC indicates that states should incorporate procedures it prescribes that provide for equal treatment of both computer based users and paper based users in order to create a media neutral environment.[49] The MLEC does not propose to change traditional rules in the offline sphere,[50] but its media neutral environment connotes non-discrimination of paper and electronic mediums.[51]

The MLEC exemplifies the media neutral approach under its definition of a 'data message'. Article 2 (a) defines a 'data message' as 'information generated, sent, received, or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy'. The definition encompasses all situations where information may be made, communicated or stored, 'irrespective of the

[43] 'Account planning methods: The Media Neutral Idea' available at *account-planning-confessions.blogspot.com/.../media-supremacy-vs-media-neutrality.html*, accessed on 12 July 2015.
[44] Deborah Tussey 'Technology Matters: Media Neutrality in Copyright' 2003 at 5-6 available at *http://www.law.tulane.edu/WIPIP/papers/techtulane.pdf*, accessed on 19 December 2004 cited in Tsai op cit note 41 at 53; Mireille Hildebrandt 'Legal protection by design: objections and refutations' (2011) 5 *Legisprudence* 223 at 237.
[45] Deborah Tussey 'Technology matters: the courts, media neutrality, and new technologies' (2004-2005) 12 *J Intell Prop L* 427 at 428; Tussey 'Technology Matters: Media Neutrality in Copyright' op cit note 44 at 53; Eliza Mik 'Certainty at last? A "new" framework for electronic contracting in Singapore' (2013) 8 *Journal of International Commercial Law and Technology* 160 at 172.
[46] Tsai op cit note 41 at 54; Tussey 'Technology matters: the court' ibid at 430.
[47] Tsai op cit note 41 at 54; See part 3.3.3.2.2 above.
[48] Bruce P Keller 'Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property' (1997-1998) 11 *Harvard Journal of Law & Technology* 401 at 427-8; See part 3.3.3.3.1 above.
[49] Para 6 of Guide to MLEC op cit note 12; See part 3.3.3.1.2 above.
[50] Para 24 of Guide to MLEC op cit note 12.
[51] Para 5 of Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001) [within the MLES] (Guide to MLES); Thomas J Smedinghoff 'The Legal Challenges of Implementing Electronic Transactions' (2008) 41 *Uniform Commercial Code Law Journal* 3 at 9.

medium on which such information may be affixed.'[52] The MLEC did not make any exclusion of form or medium lest it countered the media neutrality principle.[53] In fact, the MLEC's use of the words 'similar means' in the definition of a data message reflects that it is open to embrace future forms of transmission.[54]

The MLEC provisions illustrate that 'media neutrality can be broadly read as "technology neutrality".'[55] They encompass the principle of non-discrimination among various techniques used to communicate or store information electronically, a principle that is regularly referred to as 'technology neutrality'.[56] They also entail attributes of technology neutrality expounded on by chapter three of this study.[57] The UN validates this assertion by stating that 'technological neutrality encompasses also "media neutrality"'.[58] It follows that 'media neutrality as technology neutrality should be at the centre of new technology issues.'[59]

With these principles in mind, a discussion of Article 7 of the MLEC on the requirement of signature in data messages follows.

4.3.3 Criteria set by the MLEC for a data message to qualify as signature

The MLEC does not define an e-signature but lays down criteria to be met where the law requires a signature.[60] Article 7 provides as follows:

> '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

[52] Para 24, 30 & 31 of Guide to MLEC op cit note 12. See also Article 5 of MLEC; Para 46 of Guide to MLEC op cit note 12; Mason *Electronic Signatures* op cit note 6 at 97.
[53] Para 24 of Guide to MLEC op cit note 12.
[54] Para 31 of Guide to MLEC op cit note 12.
[55] Tussey 'Technology Matters: Media Neutrality in Copyright' at 6 op cit note 44 at 53; Tussey 'Technology matters: the courts' op cit note 53 at 434; Eliza Mik 'Evaluating the Impact of the UN Convention on the Use of Electronic Communications in International Contracts on Domestic Contract Law--The Singapore Example' (2010) 28 *Chinese (Taiwan) Yearbook of International Law and Affairs* 43 at 48-9; Mik 'Certainty at last?' op cit note 45 at 162.
[56] S Eiselen 'The UNECIC: International trade in the digital era' (2007) 2 *PER* 1 at 21; Para 5 of Guide to the MLES op cit note 51; Davidson op cit note 1 at 333; Mik 'Certainty at last?' op cit note 45 at 162 who states that in terms of CUECIC, 'technology neutrality means that the Convention covers "all factual situations where information is generated, stored or transmitted in the form of electronic communications, irrespective of the technology or medium used" '.
[57] See part 3.3.3 above.
[58] See Paras 47 & 48 of Explanatory note of the United Nations Convention on the Use of Electronic Communications in International Contracts 2005 [within CUECIC] (Explanatory note of CUECIC).
[59] Tsai op cit note 41 at 86.
[60] Eiselen S 'Fiddling with the ECT Act' op cit note 23 at 2808.

(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) …. .

(3) The provisions of this article do not apply to the following: [...].'

Article 7 has implications for the functions of an e-signature and the standard of security of an e-signature. First, in formulating this article, UNCITRAL considered and acknowledged the several functions of a paper based signature. Amongst these is that a signature identifies a person, provides certainty as to their personal involvement in the act of signing, attests to the intent of a party to be bound by a contract; endorses authorship of a text[61] and indicates that a person was at a certain place at a particular time.[62]

Additionally, UNCITRAL noted the existence of other procedures such as stamps, printed letterhead or typed signature, and their different levels of certainty. It acknowledged that the procedures are sometimes recognised as fulfilling the signature requirement.[63] It further noted situations in which a handwritten signature is required to be joined with other security methods such as a witness's validation of a signature.[64]

UNCITRAL expressed that it might be ideal for the law to create standards and procedures that are functional equivalents for the various signatures for e-commerce. This would increase levels of certainty as to the legal recognition of the authentication methods. However, it recognised that there is a risk that the MLEC will be tied to specific technological developments if these are created.[65]

For this reason, the MLEC adopted an all-inclusive approach by selecting two basic functions of a signature, that is, to identify an author of a document; and to confirm their approval of the content of the document (Article 7 (1) (a)).[66] These functions, identification and authentication are general conditions that ensure that a data message will be enforceable under signature requirements that previously constituted an obstacle to e-commerce.[67]

[61] Para 53 of Guide to MLEC op cit note 12; See part 2.5 above.
[62] Para 53 of Guide to MLEC op cit note 12.
[63] Para 54 of Guide to MLEC op cit note 12; see parts 2.6.2 & 2.6.3 above.
[64] Para 54 of Guide to MLEC op cit note 12; see also part 2.8 above.
[65] Para 55 of Guide to MLEC op cit note 12.
[66] Para 56 of Guide to MLEC op cit note 12. See part 2.6 above which shows that courts give legal recognition to a traditional signature if it performed functions of identification and authentication. Hence the MLEC tries to give the e-signature the similar effect to the traditional signature.
[67] Para 56 of Guide to MLEC op cit note 12.

The second element of article 7 is that it provides a 'flexible approach to the level of security' which the method used for identification and approval of contents is to meet.[68] The method used should be as reliable as is appropriate for the purpose for which the data is generated, in the light of the circumstances and relevant agreements.

While the MLEC does not define the word 'reliable' in its Article 7 it is described in the literature as a term 'upon which the law occasionally relies for recognizing or determining legal effects'.[69] It is intended to establish that 'the record is capable of standing for the facts to which it attests.'[70] Reliability therefore consists of an assessment or measure of systems, devices or procedures and the technologies they apply.[71] It looks at the systems that collect and treat e-communication[72] before, during and after processing (attachment of an e-signature method in this case) with the goal of ensuring its authenticity.[73] In other words, reliability is concerned with 'the degree of control exercised over the procedures that permit the data to be created.'[74] Reliability is thus strengthened by establishment of a chain of custody (provenance) when adducing evidence. The evidence may be in the form of electronic evidence (e-evidence),[75] real or oral evidence. A robust chain of provenance will increase the weight given to evidence.[76] Examples of e-evidence that can help prove reliability of a signature method or e-record include metadata,[77] time stamps,[78] audit trails[79] to e-communication and use of SSL protocol.[80]

---

[68] Article 7 (1) (b) of the MLEC; Para 57 of Guide to MLEC op cit note 12.

[69] Manuel Alba 'Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions' (2013-2014) 47 *Creighton Law Review* 387 at 388.

[70] Stephen Mason & Allison Stanfield 'Authenticating electronic evidence' in Stephen Mason & Daniel Seng (eds) *Electronic Evidence* 4 ed (2017) 193 at 193.

[71] Alba op cit note 69 at 388.

[72] The e-communication may be stored, communicated, processed, exchanged or presented.

[73] Alba op cit 69 at 412. Authenticity in the context of electronic evidence means 'the record is what it claims to be' (Mason et al 'Authenticating electronic evidence' op cit note 89 at 193).

[74] Mason et al 'Authenticating electronic evidence' op cit note 89 at 196. As an objective standard, determination of reliability considers all relevant circumstances, but mainly the technology and procedures applied in light of acceptable market practices (Alba op cit note 69 at 412).

[75] Electronic evidence is defined as '[d]ata (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system, that is relevant to the process of adjudication' (Stephen Mason (ed) *International Electronic Evidence* British Institute of International and Comparative Law (2008) xxxv cited in SALRC op cit note at 27).

[76] Aida Ashouri, Caleb Bowers and Cherrie Warden 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts' (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115 at 121.

[77] Sylvia Papadopoulos 'Electronic Wills with an Aura of Authenticity: *Van der Merwe v Master of the High Court and Another*' (2012) 24 *SA Mercantile LJ* 93 at 104; Stephen Mason, Clive Freedman & Sandip Patel 'England and Wales' in Stephen Mason (ed) *Electronic Evidence* 3ed (2012) 327 at 410. Metadata is referred to as a 'finger print'of a document. In fact '[i]n the absence of credible metadata, the admissibility and evidential weight of any electronic document may fall to be challenged' (Brendan Hughes 'The rise of electronic discovery' (2012) *De Rebus* 24); See *Hellard v Money* [2008] EWHC 2275 (Ch); *Campaign Against Arms Trade v BAE Systems PLC* [2007] ALL ER (D) 324 (Feb).

Furthermore, reliability may be measured in terms of time and purpose;[81] for example, at the time of attaching the signature. The fact that better methods of conducting the act develop at a later stage must not render the method less reliable for determining its legal effect at the time of its use.[82] Moreover, the fact that reliability is measured on grounds of purpose 'recognises that different purposes may objectively require different levels of reliability.'[83] Purposes that will determine the level of reliability of a method used to sign a data message include the 'nature of [the] trade activity',[84] 'the kind and size of the transaction',[85] 'the function of signature requirements in a given statutory and regulatory environment',[86] and 'the importance and the value of the information contained in the data message'.[87] Therefore, the purpose of one transaction may require a high technology e-signature with a high reliability level such as the digital signature based on PKI, while a low technology e-signature with a low reliability level such as a typed name in an email message may be sufficient in transaction with a different purpose.[88] Hence reliability of a method of signature depends on the purpose of an e-transaction.

Additionally, the MLEC Guide sets out technical, legal and commercial factors that determine the 'appropriateness' of the method used for signature in article 7 (1) (a).[89] The factors include: the sophistication and capacity of the equipment used by each party; the frequency of commercial transactions between the parties; the range of authentication procedures made available by intermediaries and compliance with such; compliance with trade customs and practice; the existence of insurance coverage mechanisms against unauthorised messages; the availability of alternative methods of identification and the cost of implementation; the degree of acceptance of the identification methods and any other relevant factor. Therefore, the question whether a method used to sign a data message is as

[78] Timestamp is a 'digital record of the time of occurrence of a particular event' available at *https://en.oxforddictionaries.com/definition/timestamp*, accessed on 13 March 2017.
[79] An audit trail is a '[p]aper or 'electronic' trail that gives a step by step documented history of a transaction' available at *http://www.businessdictionary.com/definition/audit-trail.html*, accessed on 13 March 2017.
[80] See part 2.9.11 above.
[81] Alba op cit note 69 at 414.
[82] Amelia H Boss 'Searching for Security in the Law of Electronic Commerce' (1999) 23 *Nova L Rev* 585 at 623.
[83] Alba op cit 69 at 415.
[84] Para 58 (2) of Guide to MLEC .
[85] Para 58 (4) of Guide to MLEC.
[86] Para 58 (5) of Guide to MLEC.
[87] Para 58 (11) of Guide to MLEC.
[88] Reliability reflects the legislator's desire to bring trust and certainty into e-transactions and use of electronic measures (Alba op cit 69 at 388 & 390).
[89] Para 58 of Guide to MLEC op cit note 12.

reliable as appropriate for the purpose it is made in the circumstances is a question of evidence.

As chapter two reflects, there is a concern that electronic data and e-records are vulnerable to fabrication or modification.[90] Thus questions of the authenticity and integrity of an e-record become crucial for the proof of reliability.[91] E-evidence, oral and circumstantial evidence will help prove authenticity of an e-record[92] to support a declaration that e-communication has not been modified or corrupted.[93] Consequently, rules on admissibility of e-evidence and its due evidential weight will facilitate proof of the authenticity and integrity of data messages. They may help guard against manipulation of data.[94]

Article 9 of the MLEC provides rules on the admissibility and evidential weight of data messages as follows:

> (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
> *(a)* on the sole ground that it is a data message; or,
> *(b)* if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
>
> (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Article 9 (2) refers to the chain of evidence and how a party can prove that a data message is what it purports to be by the use of, among others, meta data or check sums.[95] It further deals

[90] See parts 2.9 above; South African Law Reform Commission Discussion Paper 131 (Project 126) *The Review of the Law of Evidence* (2015) (SALRC) para 3.49 & 3.50; DW Collier 'Electronic evidence and related matters' in PJ Schwikkard & SE van der Merwe *Principles of evidence* 3ed (2012) 411. For challenges to authenticity of electronic evidence see Mason et al 'Authenticating electronic evidence' op cit note 89 at 196.
[91] SALRC op cit note 90 at Para 3.49 & 3.50.
[92] Mason et al 'Authenticating electronic evidence' op cit note 89 at 219.
[93] Stephen Mason 'Authenticating digital data' in Stephen Mason (ed) *Electronic evidence* 3ed (2012) 109 at 118; Aida Ashouri, Caleb Bowers and Cherrie Warden 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts' (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115 at 117.
[94] SALRC op cit note 90 para 3.50.
[95] Dana van der Merwe, Anneliese Roos & Tana Pistorius et al (eds) *Information and Communications Technology Law* 2 ed (2016) 120.

with authorship of a data message which is a component of authentication.[96] The article therefore facilitates the admission of data messages as evidence in proceedings to establish, among others, that an e-signature was as reliable as appropriate in the circumstances.

To summarise, the minimum requirements of an e-signature are identification, authentication and security.[97] The MLEC implies that an ordinary e-signature[98] is a functional equivalent of handwritten signature if it identifies a person, authenticates a message, and there is evidence that it was as reliable as appropriate in the circumstances. The security standard addresses the issue of susceptibility of e-signatures to modification and fabrication. The MLEC further facilitates the admission of e-evidence to help prove the reliability of an e-signature method. It acknowledges that users may require differing reliability levels of e-signature methods depending on the nature of their transaction. These e-signature criteria apply to parties with or without previous contractual relationships.[99]

The MLEC has led the process of development in law as it was a pre-emptive harmonisation instrument that delivers answers to issues that were yet to arise.[100] UNCITRAL suggested that states incorporate the legislative instrument into their national laws,[101] and this was done by several states. The legislation of at least 67 states out of a total of 143 jurisdictions has been based on or influenced by the MLEC.[102]

4.4 The UNCITRAL Model Law on Electronic Signatures (MLES)

4.4.1 Origin and purpose

UNCITRAL adopted the MLES in 2001 in response to the increasing use of electronic authentication technologies which sought to replicate the functions of hand written signatures and other paper based authentication procedures.[103] Business sought clarity on the use of the different electronic authentication technologies for purposes of certainty as to their legal

[96] Van der Merwe et al *Information* ibid at 120.
[97] Eiselen 'Fiddling with the ECT Act' op cit note 23 at 2808 deduced from on Paras 53-54 of Guide to MLEC op cit note 12.
[98] See part 2.9 above.
[99] Para 59 of Guide to MLEC op cit note 12.
[100] Faria 'e-commerce' op cit note 18 at 531.
[101] Faria 'e-commerce' op cit note 18 at 530.
[102] UNCITRAL 'Status UNCITRAL Model Law on Electronic Commerce (1996)' 2015 available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html*, accessed on 16 October 2016.
[103] Para 3 of Guide to MLES op cit note 51.

effect in e-commerce.[104] Thus, UNCITRAL developed an international model law that provides a uniform set of rules to encourage e-signature use and promote legal harmony.[105]

The objectives of the MLES include enabling and facilitating the use of e-signatures, the provision of equal treatment to users of computer-based information and paper based documents and the creation of a media neutral environment.[106] This is in order to foster international trade and economic development.

The MLES builds on the essential principles central to signature provisions in Article 7 of the MLEC so as to address e-signature issues more efficiently.[107] It sets practical standards that test the technical reliability of an e-signature technology. It further offers a connection between the technical reliability and the legal effectiveness to be expected from the e-signature.[108] The MLES' definition of 'electronic signature' follows.

4.4.2 Definition of an e-signature under the MLES

Whereas the MLEC does not define an e-signature, but refers to a method used for a data message to fulfil the signature requirement, article 2 (a) of the MLES defines an e-signature. It provides that:

> 'For the purposes of this Law:
> *(a)* "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.'

The definition has two components.[109] First it establishes a connection between different kinds of data,[110] describing an e-signature as electronic data that is 'in, affixed to or logically associated with, a data message.'[111] The word 'in' means the e-signature is within the data message, it can be found when the message is opened. The words 'logically associated with'

[104] Para 3 of Guide to MLES op cit note 51.
[105] Para 3 of Guide to MLES op cit note 51.
[106] Para 5 of Guide to MLES op cit note 51.
[107] Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/56/588)]; Para 4 & 63 of Guide to MLES op cit note 51.
[108] Para 4 of Guide to MLES op cit note 51.
[109] Mason *Electronic Signatures* op cit note 6 at 102.
[110] Mason *Electronic Signatures* op cit note 6 at 102.
[111] Mason *Electronic Signatures* op cit note 6 at 102.

or 'affixed to' mean that the signature data is in a file distinct from the data message that has been signed, it cannot be found in the message, but is sent as an attachment to the message.[112]

The second component of the definition relates to the two purposes of the data. It says the e-signature may identify the signatory and indicate their approval of information which establishes their connection to the information.[113] Hence an e-signature may serve the basic functions of a handwritten signature as to render an e-signature as a functional equivalent of a handwritten signature.[114] However, e-signature does not always produce legal results.[115] The MLES clarifies that

> 'defining an electronic signature as capable of indicating approval of information amounts primarily to establishing a technical prerequisite for the recognition of a given technology as capable of creating an equivalent to a handwritten signature.'[116]

Thus a user must not confuse an authentication technology that only identifies a signer but does not establish the signer's connection to the document as producing the legal effect of a 'signature':[117] it should have both functions for legal recognition.[118] Article 2 (a) is to be read together with article 6 of the MLES.

4.4.3 Compliance with the requirement for a signature

Article 6 of the MLES provides guidance on how to test the reliability of a method of signing. It states that:

> '1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that 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. ….
>
> 3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

[112] Mason *Electronic Signatures* op cit note 6 at 102.
[113] Mason *Electronic Signatures* op cit note 6 at 102; Para 93 of Guide to MLES op cit note 51.
[114] Para 93 of Guide to MLES op cit note 51.
[115] Para 93 & 94 of Guide to MLES op cit note 51.
[116] Para 93 of Guide to MLES op cit note 51.
[117] Para 94 of Guide to MLES op cit note 51.
[118] See part 2.9 above.

(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.

4. Paragraph 3 does not limit the ability of any person:

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].'

The content of para 1 above draws from article 7 (1) (b) of the MLEC, whilst the definition of an e-signature in article 2 (a) of the MLES reiterates article 7 (1) (a) of the MLEC.[119]

Paragraphs 3 (a) to (d) tabulate objective criteria that determine the reliability of e-signature technology. If these are adhered to, the e-signature will meet the law's requirement in respect of signature. First, subpara (a) refers to the objective characteristics of signature creation data (SCD). SCD in digital signatures based on PKI refers to the cryptographic key pair, while in ordinary e-signatures, it refers to codes, secret keys and the likes which are to provide a secure connection between an e-signature they create and the signatory.[120] An example is a finger print where biometric signature is employed.[121] It declares that the connection between the SCD and the signatory is crucial.[122] Thus, the SCD must be capable of identifying unmistakably one person, the signatory.[123] Subparagraph (b) refers to the use of the SCD stating that it should be capable of being used by one person at the time of signing,

[119] Para 116 of Guide to MLES op cit note 51.
[120] Para 97 of Guide to MLES op cit note 51.
[121] Para 97 of Guide to MLES op cit note 51.
[122] Para 121 of Guide to MLES op cit note 51. Among currently available e-signature technologies, the forms of e-signature technologies that may meet this element are usernames, passwords, PINS, electronic sound, typing a name into an e-document, email signature, digitized signature, a digital signature based on PKI and biometrics technology. But the other forms of e-signature are ultimatey excluded from coverage by the article as they donot meet other requirements of the article such as para (d). The digital signature based on PKI presumably meets these requirements. As reflected in chapter 2 above, it is also possible for the link between the e-signatures and the signatory to be interrupted.
[123] Para 121 of Guide to MLES op cit note 51.

and not by someone else as well.[124] Subpara (c) deals with the integrity of an e-signature to the extent that it is reliable enough to be accepted as a signature,[125] and subpara (d) deals with the integrity of the information signed electronically.[126]

It follows that article 6 of the MLES has a dual purpose: it establishes that legal effects will result from the application of an e-signature that meets the requirement of reliability; and, that no legal effects will flow from an e-signature of a lesser reliability.[127] The reliability of an e-signature may be established by proof that it meets the criteria in article 6 (3) or by proof in other ways as indicated by article 6 (4).

The MLES conceded that it needed to make a subtle distinction between e-signature technologies to differentiate their levels of technical reliability through the criteria it set in Article 6 (3).[128] It refers to the criteria as the concept of an 'enhanced electronic signature'.[129] For this reason, MLES creates 'a benefit in favour of certain techniques, which are recognised as particularly reliable, irrespective of the circumstances in which they are used.'[130] It thus extends the provisions of the MLEC by clarifying the kind of e-signature technologies that are legally recognised as valid functional equivalents of handwritten signatures even before their use.[131] Consequently, it inspires confidence and promotes certainty in e-commerce as users know which e-signature to use in 'legally significant transactions.'[132] At the same time article 6 (4) maintains the spirit of the MLEC of non-discrimination between e-signature technologies.[133]

[124] Para 122 of Guide to MLES op cit note 51.
[125] Para 124 of Guide to MLES op cit note 51.
[126] Para 125 of Guide to MLES op cit note 51.
[127] Para 118 of Guide to MLES op cit note 51; John D Gregory 'Legislating Trust' (2014) 12 *Canadian Journal of Law and Technology* 1 at 10.
[128] Para 118 of Guide to MLES op cit note 51.
[129] Para 118 of Guide to MLES op cit note 51.
[130] Para 118 of Guide to MLES op cit note 51; See part 2.8 above which illustrates that law favours some methods of paper based authentication, for example, notarised documents have more legal credibility and have better chances when tested in court.
[131] Paras 4 & 71 of Guide to MLES op cit note 51. This is differentfrom the MLEC where a trier of fact determines the reliability of an e-signature based on circumstances in which it was used, and the determination is made after signature use.
[132] Davidson op cit note 1 at 333; Para 4 of Guide to MLES op cit note 51.
[133] Para 118 of Guide to MLES op cit note 51.

4.4.4 Rules of conduct for parties involved in e-signing

The MLES focused on roles involved in a PKI system, namely the signatory,[134] relying party[135] and the certification function.[136] This was due to the seemingly predominant role played by public key cryptography in e-commerce, hence the need for guidance on its regulation.[137] It thus set flexible rules of conduct for parties involved with signature with the objective of shaping harmonious commercial practices.[138]

The MLES sets out duties of a signatory. It states that among others, a signatory has a duty to exercise reasonable care to protect their SCD from misuse.[139] They must also ensure that the contents of the certificate are correct.[140] If they know or suspect the signature data to be compromised, they must make reasonable efforts to notify persons who might rely on the signature.[141]

Additionally, the MLES sets out the conduct of a certification service provider (CSP).[142] It provides inter alia, that the CSP must follow its policies, give the relying party access to information as to the signatory's use and validity of the signature and must employ trustworthy systems and human resources.[143] The CSP and the signatory will be legally liable for failure to comply with the MLES requirements.[144]

Last, the relying party's duties include taking reasonable steps to confirm the reliability of an e-signature.[145] For instance, they should confirm the validity status of a certificate together with its limitations before its use.[146] Where they fail to take such reasonable steps, they will bear the legal consequences provided the observance of limitations of verification or validity was readily available.[147]

---

[134] Article 2 (d) of the MLES.
[135] Article 2 (f) defines a 'Relying party' as person that may act on the basis of a certificate or an electronic signature.
[136] Paras 20 & 32 of Guide to MLES op cit note 51; Mason *Electronic Signatures* op cit note 6 at 100.
[137] Para 14 & 20 of Guide to MLES op cit note 51.
[138] Para 4 of Guide to MLES op cit note 51; Mason *Electronic Signatures* op cit note 6 at 100.
[139] Article 8 (1) (a) of the MLES; See part 2.9.10.2.5 above.
[141] Article 8 (1) (b) of the MLES; See part 2.9.10.2.5 above.
[142] Article 2 (e) of the MLES defines a Certification Service Provider as a person that issues certificates and may provide other services related to electronic signatures.
[143] Article 9 (1) (a) – (f) & 10 of the MLES; See part 2.9.10.2.2 above; Para 61 of Guide to MLES.
[144] Articles 9 (2) & 8 (2) of the MLES; Para 146 of Guide to MLES op cit note 51.
[145] Article 11 (a) of the MLES.
[146] Para 148 of Guide to MLES op cit note 51.
[147] Article 11 of the MLES & Para 151 of Guide to MLES op cit note 51.

4.4.5 The hybrid approach of the MLES

The MLES adopts both the technology neutral approach and the technology specific approach in regulation of e-signatures. Specifically, article 3 on equal treatment of signature technologies consists of a principle that no e-signature technology should be discriminated against; all e-signature technologies must be given a chance to fulfil the requirements of Article 6.[148] The MLES notes that, although the PKI system requires a trusted third party to certify the identity of a signatory, such identity can be established by two parties alone, depending on the signing system used.[149] The MLES further insists that it has set rules that can be used beyond the PKI system as it predicts the interaction between two functions which are available in all e-signatures, namely, the creation of a signature and reliance on a signature.[150] The third function, certification of an e-signature, is only available in respect of certain types of signature,[151] but these include the digital signature based PKI system and other kinds of e-signature technologies,[152] implying that the MLES is technology neutral in nature.[153]

In addition however, the MLES creates reliability criteria that favour PKI technology (an enhanced electronic signature).[154] It concedes that the interplay between the signatory, certification authority and relying parties presupposes one possible PKI model.[155] It also acknowledges that techniques such as biometrics are not covered in the model law.[156] The MLES consequently facilitates recognition of digital signatures based on the PKI system and prefers it over other e-signature technologies.[157] This is a technology specific approach.[158] Nonetheless, its Art 6 (4) permits other methods to be used to satisfy the reliability of an e-

[148] Para 5, 107 & 14 of Guide to MLES op cit note 51; Seamus Keating 'Digital signatures and the electronic transfer of land' (2013) 7 *Masaryk University Journal of Law and Technology* 49 at 53-54.
[149] Mason *Electronic Signatures* op cit note 6 at 100.
[150] Para 28 of Guide to MLES op cit note 51.
[151] Para 28 of Guide to MLES op cit note 51.
[152] AO Orifowomo & JO Agbana JO 'Manual signature and electronic signature: significance of forging a functional equivalence in electronic transactions' (2013) 24 *International Company and Commercial Law Review* 357 at 363-4.
[153] Para 107 of Guide to MLES op cit note 51.
[154] Article 6 (3) of the MLES; Eiselen 'Fiddling with the ECT Act' op cit note 23 at 2810-2811; Para 118 of Guide to MLES op cit note 51.
[155] Para 32 of Guide to MLES op cit note 51.
[156] Mason *Electronic Signatures* op cit note 6 at 100.
[157] Jay Forder 'The inadequate legislative response to e-signatures' (2010) 26 *Computer Law & Security Review* 418 at 424.
[158] See part 3.3.3.2.1 above.

signature requirement without reference to the criteria it set in Art 6 (3).[159] Hence, the MLES attains a two tier approach of technology neutrality and technology specificity.

Like the MLEC, the MLES is a template for states to incorporate into their national laws.[160] As of July 2015, at least thirty two states had either based their law on the MLES or adopted it.[161] Subsequent to the MLES, the UN adopted a convention on e-communications.

4.5 United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC)

4.5.1 Purpose of the CUECIC

The UN adopted the CUECIC as prepared by UNCITRAL, in November 2005.[162] UNCITRAL developed CUECIC with the aim of removing obstacles to the use of e-communications in international contracts caused by international trade laws. Its purpose was to increase legal certainty and commercial predictability in international contracts.[163] CUECIC is aimed at removing the obstacles in a way that will be acceptable to states with different economic, social and legal systems.[164] Members of UNCITRAL called for a convention with the underlying belief that only a binding document would effectively remove such obstacles.[165] CUECIC is also based on the principles of functional equivalence and technology neutrality.[166]

4.5.2 CUECIC's test for signature in e-communications

Although CUECIC does not define an e-signature,[167] it lays down criteria for the legal recognition of a signature in e-communications.[168] The criteria set by CUECIC are different

[159] Forder op cit note 157 at 424.
[160] Para 26 of Guide to MLES op cit note 51.
[161] UNCITRAL 'Status: UNCITRAL Model Law on Electronic Signatures (2001)' available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html*, accessed on 16 October 2016.
[162] Para 1 of Explanatory note by UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts, 2006 (Explanatory note on CUECIC).
[163] Fourth paragraph of Preamble & Para 45 of Explanatory note on CUECIC ibid.
[164] Sixth paragraph of the Preamble.
[165] José Angelo Estrella Faria 'The United Nations Convention on the Use of Electronic Communications in International Contracts — An Introductory Note' (2006) 55 *International and Comparative Law Quarterly* 689-694 at 689.
[166] Fifth paragraph of Preamble to CUECIC.
[167] CUECIC uses the term 'electronic signature' to refer to electronic authentication techniques used as substitutes of handwritten signatures and traditional authentication procedures (See para 147 of Explanatory note on CUECIC op cit note 162).
[168] Chong Kah Wei & Joyce Chao Suling 'United Nations Convention on the use of Electronic Communications in International Contracts - A new global standard' (2006) 18 *SACLJ* 116 at 137 & 128.

from those set by the MLES, for CUECIC introduces another reliability test,[169] by reiterating and extending former MLEC provisions on e-signature. Article 9 (3) of CUECIC states that:

> 'Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
>
> *(a)* A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and
>
> *(b)* The method used is either:
>
> (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
>
> (ii) Proven in fact to have fulfilled the functions described in subparagraph *(a)* above, by itself or together with further evidence.'

It is noted that article 9 (3) (a) and (b) (i) reiterate the contents of article 7 of the MLEC. The wording of the two instruments is, nevertheless, slightly different in that the MLEC refers to a method used to indicate a signatory's 'approval' of content, while CUECIC refers to the signatory's 'intention' towards information.[170] UNCITRAL realised that it is not always that a signatory approves contents of information they sign. For example, a witness to a document does not approve of the contents of the documents, but merely indicates their identity and associates themselves with contents of the document they signed.

Secondly, CUECIC uses 'e-communication' instead of 'data messages' used by the two previous model laws.[171] The advantage is that CUECIC streamlines the language of the older Model laws to accommodate the influence of digital technologies.[172]

---

[169] Mason *Electronic Signatures* op cit note 6 at 111.

[170] Para 160 of Explanatory note on CUECIC op cit note 162.

[171] ' "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy' (See Articles 2 (a) of MLEC, Article 2 (c) of MLES & Article 4(c) of CUECIC). ' "Electronic communication" means any communication that the parties make by means of data messages' (Article 4 (b) of CUECIC). Thus '"Electronic communication" includes any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, made by electronic, magnetic, optical or similar means in connection with the formation or performance of a contract' (Para 5 of Explanatory note on CUECIC op cit note 162); Wei et al op cit note 168 at 136.

[172] Paul Przemyslaw Polanski Paper 20 (BLED 2006 Proceedings) *Convention on E-Contracting: The Rise of International Law of Electronic Commerce?* (2006) *http://aisel.aisnet.org/bled2006/20* at 8.

Article 9 (3) (b) above indicates that the reliability of an e-signature can be determined in two different ways. That is reliability in principle (article 9 (3) (b) (i)) or reliability in fact (article 9 (3) (b) (ii)).[173]

With reliability in principle, CUECIC reiterates the MLEC's standard of security expected of an e-signature method. It creates an elastic approach to the security levels to be reached by the method that identifies and shows the intent of the signatory. That is, the method should be reliable as is appropriate for the purposes for which the e-communication is made.[174] Similar to the MLEC, CUECIC does not explain the reliability standard it calls for. As a result, this study adopts its interpretation of the reliability standard of the MLEC as set out in part 4.3.3 above.

Further, CUECIC reiterates the legal, technical and commercial factors that should be considered to determine the 'appropriateness' of the method used to sign e-communication as set out by the MLEC.[175] Thus like the MLEC, CUECIC shows that the level of security of a method used to sign is a relative notion, it is not in all cases that maximum security is required.[176]

CUECIC's adoption of the reliability in principle standard in article 9 (3) (b) (i)[177] reflects its desire to maintain a functional equivalence approach with respect to e-signatures.[178] It reminds the courts in the event of a dispute that there are other important factors apart from technology that can be used to determine whether an e-signature adequately identified a signatory as required by Article 9 (3) (a).[179] An example is the purpose for which the transaction was made.[180] UNCITRAL states that failure to raise this issue might lead states to the belief that only high level security technologies are adequate to identify a signatory despite parties' agreement to use simpler signature technologies.[181]

Alternatively, article 9 (3)(b)(ii) on reliability in fact validates any method of signing despite its reliability in principle. This is provided the method is factually proven to have identified the signatory and indicated their intention with respect to the information in the e-

[173] Chris Connolly & Prashanti Ravindra 'International eCommerce regulation: First UN Convention on eCommerce finalised' (2006) 22 *Computer Law & Security Report* 31 at 36.
[174] Para 161 of Explanatory note on CUECIC op cit note 162.
[175] See Para 162 of Explanatory note on CUECIC op cit note 162 which is similar to Para 58 of Guide to MLEC op cit note 12; see also part 4.3.3 above.
[176] Thomas J Smedinghoff 'Challenges to privacy, integrity, and security in a borderless world: it's all about trust: the expanding scope of security obligations in global privacy and e-transactions law' (2007) 16 *Michigan State Journal of International Law* 1 at 31.
[177] Which is similar to article 7(1) (b) of the MLEC.
[178] Para 163 of Explanatory note on CUECIC op cit note 162.
[179] Para 163 of Explanatory note on CUECIC op cit note 162.
[180] Smedinghoff 'Challenges to privacy' op cit note 176 at 31.
[181] Para 163 of Explanatory note on CUECIC op cit note 162.

communication.[182] Through this article, UNCITRAL indicates that parties should not be allowed to misuse the reliability test set by the Convention to deny the validity of their signature. That is, a party or court should not be allowed to allege that a signature was not 'as reliable as appropriate' in instances where the party's identity and intention in respect of the content of information is verifiable or there is no dispute as to the authenticity of the e-signature.[183] CUECIC guards against such possibilities.

Although CUECIC makes no provision for rules on admissibility of evidence, both electronic and non-electronic evidence will assist to proving that a method used to sign meets the reliability requirements of signature. Hence the MLEC's rules on admissibility and evidential weight of evidence will be applicable.[184]

In summary, according to CUECIC a requirement for signature is met by an e-signature on two occasions: first if it is used to identify a party, show their intent towards e-communication and its reliability is proven. Secondly if there is proof that it identifies a party and shows their intent without proving its reliability.[185]

4.5.3 Criticisms of CUECIC on signatures

At least six limitations of the convention have been identified. First, there is a fear that international harmonised laws are not uniform since each state interprets the instruments as it deems fit.[186] However, the success of the United Nations Convention on Contracts for the International Sale of Goods, 1980 (CISG) shows that with the presence of several aids that assist in the reliable interpretation and application of the international instrument, uniformity in application is possible. These include an instrument's articles consisting of definitions, general interpretation clauses, and states' collection and distribution of proper information pertaining to the legislative history of an instrument called the *travaux préparatoires*.[187] Courts are also expected to consider foreign court decisions on application of a convention,

[182] Para 164 of Explanatory note on CUECIC op cit note 162.
[183] Para 164 of Explanatory note on CUECIC op cit note 162. This emphasises that an e-signature is a legal notion of signature which sometimes, not always, serves to safeguard the integrity of a document in e-communication (see part 2.9 above).
[184] Article 9 of the MLEC.
[185] Wei et al op cit note 168 at 130.
[186] Rosett A 'Critical Reflections on the United Nations Convention on Contracts for the International Sale of Goods' (1984) *Ohio State LJ* 265.
[187] Eiselen S 'The UNECIC' at 15; Ingeborg Schwenzer (ed) *Schlechtriem & Schwenzer Commentary on the UN Convention on the International Sale of Goods (CISG)* 4 ed (2016) Art 7 paras 7 - 26.

even though not binding.[188] Hence CUECIC as an international harmonised law can maintain uniform application if states resort to the above listed aids in its interpretation.

Additionally, CUECIC provides that in the interpretation of the Convention regard must be had to principles of good faith, internationality and uniformity.[189] Any questions regarding e-communications that fall within the scope of the Convention but are not expressly provided for should be settled in conformity with the general principles on which it is based.[190] These include functional equivalence and technology neutrality specified in the Preamble.[191] Thus the Convention is autonomous in nature in that it can be interpreted through its own principles and not national rules.[192] This will consequently reinforce CUECIC's uniform application.

Nevertheless, Polanski raises a second criticism against CUECIC. He contends that CUECIC's autonomous nature is negatively affected as it does not consider significant principles and values of the Internet community.[193] Contrary to these, however, research has distinguished Internet community principles underpinning CUECIC. These consist of harmonisation, trade facilitation,[194] legal certainty and commercial predictability,[195] freedom of contract,[196] freedom of form,[197] good faith,[198] protection of reasonable reliance[199] and physical location of the parties.[200]

Thirdly, detractors of CUECIC allege that it fails to recognise binding trade usages similar to those in article 9 of the CISG.[201] Thus it is profoundly flawed for failure to recognise important norms of e-commerce.[202] Article 9 of the CISG states that parties to a contract are bound by trade usages they agree to between themselves, and are considered to

[188] Schlechtriem Peter 'Recent Developments in International Sales Law' (1983) 18 *Israel Law Review* 309 at 325-326; See also Case law: Italy *Agricultural products case* at 8 available at *http://cisgw3.law.pace.edu/cases/040225i3.html*, accessed on 21 August 2015.
[189] Article 5 (1) of CUECIC.
[190] Article 5 (2) of CUECIC.
[191] Paul Przemyslaw Polanski *Customary Law of the Internet: In search for a supranational cyberspace law* (2007) 61. Article 5 (2) further provides that it is only in the absence of the principles that resort can be had to the law applicable by virtue of the rules of private international law (law of a given national state).
[192] Polanski 'Convention on E-Contracting' op cit note 172 at 8; Juana Coetzee 'The Convention on the Use of Electronic Communications in International Contracts: Creating An International Legal Framework for Electronic Contracting' (2006) 18 *SA Merc LJ* 245 at 248.
[193] Polanski 'Convention on E-contracting' op cit note 172 at 8.
[194] See para 3 & 4 of the Preamble to CUECIC; Article 8 (1) of CUECIC.
[195] Para 3 & 4 of the *Preamble* to CUECIC.
[196] Article 3 of CUECIC.
[197] Article 9 of CUECIC.
[198] Article 5 of CUECIC.
[199] Articles 6 (1)-(2) & 9 (2)-(3) of CUECIC.
[200] Eiselen 'The UNECIC' op cit note 56 at 17 - 25.
[201] Polanski 'Convention on E-contracting' op cit note 172 at 8.
[202] Polanski 'Convention on E-contracting' op cit note 172 at 8.

have impliedly accepted application of widely known trade usages to their contract.[203] Bianca and Bonell's *Commentary on the International Sales Law* defines the concept of 'usage' as 'any practice or line of conduct regularly observed within a particular trade sector or at a particular market place.'[204] The critics postulate that the result of the Convention's flaw will negatively affect the flexibility of the Convention's norms.[205]

Notwithstanding this criticism, upon closer look, the Convention does, in fact, recognise trade usage. It makes a list of factors to be considered when analysing the appropriateness of a method of signature required by its article 9 (3) (a). Amongst these is 'compliance with trade customs and practice'.[206] 'Custom' on the one hand is 'a habitual or usual practice; usage of a community; an established usage which by long continuance has acquired the force of law or right … especially usage of a particular trade'.[207] 'Practice', on the other hand, is the essence of custom. It should be widespread, exercised for a long time, generally accepted as law and consistently applied.[208] Consequently, it seems that the terms 'usage' and 'trade customs and practice' mean the same thing. They both refer to established, recognised practices in a certain type of trade. Bonell validates this where he states that the distinction between 'custom' and 'trade usage' is irrelevant for purposes of article 9 of the CISG.[209] Arguably therefore, the Convention does recognise trade usages in its application in e-commerce.

It is conceded however, that CUECIC has contradictory provisions regarding the applicability of the *lex mercatoria* (also referred to as trade usage) under its scope.[210] *Lex mercatoria* is defined as a body of customary rules developed by the trade community independent of state laws, which may complement formal laws, to aid international trade.[211]

---

[203] Article 9 (1) & (2) of the CISG.

[204] Michael Joachim Bonell 'Article 9' in Bianca-Bonell *Commentary on the International Sales Law* (1987) 103 at 111 & 108 available at *http://www.cisg.law.pace.edu/cisg/biblio/bonell-bb9.html*, accessed on 20 August 2015.

[205] Polanski *Customary law of the internet* op cit note 191 at 62.

[206] Para 162 (i) of the Explanatory note on CUECIC op cit note 162.

[207] Polanski *Customary Law of the internet* op cit note 191 at 9.

[208] Polanski *Customary Law of the internet* op cit note 191 at 151-158; TUC Work smart 'What is meant by custom and practice?' 2015 available on *https://worksmart.org.uk/work-rights/pay-and-contracts/contract-terminology/what-meant-custom-and-practice*, accessed on 21 August 2015; Lesley Furber 'Custom and practice, and employment contract terms (implied and express terms)' 21 October 2011 available at *https://www.crunch.co.uk/blog/small-business-advice/2011/10/21/custom-and-practice-and-employment-contract-terms/*, accessed on 21 August 2015.

[209] Bonell op cit note 204 at 111.

[210] Charles H Martin 'The UNCITRAL electronic contracts convention: will it be used or avoided?' (2006) 17 *Pace Int'l L Rev* 261 at 503.

[211] Ana Mercedes López Rodríguez 'Lex Mercatoria' University of Aarhus available at *http://law.au.dk/fileadmin/site_files/filer_jura/dokumenter/forskning/rettid/artikler/20020046.pdf*, accessed on 19 August 2015; Polanski *Customary law of the internet* op cit note 191 at 1-2.

Although the Convention includes 'compliance with trade customs and practice' among factors that determine the appropriateness of a signature method, it explains that reference to 'the law' in its article 9 excludes laws that have not become part of a state like the *lex mercatoria.*[212] This contradiction should be resolved as the *lex mercatoria* may be advantageous to online transactions. Customary Internet contract law has prospective advantages such as its flexibility as a source of Internet norms, speed at reflecting changes in practice of participants, knowledge and acceptance by users, the capacity to supersede outmoded legislative norms and, to assist interpret and fill in gaps in legislation. It might further help to harmonize varying national legislation where there is no relevant international convention.[213]

Fourth, opponents of CUECIC allege that most of its provisions are of a general nature, so they will be difficult to apply in practice since they may lead to more legal ambiguity than certainty.[214] Conversely, the purpose of the general provisions is to respect party autonomy in contracts.[215] Thus, the generality aspect is an advantage of the instrument.

Fifth, CUECIC excludes online financial transactions from its scope of application.[216] This is a weakness of CUECIC as Internet mediated investments and Internet banking are used extensively and thus necessitate uniform international rules.[217]

Lastly, Forder points out that different forms of signature methods may meet CUECIC's reliability requirement but the nature of evidence required to prove their reliability is unclear. Reliability levels of e-signatures differ based on the purpose of signature in each case and may be proved through different forms of factual evidence. This implies that clarification of which factual evidence is necessary to prove reliability will be developed through case law, a process which is time consuming and thus unsatisfactory.[218]

Nonetheless, the challenges Forder raised are not unique to proof of the reliability of an e-signature under CUECIC. The same challenges and procedures equally occur regarding the proof of signature in the offline world.[219] As reflected earlier, the principle of equivalence maintains that the same norms that apply offline should apply online; the norms should not be

[212] Para 127 of Explanatory note on CUECIC op cit note 162.
[213] Polanski *Customary law of the internet* op cit note 191 at 1-4.
[214] Polanski 'Convention on E-contracting' op cit note 172 at 1 & 7.
[215] Coetzee 'The Convention on the Use of Electronic Communications' op cit note 192 at 255.
[216] Polanski 'Convention on E-Contracting' op cit note 172 at 4.
[217] Paul Przemyslaw Polanski 'International electronic contracting in the newest UN Convention' (2007) 2 *Journal of International Commercial Law and Technology* 112 at 118; Polanski *Customary Law of the Internet* op cit note 191 at 62.
[218] Forder op cit note 157 at 426.
[219] See para 49 of Explanatory Note to CUECIC.

stricter or less strict for the online world.[220] Thus CUECIC upholds the principle by treating e-signature no differently from how offline rules treat the traditional signature.[221]

Despite many criticisms, CUECIC entered into force on 1 March 2013.[222] It currently has 18 signatories and seven parties.[223]

4.6 Analysis of UNCITRAL model laws and CUECIC

Despite its shortcomings, CUECIC is an improvement on the MLEC and MLES.[224] When one compares it to the MLEC, CUECIC increases the chances of using accessible e-signature technologies as long as factual evidence can be produced to prove that the method used identifies and shows the signatory's intent.[225] It thus facilitates admission of an e-signature without the need to prove its authenticity and integrity if the latter are not disputed. This provision on reliability of fact was not included in the MLEC. Put differently, by adding onto the MLEC-based signature requirements, CUECIC increased cost effectiveness.[226] It thus fulfils the requirement that functional equivalence rules should be practicable.[227] It also enhances technology neutrality by allowing the use of the same kind of evidence to prove handwritten signatures, to authenticate signature in e-communications.[228]

Again, as previously discussed CUECIC's criterion that a method of signature must reflect a signer's intent regarding information rather than their approval facilitates document authentication procedures online.[229] Thus parties may use an ordinary e-signature coupled with other online authentication methods as functional equivalents of paper based authentication procedures.[230]

When one compares CUECIC to the MLES, CUECIC appears to be more technology neutral. CUECIC embraces authentication technologies without preference to PKI technology

[220] See part 2.2 above.
[221] See part 3.2 above.
[222] Guillermo Coronado Aguilar & Jose Luis Barba Ortega 'United Nations Convention on the Use of Electronic Communications in International Contracts (E-CC)' (2014) 18 *Vindobona Journal of International Commercial Law & Arbitration* 41.
[223] See UNCITRAL 'Status United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)' available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html*, accessed on 16 October 2016.
[224] Wei et al op cit note 168 at 130.
[225] Eiselen 'Fiddling with the ECT Act' op cit note 23 at 2812; Lee Swales 'The Regulation of electronic signatures: Time for Review and Amendment' (2015) 132 *SALJ* 257 at 269.
[226] Martin 'The UNCITRAL electronic contracts convention' op cit note 210 at 287.
[227] See part 3.2.3.2 above.
[228] Martin 'The UNCITRAL electronic contracts convention' op cit note 210 at 287; see part 3.3.3.1.2 above.
[229] See part 4.5.2 above.
[230] See parts 2.8 & 2.9.11 above.

as is done by the MLES.[231] As discussed earlier, digital signature based on PKI is difficult to set up, its acquisition involves cumbersome, costly processes, it imposes a large burden on the online user,[232] and thus its use is less feasible in practice. But CUECIC permits use of less sophisticated authentication technology such as typed names, digitized signatures, usernames and passwords which work well and are easily accessible to the online user in practice.[233] It thus provides clear, sensible and practical solutions to legal questions and any legal uncertainties that arise where e-communications are used in e-commerce.[234]

Further, upon one's application of the new criteria set by CUECIC, it is no longer necessary to determine whether an authentication method falls within the definition of an e-signature. This caters for future authentication technologies which might fall between e-signatures and non-electronic signatures.[235] Thus CUECIC is both innovative and futuristic. The change of wording from data messages to e-communications is also indicative of this. These are attributes of a technology neutral law.[236]

It follows that in the advent of technology convergence,[237] technologies that fall under broadcasting or telecommunications may fulfil the law's requirement of signature if they meet the standards set by CUECIC.[238] For instance, a video, audiotape or online representation can meet the law's requirement of signature in a will.[239] The technology neutrality principle which connotes that the law should not discriminate between technologies that can perform the same function supports this view.[240]

However, technology convergence calls for legal convergence.[241] The technologies are to be regulated under one umbrella to work together. This is to ensure the regulation of communication technology standards such as user control, privacy and access.[242] South Africa's Electronic Communications Act[243] is an example of a statute that means to regulate

[231] See para 155 of Explanatory Note on CUECIC op cit note 162; Martin 'The UNCITRAL electronic contracts convention' op cit note 210 at 288.
[232] See part 2.9.10.2.6 above.
[233] Polanski *Customary Law of the Internet* op cit note 191 at 28.
[234] Faria 'The United Nations Convention' op cit note 165 at 690; Eiselen 'The UNECIC' op cit note 56 at 2; Alba op cit note 69 at 389.
[235] Wei et al op cit note 168 at 166.
[236] See parts 3.3.3.2.2 & 3.3.3.3.1 above.
[237] See part 3.3.3.2.1 above.
[238] See Part 4.5.2 above.
[239] Katherine Melnychuk 'One Click Away: The Prospect of Electronic Wills in Saskatchewan' (2014) 77 *Saskatchewan Law Review* 27; James W Martin 'I Want To Sign An Electronic Will' (2009) *The Practical Lawyer* 61 at 63.
[240] See part 3.3.3.2.1 above.
[241] Van der Merwe et al *Information* op cit note 95 at 7.
[242] Van der Merwe et al *Information* Ibid 8.
[243] No 36 of 2005.

the broadcasting, telecommunications and computing sectors under a single umbrella. Thus, it is advisable that a state that wishes to legally recognise technologies from the other two sectors as authentication technologies, should develop umbrella legislation that will regulate their use. But, more research will be necessary towards this end.

In addition,

> '[t]he CUECIC test of reliable identification of the signer and of their intention in respect of the electronic communication might permit proof of intent to sign through the objective record of performance of an identification method, rather than requiring proof of subjective intent.'[244]

This can be proved by evidence of facts on the functions that the signature method performed in order to avoid allegations that a method was not reliable as appropriate.

Although CUECIC applies to international contracts,[245] it is noted that there is nothing stopping it from applying also to domestic contracts.[246] It is advisable that it should also apply to domestic transactions to avoid duality of systems when transacting internationally and or domestically.[247] This will improve efficiency.

It follows that legislative instruments which adopt the principles of the MLEC further complemented by CUECIC are likely to be more effective in their application. Since their e-signature provisions will be practicable to the user, they will be both meaningful and observed.[248] The instruments will remain stable over time as they will not rely on specific technologies that may change quickly, resulting in confusion on the part of the user.[249] Consequently the legal instruments will address the concerns of users in e-signature use. That is, e-commerce users will be able to securely sign their transactions practicably. They will bring certainty and confidence in use of e-signature, and achieve their aim of promoting the use of e-signatures and facilitating e-commerce.[250]

Apart from UNCITRAL, the ICC took an initiative to facilitate authentication in e-commerce.

[244] Martin 'The UNCITRAL electronic contracts convention' op cit note 210 at 288.
[245] Article 1 of CUECIC.
[246] Wei et al op cit note 168 at 134.
[247] Wei et al op cit note 168 at 134
[248] See part 3.4.1.1 above.
[249] See part 3.4.1.2 above.
[250] See part 3.4 above.

4.7 The ICC's General Usage for International Digitally Ensured Commerce guidelines (GUIDEC)

The ICC is an organisation of practitioners, corporations and professionals established in 1919.[251] Its objectives comprise the promotion of trade and investment, and the opening of markets and services.[252] It deals with a plethora of issues relating to the betterment of trade, and presents views to national governments worldwide and to the United Nations.[253] It thus forms rules that oversee business conduct at an international level and offers other services to the international business community.[254]

In 1997, the ICC produced a set of non-binding guidelines relating to e-commerce called the General Usage for International Digitally Ensured Commerce (GUIDEC).[255] GUIDEC introduces elements involved in the concept of e-commerce with the aim of assisting the world business community to understand issues regarding e-commerce.[256] It also addresses terminology by using the term 'ensure'[257] to refer to a 'digital signature'[258] or 'authentication'[259] in an effort to indicate that 'electronically signed messages… are not signed physically, but require the intervention of an electronic medium.'[260]

The ICC revised the 1997 guidelines in 2001, resulting in GUIDEC II. GUIDEC II regulates the utilisation of public key cryptography in digital signatures, the role of a trusted third party namely, the certification service provider, and the allocation of risk and liability between the contracting parties.[261] Nonetheless, it states that its principles apply to other technologies outside the digital signature as well.[262]

GUIDEC II further provides for authentication of digital messages.[263] It sets out best practices for the authentication of a message which may be adopted upon formation of an e-transaction.[264] The ICC's objective is to reduce risks of fraud or unauthorised access to

[251] Davidson op cit note 1 at 340 - 341.
[252] Davidson op cit note 1 at 340.
[253] Davidson op cit note 1 at 341.
[254] Davidson op cit note 1 at 341.
[255] Davidson op cit note 1 at 341.
[256] Scope and objectives GUIDEC 18 November 1997 available at *http://www.iccwbo.org/guidec2.htm*, accessed on 15 July 2015.
[257] It defines 'ensure' under its Glossary of terms as '[t]o record or adopt a digital seal or symbol associated with a message, with the present intention of identifying oneself with the message.'
[258] Part VI of GUIDEC.
[259] Authenticate is 'often used to denote the act of identifying oneself with a message' (Part XI of GUIDEC).
[260] GUIDEC Preface; Mason *Electronic Signatures* op cit note 6 at 107.
[261] Davidson op cit note 1 at 341; Aim of the GUIDEC II.
[262] Aim of the GUIDEC II.
[263] Part I (1) Objective of the GUIDEC.
[264] Part IX of GUIDEC II.

messages and so enhance legal predictability.[265] The best practices it tabulates are, however, centered on digital signatures.[266] Some scholars note that it is unusual for one of GUIDEC's best practices to require a person who signs a message to authenticate it when communicating online. This is because a party transacting offline through telegrams or post for instance, was not requested to authenticate a message.[267] This implies a failure to treat online users equally to offline users contrary to the functional equivalence principle.

Part X of GUIDEC II deals with the effect of a certificate in the use of digital signatures. It states that a party may rely on a valid certificate as presenting correct facts set out in it provided he/she had no notice that the certificate issuing party failed to follow authentication procedures.[268] The commentary to the Part makes a presumption that 'the parties are acting in good faith and without deception or negligence in conducting their business.' Nevertheless, Mason contends that this Part undermines the objective of implementing GUIDEC.[269] He contends that if the parties know and trust each other, and are familiar with communication between them, the need for a digital signature and implementation of the GUIDEC falls away.[270] He further states that parties might as well go back to reliance of any e-signature technology such as an email address and its contents to prove the authenticity of the communication.[271] This argument reflects the need to go back to a technology neutral approach for the regulation of a signature in e-communication.

4.8 Conclusion

To sum up, when the MLEC adopted functional equivalence and technology neutrality principles,[272] it noted that an electronic record provides security similar to that of paper documents, but provides more reliability as to identification of the source and content of data than does paper. It noted further the hierarchy of form requirements in paper documents and their differing levels of reliability, inalterability and traceability. It paid attention to the several kinds of signature in paper based documents, their numerous functions and their different levels of certainty. However, the MLEC realised that making a functional equivalent

[265] Part I (1) & Part III of GUIDEC.
[266] Part IX of GUIDEC II.

[268] Part X (1) of GUIDEC II.
[269] Mason *Electronic Signatures* op cit note 6 at 110.
[270] Mason *Electronic Signatures* op cit note 6 at 110.
[271] Mason *Electronic Signatures* op cit note 6 at 110.
[272] Tana Pistorius 'Contract formation: a comparative perspective on the Model Law on Electronic Commerce' (2002) XXXV *CILSA* 129 at 135.

of all types of signature might lead to the preference of a particular technology, which will be technology specific, and thus undesirable. It noted further that the application of functional equivalence should not result in the imposition of stricter standards of security and high costs for computer based documents.

UNCITRAL subsequently identified two fundamental functions of paper based signatures that will give comprehensive credibility to the authentication of a data message, namely identification and authentication. It then adopted a flexible level of security for a method of authentication – that it should be as reliable as appropriate considering the circumstances, which indicates a number of factors. For example, it shows that the reliability levels of e-signatures differ depending on time and purpose of differing transactions; it guards against undetected manipulation or malpractices to which e-signatures are susceptible and may have the reliability proved by evidence. Hence the level of e-signature security reflects the MLEC's non-discriminative nature towards authentication methods, present and future. The MLEC thus avoids the danger of being technologically outdated.[273] Consequently, the MLEC leads to equal treatment of offline users and online users in fulfilment of signature requirements on contract formation.

The MLES on the other hand adopted a hybrid approach in respect of technology neutrality and technology specificity. There is a risk that states which adopt it in their legislation will face a number of disadvantages. For instance, their legislation may be based on a favoured technology which fits the MLES' reliability criteria in art 6(3), yet the technology may either be difficult to comply with or soon become outdated, thus the legislation will become ineffective and ignored by users.[274]

CUECIC took significant strides to eliminate obstacles imposed by former international instruments on e-signature regulation. For example, the preferred use of PKI technology set by the MLES has been replaced with signature by any method that can be proved to identify a signatory and their intention towards e-communication. CUECIC thus promotes equal treatment of online users to offline users more effectively than the former Model Laws. It has been acknowledged that '[t]he new Convention is certainly the most important international development in the field of Internet law, which can bring more predictability to global electronic trade.'[275] It is currently the latest legal instrument developed by UNCITRAL on e-signatures in e-commerce. The rules contained in it are

[273] Swales op cit note 225 at 268.
[274] Swales op cit note 225 at 261.
[275] Polanski 'Convention on E-contracting' op cit note 172 at 8.

expected to supersede legislations based on the MLEC and MLES. [276] As a result, it is submitted that CUECIC is the preferred international model for states to adopt for adequate e-signature regulation.

Guidelines proposed by the ICC on the other hand are based on digital signature technology and technology specific in nature. Shortcomings of GUIDEC II have been identified which weaken the purpose of the guideline. For this reason and their lack of legal effect, GUIDEC will not be considered further in this research.

Having established that CUECIC proposes a better model for regulation of e-signatures, the next chapter considers whether the Lesotho and Southern African Development Community (SADC) e-signature legal instruments adequately observed the ICT principles and whether their e-signature provisions will lead to effective regulation. It also looks into how other jurisdictions such as South Africa, USA and the EU deal with e-signature regulation to see if SADC and Lesotho can learn any lessons from them.

[276] Wei et al op cit note 168 at 117 & 119.

CHAPTER FIVE: ASSESSMENT OF THE ADEQUACY OF LESOTHO AND SADC INSTRUMENTS ON E-SIGNATURE REGULATION WITH REFLECTIONS FROM SOUTH AFRICA, EU AND USA

5.1 Introduction

The objective of this chapter is to assess the extent to which the proposed legal instruments of Lesotho on e-commerce[1] together with the draft Southern African Development Community (SADC) Model Law on Electronic transactions and Electronic commerce (SADC ML)[2] align with the concepts of functional equivalence, technology neutrality and effectiveness with specific reference to e-signatures. The central argument of this study is that the Lesotho Bill and SADC ML's mandatory use of a Secure e-signature (SeS) does not treat online and offline signature users equivalently; is not practicable; discriminates against ordinary e-signatures; is unsustainable and is out of step with the latest instrument of the United Nations Commission on International Trade Law (UNCITRAL), namely the Convention on the Use of Electronic Communications in International Contracts (CUECIC), thus will not effectively promote the use of e-signature. It argues that any e-signature technology that meets CUECIC's criteria of functional equivalence and technology neutrality will reliably address users' concerns on e-signature and promote confidence in its use. The assessment will therefore investigate the extent to which the legal instruments are potentially effective.

To achieve its objective the chapter first sets out three inquiries to be investigated and the principles that will help determine the answers. It then discusses the origin of the SADC ML and introduces the legal system of Lesotho on e-signature regulation. Subsequently, it assesses the provisions of the Lesotho Bill, the draft Lesotho Digital Signature Regulations[3] and SADC ML and inquires as to their technology neutrality, functional equivalence and potential effectiveness. At the same time, the chapter examines South Africa's e-signature regulation with relation to these concepts and whether it has been effective in practice. South Africa is selected for this study because it has the most comprehensive and advanced

[1] Lesotho Electronic Transactions & Electronic Commerce Bill 2013 (The Lesotho Bill) and the Draft Lesotho digital signatures regulation. Regulations presented at Lesotho in-Country Transposition of the SADC Cybersecurity Model laws (2nd mission) (2 - 5 April 2013) Maseru Lesotho available at *http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/in-country-assistance/Lesotho.aspx*, accessed on 19 March 2015.

[2] Harmonization of ICT Policies in Sub-Saharan Africa 'Electronic Transactions & Electronic Commerce: SADC Model Law' ITU 2013.

[3] See note 1 above.

legislation on e-commerce in the SADC region. Again, South African law is highly persuasive in Lesotho as the two states apply a similar contract legal system. Further, it will be reflected in due course that the South African law resembles the Lesotho Bill in some respects.

In addition, the chapter examines e-signature regulation in the European Union (EU) and the United States of America (USA) for a number of reasons. First, although the EU is different from SADC due to its use of a single Euro currency in at least nineteen of its twenty eight members states[4] and has an open border policy to encourage a single market trade[5], SADC is a regional body, much like the EU.[6] The two regional bodies have created regional instruments that have the same goal, namely to improve confidence of Internet users in e-commerce and harmonise e-commerce amongst their member states.[7]

Secondly, it is noted that the EU and USA differ in economic status with the SADC region, but the majority of their member states are members of the United Nations.[8] Recognising the disparity in economic status of its member states, the UN created UNCITRAL whose membership is representative of the world's various geographic regions and its principal economic and legal systems. UNCITRAL thus develops legal instruments meant to apply across board despite differing economies and legal systems. All three regions adopted UNCITRAL instruments to harmonise their laws on e-commerce, hence their application of the instruments is comparable despite their different economic status.

Thirdly, the EU and USA are both mature legal systems on e-commerce regulation,[9] but apply different approaches in regulation of e-signatures. The EU adopted a hybrid approach of both technology neutral and technology specific regulations for e-signatures while the USA adopted the technology neutrality approach. Therefore, a study of their

[4] European Union 'The Euro' available at *europa.eu*, accessed on 28 April 2017.
[5] European Commission 'Internal market, Industry, entrepreneurship and SMEs' available at *ec.europa.eu*, accessed on 01 May 2017.
[6] The EU is an economic and political union of twenty eight scattered countries, with separate cultures and legal systems, while the USA is a federation with a single legal system, common economic market and same culture across its states and with the same currency (Liane Colonna *Legal implications of data mining* (2016) Tallinna Raamatutrükikoda, Tallinna 219).
[7] See EUROPA 'Legal Aspects of electronic commerce' available on *europa.eu/legislation_summaries/information_society/other_policies/124204_en.htm,* accessed on the 22 June 2013; Preamble of SADC Model Law.
[8] Currently the UN has membership of fourteen SADC member states, the USA, and 27 EU member states (United Nations available at *http://www.un.org/en/member-states/*, accessed on 28 March 2017).
[9] EU adopted e-signature regulation instruments in 1999 while the USA adopted e-signature regulation instruments in 1999 and 2001.

different approaches will provide valuable lessons on which is the most effective approach for e-signatures regulation in Lesotho and the SADC region.[10]

Fourthly, the EU and USA are some of SADC's main trading partners.[11] Hence placing e-commerce instruments of Lesotho and SADC at an international level will enhance trade between the regions, which is in line with objectives of UNCITRAL and Lesotho's ICT Policy.[12] The chapter examines the EU, USA and South African legal systems in order to gain knowledge from their experiences and where possible, recommend that Lesotho and SADC member states avoid shortcomings identified by the study. The three inquiries made by this study are elaborated on below.

5.2 Inquiries on e-signature regulation

Three primary enquiries emerge from an assessment of Lesotho's e-signature regulation and the SADC ML. On the technology neutrality principle, the main inquiry is: to what extent are the SeS provisions technology neutral? Presumptions that inform this analysis include the following. First, a rule should not discriminate among the numerous techniques that may be used to generate, communicate or store information.[13] Second, a technology neutral rule promotes equal legal treatment of both computer based users and paper based users.[14] Regulation achieves this by controlling the effects of peoples' behaviour, not the means they use to achieve the effects.[15] Third, technology neutral legislation should be able to withstand and incorporate technology changes, hence be sustainable.[16]

Under the functional equivalence principle, the primary enquiry is: to what extent is the SeS in the Lesotho legislature and SADC ML a functional equivalent of a handwritten signature? Presumptions that inform the analysis are the following. First, CUECIC set the

[10] See Maurice Schellenkens 'What holds off-line, also holds on-line' in Bert-Jaap Koops, Miriam Lips, Corien Prins and Maurice Schellenkens (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One-Liners* (2006) 54; Reed *Making Laws for Cyberspace* (2012) 110 & 137.

[11] See for example, the African Growth and Opportunity Act 2000 (AGOA) agreement with the USA and Economic Partnership Agreement (EPA) of 2014 with the EU.

[12] 'ICT Policy for Lesotho: Policy Measures, Instruments and Initiatives' available at *http://research.businessonlybusiness.com/matrix.php?Electronic%20transactions%20of%20Lesotho* accessed on 04 June 2013.

[13] See part 3.3.3.2.1 above; para 5 of Guide to Enactment of the UNCITRAL Model law on Electronic Signatures 2001 (Guide to MLES); para 155 of the Explanatory note by the UNCITRAL secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts 2005 (Explanatory Note on CUECIC).

[14] See part 3.3.3.1.2 above; See also para 6 of Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce 1996 (Guide to MLEC); part 4.3.2.2 above.

[15] Sec part 3.3.3.1.1 above.

[16] See part 3.3.3.3.1; para 48 of Explanatory note on CUECIC; para 24 of Guide to MLEC; para 82 of Guide to MLES.

criteria that will enable an authentication technology to qualify as a functional equivalent of a handwritten signature where the law requires a signature. It states that a method should be used that can identify a party and indicate the party's intention with respect to information in the e-communication; the method used should be as reliable as appropriate for the purpose of the e-communication in the circumstances; alternatively, the method should be proved to identify a party and their intention, with the use of factual evidence where necessary.[17]

Secondly, states' application of the functional equivalence approach should not result in imposing on online users stricter standards of security and related costs than those found in a paper based sphere.[18] The obligations that online and offline rules impose on their subjects should be approximately equivalent in burden. Hence an online rule must be practicable, failing which, it will not be functionally equivalent.[19] It is noted that an e-record can provide a similar level of security to paper with respect to paper functions, and is more reliable in identifying a source and content of data provided it meets certain technical and legal requirements.[20] If the Lesotho Bill and SADC ML's provisions on SeS and e-signature meet these presumptions then they provide functional equivalents of the handwritten signature.

The last inquiry regarding effective law is whether the Lesotho Bill and SADC ML have the potential to achieve their social aim having prescribed the use of a SeS. The following presumptions help gauge the effectiveness of the instruments: an effective rule is understandable by its subjects,[21] is stable over time,[22] and attracts and maintains participants who actively take part in its use.[23]

The chapter further analyses the Lesotho Bill and SADC ML's ordinary e-signature provisions on technology neutrality, functional equivalence and effectiveness. These exercises are also conducted in comparison to the SA, EU and USA jurisdictions. These themes clarify whether e-signatures are appropriately regulated in Lesotho for purposes of promoting the growth of e-commerce in Lesotho. But it is noted that some topics will overlap during analysis.

[17] Article 9 (3) (a) & (b) of CUECIC; para 13 & 163 of Explanatory note on CUECIC; part 4.5.2 above.
[18] See part 4.3.2.1 above.
[19] See part 3.2.3.2.1 above.
[20] Paragraph 16 of Guide to MLEC in para 4.3.2.1 above.
[21] See part 3.4.1.1 above.
[22] See part 3.4.1.2 above.
[23] See part 3.4.2 above.

5.3 Inception of the SADC Model Law on e-commerce

The SADC ML is a product of the Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSSA) project[24] following SADC's declaration to enable e-commerce.[25] In 2008, African Union member states adopted a 'Reference Framework for Harmonization of the telecommunication and ICT Policies and Regulation in Africa' from which HIPSSA was born.[26] HIPSSA was developed in response to African economic integration organisations and regional regulation associations' request for assistance in harmonisation of ICT policies and rules in Sub-Saharan Africa. The assistance was requested from the International Telecommunication Union (ITU) and European Commission (EC).[27] In its effort to harmonise ICT rules, the ITU divided the HIPSSA project into four sub-regional programs. This was due to the diversity in the geographical and political conditions of the African continent, and their differing economic and regulatory associations. The sub regions of HIPSSA are East Africa, Central Africa, West Africa and Southern Africa.[28] SADC has a membership of fifteen countries.[29]

In pursuance of the project, in 2012 the United Nations Economic Commission for Africa (UNECA) and SADC worked together to conduct an E-commerce readiness study in the Southern Africa sub region.[30] The mission of the study was to enhance Business to Business trade and Business to Customer e-commerce inside the countries and between them,[31] in line with objectives of the SADC Treaty.[32]

UNECA and SADC conducted a Strength, Weaknesses, Opportunities, and Threats (SWOT) analysis for e-commerce readiness of SADC countries. The SWOT analysis

---

[24] ITU 'Support for harmonization of the ICT Policies in Sub-Saharan Africa' 2015 available at *http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx,* accessed on 14 April 2015.

[25] SADC: Towards a common future 'SADC Declaration on Information and Communications Technology (ICT)' 14 August 2001 para 2(d) available at *http://www.sadc.int/documents-publications/show/830,* accessed on 10 March 2016; Nnaemeka Ewelukwa 'Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for Ecommerce in Africa' 2011 (13) *European Journal of Law Reform* 550 at 567.

[26] ITU 'Support for harmonization of the ICT Policies' op cit note 24.

[27] ITU 'Support for harmonization of the ICT Policies' op cit note 24. The ITU is an agency of the United Nations which specializes in ICT. As a result it provides among others, access to ICT to communities worldwide (ITU 'About ITU' available on *http://www.itu.int/en/about/Pages/default.aspx,* accessed on 10 March 2016); T Tšiu 'Minister launches HIPSSA project in Lesotho' Lesotho Communications Authority Press Release 29 March 2013 available at *www.lca.org.ls,* accessed on 03 March 2015.

[28] ITU 'Support for harmonization of the ICT Policies' op cit note 24.

[29] These are Angola, Botswana, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, the Republic of South Africa, Swaziland, Tanzania, Zambia and Zimbabwe (SADC 'South African Community Development: Towards a common future' available at *http://www.sadc.int/member-states,* accessed on 13 December 2015).

[30] Mustapha Mezghani 'E-Commerce Readiness Study in the SADC sub-Strategy' (16-17 April 2012) Validation workshop by UNECA and SADC, Balaclava Mauritius.

[31] Mezghani ibid.

[32] See Article 5 (1) (a) & (d) to (h) of Treaty of the Southern African Development Community 1992.

identified lack of trust and confidence in e-commerce, lack of infrastructure and lack of cyber legislation as part of SADC's weaknesses. To curb this, the study noted that SADC had to create an enabled e-commerce environment. The study further set out objectives to achieve this. These included the increase of confidence in e-commerce, to support and inspire its practice and to harmonise e-commerce legislation. The study advised that to harmonise legislation, SADC member states should define the guidelines for harmonisation so as to increase the states' commitment; reflect on the UNCITRAL Model Laws on e-commerce and E-signatures; harmonise regulation for interchange of e-documents and on recognition of e-signatures; align electronically delivered goods and services regulation with regulation of physically delivered products, and enable member states to take the guidelines into consideration when drafting their national laws.[33] These studies subsequently lead to HIPPSA's production of the draft SADC ML.

In its preamble, the SADC ML recognises that the 'fundamental benefit of e-commerce is enhanced communication, which allows for simplicity, flexibility and new business opportunities.'[34] It proclaims that for e-commerce to succeed, it requires 'an accessible, predictable, safe and transparent trading environment, which operates across territorial borders and jurisdictions.'[35] The preamble states that the model law is framed in technology neutral terms.

5.4 The legal system of Lesotho on e-commerce

The Lesotho law of contract relies heavily on South African jurisprudence. This is due to Section 2 of Proclamation 2B of 1884 which provides that the law applicable in Lesotho shall be the same as the law applicable in the Cape Colony of Good Hope, with the exception of statutory law of the Colony. The Proclamation came to fore after Lesotho became a British protectorate in 1868. Consequently, decisions of South African courts are highly persuasive in Lesotho, although not binding.[36]

Lesotho had no legislative instruments on e-commerce before the Lesotho Bill on e-transactions. Laws in Lesotho were predominantly enacted before the ICT era,[37] and only a

[33] Mezghani op cit note 30.
[34] Preamble Draft SADC Model Law on e-commerce.
[35] Preamble Draft SADC Model Law on e-commerce.
[36] Section 2 of Proclamation 2B of 1884.
[37] Nthabiseng Motjolopane 'An Overview of the SADC Model Law on Electronic Transactions and Electronic Commerce' (2013) Support for Harmonization of ICT Policies in Sub Sahara Africa (HIPSSA Project) workshop/conference on Transposition of SADC Cybersecurity Model Laws into national laws for Lesotho Ministry of Communication Science and Technology (MCST) Lesotho.

few legal instruments recognised ICT.[38] Nevertheless none of these instruments give legal recognition or legal effect to e-signatures.[39] As the number of Internet users increased in Lesotho, e-commerce grew; this gave rise to Lesotho's need to facilitate and legally regulate e-transactions.[40] Consequently, the former Minister of Communications, Science and Technology, Mr. Tšeliso Mokhosi launched the HIPSSA project in Lesotho in March 2013.[41] The ministry's goal was to identify challenges in ICT regulation in Lesotho, to build a legal framework for e-transactions and e-commerce, and thus create a secure environment for ICT users.[42] It is from this project that Lesotho drafted the Electronic Transactions and Electronic Commerce Bill in 2013. Consultants subsequently put together the Lesotho Digital Signature Regulations. The two instruments are the subject of discussion in this chapter.

This said, the next section examines e-signatures that the Lesotho Bill and the SADC ML give legal effect to in order to establish whether they comply with the technology neutrality presumption of non-discrimination of technologies.

5.5 Legal recognition of e-signatures

Section 9 of the Lesotho Bill recognises two forms of signature in electronic communications (e-communications) as follows:

> '9. (1) Where a law requires the signature (manuscript) of a person, that requirement is met by a secure electronic signature.
>
> (2) Subject to subsection (1) an electronic signature shall not be denied legal force merely on the grounds that it is in electronic form.'

[38] For instance, the Criminal Procedure and Evidence (Amendment) Act 3 of 2001; the Communications Policy 2005 embraces e-commerce, e-government and data protection (see Motjolopane op cit note 37); Penal Code of 2010 (Act 6 of 2012) s 4; Communications Act 4 of 2012; Companies Act 18 of 2011, s 84 (4), s 182 (d) & s 183 (1) (d); Data Protection Act 5 of 2012; Info-Communications Authority Act 5 of 2000 (the name was changed from Lesotho Telecommunications Authority Act by the Info-Communications Authority (Amendment) Act of 4 of 2006); Lesotho Telecommunications Authority Regulations 34 of 2001 on Service Providers, regs 28, 32 and Part 5; 'Financial regulation (Mobile Money Guidelines – Consumer Protection) and Draft Information Technology Act' (Motjolopane 'An Overview of the SADC Model Law' op cit note 37 at slide 8).

[39] Motjolopane 'An Overview of the SADC Model Law' op cit note 37 slide 9.

[40] Wade Publications CC 'The Lesotho Review: An overview of the Kingdom of Lesotho's economy, Information and Communications Technology' 2015 available at *www.lesothoreview.com,* accessed on 1 May 2017; Mochebele M (ed) *The state of ICT in Key sectors: Business, Education, Health and Tourism Lesotho 2013* 2ed (2015) Lesotho Communications Authority.

[41] T Tšiu op cit note 27.

[42] T Tšiu op cit note 27.

In other words, the Lesotho Bill recognises ordinary e-signatures and a specific kind of e-signature technology, namely the secure electronic signature (SeS). Section 2 of the Lesotho Bill defines an SeS as

> '[A] signature duly recognised in terms of subsection 8(1), which is created and can be verified through the application of a security procedure or combination of security procedures that ensures that an electronic signature:
>
> (a) is unique to the signer for the purpose for which it is used;
>
> (b) can be used to identify objectively the signer of the electronic communication;
>
> (c) was created and affixed to the electronic communication by the signer or using a means under the sole control of the signer; and
>
> (d) was created and is linked to the electronic communication to which it relates in a manner such that any changes to the electronic communication would be revealed.'

The Lesotho Bill is technology neutral by giving effect to the ordinary e-signature. At the same time it is discriminatory by prescribing use of the SeS to the exclusion of other e-signature in cases where law requires signature. This way the Lesotho Bill adopts a two tier approach lay out by the MLES.[43]

Unlike the Lesotho Bill, the SADC ML legally recognises the ordinary e-signature in two scenarios. Section 7 of SADC ML states that:

> '(1) If a law requires the signature of a person, an electronic signature will be deemed to be valid, provided the electronic signature complies with the requirements as prescribed by Regulation.
>
> (2) The requirements for an electronic signature referred to in subsection 1 above will be met if:
>
> a. the method is used to identify the person and to indicate the person's intention in regard to the information communicated; and
>
> b. at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated in light of all the relevant circumstances.
>
> (3) Where two persons or parties agree to make use of electronic signatures they may agree to use any method of signing as they deem appropriate.'

[43] Article 6 of MLES & part 4.4.5 above.

Consequently, the SADC ML recognizes an ordinary e-signature where law requires signature, and where parties agree to use a signature. It does not impose use of a SeS where law requires a signature. Hence it does not discriminate among e-signature technologies to this extent. This feature complies with the non-discrimination presumption of technology neutrality together with the MLEC and CUECIC.[44] Because of its technology neutral approach, the SADC ML also recognises the concept of party autonomy.[45]

Nonetheless, the SADC ML provides that member states *may* develop regulation that recognises accredited authentication products and services as SeS. [46]

On the one hand, the Electronic Communications and Transactions Act (ECTA) of South Africa recognises two forms of e-signature, namely the Advanced Electronic Signature (AeS) and the e-signature.[47] First, it states that only an AeS will suffice where law requires signature if the law has not specified the kind of signature it requires.[48] The ECTA tries to make its provision technology neutral by accommodating statutes that stipulate a particular e-signature as sufficient.[49] However, it effectively renders only the AeS sufficient when the law requires signature as not many statutes specify an e-signature they require.[50] To illustrate, in *South African Municipal Workers Union (SAMWU) v Rycroft*[51] the Labour Appeal Court held that a Commissioner's arbitration award sent on email did not meet the Labour Relations Act's (LRA)[52] requirement that an award shall be signed. Since the LRA is silent about the signature it requires, the court read it together with the ECTA and held that the award was not valid since it was not signed with an AeS.

Secondly, the ECTA stipulates that where signature is required by parties to a contract, an ordinary e-signature will be sufficient provided it identifies a party, shows their approval of information, and is as reliable as appropriate in the circumstances.[53] The ECTA further states that an ordinary e-signature must not be denied legal effect due to its electronic form.[54] In

[44] See part 3.3.3.2.1 above; Article 7 (a) of MLEC & art 9 (3) (a) of CUECIC.
[45] See part 3.3.4 above.
[46] Section 8 (1) of the SADC ML.
[47] Act No 25 of 2002; Dana van der Merwe, Anneliese Roos & Tana Pistorius et al *Information and Communications Law* 2 ed (2016) 177; Lee Swales 'The Regulation of electronic signatures: Time for Review and Amendment' (2015) 132 *SALJ* 257 at 258.
[48] Section 13 (1) of the ECTA.
[49] Van der Merwe et al *Information* op cit note 47 at 131.
[50] Van der Merwe et al *Information* op cit note 47 at 118.
[51] [2009] ZALC 252; See also *South African Municipal Workers Union (SAMWU) v South African Local Government Bargaining Council and Others (DA7/2012)* (2014) 35 ILJ 2824 (LAC) (13 February 2014).
[52] Section 138 (7) (a) of Act 66 of 1995.
[53] Section 13 (3) of the ECTA; *Wilbery (Pty) Ltd t/a Ecowash v Springforest Trading 599 CC & Another* (2994/2013) [2013] ZAKZDHC 37 (31 May 2013).
[54] Section 13 (2) of the ECTA.

other words, the ECTA gives effect to ordinary e-signatures but prescribes use of the AeS where law requires signature if the law is silent on type of signature to be used.[55] Consequently, the ECTA and the Lesotho Bill are alike in adopting a two tier approach.

On the other hand, the European Union's Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (Directive)[56] provides for three forms of signature namely the ordinary e-signature,[57] an AeS,[58] and a qualified e-signature (QeS).[59] It stipulates that an ordinary e-signature should not be denied legal effect due to its electronic form.[60] Further a QeS satisfies legal signature requirements in data just as the handwritten signature in paper documents.[61] Hence the Directive legally endorses the use of ordinary e-signatures and the QeS.

Subsequently, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for electronic transactions in the internal market (eIDAS Regulation) repealed the Directive on e-signatures.[62] The EU realized that the regulation of e-signatures alone was not sufficient to guarantee security and legal validity of e-transactions at national and cross border levels.[63] It noted that other trust services were required; these included regulation of e-time stamps, e-

[55] See also s 13 (5) of the ECTA; s 5 of SADC ML; s 7 (2) of the Lesotho Bill.

[56] Available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093,* accessed on 01 December 2015. The Directive was a legal framework for e-signatures and certification-service in the EU region. It came into force on 19 January 2000 (Stephen Mason *Electronic Signatures in Law* 4 ed (2016) 149).

[57] Article 2 (1) of the Directive.

[58] Article 2 (2) of the Directive.

[59] Article 5 (1) of the Directive. A qualified e-signature consists of three components, an advanced e-signature, a qualified certificate and a secure-signature-creation device.

[60] Article 5 (2) of the Directive; See also Recital 21 of the Directive; Odvetniska Druzba Colja 'Case note: Republic of Slovenia' (2007) 4 *Digital Evidence and Electronic Signature Law Review* 97 where the Supreme Court held that an email and the electronic signature typed in the email message should not be denied validity due to their electronic form.

[61] Article 5 (1) of the Directive. It grants a QeS legal certainty by treating it as functional equivalent of a handwritten signature (Hans Graux 'Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union' (2013) 8 *Journal of International Commercial Law and Technology* 110).

[62] Article 50 (1) of eIDAS Regulation.

[63] Para (2) of eIDAS Regulation; The European Commission through its Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe (2010) available at *http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R(01),* accessed on 14 December 2015, proposed that the eSignature Directive should be reviewed 'with a view to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems' (See para 2.1.2); Hans Graux 'Rethinking the e-signatures Directive: on laws, trust services, and the digital single market' (2011) 8 *Digital Evidence and Electronic Signature Law Review* 9 at 17; Graux 'Moving towards a comprehensive legal framework' op cit note 61 at 117; Manuel Alba 'Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions' (2013-2014) 47 *Creighton Law Review* 387 at 392.

seals, e-delivery, legal admissibility of e-documents and website authentication.[64] The eIDAS Regulation therefore regulates these activities in addition to e-signatures. The eIDAS Regulation came into in force on 17 September 2014. It applied from 1 July 2016[65] and repealed the Directive with effect from 1 July 2016.[66] This study discusses both instruments.

Like the Directive, eIDAS Regulation provides for three forms of signature, namely an ordinary e-signature,[67] an AeS[68] and a QeS.[69] As far as recognition of e-signatures is concerned, the spirit of the two instruments is the same; it legally recognizes e-signatures and confirms the status of the QeS as equivalent to a handwritten signature.[70] It follows that both the Directive and eIDAS Regulations adopt the two-tier approach on e-signature regulation.

Conversely, the USA legally recognises the use of ordinary e-signatures through two instruments that regulate e-transactions, namely the Uniform Electronic Transactions Act (UETA),[71] and the Electronic Signatures in Global and National Commerce Act (E-SIGN).[72] UETA stipulates that '[a] record or signature may not be denied legal effect or enforceability solely because it is in electronic form'.[73] Furthermore '[i]f a law requires a signature, an electronic signature satisfies the law.'[74] It adopts the basic principle 'that the medium in which a record, signature, or contract is created, presented or retained does not affect its legal significance.'[75] UETA uses the MLEC as its base.[76] E-SIGN reiterates the spirit of UETA,[77]

---

[64] European Commission 'Digital agenda for Europe: A Europe 2020 Initiative' available at *http://ec.europa.eu/digital-agenda/en/trust-services,* accessed on 02 December 2015; Jos Dumortier, Stefan Kelm & Hans Nilsson et al *The legal and market aspects of electronic signatures* Interdisciplinary Centre for Law and Information Technology, Katholieke Universiteit 14; Graux 'Rethinking the e-signatures Directive' op cit note 63 at 16.

[65] EUR-Lex 'Access to European Union law - eSignature in the EU' available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24118,* accessed on 02 December 2015.

[66] Article 50 (1) of eIDAS Regulation.

[67] Article 3 (10) of eIDAS Regulation.

[68] Article 26 of eIDAS Regulation.

[69] Article 3 (12) of eIDAS Regulation.

[70] Article 25 (1) & 25 (2) of eIDAS Regulation.

[71] Uniform Electronic Transactions Act 1999. UETA is a non-binding USA model law adopted by the National Conference of Commissioners on Uniform State Law (NCCUSL). It becomes binding on a state only if a state adopts it in its legislature (MinyanWang 'Do the regulations on electronic signatures facilitate international electronic commerce? A critical review' (2007) 23 *Computer law & Security Report* 32 at 37).

[72] Electronic Signatures in Global and National Commerce Act 2000. E-SIGN is a binding federal law enacted by Congress. Federal Government enacted E-SIGN with the purpose of binding states to apply principles in UETA and have uniform laws (Henry D Gabriel 'United Nations Convention on the use of electronic communications in international contracts and compatibility with the American domestic law of electronic commerce' (2006-2007) 7 *Loyola Law and Technology Annual* 1 at 6); E-SIGN and UETA do not apply to contracts regulated by the Uniform Commercial Code (UCC) 'other than sections 1-107 and 1-206 and Articles 2 and 2A' (15 USC § 7003 (a) (3) E-SIGN & UETA § 3 (b) (2)). Again, UETA does not apply to transactions regulated by UCC (§ 3 (b) (3) of UETA).

[73] § 7 (a) of UETA.

[74] §7 (d) of UETA.

[75] Section 7 Comment 1 of UETA.

stating that 'a signature, contract, or other record relating to such transaction (in interstate or foreign commerce) may not be denied legal effect, validity, or enforceability solely because it is in electronic form'.[78] E-SIGN further prevents states from applying electronic or digital signature laws that are inconsistent with it or the UETA.[79]

Moreover, UETA recognises the concept of party autonomy.[80] In effect, the USA rejected the two tier approach of the MLES which establishes criteria for legal validity of e-signatures.[81] It is consistent with the MLEC and CUECIC which legally recognise any form of e-signature whether required by law or not,[82] and thus maintains technology neutrality.[83] The USA statutes 'confirmed that electronic signatures have the same legal standing as pen-and-paper signatures'.[84] They intend to give legal recognition to the 'use of electronic media, bringing e-contracts to the same legal status as their paper counterparts'.[85]

To summarise, the Lesotho, SA and EU instruments do not fully meet the non-discrimination presumption of technology neutrality. They legally recognise the ordinary e-signature in the formation of e-contracts or e-communication, but like the MLES favour the SeS and Aes to other ordinary e-signatures.[86] The USA and SADC ML differ from these jurisdictions as they give legal effect to all e-signature technologies without distinction. They comply with the non-discrimination presumption of technology neutrality like the MLEC and CUECIC.

---

[76] Roberto Rosas 'Comparative Study of the Formation of Electronic Contracts in American Law with references to International and Mexican Law' (2004-2005) 8 *Newcastle L Review* 79 at 81; see also part 4.3.2.2 above.
[77] Rosas op cit note 76 at 81.
[78] General Rule of Validity 15 USC §7001 (a) (1). It further states that a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation (15 USC §7001 (a) (2)).
[79] Stephanie Lillie 'Will E-SIGN force states to adopt UETA?' (2001-2002) 42 *Jurimetrics* 21; Rosas op cit note 76 at 86; 15 USC § 7002 (a) (1). Alternatively, a state need not adopt UETA but must ensure that provisions of its statutes are in line with E-SIGN and technology neutral (Stephanie Curry 'Washington's Electronic Signature Act: an anachronism in the new millennium' (2013) 88 *Washington Law Review* 559 at 576); *Progressive Casualty Insurance Company v Estate of Jose Juan Palomera-Ruiz* 2011 WL 291137.
[80] § 5 (a) & (b) of UETA; *Brantley v Wilson* 2006 US Dist LEXIS 17722; 15 USC § 7001 (b) (2).
[81] Article 6 (3) of MLES in part 4.4.3 above; Charles H Martin 'The UNCITRAL Electronic contracts Convention: will it be used or avoided?' (2005) 17 *Pace International Law Review* 261 at 288.
[82] Article 7 (1) (a) of MLEC & Art 9 (3) of CUECIC; See Christina Spyrelli 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) 2 *Journal of Information, Law and Technology http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html*, accessed on 16 January 2014.
[83] See parts 3.3.3.2.1 & 4.3.2.2 above.
[84] 'The ESIGN Act' June 2011 available at *http://electronicsignature.com/esignact/*, accessed on 1 December 2015.
[85] Sarah E Smith 'The United Nations Convention on the use of electronic communication in international contracts (CUECIC): Why it should be adopted and how it will affect international e-contracting' (2007) 11 *SMU Science and Technology Law Review* 133 at 147; Jennifer L 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 law & contemporary problems* 491 at 507.
[86] The study below explains that an AeS is similar to a SeS.

5.6 Examination of the technology neutrality of SeS regulation

This section examines the extent to which the Lesotho Bill and SADC ML provisions on SeS observe technology neutrality presumptions.

5.6.1. Description of a SeS favours features of a digital signature and PKI technology

Although the Lesotho Bill does not specify e-signature technology that is a SeS, it is argued that among currently available e-signature technologies,[87] the features of a SeS favour the digital signature based on PKI to the exclusion of other e-signature technologies. Section 2 of the Lesotho Bill interprets a SeS as

> ‘[A] signature duly recognised in terms of subsection 8(1), which is created and can be verified through the application of a security procedure or combination of security procedures that ensures that an electronic signature:
> (a) is unique to the signer for the purpose for which it is used;
> (b) can be used to identify objectively the signer of the electronic communication;
> (c) was created and affixed to the electronic communication by the signer or using a means under the sole control of the signer; and
> (d) was created and is linked to the electronic communication to which it relates in a manner such that any changes to the electronic communication would be revealed.’

First the Lesotho Digital Signature Regulations’ definition of a digital signature supports the contention that a SeS is met by a digital signature based on PKI. Regulation 1 provides that

> ‘ "digital signature" means an electronic signature consisting of a transformation of an electronic communication using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic communication and the signer’s public key can accurately determine -
> (a) whether the transformation was created using the private key that corresponds to the signer’s public key; and
> (b) whether the initial electronic communication has been altered since the transformation was made’.

[87] See part 2.9 above.

To elaborate, forms of e-signatures that are unique to the signer and thus meet the first requirement of SeS include among others, a digital signature based on PKI, biometrics signature, a digitized signature, a PIN, password or email signature. But these are not enough to meet all requirements of the SeS. Biometrics is compared to digital signature based on PKI in this case as they have more authentication features than the other ordinary forms of e-signature.[88] As Regulation 1 (a) of the Digital Signature Regulations indicates, a message receiver uses a public key of the signer which corresponds to the signer's private key to decrypt the digital signature and verify. If a message is not decrypted, it is possible that the message was encrypted with a public key that does not correspond to the signer's private key. Consequently, successful decryption of a message presumes that the private key is unique to the signer.[89] With biometrics, a signer uses their physical or behavioural characteristic (biometric) to sign a message. He/she uses a distinctive behavioural or physical attribute such as a finger print, 'that is inherently extremely difficult to imitate by a would-be cyber-thief.'[90] This also renders biometrics unique to the signer.

The Lesotho Bill's second requirement is that a SeS should identify objectively the signer of e-communications. For biometrics to objectively identify the signer, the recipient of the e-communication should have the database of physical or behavioural characters of the parties they contract with for comparison purposes.[91] If a signer is not enrolled on the recipient's data base, then the biometric will fail to objectively identify the signer.[92] With the digital signature based on PKI, a recipient of digitally signed e-communication verifies the signer's identity through a public key certificate [93] and thus objectively identifies them as the

[88] See parts 2.9.1 – 2.9.10 above.

[89] Some authors challenge the assertion that a private key is unique to a signer and assert that the unique link is between the private key and the digital signature, not between the (signer) user of the private key and the digital signature. This is since the private key is too complicated to be memorized by its holder, instead it is stored in a computer, smartcard or other support technology. Therefore, they assert that not even the digital signature can fulfill this requirement that the e-signature should be unique to its user (Mason op cit note 56 at 152, 154-155). Other authors argue that a digital signature is 'uniquely linked to the signatory's PC or to a storage device rather than to the signatory' (G Chondrocoukis & P Lagou 'Non Repudiation: Gap between Legislation and Practice' at 7 available at *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.2154&rep=rep1&type=pdf*, accessed on 14 December 2015).

[90] Stephen E Blythe 'Lithuania's Electronic Signature Law: Promoting the Growth of Secure E-commerce Transactions' (2007) 8 *Barry Law Review* 23 at 26.

[91] Blythe 'Lithuania's Electronic Signature Law' ibid; See part 2.9.9 above.

[92] Salil Prabhakar, Sharath Pankant & Anil K Jain 'Biometric Recognition: Security and Privacy Concerns' March/April 2003 *IEEE security & privacy* 33 at 34 available at *http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf*, accessed on 23 November 2015.

[93] See part 2.9.10.2.1 above.

key pair holder.[94] Hence both biometrics and the digital signature based on PKI system fulfil the second feature of a SeS.

Moreover, the Lesotho Bill provides that a SeS is to be created and affixed to e-communications using a means that is under the sole control of the signer. The holder of a private key in cryptography is expected to have the sole control of the private key and to keep it safe from falling into wrong hands. Consequently, the assumption is that the digital signature based on PKI can be created with means under the sole control of the signer.[95] On the other hand, in biometrics methods the signer has sole control of a biometric that creates the signature, for example, they have sole control of their finger print. Hence biometric signatures and digital signature based on PKI may satisfy the third element of a SeS.

The Lesotho Bill describes the last feature of a SeS as a signature attached to e-communication in such a manner that it reveals any changes made to the e-communications. A signer's attachment of a biometric signature to e-communication will not show when the contents of the message have been changed.[96] By contrast, as Regulation 1 (b) of the Digital Signature Regulations indicates, a digital signature attached to a message reveals if any changes were made to a signed message, regardless of how minor the change. This reflects when the digital signature is not verified upon the receiver's decryption of a message.[97] It follows that the digital signature, amongst current technologies, can reliably fulfil the last requirement of a SeS.[98]

The above factors show that amongst the currently available e-signature technologies the provisions of the Lesotho Bill on a SeS can be performed by a digital signature based on PKI. In fact, Regulation 2 of the Digital Signature Regulations states that '[w]hen any portion of a data message is signed with a digital signature, the digital signature shall be treated as a SeS with respect to such portion of the record'. Thus, although the features of the SeS are general enough to accommodate possible future technologies that will meet the criteria, the provisions are technology specific with their preference of a digital signature based on PKI amongst current e-signature technologies. It is noted that the features of a SeS are akin to the criteria set by the MLES.[99]

[94] See Regulation 1 (a) of Digital Signature Regulations.
[95] See parts 2.9.10.2.5 & 2.9.10.2.6 above which reflect the difficulty of 'sole control' over a private key.
[96] Blythe op cit note 90 at 26. Other forms of e-signature are also incapable of revealing the changes.
[97] See part 2.9.10.2 above; Blythe op cit note 90 at 27.
[98] Mason op cit note 56 at 159; Gregory 'Legislating Trust' (2014) 12 *Canadian Journal of Law and Technology* 1 at 12.
[99] Article 6 (3) of the MLES in part 4.4.3 above.

SADC ML defines the SeS like the Lesotho Bill's.[100] Accordingly, in terms of the currently available technologies, the SADC ML implicitly prefers the digital signature technology based on a PKI system for purposes of a SeS. But like the Lesotho Bill, the SADC ML's SeS provisions are general enough to fit possible future technologies.

The ECTA of South Africa follows suit in its definition of an AeS. It describes an AeS as 'an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37'.[101] An Accreditation Authority may accredit or recognize authentication products or services in support of AeS.[102] The ECTA lays down the criteria for accreditation of authentication products or services.[103] The criterion is similar to features of the Lesotho SeS,[104] with exception of the ECTA's last requirement that the authentication product is based on face to face identification of the user.[105] This last feature is nonetheless part of a signer's application process for a key pair and certificate for a digital signature. In other words, although the ECTA tries to be technology neutral in its criteria for accreditation of authentication products that support an AeS by not specifically requiring a technology,[106] the features of the products also center on a digital signature based on PKI technology.

It is noted that South Africa is considering developments in further regulation of e-commerce. It has subsequently drafted the Electronic Communications and Transactions Amendment Bill (ECT Amendment Bill).[107] The ECT Amendment Bill proposes a new definition of AeS. However, the proposed definition is not very different from the ECTA's

[100] Section 1 (19) of SADC ML. See also s 8 (1) of the SADC ML.
[101] Section 2 of the ECTA.
[102] Section 37 & 33 of the ECTA.
[103] Section 38 (1) of ECTA states that the 'Accreditation Authority must be satisfied that the e-signature to which the product or service relates is: uniquely linked to the user; capable of identifying that user; created using means that can be maintained under the sole control of that user; and 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 and; based on the face-to-face identification of the user.'
[104] Section 2 of the Lesotho Bill.
[105] Aashish Srivastava & Michel Koekemoer 'The legal recognition of electronic signatures in South Africa: A Critical Overview' (2013) 21 *African Journal of International and Comparative Law* 427 at 431 believe that the latter requirement of face to face identification was prompted by the alarming rise of identity frauds online and was aimed at avoiding such.
[106] Van der Merwe et al *Information* op cit note 47 at 131.
[107] GN 888 GG35821 of 26 October 2012. The Department of Communications circulated the document for comment in 2012. As of 2016, there was no indication of when it will come into force, but it is currently closed for public comment (Van der Merwe et al *Information* op cit note 47 at 132; Swales op cit note 47 at 265).

definition of AeS for purposes of technology neutrality.[108] It still relies on the digital signature technology based on PKI like the ECTA.

Incidentally, features of the ECTA AeS are analogous to the requirements of an AeS set out by the Directive except for the ECTA's last requirement of face to face identification.[109] In fact the Directive appears to have been the foundation of the ECTA in this regard.[110] Just like Lesotho, although the provision on a SeS appear to be technology neutral, the Directive's AeS is in essence a digital signature based on PKI.[111] The eIDAS Regulation has maintained the same spirit as the Directive in its interpretation of AES.[112] Its Art 3 (11)[113] read with Art 26[114] impliedly prefer the digital signature based on PKI.[115]

It follows that despite the seemingly technology neutral language of the Lesotho Bill and above instruments on their description of a SeS, the instruments indirectly favour the digital signature based on PKI technology to the exclusion of other existing e-signature technologies. This is a technology specific feature that contradicts the technology neutrality principle of non-discrimination of technologies.

5.6.2 The grading of e-signatures not technology neutral

The Lesotho Bill and the SADC ML make several presumptions for a SeS and it is questionable whether the presumptions observe the technology neutrality principle. The Lesotho Bill equates a SeS to a manuscript signature. It provides that '[w]here a law requires

---

[108] Section 1 (b) of ECT Amendment Bill: 'advanced electronic signature' means 'an electronic signature which has been accredited by the Accreditation Authority as provided for in section 37, and which is admissible in legal proceedings.'

[109] Article 2 (2) of Directive: '"advanced electronic signature" 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.'

[110] S Eiselen 'Fiddling with the ECT Act – electronic signatures' (2014) 17 *PER* 2805 at 2813. See also the United Kingdom electronic signature regulations 318 of 2000 on which the ECTA relied.

[111] Forder J 'The inadequate legislative response to e-signatures' (2010) 26 *Computer law & Security Review* 418 at 422; Dumortier et al op cit note 64 at para 1.2.1 at 30. See also Bert-Jaap Koops 'Should ICT Regulation be technology-neutral?' in Bert-Jaap Koops, Miriam Lips, Corien Prins & Maurice Schellekens (eds) *Starting Points for ICT regulation* (2006) 77 at 94. Hence it is not completely technology neutral (Graux 'Rethinking the e-signatures Directive' op cit note 61 at 10).

[112] Mason op cit note 56 at 152.

[113] Article 3 (11) of eIDAS Regulation: '"advanced electronic signature" means an electronic signature which meets the requirements set out in Article 26.'

[114] Art 26 of eIDAS Regulation: 'An advanced electronic signature shall meet the following requirements:
(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.'

[115] The only difference with the Directive is that the eIDAS Regulation recognizes the difficulty of maintenance of sole control of a signing mechanism. It therefore states that the AeS is created by means which 'the signatory can, with a high level of confidence, use under his sole control.'

the signature (manuscript) of a person, that requirement is met by a secure electronic signature'[116] In addition, the Lesotho Bill and SADC ML give the SeS a presumption of attribution,[117] stating that '[a] secure electronic signature is deemed to have been applied by the holder of the secure electronic signature, unless the contrary is proved.'[118] Moreover, the SADC ML gives a SeS the presumption of validity and proper application. It states that '[w]here a secure electronic signature has been used, the signature is regarded as being a valid electronic signature and having been applied properly, unless the contrary is proved.'[119] It also explains that other e-signature technologies that are not SeS are not subject to the presumptions.[120]

Note is taken that a presumption exists where two situations connect in such a way that proof of the first situation makes one to believe that the second situation is proved as well.[121] Therefore '[a] presumption is a rule of law which gives an extra effect to a finding of fact by declaring that another fact shall be presumed to exist once the first fact is established.'[122]

A presumption of law may be rebuttable or irrebuttable. An irrebuttable presumption does not invite any challenge,[123] it cannot be rebutted with contrary evidence.[124] Hence, an irrebuttable presumption is in effect a rule of substantive law.[125] On the contrary, a rebuttable presumption assumes a certain exists until proven otherwise. It invites challenge,[126] and imposes an onus to rebut the presumption on an opposing party.[127]

The Lesotho Bill's provision that a SeS meets the law's requirement of signature is an irrebuttable presumption. Its language shows that the position of a SeS cannot be rebutted by evidence. Article 6 (3) of the MLES creates a presumption that e-signature technologies that meet its reliability criteria give legal effects equivalent to those of a handwritten signature.[128] The purpose of the MLES was to create certainty at or before the time of signing on the legal

[116] Section 9 (1) of the Lesotho Bill.
[117] See part 2.5.7 above.
[118] Section 18 (2) of the Lesotho Bill & s 18 of the SADC ML.
[119] Section 8 (3) of SADC ML.
[120] Section 8 (4) of SADC ML.
[121] James C Morton & Scott C Hutchison *The Presumption of Innocence* (1987) 11.
[122] Morton et al ibid at 26.
[123] Morton et al ibid at 13.
[124] Schwikkard PJ 'Rebuttable presumptions of law' in SE van der Merwe *Principles of evidence* 4 ed (2016) 538.
[125] DT Zeffertt, AP Paizes & A St Q Skeen *The South African Law of Evidence* (2003) 167; Morton et al op cit note 121 at 13.
[126] Zeffert et al ibid at 170; Morton et al op cit note 121 at 14.
[127] Zeffert et al ibid at 170 – 171 & 214.
[128] Paragraph 118 of Guide to the MLES in part 4.4.3. The MLES' e-signature reliability criteria closely resembles features of the Lesotho Bill's SeS set out in its s 2.

effects of e-signatures.[129] It noted that states may adopt the presumption as a rebuttable presumption or substantive rule.

On the contrary, the SADC ML and the Lesotho Bill provide rebuttable presumptions to the SeS. Their wording grants a SeS the presumptions of attribution, validity and proper application 'unless the contrary is proved'.

Presumptions exist for several reasons in our legal systems. For one, a rebuttable presumption distributes the burden of proof[130] by placing the onus to rebut the presumption on an opposing party.[131] It thus falls within the law of evidence.[132] Moreover, presumptions help courts reach valid affirmative verdicts that enable authoritative action in a functional system;[133] they save time by making it unnecessary to prove well known facts in legal proceedings[134] and they reflect policy preferences with regard to favoured results.[135]

Nonetheless, the Lesotho Bill and SADC ML presumptions on the SeS are problematic. For one, The Lesotho Bill's irrebuttable presumption on a SeS reflects that it recognizes only the SeS as equivalent to a handwritten signature. It thus treats the SeS as superior to other e-signatures. Such a discriminatory act of the Lesotho Bill is against the principles of technology neutrality. The irrebuttable presumption further denies parties an opportunity to challenge the SeS despite the potential shortcomings faced by a digital signature based on PKI.[136] Thus the irrebuttable presumption is technology specific and misplaced.

Moreover, the instruments' rebuttable presumptions on a SeS shift the burden of proof in favour of a holder of the SeS. They reduce the burden of proof on an online user where the validity or attribution of a SeS is challenged in litigation yet the burden is not moved when ordinary e-signatures apply.[137] This favours a particular e-signature technology contrary to the technology neutrality principle.[138]

---

[129] Para 118 of Guide to MLES.
[130] Morton et al op cit note 121 at 14; Edward W Cleary 'Presuming and Pleading: An Essay on Juristic Immaturity' (1959) *12 Stanford Law Review* at 5.
[131] Zeffert et al op cit note 125 at 167 & 173.
[132] Schwikkard et al op cit note 125 at 538.
[133] Morton et al op cit note 121 at 11.
[134] Ronald J Allen 'How presumptions should be allocated: burdens of proof, uncertainty, and ambiguity in modern legal discourse' (1994) 17 *Harvard Journal of Law & Public Policy* 628 at 635-639.
[135] Allen ibid at 634.
[136] See parts 2.9.10.2.5 above.
[137] Desiree De Andrade 'Is the pen mightier than the electronic signature?' 2005 December *De Rebus* at 26; Van der Merwe et al op cit note 47 at 119.
[138] See part 3.3.3.2.1 above.

Although offline rules make presumptions in document authentication, these do not depend on the form of signature. For example, the Authentication of Documents Proclamation gives the certificate of authentication the presumption of attribution irrespective of the form of signature used. It also makes a presumption that a document is signed by the purported signer if it is signed by an officer of the Crown and bears a stamp of the office.[139] But it is silent on which form of signature is to be used by the officer. As a result, the SADC ML and Lesotho Bill's presumptions do not target the same effect as offline presumptions. They consequently do not promote online and offline equivalence.[140]

Like the SADC ML, the South African legislation also renders an AeS superior to other e-signatures by granting it presumptions of validity and proper application.[141] Additionally, the ECT (Amendment) Bill renders an AeS admissible as proof in legal proceedings.[142] By so doing, it grants the AeS an evidential presumption which it does not afford to ordinary e-signatures.[143]

The EU's Directive on e-signatures followed this grading approach. It stipulated that a QeS fulfils legal requirements of signature on data in the same way as a handwritten signature in paper documents.[144] But the eIDAS Regulation modified this provision. It provides that '[a] qualified electronic signature shall have the equivalent legal effect of a handwritten signature'.[145] Effectively, it introduces an obligation that a QeS be granted the same legal effect as a handwritten signature. Hence, eIDAS Regulation emphasizes the grading of e-signature technologies.

The USA holds a different view on grading of e-signatures. E-SIGN restricts regulatory agencies from developing rules that 'require, or accord greater legal status or effect to the implementation or application of a specific technology or technical specification for performing functions of creating…or authentication of electronic records and electronic signatures.'[146] Moreover, UETA does not give the presumption of attribution to any specific e-signature, stating that an e-record or e-signature is attributable to a person if it was the act of the person.[147] If there is a dispute on verification of identity of a signer, UETA permits parties to prove the attributable person in any manner available, including the efficacy of the

[139] See first schedule & s 7 of the Authentication of Documents Proclamation in part 2.8 above.
[140] See parts 3.3.3.1.2 & 4.3.2.2 above.
[141] Section 13 (4) of ECTA; see also De Andrade op cit note 137 at 24.
[142] Section 1 (b) of ECT Amendment Bill.
[143] Eislen 'Fiddling with the ECT Act' op cit note 110 at 2814.
[144] Article 5 (1) (a) of Directive.
[145] Article 25 (2) of the eIDAS Regulation.
[146] 15 USC § 7004 (b) (*2*) (C) (*iii*).
[147] § 9 (a) UETA.

security process used to connect the person to the e-communication.[148] Therefore UETA and E-SIGN do not grade e-signatures. The USA approach is similar to CUECIC's approach of proving e-signatures through evidence of fact.[149]

The E-SIGN's objective of not grading e-signatures is to eliminate obstacles to the use and promotion of e-signatures in e-commerce.[150] This is in accordance with four principles, namely, lawmakers should eliminate paper based obstacles by adopting principles set by the MLEC; they should allow parties to a contract to choose authentication methods that suit their transaction with the assurance that the methods will be legally recognised; to allow parties to prove in legal proceedings that their authentication methods are valid and lastly, to adopt a non-discriminatory approach towards e-signatures.[151] E-SIGN's objective corresponds with principles of this study.

It is submitted that it is not necessary to deny an ordinary e-signature the presumption of attribution. The Lesotho Bill's definition of e-signature which states that it is data adopted to identify a party indicates that the law requires the e-signature to sufficiently link a person to a message. Hence an ordinary e-signature provides the functions of identification and attribution.[152] Again, an ordinary e-signature can be presumed to be a functional equivalent of a manuscript signature and applied properly if its reliability is evidenced.[153]

To summarize, although the SADC ML does not equate a SeS to a manuscript signature, it considers the SeS superior to the ordinary signature like the Lesotho Bill, the ECTA and the EU instruments. These provisions contradict the non-discrimination presumption and promotion of offline and online equivalence presumptions of technology neutrality. On the other hand, the USA instruments do not grade e-signatures and thus comply with the technology neutrality presumptions.

Accordingly, it is proposed that the lawmaker should remove presumptions of the Lesotho Bill and SADC ML which favour an SeS. Alternatively, because presumptions play a significant role in law as reflected above the instruments could maintain the concept of presumptions, but the lawmaker must 'reformulate' the presumptions to ensure that they are technology neutral and inclusive of functional equivalence. For example, they can create a presumption that an ordinary e-signature that is supported with metadata is attributable to the

[148] § 9 (a) Comment 4 of UETA.
[149] Article 9 (3) (b) of CUECIC in part 4.3.3 above.
[150] 15 USC 7031 (a) (1) of E-SIGN.
[151] 15 USC 7031 (a) (2) of E-SIGN.
[152] Van der Merwe et al *Information* op cit note 47 at 178.
[153] See part 4.3.3 above.

signer, and is presumed valid and properly applied, unless the contrary is proved. In addition to presumptions of the SeS, the Lesotho Bill renders the use of a SeS mandatory in certain situations.

5.6.3 Implications of compulsory use of a SeS

The Lesotho Bill stipulates that a SeS must be applied in three particular cases, namely where the law requires signature, writing, and document authentication services including the use of a seal. The SADC ML requires use of a SeS in fewer situations, that is in document authentication services and use of a seal.[154] These cases are discussed below.

5.6.3.1 Use of a SeS where law requires signature

The Lesotho Bill states that a law's requirement of signature is met by a SeS.[155] This provision indicates two things. First, the Lesotho Bill discriminates amongst e-signature technologies by giving SeS legal recognition to the exclusion of other technologies. Secondly, it addresses how conduct (signing) is carried out instead of the effects of signature contrary to the principles of both technology neutrality and functional equivalence. The first effect is traversed above[156] hence just the second effect is elaborated on below.

Chapter two of this study explains that if a law addresses the effects of a signer's signature or the mental state of a signer during signature instead of how they carry out the act of signing, it will result in equivalent treatment of online and offline users.[157] The Lesotho Bill provides that for an e-signature to meet the law's requirement of signature, a method should be used to identify the signer and show their intention with respect to the e-communication.[158] However, these requirements become irrelevant as it expects only the SeS to meet such requirements. Accordingly, the Lesotho Bill withdraws from addressing a signer's state of mind or effects of a signature, and instead focuses on how and what signature method the signer must apply when law requires signature. To accentuate the point, the Lesotho Bill authorises the Minister to make regulations that will define when authentication products may qualify as a SeS, that will prescribe the content of a digital certificate or key, make rules on regulation and licensing of Certification Authorities (CA) and so on.[159] Thus

[154] Sections 23 & 24 (3) of SADC ML.
[155] Section 9 (1) of the Lesotho Bill.
[156] See part 5.6.2 above.
[157] See part 3.2.5 above.
[158] Section 9 (3) (a) of the Lesotho Bill.
[159] Section 25 (1) of the Lesotho Bill.

the Lesotho Bill's prescription of a SeS fails to address the effects of signature contrary to functional equivalence and technology neutrality presumption.

The law's tendency to regulate the way signature is carried out instead of the results of signature is evident in both the South African and EU instruments. In South Africa, the ECTA prescribes use of an AeS where the law requires signature.[160] Unlike the Lesotho Bill the ECTA already contains detailed provisions that regulate this exercise. It sets out factors an Accreditation Authority (AA) is to consider before it accredits authentication products and services in support of an AeS;[161] factors it should consider before it accredits products of an authentication service provider (ASP);[162] and conditions the AA can set for a certification service provider (CSP) before it accredits its products in support of AeS.[163]

In furtherance of e-signature regulation, South Africa issued Accreditation Regulations under the ECTA in 2007.[164] The Regulations tabulate procedures that ASP and CSPs have to follow to apply for accreditation of products.[165] For example, it requires payment of a non-refundable application fee of twenty thousand rand (R20, 000).[166] They further tabulate the standard conduct the CSPs have to practice in issuance of public key certificates such as verifying the identity of the applicant on a face to face basis.[167]

Moreover, the Regulations stipulate technical requirements that a CSP must meet. For instance, if its products or services are based on PKI it must comply with the South African National Standard (SANS) 21188 PKI standard;[168] a certificate issued by a CSP must conform to the X.509 ITU Standard,[169] and the ASP or CSP must conform to the SABS/ISO 17799 information security principles.[170] Additionally, a CSP is to use trustworthy services to perform its services including generation and management of keys.[171] It should ensure that its personnel have the required knowledge, technical qualifications and skill to efficiently carry

[160] Section 13 (1) of ECTA.
[161] Section 38 (1) of the ECTA. These consist of features of an AeS.
[162] Section 38 (2) & (3) of ECTA: These include the financial and human resources of the ASP, its assets; its procedures for processing products; that the hardware and software systems must be secure from intrusion and misuse and observe generally accepted standards.
[163] Section 38 (4) of ECTA. For example, an AA may stipulate technical requirements the certificate must meet; requirements for certification practice statements (CPS); responsibilities and liabilities of CSPs and requirements on certificate revocation procedures.
[164] Government Gazette 29995 on 20 June 2007 created under ss 41 & 94 of ECTA.
[165] See chapter III of the Accreditation Regulations.
[166] Regulation 6 of Accreditation Regulations.
[167] Regulation 14 (1) of Accreditation Regulations. See also Regulations 14, 15, 19, 21, 22 & Chapter IV of Accreditation Regulations.
[168] Regulation 13 (1) of Accreditation Regulations.
[169] Regulation 13 (2) of Accreditation Regulations.
[170] Regulation 26 (1) of Accreditation Regulations; See Van der Merwe et al *Information* op cit note 47 at 135-136.
[171] Regulation 17 (b) of Accreditation Regulations.

out its functions.[172] These provisions are evidence that the instruments regulate how signature should be carried out when it is required by law, and not the effects of an e-signature. As a result, the instruments' prescription of the AeS will not lead to equivalence between online and offline. The provisions of the ECTA and Accreditation Regulations echo the contents of article 9 of the MLES.

Similarly, in the EU, the Directive and new eIDAS Regulation regulate the means of signing and not the effects of signature. Initially, the Directive stated that only a QeS fulfils the legal requirements of signature.[173] It interpreted a QeS as a combination of an AeS, a qualified certificate and a secure-signature-creation device (SSCD) which meet requirements set in Annex I, II and III of the Directive.[174] The Directive described performance characteristics an AeS must have;[175] and listed the requirements a SSCD that creates an AeS for a QeS must meet in Annex III.[176] It further listed information that the qualified certificate must contain under Annex I; while Annex II consisted of lengthy requirements that a CSP must meet before it could issue a qualified certificate. The requirements listed by the Directive related to conduct and capacity of CSPs, and the nature and contents of technology used to create a QeS.

In a similar vein, the eIDAS Regulation regulates means of signature in its regulation of the QeS. It provides that QeS means an AeS created by a 'qualified electronic signature creation device' that is based on a 'qualified certificate for electronic signatures'.[177] Hence the EU legal provisions regulate the means used to sign and not the effects of signature.

It follows that the Lesotho Bill, the South African and EU instruments contradict provisions of the MLEC and CUECIC regarding the law's requirement of signature[178] and follow the MLES instead. The MLES prescribes technical criteria an e-signature should meet to fulfil the law's requirement of signature and sets out duties of the signer and the CSP towards the signature technology.[179] These are observed by the SeS, AeS and QeS.

Contrary to the Lesotho Bill, the UETA renders an ordinary e-signature sufficient where law requires signature.[180] It defines an e-signature as 'an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person

[172] Regulation 17 (f) of Accreditation Regulations.
[173] Article 5 (1) (a) of the Directive.
[174] Article 2 (10) of the Directive.
[175] Article 2 (2) of Directive.
[176] Article 2 (6) read with ANNEX III.
[177] Art 3 (12) of eIDAS Regulation. See also Arts 3 (22), (11), (23), 24, 26, Annex I & II of eIDAS Regulation.
[178] Articles 7 (a) of the MLEC & Art 9 (3) of CUECIC in parts 4.3.3 & 4.5.2 respectively.
[179] Articles 8 & 9 of MLES in part 4.4.4 above.
[180] § 7 (d) of UETA.

with the intent to sign the record.'[181] Accordingly, its definition complies with the presumption of non-discrimination of technologies. It further addresses the state of mind of a signer at the time of signature, not how a signature should be made.

The SADC ML like UETA does not prescribe the use of a SeS when law requires signature. It provides that an ordinary e-signature is deemed valid if a law requires signature.[182] Consequently, it does not discriminate between e-signature technologies. The e-signature will be valid if it identifies the signer and shows their intention regarding the e-communication.[183] Hence it addresses effects of signature not how an e-signature must be made to fulfill requirements of the law as well.

The SADC ML and UETA comply with CUECIC. CUECIC legally recognises any e-signature technology as meeting the law's requirements of signature provided the e-signature shows the identity of a signer and their intent towards information.[184]

To sum up, the Lesotho Bill's act of prescribing use of a SeS if law requires signature does not observe the technology neutrality principles of non-discrimination and the need to address effects of signature. The South Africa and EU instruments do not meet these principles either. By contrast, the SADC ML and UETA meet the principles. The Lesotho Bill also does not meet the standard set by CUECIC while the SADC ML and UETA meet it.

5.6.3.2. Use of a SeS where the law requires writing

Section 2 of the Lesotho Bill interprets a SeS as an e-signature recognised under s 8(1). The latter section regulates the formality of writing in e-communications when required by law. The two sections read together imply that a SeS is legally recognised as writing. The Lesotho Bill's act of imposing use of a SeS where law requires writing reflects that it is discriminatory to other e-signatures.[185]

Conversely the SADC ML does not refer to the SeS where it regulates the formality of writing required by law,[186] neither does the ECTA.[187] Similarly UETA, provides that '[i]f a

[181] § 2 (8) of UETA Comment 7.
[182] Section 7 (1) of SADC ML.
[183] Section (7) (2) (a) of SADC ML.
[184] Article 9 (3) of CUECIC in Para 4.5.2 above.
[185] See part 3.3.3.2.1 above.
[186] Section 6 of SADC ML.
[187] Section 12 of the ECTA.

law requires a record to be in writing, an electronic record satisfies the law.'[188] It does not include e-signatures in the writing requirement.

5.6.3.3 Use of a SeS in the hierarchies of document authentication

Both the Lesotho Bill and the SADC ML prescribe use of a SeS where the law requires different hierarchies of document authentication, but it is questionable whether the instruments' provisions are technology neutral. The hierarchies of document authentication include notarisation, acknowledgment, verification, a statement made under oath,[189] certification[190] and use of a seal.[191]

It is contended that the Lesotho Bill and SADC ML provisions contradict principles of technology neutrality as they discriminate among numerous e-signature technologies that an authenticating officer could use to authenticate a signature or a document.[192] This is not the position offline. For example, the Authentication of Documents Proclamation states that a signature and 'sign' required for authentication of documents is any lawful means used to execute documents.[193] It does not prescribe use of a specific form of signature for authentication. Again, the Lesotho Bill and SADC ML's imposition of an SeS in document authentication implies that the instruments regulate the means used to sign, not the effects of signature.[194] Moreover, the instruments impose a stricter form of authentication than that required offline. As chapter two illustrated, the stamp obtaining process is simple[195] and is incomparable to the process involved in obtaining an SeS.[196] Hence the Lesotho Bill and SADC ML do not promote equal legal treatment of paper based users and computer based users as required by the functional equivalence and technology neutrality principles.[197]

The ECTA has identical provisions to the Lesotho Bill and SADC ML on notarization and other authentication processes.[198] Thus the same arguments above apply to it.

---

[188] § 7 (c) of UETA. See case law to the effect that email communication is 'signed writing' under 15 USC § 7006 (4) & (5): *Kevin C McMunigal v Kate E Bloch* 2010 WL 4636549 (2010); *On Line Power Technologies Inc v Square D Co* 2004 US Dist LEXIS 9655 (April 30 2004) ; *Naldi v Grunberg* 2010 NY App Div Lexis 7173 (2010).
[189] Section 23 (1) of the Lesotho Bill; Section 23 (1) of SADC ML.
[190] Section 23 (3) of the Lesotho Bill; Sections 23 (3) of SADC ML.
[191] Section 24 (3) of the Lesotho Bill; Section 24 (3) of the SADC ML.
[192] See part 3.3.3.2.1 above.
[193] Authentication of Documents Proclamation 2 of 1964 s 2.
[194] See part 3.3.3.1.1 & 5.6.3.1 above.
[195] See part 2.8 above.
[196] See part 2.9.10.2 & 5.6.3.1 above.
[197] See part 3.2.3.2.1 & 3.3.3.1.2 above.
[198] Sections 18 (1) & (3) of ECTA.

UNCITRAL highlights in CUECIC that there are times when the law requires a signature not to show a signer's approval of contents of e-communication but to show their intention with respect to the e-communication.[199] It mentions examples of the law's requirement of signature in notarization, attestation by a commissioner of oaths or signature by a witness. In these cases, a signature only identifies the notary, commissioner of oaths or witness and indicates their association with the contents of the e-communication, not their approval of the contents. UNCITRAL thus agreed that any e-signature which identifies a signer and shows their intention in respect of the contents of an e-communication is sufficient for document authentication.[200] Where challenged, the reliability of an ordinary e-signature used for document authentication can be proved by either of the tests set out in art 9 (3) (b) of CUECIC. Thus, the e-signature can be proved with factual evidence as it would be done when the authenticator's handwritten signature is disputed in a paper document. This approach will promote equal treatment of online and offline transactions. This is mindful of the fact that an e-record can provide a similar level of security to paper with respect to paper functions, and is more reliable in identifying a source and content of data if certain criteria is followed.[201]

Therefore, in an alternative approach supported by UNCITRAL, an authenticating officer can employ an ordinary e-signature technology that meets CUECIC's criteria to authenticate a document. This approach leads to achievement of a technology neutral e-document authentication.

UETA reflects that it is possible for a notary to notarize e-communication with an ordinary e-signature. It states that:

> 'If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record.'[202]

It mentions the example of a buyer who wants to send a notarised real estate purchase agreement to a seller. The notary simply must be present in the buyer's room to confirm the

[199] Para 160 Explanatory note on CUECIC in part 4.5.2 above.
[200] Article 9 (3) (a) of CUECIC & Para 160 Explanatory note on CUECIC in part 4.5.2 above.
[201] Paragraph 16 of Guide to MLEC in part 4.5.2 above. For other possible electronic signature verification methods, see Phil Kongtcheu 'Method and systems to facilitate online electronic notary, signatures and time stamping' 2004 available at *https://www.google.com/patents/US20040221162,* accessed on 26 November 2015; Nicholas N Nassiri 'Signature verification using a third party authenticator via a paperless electronic document platform' 2005 available at *https://www.google.com/patents/US6904416,* accessed on 26 November 2015.
[202] § 11 of UETA.

buyer's identity. He/she can then attest to the buyer's identity and sign the agreement with their ordinary e-signature such as a digitized signature.[203] The notary will then protect the content of a signed document by putting it in the form of a password protected attachment (on Microsoft or Adobe reader) attached to an email message, alternatively they can send the signed document on a secure TLS network.[204] The agreement will be notarized.[205] E-SIGN contains an identical provision to UETA.[206] Hence UETA and E-SIGN do not discriminate between e-signature technologies regarding document authentication.

Although UETA effectively does away with the requirement of a seal or stamp by authorising an authenticating officer to use an ordinary e-signature to authenticate an e-record, it does not dispose of other law requirements in an authentication act. [207] Any other information which the law requires for document authentication, such as the information contained in a notarial seal or notarial certificate still needs to be attached to or logically associated to the electronically notarized document.[208] The section is thus consistent with the purpose of UETA which is to render signature and other required information available in an electronic medium.[209] Hence states can develop guidelines that indicate which methods or technologies authentication officers can adopt together with ordinary e-signatures to ensure that other document authentication requirements are met online.

The National Association of Secretaries of State (NASS) national e-notarization standards[210] are an example of guidelines adopted by NASS to aid USA notaries on how to conduct e-notarisation. The document lays down the standards to be met by a notary's e-signature[211] and features of an electronic seal[212] and of a notarial certificate[213] that a notary is

[203] See part 2.9.7 above.
[204] See part 2.9.11 above.
[205] Comment on § 11 of UETA.
[206] 15 USC § 7001 (g) of E-SIGN.
[207] Comment on § 11 of UETA.
[208] American Society of Notaries 'E-notarization' available at *http://www.asnnotary.org/?form=enotary*, accessed on 16 January 2017.
[209] Comment on § 11 of UETA.
[210] National association of secretaries of state national e-notarization standards 2006 available at *http://www.asnnotary.org/img/NASS%20Natl%20Standards%20on%20ENotarization%20July%202006.pdf*, accessed on 16 January 2017.
[211] Standards 5 & 7 of NASS e-notarisation standards.
[212] Standards 8 & 9 ibid. The guide defines "Electronic notary seal" and "official electronic seal" as 'information within a notarized electronic document that includes the notary public's name, jurisdiction of appointment, commission number, and commission expiration date, and generally corresponds to data in notary public seals used on paper documents.'
[213] Standard 6. It defines an "Electronic notarial certificate" as 'the portion of a notarized electronic document that is completed by the notary public, bears the notary public's electronic signature and/or official electronic seal, official title, commission number, commission expiration date, any required information concerning the date and place of the electronic notarization, and states the facts attested to or certified by the notary public in a particular electronic notarization.'

to put in an e-document. NASS offers the standards for voluntary adoption by states, they are not mandatory.[214] Consequently, states in the USA are free to design guidelines borrowing from UETA, E-SIGN and/or NASS e-notarisation standards to guide e-notarisation and e-document authentication.[215]

UETA further caters for certification of e-communication. It states that if a security method can be used to prove that an e-signature attached to e-communication is attributable to a certifying officer, the e-communication is deemed certified. UETA defines a security procedure as '[a] procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.'[216] For example, a certifying officer can sign a copy of a document with an ordinary e-signature such as a scanned signature then email the document to the owner on a secure communication network such as Transport Layer Security standard on Gmail. The security method they used provides information security and will be sufficient proof that the e-signature is attributable to the certifying officer.[217] The instrument therefore ensures that an e-signature used for authentication is reliable and free from manipulation. It thus aligns with the e-signature reliability requirement of the MLEC and CUECIC.[218]

It follows that the UETA and E-SIGN are technology neutral on e-document authentication while ensuring that is the exercise is conducted reliably. At the same time, the instruments acknowledge the pertinent role of soft laws in support of technology neutral laws.[219] The soft laws provide guidance on how authenticating officers can ensure that differing law requirements of authentication are met in a technology neutral manner.

In another alternative approach to a technology neutral e-document authentication, emphasis is placed on the purpose of a seal or stamp in offline document authentication. The seal is used for authenticating documents and safeguards their originality.[220] The Lesotho Bill and SADC ML regulate the law's requirement of original information. They stipulate that

[214] American Society of Notaries op cit note 208.
[215] American Society of Notaries op cit note 208. See also s 3 (b) & (c) of the Uniform Real Property Electronic Recording Act (URPERA) 2004 of USA.
[216] See § 2 (14) of UETA; Timothy Reiniger & Jacques R Francoeur 'Justice and sheriff: practical and authoritative methods for the electronic issuance of officially certified documents in the United States' (2010) 7 *Digital Evidence & Electronic Signature Law Review* 42 at 46.
[217] See part 2.9.11 above.
[218] See part 4.3.3 above.
[219] See part 3.3.7 above.
[220] Elliot op cit note 120 at 905 & 908.

where law requires information to be produced in its original form, e-communication will meet this requirement if there is reliable assurance of the integrity of the information.[221] The criteria for assessing integrity of information is whether it remained complete and unaltered; while assessment of the reliability level will depend on the purpose of creating the information and the circumstances involved.[222]

It is argued that there are other e-technologies that can equally safeguard the originality of e-communication as the SeS and they can be used in conjunction with the ordinary e-signature to meet the requirement of a seal. For example, the use of metadata can ensure that e-communication remains unaltered.[223] Metadata 'includes the contextual, processing and use information that is used to identify and certify the scope, authenticity and integrity of electronic information.'[224] It comprises of information such as the date on which the communication was created, how it was created, when it was modified, the file name, file size, its format, location from where the file was opened, stored, when it was printed, date on which the metadata itself was modified and so on.[225] The metadata may be descriptive, structural or administrative.[226] Since metadata is automatically generated by a computer that follows software instructions without human intervention, it is more difficult to manipulate, change or erase.[227] Although metadata may be altered or removed, tampering with it[228] can evidence bad faith;[229] it also negatively affects the admissibility and evidentiary weight of the e-communication in question.[230] Therefore metadata can demonstrate the authenticity and integrity of a document.[231] It follows that technologies such as metadata used in conjunction

[221] Section 19 (1) of the Lesotho Bill; s 19 (1) of SADC ML.
[222] Section 19 (3) of Bill; s 19 (3) of SADC ML.
[223] Sylvia Papadopoulos 'Electronic Wills with an Aura of Authenticity: *Van der Merwe v Master of the High Court and Another*' (2012) 24 *SA Mercantile LJ* 93 at 104; See part 4.3.3 above on prove of an e-signatures reliability.
[224] Papadopoulos ibid at 104.
[225] Papadopoulos ibid at 104; Burkhard Schafer & Stephen Mason 'The characteristics of electronic evidence' in Stephen Mason & Daniel Seng (eds) *Electronic Evidence* 4 ed (2017) 18 at 27.
[226] Schafer et al ibid at 38.
[227] Schafer et al ibid at 36. For shortcomings of metadata see Schafer at 36.
[228] Tampering of metadata is detectable, for example, inconsistencies across different metadata points can divulve evidence of tampering (Forensicon 'What is Metadata?' 2016 available at *http://www.forensicon.com/resources/articles/what-is-metadata/*, accessed on 13 January 2016).
[229] 'The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age' A Project of The Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production Second Edition November 2007 at 30 available at *file:///C:/Users/user/Downloads/Guidelines.pdf*, accessed 26 November 2015; Lee H Rosenthal 'Metadata and Issues Relating to the Form of Production' (2006-2007) 116 *The Yale Law Journal* available at *http://www.yalelawjournal.org/forum/metadata-and-issues-relating-to-the-form-of-production*, accessed on 20 November 2015.
[230] The Sedona Guidelines ibid at 29 & 30.
[231] South African Law Reform Commission Discussion Paper 131 (Project 126) *The Review of the Law of Evidence* (2015) (SALRC) para 3.54; See part 4.3.3 above.

with an ordinary e-signature can perform functions of authentication by signature and a seal.[232] It is submitted that this approach is non-discriminatory of e-signature technologies for purposes of document authentication, while it secures reliable means of authentication. It will promote equivalent legal treatment of offline and offline spheres in hierarchies of document authentication.

While the Directive does not regulate seals, the eIDAS Regulation does. It creates an electronic seal (e-seal) and defines it as 'data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity'.[233] It subsequently gives legal effect to any e-seal that a user applies and recognises it as admissible in court.[234] It then creates a qualified electronic seal (qualified e-seal).[235] The definition or features of a qualified e-seal correspond with the definition of QeS. In fact, a QeS can meet a requirement of an advanced e-seal.[236] The eIDAS Regulations' definition of an e-seal is technology neutral for its acceptance of any technology, such as metadata, that will sufficiently show data's origin and integrity while the qualified seal is not.

In summary, the Lesotho Bill, SADC ML and ECTA provisions on use of a SeS for document authentication are not technology neutral. It is recommended that the instruments should adopt a combination of the two approaches discussed above for document authentication. That is, the instruments should recognize an ordinary e-signature as sufficient for document authentication, provided it meets CUECIC's reliability standard. As chapter four illustrates, one of the factors which determine the reliability of an e-signature is the purpose of a transaction.[237] Hence guidelines must propose the use of an e-signature with a high reliability level, and yet practicable. This can be achieved by proposed use of the ordinary e-signature supported by metadata that shows it is free from manipulation. In fact, a presumption that an ordinary e-signature that identifies a signer and shows their intention, supported by metadata is attributable to the signer suggested earlier can support the document authentication exercise. This would effectively do away with the requirement of a seal or stamp. Where the law requires additional requirements for authentication such as attachment

[232] See part 2.9.11 above for other methods of online authentication that can enhance information security.
[233] Article 3 (25) of eIDAS Regulation.
[234] Article 35 (1) of eIDAS Regulation.
[235] Article 3 (27) of eIDAS Regulation: '"qualified electronic seal" means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal'; See part 2 (26) of eIDAS Regulation.
[236] See para (58) of eIDAS Regulation.
[237] See part 4.3.3 above.

of a certificate of authentication or an Apostille[238] the guidelines must indicate how an authenticating officer should meet the formalities as is conducted in the USA. This would be an efficient technology neutral method of document authentication.

5.6.3.4 Sustainability of SeS legislative provisions

Chapter two indicates that a regulator must draft e-signature regulation in a way that it will accommodate and endure technology developments without the need for amendment.[239] This is due to rapid technology development which advancements may lead to new bases for e-signature.[240] E-signature regulation should be capable of accommodating these changes.

Research shows that advanced e-signatures are not broadly used in the EU due to, amongst others, the difficulty of designing a fitting legal framework for technology that changes fast so as to properly respond to security risks.[241] For example new standards are developed regularly and algorithms for AeS constantly change once a weakness is detected.[242] Therefore bodies involved in regulation of QeS must look at the technologies with an open mind and not restrict themselves to what is available and known today.[243]

The Utah Act is an example of failed law in e-commerce. In 1994, Utah became the first USA state to enact e-commerce legislation and it prescribed use of the digital signature in e-transactions.[244] However, after its enactment, digital signature technology was not used extensively; this was exacerbated by users' realisation that security and reliability of digital signature technology could be undermined.[245] Online users introduced and used e-signature technologies not covered by the Utah Act. The Act was eventually repealed for, among other reasons, its failure to keep up with e-signature technology developments.

It is worth noting that the Lesotho Bill and SADC ML's definition of a SeS is general enough to accommodate future technologies that will meet the specific features. However, if technologies that do not have features of a SeS are created in future, but such technologies do a better job and are more cost effective than a SeS, the legislation on SeS will have to be

[238] For example the Authentication of Documents Proclamation in part 2.8.
[239] See parts 3.3.3.3.1 & 3.3.3.2.2 above.
[240] For examples of developments in authentication technologies see ChamberSign *Position paper in light of the review of the esignature framework* (October 2010) 4; Dumortier et al op cit note 64 at 136-7.
[241] Graux op cit note 63 at 14.
[242] Graux op cit note 63 at 14.
[243] Graux op cit note 63 at 14.
[244] Utah code ann §§ 46-3-201 to 46-3-504 (1998).
[245] Robert A Wittie and Jane K Winn 'Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA' (2000-2001) 56 *The Business Lawyer* 293 at 294.

amended to accommodate the new technologies. Hence the sustainability of the instruments' SeS provisions is limited.

The next section analyses the technology neutrality of the Lesotho Bill and SADC ML's ordinary e-signature.

5.7 To what extent are ordinary e-signature provisions technology neutral?

Section 2 of the Lesotho Bill interprets an 'electronic signature' as,

> 'data, including an electronic sound, symbol or process, executed or adopted to identify a party and to indicate a party's approval or intention in respect of the information contained in the electronic communication and which is attached to or logically associated with such electronic communication'.

This definition has three components, namely, the scope of data that forms an e-signature, effects of the data and the way the data links to the signed e-communication. These components help analyse the technology neutrality of an e-signature as discussed below.

5.7.1 The scope of data that forms an e-signature

The Lesotho Bill's definition of e-signature illustrates that it meets three principles underlying technology neutrality. That is, it does not discriminate nor prefer one e-signature technology over another; it is sustainable and it enables innovation.[246] This is because the words 'data including…' connote that the Lesotho Bill embraces all forms of existent e-signature technologies, and will accommodate new e-signatures technologies developed in future. Section 9 (2) of the Lesotho Bill verifies the non-discriminatory nature of e-signature by stating that an e-signature should not be denied validity due to its electronic form. The accommodative nature of the definition promotes innovation of e-signature technologies.[247] The SADC ML gives an identical definition for e-signature.[248] The instruments' interpretation of e-signature echoes the MLES' definition of e-signature.[249]

Interestingly the ECTA defines an e-signature broadly like the Lesotho Bill yet the ECT Amendment Bill contemplates something different. The ECTA defines e-signature as

[246] See part 3.3 above; para 5 of Guide to MLES & para 155 of Explanatory note on CUECIC.
[247] See part 3.3.3.2.2 above.
[248] Section 1 (11) of SADC ML.
[249] Article 2 (a) of MLES in part 4.4.2 above.

'data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature'.[250] It continues to define 'data' as 'electronic representations of information in any form.'[251] These definitions are broad enough to cover any form of e-signature technology without distinction, together with future technologies. For example, in *Spring Forest Trading*[252] the court stated that if data in an email is used to serve as a signature, and is logically associated with contents of the email, such as a type written name at the foot of an email message, it constitutes an electronic signature and sufficiently authenticates contents of the email.

On the other hand, the ECT Amendment Bill proposes a new definition of e-signature. It does away with the definition of 'data'[253] in the ECTA and then substitutes the definition of e-signature with

> 'a sound, symbol or process that is; uniquely linked to the signatory; capable of identifying the signatory; created using means that the signatory can maintain and which are under his control: linked to the data to which it relates in such a manner that any subsequent change of the data can be detected; and is intended by the user to serve as a signature.'[254]

This proposed definition consists of features of an AeS set out in s 38 of the ECTA, except for the face to face identification provision. The ECT Amendment Bill has also adopted the Directive's definition of AeS and art 6 (3) of the MLES. Consequently, the proposed definition of e-signature impliedly prefers the digital signature technology based on the PKI system amongst currently available technologies, even if it is general enough to fit possible future technologies. Accordingly, it discriminates against currently available technologies, addresses conduct of signing, and may impede future developments on e-signature. Thus, the proposed definition is contrary to the minimum standard of signature set out in the definition of e-signature in the MLES and fulfilment of signature requirement in the MLEC.[255]

Similar to Lesotho and the ECTA, the UETA defines an e-signature as 'an electronic sound, symbol, or process attached to or logically associated with a record and executed or

[250] Section 1 of the ECTA.
[251] Section 1 of the ECTA
[252] *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 (21 November 2014). at 12.
[253] Section 1 (p) of ECT Amendment Bill.
[254] Section 1 (u) of ECT Amendment Bill.
[255] Article 2 (a) and Art 7 respectively; Eiselen 'Fiddling with the ECT Act' op cit note 110 at 2810.

adopted by a person with the intent to sign the record.'[256] It does not require a particular technology to produce a valid signature.[257] It further defines 'electronic' as 'relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.'[258] This definition is broad enough to accommodate developing technologies in the future, hence its sustainable nature.[259] E-SIGN is similarly flexible; it allows e-signature developments without a need for a new law.[260]

5.7.2 Effects of data in an e-signature

The Lesotho Bill and SADC ML's interpretation of an e-signature spell out the effects that data (an e-signature) should have in e-communications. They stipulate that the e-signature is to identify a signer and to indicate the signer's approval of or intention in respect of the contents of an e-communication. They therefore require an e-signature to authenticate a document. This way, the instruments address effects of the act of signing hence promote equal treatment of offline and online users.[261]

Likewise, the ECTA addresses effects of signature. Its definition of e-signature is 'data …intended by the user to serve as a signature'.[262] The ECTA further states that the requirement of e-signature is met if a method is used that identifies a signer and their approval of information communicated and the method was reliable.[263] The ECTA's provisions on e-signature therefore also strive for equivalent legal treatment of offline and online users of signature. Although the ECT Amendment Bill addresses the effect of a signature in that the signer will attach a symbol or process with the intent for it to be a signature, the challenge is that only technologies which meet its stipulated features will qualify as the e-signatures.

Equally, the eIDAS Regulation addresses effects of signature in its definition of e-signature. It defines an e-signature as 'data in electronic form which is … used by the signatory to sign.'[264] UETA's definition of e-signature focuses on the effect of signature as well.[265] The crucial component of the definition is the signer's intent to attach a symbol to a

[256] § 2 (8) of UETA.
[257] § 2 Comment 7 of UETA.
[258] § 2 (5) UETA.
[259] § 2 Comment 4 of UETA; Koger op cit note 85 at 507.
[260] 15 USC § 7006 (2) & (5): Michael J Hays 'The E-SIGN Act of 2000: The triumph of function over form in American contract law' (2000 – 2001) 76 *Notre Dame L Rev* 1183 at 1200.
[261] See parts 3.3.3.1.1 & 3.3.3.1.2 above.
[262] Section 1 of ECTA.
[263] Section 13 (3) of ECTA.
[264] Article 3 (10) of eIDAS Regulation. See difference from art 2 (1) of Directive which defined e-signature as electronic data that serves as a method of authentication.
[265] § 2 (8) of UETA.

record with a purpose to sign it and to 'do a legally significant act'.[266] Without such intent, the adopted symbol does not constitute a signature.[267]

5.7.3 How e-signature data links to e-communication

The Lesotho Bill and SADC ML state that data is to be 'attached to or logically associated with' e-communication. This connotes that the e-signature technology may be in a file distinct from the e-communication that is signed and is sent as an attachment to the message.[268] It is noted that in its definition of e-signature, the MLES adds that an e-signature is data 'in' a data message. That is, that an e-signature can also be found within an e-communication when it is opened and read.[269] It is argued that the instruments' definition of e-signature will be more comprehensive if they include the word 'in' among links between e-signature data and the e-communication.

In comparison, the EU Directive had a slightly different definition of e-signature.[270] Although it accommodated all e-signatures capable of showing intent, it did not provide the necessary link that the e-signature should authenticate the data it is attached to.[271] The eIDAS regulation has improved the definition of an e-signature. It states that '[t]he electronic signature is to be used by the signatory to sign the data.'[272] However, both instruments establish authentication between software protocols alone, not human beings. Hence it is unclear whether they authenticate the origin of communication or the identity of the signer.[273] On the contrary, the Lesotho Bill and SADC ML establish a link between the e-signature and communication signed.

Both UETA and E-SIGN require that an e-signature must be attached to or logically associated with an electronic record.

5.7.4 Definition of 'signed' or 'signature'

The Lesotho Bill defines the word(s) 'signed' or 'signature' in a manner that compliments the definition of e-signature and promotes a technology neutral spirit. It states that

[266] See § 2 Comment 7 of UETA.
[267] § 2 Comment 7 of UETA. The signer's intent is determined by looking at the context in which the symbol was attached (Thomas J Smedinghoff 'The Legal Challenges of Implementing Electronic Transactions' (2008) 41 *UCC Law Journal* 1).
[268] Mason op cit note 56 at 102.
[269] Mason op cit note 56 at 102.
[270] Article 2 (1) of Directive.
[271] Mason *Electronic Signatures in Law* 3 ed (2012) 115 & 117, it can only be inferred that the signer attached the data with the intention to prove his connection to the communication.
[272] Mason op cit note 56 at 151.
[273] Mason op cit note 56 at 152.

> '"signed" or "signature" and its grammatical variations include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods.'[274]

The Lesotho Bill's language is therefore open to accommodate any form of current and future technologies and is concerned with the effect of signature to authenticate a record.

The definition of signature in the Lesotho Bill is analogous to the definition some courts have given to the meaning of sign in offline transactions.[275] It therefore attempts to strive for equivalence of offline and online transactions. It follows that the Lesotho Bill and SADC ML's definition of e-signature meets the presumptions of technology neutrality.

5.8 Conclusion on technology neutrality of the Lesotho Bill and SADC ML

The above discussions indicate that the Lesotho Bill's concept of an ordinary e-signature is technology neutral while the Lesotho Bill's and Digital Signature Regulations' provisions on a SeS are both technology neutral and technology specific. This is because although the Lesotho Bill's definition of a SeS is general enough to fit future technologies, it implicitly prefers the digital signature based on a PKI amongst currently existing technologies; the SeS provisions further treat a SeS as superior to ordinary e-signatures and address conduct of signing instead of effect of signing contrary to the technology neutrality principle. Lesotho is at risk of drafting laws similar to the EU and South Africa's instruments which regulate means of signing with an AeS and QeS. Moreover, the SeS provisions' sustainability is limited as they may not be able to sustain future technological developments that have different features to the SeS. The Lesotho Bill's SeS therefore falls short of meeting the technology neutrality standard of the MLEC and CUECIC.

The SADC ML on the other hand is commended for legally recognising e-signatures when the laws requires signature. It complies with technology neutrality principles of non-discrimination and sustainability of regulation to this extent. It further strives to place online and offline users on the same level by addressing effects of signature. It thus closely aligns with CUECIC. Its provisions on document authentication and grading of e-signatures deflect from this though.

---

[274] Section 2 of the Lesotho Bill.

[275] See the dissenting judgement of Bell J in *Van Vuuren v Van Vuuren* (1854) 2 *Searle* 116 at 121 cited in *Mellvill & Ano v The Master & Ano* 1984 (3) *SA* 387 at 389; See also part 2.4 above.

The South African and EU instruments are not fully accommodating of technology neutrality principles with their favouring of AeS and QeS while the USA instruments comply with technology neutral principles of e-signature regulation set by CUECIC. Consequently, for this study which advocates technology neutral regulation, the USA instruments are preferred. The subsequent section discusses the functional equivalence of the Lesotho Bill and SADC ML.

5. 9 The extent of functional equivalence of a SeS

This section assesses whether the Lesotho Bill and SADC ML's provisions render a SeS a functional equivalent of a handwritten signature. It conducts the same assessment on their e-signature provisions. The instruments' provisions are measured against CUECIC criterion that establishes functional equivalence between electronic authentication methods and the handwritten signature.[276] CUECIC's criterion is divided into three parts for ease of assessment, namely the method of signature sufficient to meet the law's requirement of signature, functions that the method should perform and the reliability standard of such a method.

5.9.1 The sufficient method of signature where law requires signature

CUECIC's criteria of functional equivalence states that where law requires signature, any method that identifies a signer and shows their intention with respect to the signed information will sufficiently meet the signature requirement.[277] Conversely, the Lesotho Bill states that where law requires a manuscript signature, the requirement will be met by the SeS.[278] The Lesotho Bill implies that any ordinary e-signature which is not a SeS does not meet the law's requirement of signature. Thus, the Lesotho Bill's provision contradicts CUECIC's criteria of functional equivalence to this extent.

5.9.2 Functions to be met by an e-signature method

An e-signature method must be used to identify the signer, and to indicate their intention with respect to information in the e-communication.[279] The Lesotho Bill's definition of an ordinary e-signature reflects that the e-signature performs functions laid down by CUECIC's criteria of

[276] Article 9 (3) of CUECIC & para 13 of Explanatory Note on CUECIC in part 4.5.2 above.
[277] Article 9 (3) (a) of CUECIC.
[278] Section 9 (1) of the Lesotho Bill.
[279] Article 9 (3) (a) of CUECIC; para 159 of Explanatory Guide on CUECIC.

functional equivalence plus approval of information as required by the MLEC.[280] The SeS must also perform the two functions required by CUECIC.[281] Thus the Lesotho Bill requires all e-signatures to observe signature functions stipulated by CUECIC irrespective of form.[282]

It is noted that the ECTA's provisions on the ordinary e-signature closely follow CUECIC's criteria of functional equivalence.[283] The ECTA states that when parties to an e-transaction require an e-signature, that e-signature should first be capable of identifying a party.[284] That is, it requires the e-signature to be sufficient to link a person to a message, hence provides the functions of identification and attribution.[285] Secondly, the e-signature must be capable of indicating a party's approval of information that is communicated.[286] That is it should confirm the party's assent and authentication.[287] The ECTA's requirement that an e-signature should indicate a party's approval of information is based on the MLEC's criteria of functional equivalence.[288] However, this requirement is outdated as CUECIC has improved it to an e-signature to show a party's intent with respect to information.[289] Hence the ECTA's ordinary e-signature's functions are similar to those of the Lesotho Bill's ordinary e-signature and SeS.

5.9.3 The standard of reliability for method used for signature

CUECIC gives two alternative standards of reliability that a method used to fulfill the law's requirement of signature should meet to be a functional equivalent of a handwritten signature. These are reliability in principle and reliability in fact.

5.9.3.1 Reliability in principle

CUECIC states that where law requires signature the method used should be as reliable as appropriate for the purpose which the e-communication was created, in the circumstances.[290]

---

[280] Section 2 of the Lesotho Bill.
[281] Section 9 (3) (a) of the Lesotho Bill.
[282] It is noted that features of the SeS provide more functions than those expected of a handwritten signature. For example, it focuses on integrity, confidentiality and security criteria for an e-signature. These cannot always be performed by a handwritten signature (Sylvia Mercado Kierkegaard 'E-contract formation: U.S. and EU perspectives' (2007) 3 *Shidler J L Com & Tech* 1).
[283] LF Van Huyssteen, GF Lubbe & MFB Reinecke *Contract General Principles* 5 ed (2016) 164.
[284] Section 13 (3) (a) of the ECTA.
[285] Van der Merwe et al *Information* op cit note 47 at 178.
[286] Section 13 (3) (a) of the ECTA. See *Spring Forest Trading* supra note 252 at 9; *Rumarch Investment Holdings (Pty) Ltd v Old Fashioned Fish and Chips (Pty) Ltd* unreported case no 21168/2014 of 25 March 2015.
[287] Van der Merwe et al *Information* op cit note 47 at 178.
[288] See Artictle 7 (1) (a) of the MLEC in part 4.3.3 above.
[289] See part 4.5.2 above.
[290] Article 9 (3) (b) (i) of CUECIC.

This is a 'flexible approach to the level of security to be achieved by the method of identification used'.[291] The level of security is provable by evidence.

Interestingly, the Lesotho Bill states that the law's requirement of signature will be met if the method used was as reliable as appropriate in the circumstances, but the method it anticipates is the SeS.[292] It is submitted that the Lesotho Bill measures the reliability of a signature method based on the high security level technologies used in a SeS. It does not permit users to consider other factors apart from technical aspects to determine the reliability of an e-signature. Thus, it limits the flexibility of the security level that an identification method is to meet to be a functional equivalent of a handwritten signature. This is contrary to the reliability principle reinforced by CUECIC in its interpretation of functional equivalence.[293]

On the other hand, the Lesotho Bill's definition of an ordinary e-signature is silent on the standard of reliability that an ordinary e-signature is to meet. It simply states that an e-signature should not be denied legal effect due to its electronic form.[294]

Despite the Lesotho Bill's failure to meet CUECIC's reliability in principle standard for e-signatures, it consists of rules that facilitate admissibility and assessment of the evidential weight of e-evidence. Its section 20 provides that

> (1) In any legal proceedings, nothing in the application of the rules of evidence shall [apply] so as to deny the admissibility of an electronic communication in evidence:
>
> a. on the sole grounds that it is constituted by an electronic communication; or
>
> b. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
>
> (2) Information in the form of an electronic communication must be given due evidential weight.
>
> (3) In assessing the evidential weight of an electronic communication, regard must be had to:
>
> a. the reliability of the manner in which the electronic communication was generated, stored or communicated;
>
> b. the reliability of the manner in which the integrity of the electronic communication was maintained;
>
> c. the manner in which its originator was identified; and

[291] Paragraph 161 of Explanatory Note on CUECIC; See parts 4.3.3 & 4.5.2 above.
[292] Section 9 (1) read with s 9 (3) of the Lesotho Bill.
[293] See Article 9 (3) (b) (i) of CUECIC; Paras 162 & 163 of Explanatory Note on CUECIC in part 4.5.2 above.
[294] Section 9 (2) of the Lesotho Bill.

d. any other relevant factor.

Section 20 (3) (a) and (b) deal with the chain of evidence and a party's proof that e-communication consists of its original contents, while s 20 (3) (c) deals with authorship as part of authentication.[295] It is noted that the Lesotho Bill adopted the contents of art 9 of the MLEC on admissibility and evidential weight of e-communication.[296]

Moreover, the Lesotho Bill creates a presumption in favour of e-communication developed in the ordinary course of business, which presumption is non-existent in the MLEC. It provides that such e-communication or a certified copy thereof is admissible as evidence of facts contained in it upon its mere production in proceedings provided it is supported by an affidavit of a person who controlled the system at the time of development of the e-communication.[297] It follows that any e-signature method attached to e-communication developed in the ordinary course of business will have a high evidential weight.

By contrast, the SADC ML stipulates that where the law requires a signature, an e-signature will suffice.[298] This is provided the method is used to identify and signify the signer's intention towards the information and the method is as reliable as appropriate for communication.[299] Consequently, the SADC ML does not assess the reliability of a signature method based on high security level technologies alone. Instead it considers legal, technical and commercial factors involved to determine whether a method used was appropriate. Additionally, it facilitates the use of e-evidence if required to prove the reliability of the method used for signature. This is provided by its s 20 on admissibility and evidential weight of e-evidence.[300] Hence the SADC ML aligns with CUECIC to the extent of the functions that an e-signature method must perform and its reliability in principle standard. Nonetheless, the SADC ML is silent about CUECIC's standard of reliability in fact. It is noted that the SADC ML's presumptions of validity and proper application of an SeS indicate that it does not apply CUECIC's reliability criteria on a SeS.

[295] Van der Merwe et al *Information* op cit note 47 at 120.
[296] See part 4.3.3 above. See also the Lesotho Computer Crime and Cybercrime Bill of 2013 s 27 (1).
[297] Section 20 (4) of the Lesotho Bill.
[298] Section 7 (1) of SADC ML.
[299] Section 7 (2) of SADC ML.
[300] See s 20 of the SADC ML which is similar to s 20 of Lesotho Bill.

5.9.3.2 Reliability in fact

Alternatively, CUECIC states that a method used where law requires signature is sufficiently reliable if it is proved either in itself or with additional evidence, to have identified the signer and indicated their intention regarding e-communication.[301] The purpose of this alternative standard is to prevent parties from denying a signature on the ground that it is not 'as reliable as appropriate' yet the identity of the signer nor their act of signing is not disputed.[302] CUECIC therefore permits parties to adduce evidence to prove that the two pertinent functions of signature were complied with. However, the Lesotho Bill does not have a provision that establishes this alternative e-signature reliability standard from CUECIC.

Though the ECTA stipulates that the AeS will meet the law's requirement of signature, it does not require the AeS to perform functions of signature provided by CUECIC or subject it to CUECIC's reliability standards.[303] It simply states that the AeS should be regarded as a valid signature.[304] The ECTA therefore considers the technology of the AeS determinative of the e-signature's reliability which is contrary to CUECIC's principles of reliability.

However, the ECTA's ordinary e-signature applies CUECIC's standard of reliability in principle.[305] In other words evidence of legal, technical and commercial factors will help determine the appropriateness of the e-signature, while procedures used at the time of signature and purposes of a transaction will determine its reliability.

Although the ECTA does not expressly provide for CUECIC's reliability in fact standard for e-signatures, it applies it in practice. This was reflected in the case of *Spring Forest.*[306] The court held that a party cannot contend that there was no reliable method used to identify the parties and show their approval of the information in an email if the identities of the parties who typed their names into email communication are not disputed, there is ample evidence from the emails submitted that the parties intended to cancel their agreement and the reliability of the emails was not disputed. Hence the typed name was a sufficiently reliable signature.[307] The ECTA's provisions on ordinary e-signature are therefore a good attempt to create a functional equivalent of a handwritten signature.

[301] Article 9 (3) (b) (ii) of CUECIC & part 4.5.2 above.
[302] See part 4.5.2 above.
[303] Section 13 (1) of the ECTA.
[304] Section 13 (4) of the ECTA.
[305] Section 13 (3) (b) of the ECTA.
[306] Supra note 252 at 12-13.
[307] Van Huyssteen et al op cit note 283 at 164. See also *Novartis v Maphil* [2015] ZASCA 111.

Like the Lesotho Bill and the SADC ML, the ECTA integrated provisions of the MLEC on admissibility of data messages[308] to facilitate proof of reliability of e-signature methods, especially where there is suspicion of manipulation.[309] The provisions of the ECTA imply that data messages are subject to normal rules of admissibility of evidence.[310] Excluding them from such would be contrary to the principle of functional equivalence.[311] Thus where a data message to be presented as evidence is a functional equivalent of a document, for example a computer printout, it must be relevant, authentic and original to be admissible.[312] The ECTA consists of provisions that deal with the concepts of original and authentic.[313] Real evidence such as videos on the other hand must be relevant and meaningful to be admitted as evidence.[314]

Once courts admit a data message, they must give it due weight.[315] The ECTA sets out guidelines on assessing the evidential weight of data messages.[316] Just like the Lesotho Bill and SADC ML, the ECTA adopted the guidelines from the MLEC.[317] When applying these guidelines, courts may call experts to assist in clarifying the technical procedures involved.[318] Thus, the ECTA caters to the admissibility and assessment of weight of data messages as evidence which will assist in proof of the reliability of an e-signature.[319]

Like the Lesotho Bill and SADC ML, the ECTA does not subject documents made in the ordinary course of business to the assessment of evidential weight. [320] Further, the ECTA

[308] See s 15 (1) of the ECTA; *Jafta v Ezemvelo KZN Wildlife* [2008] 10 BLLR 954 (LC).
[309] Debbie Collier 'Evidently not so simple: Producing computer print-outs in court' (2005) 13 *Juta's Business Law* 6.
[310] DW Collier 'Electronic evidence and related matters' in PJ Schwikkard & SE van der Merwe *Principles of evidence* 3ed (2012) 411.
[311] *LA Consortium & Vending CC v MTN Service Provider (Pty) Ltd* 2011 (4) *SA* 77 (GSJ) A. See also *Ndlovu v Minister of Correctional Services* [2006] 4 *ALL SA* 165 (w) where the court applied rules on hearsay on data messages submitted as evidence in court.
[312] *Ndlovu* ibid at 172.
[313] Section 14, 17 & 15 (1) (b) of the ECTA; Collier 'Evidently not so simple' op cit note 309 at 7; Collier 'Electronic evidence and related matters' op cit note 310 at 415. See also ss 18 & 19 of the ECTA. Nonetheless, see C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 461 for criticisms on the ECTA provisions on originality and authenticity.
[314] Collier 'Electronic evidence and related matters' op cit note 310 at 410 & 411; Julien Hofman & Justin de Jager 'South Africa' in Stephen Mason (ed) *Electronic evidence* 3ed (2012) 761 at 776.
[315] Collier 'Evidently not so simple' op cit note 309 at 6; Hofman et al 'South Africa' ibid at 779.
[316] Sections 15 (2) & (3) of the ECTA; See *Ndlovu* supra note 311 at 175; *Firstrand Bank v Venter* [2012] *ZASCA* 117.
[317] Article 9 (2) of the MLEC.
[318] J de Jager 'Electronic evidence' in PJ Schwikkard & SE van der Merwe *Principles of evidence* (2016) 444; *Jafta* supra note 308.
[319] Julien Hofman in 'Electronic evidence in criminal cases' (2006) *SACJ* 257 at 274 states that South African law has achieved functional equivalence in the treatment of e-evidence like other evidence.
[320] Section 15 (4) of the ECTA. Collier ín 'Evidenty not so simple' op cit note 315 at 8-9 states that s 15 (4) can be interpreted 'as requiring the certification of both types of documents identified by the court.'; *Firstrand Bank*

and SADC ML create a rebuttable presumption in favour of an AeS/SeS by regarding it as valid and properly applied, while the Lesotho Bill equates a SeS to a handwritten signature.[321] Thus an AeS/SeS has a heavy evidential weight in proceedings. This is not functionally equivalent.[322]

The South African Law Reform Commission (SALRC) found the ECTA lacking for want of a proper guide on 'how to establish reliability in the context of electronic evidence.'[323] The SALRC recommended that the ECTA undergo amendment modeled on the Small Commonwealth Jurisdictions Model Law of Electronic Evidence[324] (Model Law on e-evidence) and its attitude towards e-evidence.[325] The Model law focuses on the reliability of a system that produced a document to lay a basis for admissibility of the document, it does not focus on the document itself.[326] This view is supported by the Irish Law Reform Commission[327] which focuses on the reliability of processes and devices that store and transmit a document to determine its authenticity and integrity.[328] As a result, the SALRC proposed a guideline on how to establish the authenticity and integrity of documentary evidence and its evidential weight.[329] It proposes that these be determined by evidence that the computer system that created a document was working well and evidence that the integrity of the document remained intact.[330] The proposed guideline also notes that a signature can help with authentication of a document.

Nonetheless, the Model law on electronic evidence accepts any form of evidence to prove an e-signature, it does not depend on the reliability of system used to create a signature. It provides that where a law of evidence requires a signature, an e-signature will meet that requirement, and such e-signature may be proved by any manner which shows that a security procedure or symbol was executed to prove that the record is that of the signer.[331] Hence the

---

supra note 316; *Golden Fried Chicken (Pty) Ltd v Yum Restaurants International (Pty) Ltd* 2005 BIP 269 (T)/ [2005] ZAGPHC 311; *Ndlovu* supra note 311 at 173.

[321] Section 13 (4) of the ECTA.

[322] SALRC op cit note 231 para 3.17; See also Hofman et al 'South Africa' op cit note 314 at 780 & Theophilopoulos op cit note 313 for criticisms against the presumption. In its para 4.122, the SALRC suggests the replacement of s 15 (4) with different provisions.

[323] SALRC op cit note 231 at para 3.58.

[324] Draft Model Law on Electronic Evidence 2002.

[325] SALRC op cit note 231 at para 3.58.

[326] SALRC op cit note 231 at para 3.55.

[327] SALRC op cit note 231 at para 3.59.

[328] Irish Law Reform Commission *Documentary and electronic evidence CP 57 – 2009* at 25.

[329] SALRC op cit note 231 at para 4.114.

[330] SALRC op cit note 231 at para 3.61 & 3.58.

[331] Clause 12 (1) & (2) of the Model law on electronic evidence.

Model law on electronic evidence's approach on proof of an e-signature shares the same spirit with CUECIC.

Moreover, the South African law lacks detailed procedures on collection, preservation and presentation of e-evidence.[332] The SALRC proposes that a handbook should be developed which gives guidance to legal practitioners and experts on the collection and presentation of e-evidence in court.[333] It is noted that Lesotho does not have rules on this subject either.

The eIDAS Regulation which renders a QeS equivalent to a handwritten signature does not subject the QeS to CUECIC's e-signature reliability standards as well.[334] It depends on the high security level technology involved in a QeS to determine the signature's reliability. Further, the eIDAS Regulation defines an e-signature as electronic data that a signer uses to sign data in electronic form.[335] Impliedly, it indicates that an e-signature is data that identifies a party and shows their intention, hence it performs functions of a signature including those listed by CUECIC. However, the eIDAS Regulation makes no reference to standards that should determine the reliability of an e-signature.

UETA on the other hand defines an e-signature as an electronic process attached to a record that a person implements with intent to sign the record;[336] it further states that e-signatures will fulfill the law's requirement of signature.[337] Although the e-signature definition covers functions of signature under CUECIC, UETA receives criticism that its extensive scope gives legality to sub-standard signature technologies.[338] The reason is that it does not provide a reliability standard to be met by an e-signature. However, this is not correct. UETA and E-SIGN permit parties to prove in any court or proceedings that their authentication methods are valid.[339] UETA further states that evidence of a signature or record should not be rejected in proceedings due to its electronic form.[340] The USA notes that in the

[332] Collier 'Electronic evidence and related matters' op cit note 314 at 417; Hofman 'Electronic evidence' op cit note 319 at 274.
[333] SALRC op cit note 231 at paras 4.87 and 4.89.
[334] Article 25 (2) of the eIDAS Regulation. The repealed Directive had a better provision regarding functional equivalence as it stated that states must ensure that a QeS meets legal requirements of signature with respect to e-communication as a handwritten signature fulfils the requirements in paper (Article 5 (1) of the Directive).
[335] Article 3 (10) of the eIDAS Regulation.
[336] § 2 (8) of UETA; see also 15 USC 7006 (5) of E-SIGN.
[337] § 7 (d) of UETA. See *Rosenfeld v Zerneck* 4Misc3d193, 776MYS2d458 (Sup Ct Kings Co, NY May 4, 2004) where the court held that a typed name in an email was sufficient to show an intention to authenticate a contract for purchase of real property under the Statute of Frauds.
[338] G C Parry, M James-Moore & A P Graves et al 'Legal aspects of electronic signatures' 2008 available at *http://www.easysoft.nu/images/IDPIC/legal_Esignature.pdf*, accessed on 29 November 2015.
[339] See 15 USC 7031 (a) (2) (C) of E-SIGN.
[340] § 13 of UETA.

event of a dispute on an e-contract, evidence may need to be adduced to show compliance with E-SIGN. As a result, courts adopt a comprehensive approach which involves

> 'audit trail tracks [of] all signer actions; secure encryption so documents can be read and signed only by designated users; unique Signatures created by each user, accessible only to that user, and stored securely online; Sign Document Blocks so users can "initial" and "sign" specific areas of a document; User Authentication leveraging email, access code, and/ or third party ID check; Time-Stamping of every step in the document process; [and] Transaction Summary [that] provides complete document history.' [341]

This implies that UETA and E-SIGN e-signature meet CUECIC's standards of reliability. Hence the criticism does not hold.

It is noted though that not all countries have the same rules of evidence. Some countries apply an inquisitorial trial system while others apply the accusatorial system.[342] Under the accusatorial system, parties are responsible for presenting evidence in favour of their cases while the adjudicator remains passive.[343] The evidence may be oral and witnesses subjected to cross-examination. In contrast, the adjudicator in the inquisitorial system plays an active role by making fact-finding inquiries to discover the truth.[344] An important difference between the two systems is that an accusatorial system has a strict system of evidence such as rules relating to admissibility of evidence, while the inquisitorial system has a free system of evidence which dispenses of technical rules.[345] Hence while the accusatorial system is concerned with admissibility of evidence which is given due weight if admissible, the inquisitorial system is simply concerned with the weight a court grants to evidence.[346]

The inquisitorial system applies in civil law countries found in Europe, such as Sweden[347] and Germany,[348] while the accusatory system applies in common law or mixed law countries such as South Africa, Lesotho and the USA.[349] This is why Lesotho or the USA's e-

[341] DocuSign 'ESIGN Act & UETA' available on *https://www.docusign.com/esign-act-and-ueta*, accessed on 1 December 2015; Joseph J Schwerha IV, John W Bagby & Brian W Esler 'United States of America' in Stephen Mason (ed) *Electronic Evidence* 3ed (2012) 797.
[342] Van der Merwe et al *Information* op cit note 47 at 130.
[343] PJ Schwikkard & SE Van der Merwe *Principles of Evidence* 4 ed (2016) 11.
[344] Schwikkard ibid 12.
[345] Schwikkard ibid 14.
[346] Van der Merwe et al *Information* op cit note 47 at 140.
[347] Qualified Electronic Signatures Act (SFS 2000:832).
[348] Law Governing Framework Conditions for Electronic Signatures (Bundesgesetzblatt – BGB1. Teil I S. 876) of 21 May 2001.
[349] Van der Merwe et al *Information* op cit note 47 at 130.

signature instruments provide rules for admissibility and evidential weight of evidence, yet countries such as Sweden are concerned with due weight of evidence alone regardless of UNCITRAL's provisions on admissibility of evidence.

To summarise, the above discussion demonstrates that the Lesotho Bill's SeS does not meet CUECIC's criteria of functional equivalence, while its ordinary e-signature provisions only meet the functions of signature required by CUECIC, but are silent on reliability standards. On the other hand, the SADC ML's ordinary e-signature meets CUECIC's criteria while its SeS does not. Although the ECTA's AeS does not meet CUECIC's criteria, it's ordinary e-signature provisions closely follow CUECIC's criteria contrary to the position in Lesotho. UETA's e-signature observes CUECIC's criteria of functional equivalence as well while eIDAS Regulation's QeS does not. The discussion indicates that the Lesotho Bill and SADC ML align with rules of evidence provided by the MLEC to a large extent. The rules on evidence help prove the reliability of e-signatures. As much as the instruments' provisions on e-evidence are similar to the ECTA's provisions, research has reflected that the South African rules on e-evidence need reform for lack of guidance on how to prove documentary evidence and lack guidance on the collection and presentation of e-evidence. The SALRC is working towards improving e-evidence regulation with respect to these concerns. This said, the next section discusses the practicability of SeS provisions in Lesotho.

5.9.4 The practicable use of a SeS in Lesotho and SADC region

The assessment of the SeS's functional equivalence is not limited to the language of the statute, a SeS should also be feasible in practice.[350] To achieve this, the Lesotho Bill's provisions should not impose stricter standards of security and related costs in the online sphere than those imposed by signature rules in the offline sphere.[351] The three factors discussed below help assess the practicability of a SeS. These are costs of compliance with SeS provisions, changes in interaction of contracting parties and the need to seek legal and technical advice in the use of a SeS.

5.9.4.1 Costs of compliance with SeS provisions

The premise that a SeS is met by a digital signature based on the PKI system forms the basis of cost analysis of a SeS.[352] First, chapter two shows that it is expensive to set up a CA that

[350] See part 3.2.3.2.1 above.
[351] Para 16 of Guide to MLEC in part 4.3.2.1 & 3.2.3.2.1 above.
[352] See part 5.6.1 above.

has a good security system which can protect signing keys strongly.[353] Thus regulation that mandates use of a SeS can be costly to implement.[354]

Secondly, chapter two explains the processes that a PKI user must undergo to obtain a cryptographic key pair and public key certificate. These include the need to have trustworthy software to create a key pair and travelling to the CA to apply for and to collect a public key certificate.[355] The processes are onerous and inconvenient to the user. Yet an offline signer simply needs a pen and paper technology to make a signature.[356]

Thirdly, chapter two elaborates that the key holder's duty to protect and control their private key in PKI is an essential but arduous exercise.[357] The holder of a seal or stamp offline is also challenged with keeping the seal or stamp safe from theft or misuse. But a SeS is susceptible to more ways of compromise than a seal or stamp in the offline world. Furthermore, the holder of a seal or stamp must use the seal in conjunction with their signature for the seal or stamp to be legally recognised. Therefore, if the seal or stamp falls in the wrong hands, the thief will have difficulty using it for lack of the rightful holder's signature. Hence the responsibility of a seal/stamp holder offline is not as burdensome as that of a SeS.

Moreover, the Lesotho Bill's SeS will potentially impose more costs on its subjects through regulation and licensing of CAs and the authentication of certification products in support of SeS.[358] The ECTA and Accreditation Regulations together with the EU instruments reflect the kind of heavy burden the mandated use of an AeS or QeS imposes on their subjects.[359] The instruments introduce an unnecessary administration layer and costs that hinder e-commerce.[360]

Additionally Lesotho is a least developed country,[361] thus whether it has the infrastructure and resources necessary for the establishment and maintenance of a CA is questionable. A Readiness assessment report for CIRT in Lesotho of 2012 revealed a weak

[353] See part 2.9.10.2.6 above. See some requirements for a CA in reg 7 read with reg 1 of the Lesotho Digital Signature Regulations; reg 8 (1) (a) of the Lesotho Digital Signature Regulations; s 38 (3) of ECTA.
[354] Gregory op cit note 98 at 11.
[355] See part 2.9.10.2.1 above and the draft Lesotho Digital Signature Regulations.
[356] See part 2.8 above.
[357] See part 2.9.10.2.5 above.
[358] Section 25 of the Lesotho Bill.
[359] See part 5.6.3.1 above.
[360] Swales op cit note 47 at 260.
[361] 'UNDP in Lesotho' available at *http://www.ls.undp.org/content/lesotho/en/home/countryinfo.html*, accessed on 20 March 2016.

ICT infrastructure in the country.[362] The Lesotho Communications Authority (LCA) also conducted a study in businesses in the trading sector and manufacturing sector in Lesotho. The study reflected that 26% of the businesses had Internet connectivity while the rest were not connected due to lack of infrastructure such as network coverage and lack of electricity.[363] To accentuate this issue, consultants who drafted the Lesotho Digital Signature Regulations indicated that not all regulations in the draft are suitable to be included in Lesotho due to 'the infrastructure and associated costs in promulgating regulations for [SeS].[364] There is no evidence that Lesotho conducted a cost-benefit analysis study on the potential use of a SeS. Hence these available reports indicate that Lesotho will be economically challenged with establishment of a CA.

The Pretty Good Privacy (PGP) system is on the other hand less costly compared to a CA,[365] but its potential use in Lesotho is not promising. A PGP system relies on the technical competency of users and does not require establishment of a CA. However, studies have shown lack of ICT technical expertise in Lesotho. For example, the LCA study divulged that 77% of businesses with computers outsourced technical support services while a small number of the businesses relied on in-house technical support services.[366] The CIRT report also indicated that there is a 'small pool of highly skilled ICT personnel.'[367] As a result, the prospects of the PGP system succeeding in Lesotho are limited.

The lack of highly skilled ICT personnel in Lesotho implies that the country will have to train significant numbers of personnel on ICT to carry out activities of a CA or a PGP system appropriately.

The QeS has also proved to be costly in the EU. A report on the assessment of the Directive in 2003 indicated that SSCD used for QeS did not find their way into the market since the Directive set costly, high requirements for them.[368] In fact some commentators refer to the PKI system as 'highly inconvenient, intrusive and expensive.'[369]

---

[362] Anuj Singh & Jairam Ramesh (Report for Telecommunication Development Bureau) *Readiness assessment report to establish a national CIRT for Lesotho* (November 2012) at 18.
[363] M Mochebele op cit note 40 at 10. See also Wade Publications CC op cit note 40; World Economic Forum which ranks the extent of Lesotho's economy network readiness in the world in terms of infrastructure, affordability, skills and other factors (Silja Baller, Attilio Di Battista, Soumitra Dutta, Bruno Lanvin 'The Networked Readiness Index 2016' in *The Global Information Technology Report 2016* available at *http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.1_2016.pdf*, accessed on the 21 July 2017).
[364] Introduction to the Lesotho Digital Signature Regulations.
[365] See part 2.9.10.2.2 above.
[366] See Mochebele op cit note 40 at 377.
[367] Singh et al op cit note 362 at 24.
[368] Dumortier et al op cit note 64 at 11.
[369] Roger Clarke 'The fundamental inadequacies of conventional public key infrastructure' (June 27-29 2001) Paper presented at the 9th European Conference on Information Systems Bled Slovenia at 151.

With respect to South Africa, it is declared that 'the initial cost, administration, change of systems, fear of change as well as other factors, have clearly inhibited the widespread adoption of the technology.'[370] SADC state members face similar cost challenges in the implementation of SeS provisions. Apart from Lesotho and South Africa, other SADC states that mandate the use of a SeS to fulfil the law's requirement of signature include Zambia,[371] Botswana,[372] Swaziland,[373] Namibia,[374] the United Republic of Tanzania,[375] and Zimbabwe.[376] Seychelles on the one hand legally recognises digital signatures and not ordinary e-signatures;[377] while Mauritius, like the SADC ML recognises an ordinary e-signature when law requires signature.[378] The SeS cost challenges affect SADC countries irrespective of their development status.[379] It is submitted that the above cost challenges will have a negative impact on practicability of SeS rules in Lesotho and the SADC region.

5.9.4.2 Changes in interaction of contracting parties

A SeS necessitates parties contracting online to interact in a different manner from how they interact when contracting offline. Whereas offline the contracting parties enter into an agreement and sign their contract with a traditional signature,[380] parties transacting online

[370] Swales op cit note 47 at 261.
[371] Electronic Communications and Transactions Act No 21 of 2009.
[372] Electronic Communications and Transactions Act No 25 of 2013.
[373] Electronic Transactions and Communications Bill cited by Nthabiseng Motjolopane 'e-commerce: SADC Model Law on Electronic Transactions and Electronic Commerce' (28 August 2013) 2nd Stakeholder Workshop HIPSSA Project.
[374] The Use of Electronic Transactions & Communications Bill 2005.
[375] Tanzania Electronic Transactions Act No 13 of 2015.
[376] Electronic Transactions and Electronic Commerce Bill 2013.
[377] Electronic Transactions Act No 8 of 2001, Consolidated to 30 June 2014.
[378] The Electronic Transactions Act No 23 of 2000 (Mauritius ETA). Madagascar adopted the Electronic Transactions Law N° 2014-024 and Electronic Signature Law, Law N° 2014-025 on Electronic Signature (United Nations Information Service Press Releases UNIS/L/212 16 January 2015 available at *http://www.unis.unvienna.org/unis/en/pressrels/2015/unisl212.html*, accessed on 11 April 2015); The Democratic Republic of Congo has the Draft Law on Electronic Transaction (ITU in cyberwellness profile-Democratic Republic of Congo Report of 12 August 2014 available on at *http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Congo.pdf*, accessed on 18 November 2014); Malawi drafted the Draft Bill on Electronic Transactions and Management Bill 2013 (Gregory Gondwe in Biztechafrica.com at *http://www.biztechafrica.com/article/malawi-drafts-new-ict-bill/7024/#.VGsTKyKUfeI*, accessed on 18 November 2014); and Mozambique the Electronic transaction Act (ITU *Cyberwellness profile -Republic of Mozambique* (11 March 2015)). Though these states have drafted Bills and adopted Acts on e-transactions it is unclear what their position is on e-signature regulation as their instrument could not be traced.
[379] Least developed SADC countries include: Angola, Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mozambique, and Zambia (UNCTAD 'UN list of Least Developed Countries' available at *http://unctad.org/en/Pages/ALDC/Least%20Developed%20Countries/UN-list-of-Least-Developed-Countries.aspx*, accessed on 20 March 2016). Most developed SADC countries include South Africa, Namibia, Botswana, Mauritius & Seychelles (Africa Ranking 'Top 10 most developed African countries' available at *http://www.africaranking.com/most-developed-african-countries/5/*, accessed on 20 March 2016).
[380] See part 2.6 above.

have to obtain a public key certificate from a CA to use a SeS.[381] Hence, the interaction between contracting parties is changed by intervention of a CA. The complexities and inconvenience of interacting with a CA need not be reiterated. Consequently, the need to secure services of a CA before signature amounts to a drastic change in the parties' interaction; it will render the Lesotho Bill's SeS provisions less feasible.

5.9.4.3 The need for legal and technical advice in use of a SeS

Public key certificates involve standards such as the X.509. The standards are long and complicated.[382] A key pair applicant may need legal and technical experts' advice to complete the cumbersome application process for a key pair, to explain the certificate and terms of its use, including the management of the private key.[383] The technical expert's services come at a fee and are time consuming; this renders use of a SeS a daunting exercise and involves yet another party to an online transaction in addition to the CA. Therefore, the Lesotho Bill's SeS becomes less achievable.

It follows that the Lesotho Bill's SeS imposes obligations of a heavier burden than those of signature in the paper world. Hence the practicability of the SeS is limited.

On the other hand, the SADC ML's e-signature which meets the law's requirement of signature, does not impose a heavy burden on the law's subjects. Ordinary e-signatures are cost effective, user-friendly and do not change interaction of contracting parties. The SADC ML does however impose a heavy burden on online users where it mandates use of a SeS in document authentication including the use of a seal.[384] Hence the SADC ML's e-signature is more practicable compared to the SeS.

An example of a legislative instrument which was functionally equivalent in legal terms only but not feasible in practice is the Directive on its regulation of a QeS.[385] While a handwritten signature only requires accessible pen and paper technology, the QeS required costly complicated technologies.[386] For example, ordinary users had to seek technical assistance to install card specific software for each SSCD.[387] Hence only a limited number of

[381] See part 2.9.10.2.1 above.
[382] See part 2.9.10.2.2 above.
[383] See for example s 12 (2) & s 15 (5) of Accreditation Regulations on X.509 standard; Annex II (k) of Directive & art 24 (2) (d) of eIDAS Regulation.
[384] Section 23 & 24 of SADC ML.
[385] Reed *Cyberspace* op cit note 10 at 120; Article 5 (1) of Directive stipulated that a QeS will fulfil legal requirements of a handwritten signature.
[386] Reed *Cyberspace* op cit note 10 at 120.
[387] Dumortier et al op cit note 64 at 138; Report from the Commission to the European Parliament and the Council - Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures

online users employed the QeS.[388] Despite this, the eIDAS Regulation recognises only the QeS as a functional equivalent of a handwritten signature. [389] Consequently, it has the same shortcoming of lack of feasibility. These are complicated measures that Lesotho should avoid.

Inversely, UETA does not impose a heavy burden on its subjects since it recognizes the ordinary e-signature when law require signature. In fact, E-SIGN restricts regulatory agencies from imposing unreasonable costs for use of e-records.[390] It encourages them to develop e-record requirements substantially equivalent to offline records to maintain functional equivalence.[391]

5.9.5 Conclusion on functional equivalence of SADC and Lesotho instruments

To conclude, the Lesotho Bill does not render a SeS a functional equivalent of a handwritten signature. Its provisions on SeS do not comply with CUECIC's criteria of functional equivalence and its practicability is limited due to its burdensome nature. However, the Lesotho Bill's ordinary e-signature is practicable and would fit CUECIC's criteria of functional equivalence save for lack of clarification on its reliability standard. By contrast, the SADC ML's ordinary e-signature meets the functional equivalence principle where law requires signature. It however deflects from the principle when it requires a SeS for document authentication. On the other hand, the ECTA's ordinary e-signature closely aligns with CUECIC's criteria and is practicable while its AeS is not a functional equivalent of a handwritten signature. In a similar vein, the eIDAS' QeS is not a functional equivalent of a handwritten signature. But the USA's instruments seem to render an ordinary e-signature a functional equivalent of a handwritten signature, without ignoring the law's requirements on document authentication. Therefore, the USA and ECTA's ordinary e-signature appear to be better models of functional equivalence, provided the ECTA renders the ordinary e-signature sufficient where law requires signature.

The discussion indicates that the Lesotho Bill and SADC ML align with rules of evidence provided by the MLEC to a large extent. The rules on evidence help prove the reliability of e-signatures. As much as the instruments' provisions on e-evidence are like the ECTA's provisions, research has reflected that the South African rules on e-evidence need

(2006) available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0120,* accessed on 2 December 2015 (Report from the Commission on Directive) para 3.3.2.

[388] Dumortier et al op cit note 64 at 138; Report from the Commission on Directive ibid para 5.2.

[389] Article 25 (2) of eIDAS Regulation.

[390] 15 USC § 7004 (b) (2) (C) II.

[391] 15 USC § 7004 (b) (2) (C).

reform for lack of guidance on how to prove documentary evidence and lack guidance on the collection and presentation of e-evidence. The SALRC has done considerable work towards improving the e-evidence regulation in this regard. The discussion further indicates that the Model law on electronic evidence permits any form of evidence to show that an e-record is that of a signer in line with CUECIC.

It is recommended that the provisions of the Lesotho Bill should be amended. It should recognise any e-signature that meets CUECIC's criteria as sufficient where law requires signature. It should clarify that the method used to sign must meet either of CUECIC's reliability standards. By doing so, the Lesotho Bill will not rely on high level technology of a SeS to provide a functional equivalent of a handwritten signatures. It will enable e-commerce users to apply accessible reliable e-signatures where law requires signature for different purposes. The amendment will further allow an e-signature's reliability to be determined by e-evidence where necessary.

Since there is no statute in Lesotho that deals with e-evidence apart from the Lesotho Bill's provisions,[392] it is recommended that Lesotho should draw lessons from the Model law on electronic evidence and the USA's approach on proof of e-signatures. That is, it should clarify that it permits parties to produce any form of relevant evidence such as passwords applied by signers, Sign document blocks showing where a signer initialed a document, time stamps showing the document processes, metadata, encryption methods used if any, and so on which will be given due evidential weight to prove the reliability and validity of e-signatures.

Additionally, further research and guidelines are required to determine how e-evidence may be collected, preserved and presented in court. The next question is whether the Lesotho and SADC instruments will be effective.

5.10 Effectiveness of Lesotho legislation and SADC ML

This study explicates that legislation is effective if it can achieve its social aims through its provisions.[393] This section assesses the potential effectiveness of the Lesotho Bill and SADC ML and identifies drawbacks which the regulator should avoid to achieve an effective regulatory system. For legislation to succeed, the rule's provisions should be understandable to its subjects.

[392] See the Criminal Procedure and Evidence (Amendment) Act 3 of 2001 which regulates admission of bank documents in proceedings.
[393] See part 3.4 above.

5.10.1 Will the Bill's provisions on SeS be understandable by its subject?

Chapter three explains that a rule that is not understood by its subjects due to over precise descriptions of the rule or complexity becomes meaningless, loses force and cannot achieve its objective.[394] The EU and South African instruments are illustrative of laws with over precise provisions that set detailed quantitative measures their subjects must comply with to obtain an AeS or QeS.[395] The instruments are also characterised by cross-referencing of provisions, which renders them over complex and unintelligible to the user. The EU report stated that although the Directive attempted to deal with risks in the PKI system, the complexities of qualified certificates and SSCDs meant to cover the risks are incomprehensible to the regular user.[396] It recommended that the Directive's Annexes are unnecessary, extreme, constitute an obstacle to the market and should therefore be removed.[397]

The Lesotho Bill states that the Minister shall make regulations for recognition of authentication services as a SeS and prescribe standards to be met by CA's in support of its SeS provisions.[398] Like South Africa and the EU, the regulations are likely to be clouded with excessive detail and over complexity. This will render the regulations incomprehensible to their subjects and consequently hamper the use of e-commerce.

However, the Lesotho Bill's e-signature provisions are simple and can be comprehensible to the law's subject. Hence they may help the instruments achieve their objectives.

5.10.2 Potential stability of legislative provisions on SeS

Stability of SeS legislative instruments over time will also affect their effectiveness.[399] If a new technology that works better or is more user-friendly than a SeS comes up, the instruments will have to undergo amendment to accommodate that new technology.[400] Subsequently, the rule's subjects will have to change their behavior to comply with the amended rule. If these amendments occur frequently the subjects will get weary of changing

[394] See part 3.4.1.1 above.
[395] See part 5.6.3.1 above.
[396] Carl Ellison & Bruce Schneier 'Ten risks of PKI: What you're are not being told about Public Key Infrastructure' (2000) 16 *Computer Security Journal* 1.
[397] Dumortier et al op cit note 64 at 134.
[398] Section 25 of the Lesotho Bill.
[399] See part 3.4.1.2 above.
[400] See part 3.3.3.3.1 above.

their conduct to comply with amended rule and eventually ignore the rule.[401] Thus the potential lack of stability of the SeS legislative provisions will negatively affect the instruments' effectiveness.

On the other hand legislative provisions on ordinary e-signature will be stable over time. They accommodate current and future e-signature technologies or authentication technologies that meet CUECIC's criteria. Hence ordinary e-signature provisions will help the instruments be effective.

5.10.3 Can the Lesotho Bill and SADC ML fulfil their objective due to the SeS?

The Lesotho Bill states that its purpose is 'to enable and facilitate electronic communications and transactions in the public interest'.[402] To do this, it intends to remove barriers to e-transactions which result from uncertainties from requirements of signature.[403] Further, the Lesotho Bill intends to promote the development of e-transaction services which are responsive to the needs of users,[404] and promote technology neutrality in the legislation of e-transactions.[405]

Though commended for its good objective, the Lesotho Bill's mandatory provisions on SeS signify that it not responsive to the needs of users and constitutes a barrier to e-transactions. The Lesotho Bill's imposition of SeS is thus contrary to the purpose and objectives of the Lesotho Bill.

Conversely, the Lesotho Bill's provisions on the ordinary e-signature will achieve and promote its objectives. They will assist e-commerce users understand how they can legally sign documents online in a secure and practicable manner. Legislative provisions that are comprehensible to their subjects and stable due to their functionally equivalent and technology neutral effect will put trust and confidence into the use of e-signatures.

The SADC ML on the other hand will, if implemented in domestic law, be able to meet its objective to a large extent. It states that it aims to provide an accessible, safe and transparent environment for e-commerce to flourish.[406] The SADC ML meets these objectives with its e-signature provisions except for its mandatory use of SeS.

---

[401] See part 3.4.1.2 above.
[402] Section 3 of the Lesotho Bill.
[403] Section 3 (c) of the Lesotho Bill.
[404] Section 3(k) of the Lesotho Bill.
[405] Section 3 (f) of the Lesotho Bill.
[406] Preamble of SADC ML.

The AeS in South Africa also fails to meet the objectives of the ECTA. Its overall goal is to facilitate the use of e-signatures so as to provide equal treatment to users of paper-based documentation and users of computer-based information,[407] in the public interest. But the above discussions reflect that the legislature's mandatory use of an AeS does not enable and facilitate e-transactions in the public interest.[408]

The SALRC initiated review of the ECTA when it realised that e-signature regulation is not effective.[409] It subsequently produced the ECT Amendment Bill.[410] Unfortunately the ECT Amendment Bill does nothing to improve the prevailing situation as it retains the AeS together with the onerous accreditation requirements.[411] In fact it is worse since it amends the definition of an e-signature and gives it features of an AeS,[412] which this study shows is difficult to implement.[413] The only difference between the proposed e-signature and an AeS will be that the AeS is accredited while the e-signature is not. The ECT Amendment Bill asserts that the ECTA had to be amended to curb incidences of hacking and security breaches e-commerce users were experiencing.[414] Nonetheless, there is no case law or problems reported in practice that were caused by the ECTA's definition of e-signature which show the need for amendment.[415]

Experts condemn the mandatory use of AeS in South Africa.[416] It is indicated that e-signature regulation should be responsive to local conditions. South Africa is not advanced enough or ready for stringent requirements for e-signatures. Hence the two tier approach is not effective for South Africa. Instead, there is a discrepancy between the legislature's intended technology neutral approach and the predominant technology specific approach with preference for specific technologies.[417] Consequently, it is encouraged that South Africa use a technology neutral approach against dependence on current PKI based regulations.[418] It

[407] J Coetzee 'The Electronic Communications and Transactions Act' 2009 *Stellenbosch Law Review* 502.
[408] Swales op cit note 47 at 260 & 262.
[409] Ellipsis Regulatory Solutions 'Electronic Communications and Transactions Amendment Bill 2012' 2012 available at *http://mybroadband.co.za/vb/showthread.php/478510-Electronic-Communications-and-Transactions-Amendment-Bill-2012*, accessed on 18 November 2014.
[410] GN 888 *GG* 35821 of 26 October 2012.
[411] Swales op cit note 47 at 265.
[412] Section 1 (u) of the ECT Amendment Bill.
[413] See parts 2.9.10.2.6 & 5.6.3.1 above.
[414] Paras 1.2 & Para 1.3 of The Memorandum on the objects of the Electronic Communications and Transactions Amendment Act.
[415] Eiselen 'Fiddling with the ECT Act' op cit note 110 at 2807.
[416] Pria Chetty *An analysis of electronic signature regulation in South Africa* (Master of Management Research Report, University of Witwatersrand, 2013) 105; Srivastava et al op cit note 105; Eiselen 'Fiddling with the ECT Act' op cit note 110 at 2814-15.
[417] Chetty ibid at 106.
[418] Chetty ibid at 105.

should make improvements towards technologies with lower costs.[419] It is advised that South Africa should follow the approach of Article 9 (3) (b) (ii) of CUECIC[420] as '[t]his new provision in the Convention helps it retain a technology-neutral approach and also resolves the anomaly associated with the reliability test as it validates a signature method – regardless of its reliability in principle'.[421]

Like South Africa, Lesotho is not in a position to deal with PKI requirements. Hence the fear that the Lesotho Bill's mandatory SeS provisions are potentially non - responsive to the needs of users. As a result, the South African experts' recommendations on the use of lower cost technologies that meet CUECIC's requirements contrary to its reliance on PKI should be adopted by Lesotho.

In a similar vein, studies show that the Directive was challenged on achieving its aim.[422] It achieved its aim only to the extent of ensuring recognition and use of e-signatures, but the same cannot be said about ensuring free use and flow of advanced e-signatures.[423]

By contrast, the US legislative provisions achieved their aims. While '[t]he purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures',[424] E-SIGN is to facilitate use of e-signature in interstate and foreign commerce. The effect of the instruments is that e-signatures and e-records are not denied legal effect and enforceability due to their e-form.[425] Their aim is to give electronic medium legal recognition and effectiveness equivalent to the paper medium.[426] Consequently e-signatures are legally recognized in transactions between people for business, consumer,[427] commercial[428] and governmental purposes.[429] The next question is whether the substantive content of the instruments will achieve its aims.

---

[419] Chetty ibid at 105.
[420] Srivastava et al op cit note 105 at 441; See parts 4.5.2 & 5.9.3 above.
[421] Srivastava et al op cit note 105 at 441 above.
[422] European Commission 'Digital agenda for Europe: A Europe 2020 Initiative' op cit note 64.
[423] Para 2.3.1 & 5.2 of Report from the Commission on Directive op cit note 387; Cecilia Magnusson Sjoberg & Anna Norden 'Managing electronic signatures: Current challenges' 47 *Scandinavian Studies in Law* 79 at 80. See also a Study on Cross-Border Interoperability of e-signatures (CROBIES) 2010 available at *file:///C:/Users/user/Downloads/KK0113059ENN_002.pdf,* accessed on 10 January 2016.
[424] UETA Prefatory Note.
[425] § 7(a) UETA & 15 USC§ 7001 (a).
[426] Curry op cit note 79 at 572; Spyrelli op cit note 82; Patricia Brumfield Fry 'Introduction to the Uniform Electronic Transactions Act: principles, policies and provisions' (2000-2001) 37 *Idaho Law Review* 237 at 249; See *Int'l Casings Group Inc v Premium Standard Farms Inc* 358 F Supp 2d 863 (WD Mo 2005); *Crestwood Shops v Hilkene* 197 SW 3d 641 *651* (Mo Ct App 2006).
[427] *Barwick v Govt Emp Ins Co Inc* 2011 Ark 128 (2011).
[428] *Waddle v Elrod* 367 SW 3d 217 (Tenn 2012).
[429] § 2 Comment 12 UETA.

5.10.4 Effectiveness of regulatory content on SeS

An instruments' capacity to attract participants measures the effectiveness of its content as well.[430] However, the Lesotho Bill and Lesotho Digital Signature Regulations' performance is not assessable at this stage as they are not yet in force. The performance of South African, EU and USA e-signature instruments will give a guide of how the Lesotho instruments will perform instead.

Notwithstanding South Africa's cutting-edge e-signature regulation, it is lagging in accreditation of authentication products and services and the use of an AeS. The ECTA came into effect in 2002, but the SAAA only came into existence in 2007. Two authentication service providers exist to date, namely South African Post Office Limited (SAPO) and LAWTrust Third Party Services.[431] Although SAPO is the preferred ASP for AeS used in e-government services,[432] so far the SAPO has not been fulfilling its role as an ASP, but the reasons for this are not clarified.[433] LAWTrust is a private company recognised as a service provider in March 2012.[434] It provides its signature services to government and industries such as the banking and insurance sectors.[435] These services include the South African national ID cards security and border control biometrics.[436] However, it is silent about provision of its services to individuals.[437] It is inferred that the slow acceptance and use of an AeS is that it is considered to be 'too difficult, complex and expensive to obtain.'[438] As a result, South African online users have not used the AeS much since the enactment of the ECTA and inception of the Accreditation Regulations.[439]

Regarding the Directive, the 2003 European Commission's task team that investigated concerns on its implementation found that although several EU countries had transposed the Directive into national legislation, many countries had no or one accredited service provider. This was mainly due to no 'natural market demand' for qualified certificates and associated

[430] See part 3.4.2 above.
[431] Van Der Merwe et al *Information* op cit note 47 at 177; Sylvia Papadopoulos & Sizwe Snail (eds) *Cyberlaw@SAIII:The Law of the internet in South Africa* (2012) 49; Srivastava et al op cit note 105 at 443. SAPO was accredited in 2013 (Eiselen 'Fiddling with the ECT Act' op cit note 110 at 2814).
[432] Section 28 (2) of the ECTA.
[433] Srivastava et al op cit note 105 at 437.
[434] Papadopoulos et al op cit note 431 at 508.
[435] LawTrust Information Security Solutions 'About Lawtrust' available at *https://www.lawtrust.co.za/pages/about*, accessed on 14 January 2017.
[436] For more E-signing solutions offered by LawTrust see LawTrust Information Security Solutions 'Our solutions' available at *www.lawtrust.co.za*, accessed on 14 January 2017.
[437] It is noted that the Law Society of South Africa is currently running a pilot project commenced in 2014 through which it encourages Attorneys to use the AeS (Swales op cit note 47 at 266).
[438] Swales op cit note 47 at 262.
[439] Swales op cit note 47 at 261-262; Eiselen 'Fiddling with the ECT Act' op cit note 110 at 2814.

services.[440] Again, the absence of a 'secure display component' that displays the information the user intends to sign or verify and the operation of an effective revocation system slowed down the use of PKI technology.[441] Consequently, the content of the Directive on e-signatures did not attract many participants at that stage.

In 2006, the Commission submitted another report on the operation of the Directive.[442] The report revealed that the use of AeS and qualified signatures was not common within the EU, while simple e-signatures have gained common use.[443] The reasons being, among others, that e-service providers did not trust digital signatures based on PKI for non-repudiation therefore they did not permit their customers to use it for other activities for fear of liability.[444] Moreover, they were not widely used as they are cumbersome to implement and expensive to achieve,[445] while there are other secure enough, but less costly technologies that can be used to sign.[446]

Hence, the EU Digital signature's complexity, costs associated with it and lack of user-friendliness lead to users' reluctance of its use or its total discard.[447] Up to 2011, digital signatures based on PKI were practically unused.[448] It has been argued that their uptake would be better if the digital signature regulations had been kinder to CSPs.[449] In fact in 2012, some authors proposed that sections of the Directive on technicalities of AeS and QeS should be repealed.[450] Further, in 2015, Ernst and Young Baltic AS conducted a study on the use of the AeS and QeS in 28 EU member states, Norway, Switzerland and Iceland.[451] The study found that in four countries (Estonia, Luxembourg, Iceland and Austria), 10 percent of the working

[440] Dumortier et al op cit note 64 at 8.
[441] Dumortier et al op cit note 64 at 13. See Peter Gutmann 'PKI: It's Not Dead, Just resting' available at *http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf,* accessed on 16 February 2016.
[442] Report from the Commission on Directive op cit note 387.
[443] Report from the Commission on Directive op cit note 387 at para 3.1 & para 5.2.
[444] Report from the Commission on Directive op cit note 387 at para 3.3.2; Andrej Savin *EU Internet Law* (2013) 225-6. See also s 14 of the Swedish Act on Qualified Electronic Signatures 2000.
[445] Report from the Commission on Directive op cit note 387 at para 3.3.2.
[446] Christina Ramberg 'Contracting on the internet – Trends and challenges for law' in Peter Seipel (ed) *Law and Information Technology: Swedish Views* (2002) Stockholm 109 at 111. For other factors that contributed to the low use of the AES see ChamberSign op cit note 240 at 4 & Chondrocoukis et al op cit note 89 at 10.
[447] Eugene E Schultz 'The gap between cryptography and information security' (2002) 21 *Computers & Security* 674.
[448] Graux op cit note 63 at 9; Forder op cit note 111 at 419.
[449] Stefek Zaba 'Digital signature legislation: The first 10 years at 24' (2006) 11 *Information Security Technical Report* 18 at 24.
[450] Mason S & Bromby M 'Response to *Digital Agenda for Europe*: Electronic identification, authentication and signatures in the European digital single market. Public consultation' (2012) 3 *European Journal of Law and Technology* 1.
[451] Ernst & Young Baltic AS 'Summary of the study: "usage of qualified electronic signature within Europe Union", 2015 available at *https://mkm.ee/sites/default/files/summary_of_the_study_usage_of_qualified_electronic_signature_within_europe_union.pdf,* accessed on 5 January 2018.

age population used the QeS while use of other ordinary e-signatures of lower security were spread out through the countries.[452] The minimal number of participants revealed the failure of the Directive on use of a QeS.

Inversely, UETA and E-SIGN have succeeded in attracting multitudes of participants. Though UETA was developed in 1999, by 2002 it was adopted in all state jurisdictions in the USA except for four.[453] From 2010 to 2011, the overall e-signature market increased with 48 percent.[454] To date UETA is adopted by forty-seven states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands,[455] hence its high uptake. In 2014 The USA market does not mandate use of a specific technology. Because of its technology neutral nature, UETA allows users and markets to use technology that meets their needs without worries about legal structure.[456] It combines 'the appropriate blend of assurance with costs.'[457] Likewise, E-SIGN is considered a 'law without any rules'.[458] It provides secure and reliable transactions with minimal governmental intervention.[459] These characteristics render the legislation attractive to users and a success in e-commerce.[460]

The above discussions indicate that SeS provisions are less likely to be effective? while the ordinary e-signature provisions will be more so. For instance, the complex and potentially unstable nature of SeS provisions, and costs involved in its use deprive them of political, legal, functional and rationality components of legitimacy. But the e-signature provisions consist of these legitimacy components, hence their potential effectiveness.

To summarize, the Lesotho Bill will be effective to the extent of validating an ordinary e-signature, but does not observe the presumptions of effectiveness by prescribing of a SeS. The instruments' SeS provisions may not be understandable by their subjects nor likely to be

[452] Ernst ibid.
[453] These are Georgia, Illinois, New York and Washington (Gabriel op cit note 72); Renaud Sorieul, Jennifer R Clift & Jose Angelo Estrella-Faria 'Establishing a Legal Framework for Electronic Commerce: The Work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 *The International Lawyer* 107 at 115.
[454] SIGNiX '2014 E-Signature Trends: Security and Assurance Will Be King' 2014 available at *https://www.signix.com/blog/bid/108796/2014-E-Signature-Trends-Security-and-Assurance-Will-Be-King,* accessed on 5 January 2018.
[455] Steven C Bennett 'Electronic signatures in New York: an update on recent developments' (2013) 85 *New York State Bar Journal* 44; See also Uniform Law Commission available at *http://www.uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act,* accessed on 02 March 2016; Curry op cit note 79 at 559 & 561, Illinois and New York have laws that closely reflect UETA and E-SIGN though.
[456] Patricia Brumfield Fry 'Introduction to the Uniform Electronic Transactions Act: principles, policies and provisions' (2000-2001) 37 *Idaho Law Review* 237 at 250.
[457] Fry ibid at 258.
[458] Hays op cit note 260 at 1195 & 1200; 15 US § 7002 (a) (1).
[459] Spyrelli op cit note 82.
[460] The USA is considered the foremost country in e-commerce with the most established law (Smith op cit note 85 at 133).

stable over time due to their technology specificity. Further, the prescription of a SeS is contrary to the social aim of the Lesotho Bill. Though the Lesotho Bill's performance in attracting participants is currently immeasurable, the SA and EU instruments which the Lesotho Bill followed have failed to attract participants for AeS and are ineffective to this extent. Consequently, SeS provisions will not effectively address concerns in e-signature use.[461]

5.11 Conclusion

The SeS provisions of Lesotho e-signature instruments are not functional equivalents of a handwritten signature, their technology neutrality is limited and they are potentially ineffective. The Lesotho Bill's provisions on the ordinary e-signature are technology neutral and have the potential to make the Lesotho Bill effective in application. They align with the criteria for functional equivalence to a large extent but for their silence on reliability standards e-signatures must meet and their limited application to parties' voluntary use of signature in their e-transactions. Consequently the Lesotho Bill will not adequately address concerns raised in e-signature use, nor promote e-transactions and e-commerce. However SADC ML observes these functional equivalence and technology neutrality principles to the extent of its recognition of ordinary e-signatures where law requires signature. Hence SADC ML is a potentially effective law. The study shows that the South Africa and EU instruments have not succeeded to promote the use of digital signatures based on the PKI system in their respective jurisdictions for lack of technology neutrality and functional equivalence. As a result, they do not provide the best models of e-signature regulation. However the USA does not mandate use of digital signatures based on PKI, instead it observes technology neutrality and functional equivalence principles. As a result, it succeeded in promoting e-commerce through the use of ordinary e-signatures. USA instruments therefore align better with e-signature principles proposed by this study. A table that depicts the legislative instruments discussed in this chapter and their adherence to the proposed e-signature principles is attached hereto for ease of reference.[462]

With this in mind, the subsequent chapter examines whether the Lesotho Bill and SADC ML's exclusion of e-signature provisions from certain legal matters is justified under current ICT principles.

[461] See part 1.2 above.
[462] See Diagram 2: Table of legislative instruments.

CHAPTER SIX: EXCLUSION OF E-SIGNATURE APPLICATION FROM CERTAIN MATTERS

6.1 Introduction

The purpose of this chapter is to examine whether it is appropriate for both the Lesotho Electronic Transactions and Electronic Commerce Bill 2013 (Lesotho Bill) and the Southern African Development Community Model Law on electronic transactions and electronic commerce 2013 (SADC ML) to exclude application of their provisions on signature in e-communications from certain identified matters. It asks the question whether under the functional equivalence and technology neutrality approaches, an e-signature cannot meet the purposes of the signature formality required by law in those matters to warrant its exclusion. To achieve its purpose the chapter identifies the matters excluded from e-signature application, examines when and why the law requires signature in them, and whether the e-signature is capable of meeting the purposes.

The Lesotho Bill provides that,

> 'Part II and III shall not apply to any rule of law requiring … signature in any of the following matters: (a) the creation or execution of a will; (b) negotiable instruments; (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts; (d) any contract for the sale or other disposition of immovable property, or any interest in such property; (e) the conveyance of immovable property or the transfer of any interest in immovable property [and]; (f) documents of title.' [1]

Part II of the Lesotho Bill includes its provisions on e-signature. Likewise, the SADC ML states that the provisions that give legal effect to signature online should not apply to requirements of signature in: a contract for alienation of immovable property; a contract for long term lease of immovable property in excess of 20 years; execution of a will or codicil; execution of a bill of exchange; and other documents as may be prescribed by member states.[2]

The conclusions the chapter draws on application of e-signatures in the excluded matters are tentative as the Lesotho Bill and SADC ML exclude other factors inter-related

[1] Section 5 (2) of the Lesotho Bill. Section 5 (5) of the Lesotho Bill further states that the Minister may by order modify the provisions of subsection (2) by adding, deleting or amending any class of transactions or matters.
[2] Section 7 (5) of the SADC ML.

with e-signature from the same matters which aspects the study does not traverse. For example, Part II of the Lesotho Bill also includes legal recognition of e-communications and writing while Part III is on formation and validity of contracts; variation by agreement; time of dispatch of e-communications; time of receipt of e-communications; place of dispatch and receipt of e-communications; time of contract formation; automated transactions, and input errors. The thesis does not cover the latter aspects due to a limited time frame of the study. Accordingly, conclusions drawn on application of e-signatures are tentative pending further research on whether those aspects are correctly excluded by the instruments. The purpose of signature in wills follows.

6.2 Signature in the creation and execution of wills

Lesotho regulates the creation of wills through the Execution of Wills Ordinance 15 of 1845 (Ordinance). The Ordinance sets out the formalities required for the execution of a valid will. First, a testator or another person must sign the will under the direction of and in the presence of the testator. Second, they must place their signature at the foot or end of the will. Third, the testator must make or acknowledge the signature in the presence of two or more witnesses present at the same time. Fourth, the witnesses must attest and subscribe (sign) to the will in the presence of the person executing the will. Fifth, where the will consists of more than one page, the party executing the will and the witnesses 'shall sign or shall have signed their names' on at least one side of each leaf of the will.[3] In essence, the Ordinance prescribes three formalities for creation of wills namely, writing, signature and attestation by competent witnesses.[4]

The signature formality in wills serves three purposes. It identifies the script as that of the testator; it indicates that the document is final, not just a draft and it authenticates the will as a genuine property disposal document.[5] Hofmeyr explains that formalities in wills serve to 'curtail opportunities for fraud, to obviate uncertainty and to ensure, as far as possible, that the wills reflect the genuine and voluntary disposition of the testator.'[6] Therefore 'a will is

[3] Section 3 of the Ordinance 1845.
[4] Linda Schoeman-Malan, Francois Du Toit & Anton van der Linde 'Section 2(3) of the Wills Act 7 of 1953: a retrospective and critical appraisal of some unresolved issues' 2014 *Acta Juridica: South African Law of Succession and Trusts- the past meeting the present and thoughts for the future* 78 at 80.
[5] Chad Michael Ross 'Probate – *Taylor v. Holt*: The Tennessee Court of Appeals Allows a Computer Generated Signature to validate a Testamentary Will' (2004-2005) 35 *U Mem L Rev* 603 at 608; see parts 2.5.1 & 2.5.2 above.
[6] GYS Hofmeyr 'Execution of Wills or Testamentary Form' in MM Corbett, GYS Hofmeyr & Ellison Kahn *The Law of Succession in South Africa* 2 ed (2001) 49; Schoeman-Malan et al op cit note 4.

sufficiently signed if the testator make[s] some sign or mark thereon by which his final intent to give effect to the instrument as his will may be made manifest.'[7]

It is argued that e-signatures can meet the purposes of signature in wills. As previously stated,[8] the United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC) provides that the requirement of signature will be met where a method is used to identify a party, and to show the party's intent towards information in the e-communication, provided the method is reliable in principle or reliable in fact.[9] Accordingly, an e-signature technology is capable of identifying a document or will as the testator's if it is used to identify the signer. It can also authenticate the will if used to demonstrate the signer's intent towards information in the will. The method can be used as a sign that a testator assents to and adopts contents of the document which disposes of their property, including the intended finality of the document.[10]

Again, as previously indicated,[11] a testator can sign a will with a mark instead of writing their full name. In a similar vein, 'letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing'[12] can be used to sign a will provided they are intended to show the testator's assent to contents of a document.

Where parties dispute the integrity of an e-communication such as an electronic will (e-will), courts may apply e-commerce regulations which deal with admissibility and evidentiary weight of e-communications to ascertain whether the integrity of the e-communication was retained or not.[13] Moreover, the circumstances surrounding a case can help determine the reliability of the e-signature in a will. Thus the signature's purpose of rendering a will final can be complemented by the use of metadata which helps certify the original scope of a data message.[14] It follows that a will can be sufficiently signed by a testator with any mark or sign including an ordinary e-signature that reflects their intent to dispose of their assets.

Not only can e-signatures meet the requirement of a testator's signature in a will but they can also meet the law's requirement of witnesses' attestation to a will. The witnesses can

[7] Ross op cit note 5 at 608.
[8] See part 4.5.2 above.
[9] Article 9 (3) (a) of CUECIC.
[10] See part 2.5.2 above.
[11] See parts 2.6.1 & 2.6.2 above; Ross op cit note 5 at 608.
[12] James W Martin 'I Want To Sign An Electronic Will' 2009 *The Practical Lawyer* 61 at 62 from the USA.
[13] Sylvia Papadopoulos 'Electronic Wills with an Aura of Authenticity: *Van der Merwe v Master of the High Court and Another*' (2012) 24 *SA Mercantile LJ* 93 at 103; See parts 4.3.3 & 5.9.3 above.
[14] See part 5.6.3.3 above; See also part 2.9.11 above.

use e-signature technologies to identify them.[15] Again, witnesses can use an e-signature to indicate that they associate themselves with contents of the e-communication, that is, to show their intent to attest to a will.[16] Regarding the requirement that the testator must sign the will in the presence of two witnesses at the same time, it is proposed that the witnesses can be in the same room with the testator and together watch the testator sign the will with an e-signature.[17] After that the witnesses can sign the document with their e-signature as well.[18] Thus e-signatures can serve the requirement that a will be attested by two witnesses present at the same time.

6.2.1 South Africa's and the USA's response to electronically drafted wills

South African courts take cognizance of the technological world we live in by legally recognizing electronic drafts of wills notwithstanding legislation which prohibits the creation of wills with data messages.[19] This is reflected in the two cases of *MacDonald v The Master*,[20] and *Hendrik Van der Merwe v The Master of the High Court*.[21]

6.2.1.1 *MacDonald v The Master*

In this case the court condoned a document printed from a computer as a will regardless of the document's failure to comply with the formalities of a will. After a widow retrieved and printed her husband's will from the deceased's computer with his passwords, the Master of the High Court refused to accept the document as a will for failure to comply with the Wills Act.[22] The widow approached the court to condone the document for non-compliance with will formalities under s 2 (3) of the Wills Act.[23]

---

[15] The identification information will reflect whether a witness was competent to attest to a will as required by the Ordinance and s II of the Attesting Witnesses Act 22 of 1876.
[16] See Art 9 (3) (a) of CUECIC in part 4.5.2 above & para 160 of Explanatory note on CUECIC.
[17] *Taylor v Holt* 134 SW3d 830, 834 (Tenn Ct App 2003).
[18] To augment the requirement, the parties can use e-signature technologies which capture the date and time of attachment (Papadopoulos 'Electronic Wills' op cit note 13 at 106). They can also use time stamps or other unambiguous technologies (HIM Body of Knowledge 'Electronic Signature, Attestation, and Authorship (2013 update)' available at *http://library.ahima.org/doc?oid=107151#.V7Xgmfl96Uk*, accessed on 18 August 2016).
[19] Section 4 (4) & Schedule 2 (3) of the Electronic Communications and Transactions Act (ECTA) 25 of 2002; See also Sizwe Snail & Nicholas Hall 'Electronic Wills in South Africa' (2010) 7 *Digital Evidence & Elec Signature L Rev* 67 at 67 – 70.
[20] 2002 (5) SA 64 (O) (High Court).
[21] 2010 (6) SA 544 (SCA).
[22] Section 2 (1) (a) of the Wills Act 7 of 1953 of South Africa provides that for a will to be valid, it must be in writing, signed, attested by two competent witnesses and, every page must be initialled by the testator.
[23] Johann Jacobs & Leigh Lambrechts 'Valid or not? General principles for challenging a will' (2013) 535 *De Rebus* 30 at 31.

The court accepted that the document was authored by the deceased as it was typed by him in his computer and secured with his passwords.[24] It stated that it was not necessary for a document to be handwritten in this technological era.[25] It held that if there is evidence that the deceased intended the document to be his will despite his failure to observe formalities, then the document is considered a valid will.[26] The court's decision meant that it accepted the electronic draft will as proof of the existence of a valid will, despite its non-observance of prescribed formalities.[27] It is also deduced that the court accepted a password as a form of signature and analysed the surrounding circumstances of the case to decide that the password was a reliable e-signature.

6.2.1.2 *Hendrick van der Merwe v Master of the High Court*

In this case, the Appellant and deceased had been close friends for years. They agreed that they would each execute a will in which one would make the other his sole beneficiary. Subsequently, the deceased drafted a will nominating the Appellant as his sole beneficiary and sent it by email to the Appellant. The deceased inquired with Appellant whether he approved of the will and he did.[28] But, the deceased died before he signed the draft will he had emailed to the Appellant. The Master rejected the draft as a valid will for amongst other reasons, lack of observance with the prescribed will formalities. The Appellant presented the printed email to court for condonation under the Wills Act.[29]

The court noted several factors. First, that the legislature enacted s 2 (3) of the Wills Act with the resolve to guarantee that a testator's failure to observe the formalities does not frustrate his/her intention, provided the deceased testator intended the document to be his/her

[24] Evidence showed that the deceased was the only one who could access his office computer as the password to his computer was made by himself and the password had to be changed on a monthly basis. A record of each employee's password was secured in sealed envelopes and kept in a secure locked locker by a person in the deceased's office whose job was to keep the passwords safe (Michael Cameron Wood-Bodley 'MacDonald v The Master: computer files and the "rescue" provision of the Wills Act' (2004) 121 *SALJ* 34 at 35 – 37).

[25] At 71; *Bekker v Naude en Andere* 2003 (5) SA 173 (SCA) para 8.

[26] Before commiting suicide, the deceased left a note stating that his will was in a certain file in his office computer.

[27] Snail et al 'Electronic Wills in South Africa' op cit note 19 at 68. Consequently, the term 'document' in s 2 (3) of the Wills Act now encompasses computer files. It is nonetheless noteworthy that section 2 (3) does not extend to electronic documents that cannot be converted to hard copy prints such as video tape. But a recorded will is included as it can be transcribed and reduced to writing (Wood-Bodley op cit note 2424 at 37 and Schoeman-Malan et al op cit note 4 at 101). It is unclear what the positon of the law will be if a video is transcribed.

[28] To reciprocate, Appellant approached his lawyer to draft a will nominating deceased as his sole heir. He then signed the will at his lawyer's offices, a fact the deceased was aware of.

[29] Section 2 (3) of the Wills Act.

will.[30] The surrounding circumstances proved that the deceased intended the draft emailed will to be his will.[31] The court accepted that a document existed under the Wills Act though it was in electronic form at the time of the deceased's death. It therefore condoned the printed email as a will.

It is submitted that the two cases above reflect the courts' acknowledgement of society's use of technology in this day and age. They also reflect the weight that courts place on surrounding circumstances of a case to determine the intention of a testator.[32] It has been argued that the position of the ECTA which does not recognize wills created with data messages should be amended for purposes of legal certainty in South Africa since the courts effectively recognize an electronic draft will as a document.[33]

The USA Uniform Electronic Transactions Act (UETA) also excludes wills and codicils from its application. But this is on the basis that wills are not part of the transactions that fall within its scope.[34] Nonetheless certain states recognize execution of e-wills. Nevada is an example,[35] while Tennessee adopted liberal language in its wills legislation and thus accommodates use of e-signatures in execution of wills.[36] Canadian[37] and Australian courts have also accepted wills created on smart phones with only electronic copies existent.[38]

Skeptics argue that e-signatures cannot fulfill the signature requirement in the execution of a will as regulation requires numerous signatures on a will and designates the signature's positions,[39] but this is disputed. There are for example, e-signature technologies such as the digital signature based on PKI which can ensure that at least one side of each leaf

[30] Para [14]; Sizwe Snail & Siyabulela Matanzima 'Electronic wills – beyond the MacDonald v The Master decision' 2011 *Without Prejudice* 61 at 62.
[31] These included the fact that the deceased had nominated the Appellant as sole heir to his pension fund.
[32] See § 2-503 of the Uniform Probate Code of the USA which has a similar effect to s 2 (3) of the Wills Act; Joseph Karl Grant 'Shattering and moving beyond the Gutenberg paradigm: The dawn of the electronic will' (2008) 42 *University of Michigan Journal of Law Reform* 105 at 121.
[33] Steve Cornelius 'Condonation of Electronic Documents in terms of Section 2(3) of the Wills Act 7 of 1953' (2003) 1 *Tydskrif vir die Suid-Afrikaanse Reg* 208 at 210.
[34] §3 (b) (1) of UETA Comment 1.
[35] 2013 Nevada Revised Statutes Chapter 133 – Wills NRS 133.085 Electronic will enacted in 2001.
[36] Tennessee Code Ann § 1-3-105(30) 2003; *Taylor v Holt CA* Tennessee Knoxville 18 August 2003; See also the Norwegian case LB-2006-27667, 20 August 2007 Borgarting Appellate Court (translated into English with a commentary by Jon Bing in 'Norwegian case LB-2006-27667' (2008) 5 *Digital Evidence and Electronic Signature Law Journal* 134 at 137 – 140).
[37] *Rioux v Coulombe* (1996) 19 ETR (2d) 201 JE 97-263 (Quebec Sup Ct); The Electronic Commerce and Information Act CCSM c ESS Part 2 of Manitoba.
[38] See s 32 (1) of the Western Australia Wills Act 1970; s 10 of the Northern Territory Wills Act 2000; James Faber as cited in Nomfundo Manyathi-Jele 'Electronic wills discussed at FISA conference' (2014) 547 *De Rebus* 9 at 10.
[39] Juanita Jamneck (ed), Christa Rautenbach (ed) & Mohamed Paleker et al *The Law of Succession in South Africa* 2 ed (2012) 63. For example, s 3 of the Ordinance requires signatures on at least one side of each leaf of a will, and that signatures should be placed at the bottom of a will.

of a will is signed and that a signature is at the bottom of the will.[40] Moreover, as explained earlier, the testator and witnesses' multiple e-signatures can be achieved on an e-will by each signer signing the will with their e-signature in the presence of the others.[41] Hence the argument falls away.

Again, skeptics state that it will be difficult to demonstrate that an e-will has not been altered over the years due to lack of a manuscript signature.[42] However, it was previously highlighted that changes in e-communication can be traced by several technologies such as use of metadata[43] or digital signatures.[44] Boddery argues that use of e-signatures in wills introduces a new kind of evidence before courts, thus it burdens the court with 'evidentiary concerns'.[45] But courts already deal with different kinds of evidence to prove offline signatures. Moreover, concern was raised that e-wills are not durable and may be difficult to access several years later due to changing technologies.[46] But it is noted that the issue of durability of e-wills is not dependent on e-signature technologies. Nonetheless, e-wills may be stored as e-records in Portable Document Format (PDF).[47] Alternatively, their storage can be refreshed by transferring them to a new storage medium on a periodic basis to avoid technology obsolescence.[48]

It is therefore submitted that it is overly cautious for the Lesotho Bill and SADC ML to exclude e-signatures from use in wills and codicils. The law can permit the use of e-signatures that meet the standard set by CUECIC in execution of a will. These technologies

[40] The digital signature calculates the hash value of an entire data message such that new information inserted after the digital signature is created will be reflected. The e-signature attaches to an e-document in its entirety, which is 'every single page, word or letter' (Papadopoulos 'Electronic Wills' op cit note 13 at 105 -106); See also part 2.9.10.2 above.
[41] Snail et al 'Electronic wills in South Africa' op cit note 19 at 68.
[42] Alberta Law Reform Institute Final report no 96 *The creation of wills* (September 2009) Edmonton Alberta at Para 126.
[43] 'The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age' A Project of The Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production Second Edition November 2007 at 37 available at *file:///C:/Users/user/Downloads/Guidelines.pdf*, accessed 17 January 2017. The time stamp is also useful for tracking when a document was stored in media, at 38.
[44] See part 2.9.11 above for more online authentication methods that can provide information security of e-wills. For more arguments against electronic wills and counter arguments, see James Faber 'Electronic wills and jurisdictional issues surrounding a "digital estate" ' (18 September 2014) The Fiduciary Institute of Southern Africa (FISA) 4th Annual Conference, Johannesburg at slides 12 & 13; Gerry W Beyer & Claire G Hargrove 'Digital Wills: Has the Time Come for Wills to join the Digital Revolution?' (2007) 33 *Ohio NUL Rev* 865 at 890-897.
[45] Scott S Boddery 'Electronic wills: drawing a line in the sand against their validity' (2012) 47 *Real Property, Trust and Estate Law Journal* 197 at 209.
[46] Alberta Law Reform Institute (ALRI) 'The creation of wills' Final report no 96 September 2009 at para 127.
[47] Dana van der Merwe (ed), Anneliese Roos, Tana Pistorius, Sieg Eiselen & Sanette Nel *Information and Communications Technology Law* 2ed (2016) 136. See also the Open Document Format (OPF) and Open Office XML (OOXML) which may be suitable for archiving electronic documents.
[48] Sedona Guidelines op cit note 43 at 38.

achieve the purpose of the signature formality in wills. As reflected by the cases discussed above, the surrounding circumstances of a case will help determine the intention of the testator where necessary.

6. 3 Negotiable Instruments

6.3.1 Definition of negotiable instruments

Under Roman-Dutch law, a negotiable instrument is defined as

> '[a] document entitling the holder to the payment of a sum of money, which is transferable by delivery (if payable to bearer) or by endorsement and delivery (if payable to order), in such a manner that the transferee, who takes the instrument in good faith and for value and thus becomes a holder in due course, becomes indisputably entitled to payment.'[49]

A negotiable instrument is therefore a document used to record the monetary amount owed by a debtor to his creditor, and the date on which the payment is due.[50]

In Lesotho, negotiable instruments are regulated by the Bills of Exchange Proclamation 13 of 1912 (Bills Proclamation). The most common instruments categorised under negotiable instruments are bills of exchange,[51] cheques[52] and promissory notes.[53]

6.3.2 The role of signature in negotiable instruments

A signature in negotiable instruments has been described as writing one's name on the instrument with the intention to authenticate it and give effect to the contract inherent in it.[54]

---

[49] J Botha 'Negotiable Instruments' in MA Fouche (ed), J Botha, D Collier-Reed, A Haupt, C B Ncube, T Schonwetter, HJ van As *Legal Principles of Contracts and Commercial Law* 8 ed (2015) 316; FR Malan, JT Pretorius & SF Du Toit *Malan on Bills of Exchange, Cheques and Promissory notes in South African Law* 5 ed (2009) 5-6. The definition applies in Lesotho as well since the Roman-Ducth law of South Africa is applicable in Lesotho.

[50] Leonard Gering & Douglas G Tobias *Handbook on the law of negotiable instruments* 3 ed (2007) 7; Nagel et al *Business Law* 5 ed (2015) 306.

[51] Section 3 (1) of Bills of Exchange Proclamation. A bill of exchange is used for credit payments and investments in commercial transactions (Malan et al *Malan on Bills of Exchange* op cit note 49 at 1). Thus it is useful for international business transactions (Jianhong Fan & Yang Tao 'Negotiable Instruments, in Particular Bills of Exchange in Macau, China' (2007) 2 *Journal of International Commercial Law and Technology* 84).

[52] Section 72 of the Bills of Exchange Proclamation; See Fouché et al op cit note 49 at 316. The role played by cheques in commerce is to make payments. It is noted that there are other techniques which can do the same function such as credit card payments or electronic bank transfers (Malan et al op cit note 49 at 1).

[53] Section 83 (1) of Bills of Exchange Proclamation; Gering et al op cit note 50 at 6; Nagel et al op cit note 50 at 306. The main difference between bills of exchange and promissory notes is that bills are orders to pay whilst a promissory note is a promise to pay (Fouché et al op cit note 49 at 316). A promissory note is among others, used as an acknowledgement of debt, as security to acquire credit or fund foreign trade (Malan et al op cit note 49 at 3).

Signature plays three purposes in negotiable instruments, namely, validation, liability and negotiation.[55]

6.3.2.1 Validity

Signature validates or constitutes a bill.[56] A drawer[57] or maker[58] of a negotiable instrument must sign the document to make it valid.[59] The Bills Proclamation states that an instrument that does not comply with the signature condition is not a bill of exchange.[60]

6.3.2.2 Liability

Signature is one of the requirements for incurring liability for a negotiable instrument.[61] The Bills Proclamation states that 'no person is liable as drawer, endorser, or acceptor of a bill who has not signed it as such.'[62] In other words, the drawer or maker who signs a bill or note states his liability to the payee,[63] while the drawee's[64] signature of the instrument indicates his acceptance to make payment, hence his liability.[65] The Bills Proclamation states that an acceptance of the instrument is invalid if it is not written and signed by the drawee.[66]

It is argued that an e-signature can meet the functions of validity and liability in negotiable instruments. A drawer can use any mark or method including an e-signature on a negotiable instrument to identify them. If the method identifies the drawer, it will validate the bill. A signer can also use an e-signature to show his intention towards the content of the instrument, namely his liability to the payee or liability as an acceptor.[67] In *Northend v Ulbrick*[68] a South African court recognized a company stamp as a valid signature in

---

[54] Anthony Gordon Guest in *Chalmers and Guest on Bills of Exchange, cheques and promissory notes* 17 ed (2009) 157.
[55] Gering et al op cit note 50 at 6.
[56] Malan et al op cit note 49 at 39.
[57] The person who gives the order that money be paid (Fouché et al op cit note 49 at 317).
[58] A person who makes the promissory note and promises to pay (Fouché et al op cit note 49 at 317).
[59] Gering et al op cit note 50 at 52.
[60] Section 3 (2) of the Bills of Exchange Proclamation.
[61] Malan et al op cit note 49 at 81; Gering et al op cit note 50 at 53.
[62] Section 22 of the Bills of Exchange Proclamation.
[63] 'The person to whom payment was ordered or promised' (Fouché et al op cit note 49 at 317; Nagel et al op cit note 50 at 307).
[64] 'The person to whom the order to pay is addressed' such as a banker (Fouché et al op cit note 49 at 317).
[65] Section 16 (1) of the Bills of Exchange Proclamation. The drawee will then be called an acceptor (Gering et al op cit note 50 at 53 & Malan et al op cit note 49 at 81 & 82; s 55 of the Bills of Exchange Proclamation; K N Llewellyn 'Meet negotiable instruments' (1944) XLIV *Columbia Law Review* 299 at 315.
[66] Section 16 (2) (a) of the Bills of Exchange Proclamation.
[67] FR Malan, AN Oelofse & W de Vos *Provisional Sentence on Bills of Exchange, Cheques and Promissory Notes* (1986) 54.
[68] 1972 (1) SA 737 at 739.

negotiable instruments.[69] Scholars argued that if a mark such as a seal or stamp legally represents a person's signature, then there should be no protest to a person's use of other mechanical means to sign a negotiable instrument, provided they do so with the intention to sign the instrument with their name.[70] Consequently, an e-signature is sufficient to this extent.

6.3.2.3 Negotiation

A signature plays a significant role in the endorsement of a negotiable instrument to effect negotiation.[71] Negotiation of a negotiable instrument refers to the transfer of the instrument and the rights in it from one person to another in such a way that the transferee becomes a holder of the bill.[72] In other words, 'the hallmark of negotiability in the paper world is the transfer of the right to payment *(evidenced* by the note) by delivery of the paper note *itself,* along with any necessary indorsement [*sic*]'[73] Negotiation may occur in two different ways, by delivery alone,[74] or by endorsement and delivery.[75] In the latter instance where an instrument is payable to order,[76] the endorser endorses an instrument by signing it at the back,[77] with the intention to endorse, *animus indorsandi*.[78] The endorser then delivers the instrument to the indorsee with *animo contrahendi* and it is accepted with the same intention.[79] That is both parties must have an intention to contract and transfer the rights in the instrument. These will place the new holder in possession of the negotiable instrument and conclude the contract on the Bill.[80] Hence, the person to whom the instrument is made payable by the endorser becomes entitled to payment after negotiation.[81]

The question is whether an e-signature can meet the function of endorsement. Information technology experts have invented a method that makes it possible to

[69] See also *Meyer v Roberts* 1971 (1) SA 328 at 331.
[70] Malan et al op cit note 49 at 83; Malan et al *Provisional sentence* op cit note 67 at 54; part 2.6.2 above. See also s 9 (2) & (3) of the Lesotho Bill and s 7 (2) of SADC ML.
[71] Nagel et al op cit note 50 at 310.
[72] Section 30 (1) Bills of Exchange Proclamation; Malan et al op cit note 51 at 89.
[73] R David Whitaker 'Rules Under the Uniform Electronic Transactions Act for an Electronic Equivalent to a Negotiable Promissory Note' (1999-2000) 55 *The Business Lawyer* 437 at 441.
[74] See ss 20 (1), 30 (2) & 84 of Bills of Exchange Proclamation.
[75] Malan et al op cit note 51 at 89; Section 30 (3) of the Bills of Exchange Proclamation.
[76] Where the drawer specified the payee in a negotiable instrument (Fouché et al op cit note 49 at 321).
[77] Section 31 (1) of the Bills of Exchange Proclamation. To endorse means to 'sign (a cheque or bill of exchange) on the back to make it payable to someone other than the stated payee or to accept responsibility for paying it.' available at *https://www.google.co.za/#q=endorsement+of+cheque+meaning,* accessed on 21 May 2016.
[78] That is 'with the intention of undertaking the well-understood liabilities of an indorser [*sic*]' (Malan et al op cit note 51 at 115).
[79] Malan et al op cit note 51 at 111.
[80] Malan et al op cit note 51 at 111.
[81] Fouché et al op cit note 49 at 322.

electronically endorse an image of a cheque.[82] Thus an e-signature can endorse an instrument provided it is attached with animus indorsandi. Nonetheless, these technologies are not yet available in Lesotho and the majority of the SADC region. As a result, it would be premature to advocate that the law should permit e-signatures to be applied in negotiable instruments for want of negotiability.

In addition, CUECIC excludes negotiable instruments from its scope of application.[83] It acknowledges that the issue of uniqueness of negotiable instruments goes beyond the equivalence of paper and computer documents.[84] The potential consequences that could be caused by unlawful replication of negotiable instruments warrant the development of secure mechanisms which will secure singular negotiable instruments.[85] This requires a combination of market, legal and technical solutions which are yet to be developed. Therefore the issue is beyond its scope.[86]

UETA similarly excludes negotiable instruments from its scope of application. It states that negotiable instruments involve other parties beyond the ones in the basic contract. Therefore accepting electronic versions of negotiable instruments is beyond its scope.[87]

Consequently, although e-signatures can perform functions of validation and liability in negotiable instruments, it is submitted that the Lesotho Bill and SADC ML correctly exclude negotiable instruments from e-signature application due to the difficulty of effecting endorsement. The difficulty of generating singular negotiable instruments adds to this submission.

6.4 Sale, disposition, alienation, conveyance of immovable property or transfer of interest in immovable property and long term lease of immovable property

Matters of conveyance, transfer, long term lease, sale, disposition or alienation of immovable property in the Lesotho Bill and the SADC ML fall under the same category as they have a common component: the transfer of rights in immovable property. In these matters, an owner or holder transfers rights in immovable property to another person who will acquire them

[82] Leon A Pintsov & David Pintsov 'Method for electronically endorsing check images US 7797250 B2' 2010 available at *http://www.google.com/patents/US7797250*, accessed on 11 March 2015.
[83] Article 2 (2) of CUECIC; Para 79 of Explanatory note on CUECIC.
[84] Paragraph 81 of Explanatory note on CUECIC.
[85] Paragraph 80 of Explanatory note on CUECIC.
[86] Paragraph 81 of Explanatory note on CUECIC.
[87] §3 of UETA Comment 5 and 6; see also §16 of UETA Comments 1, 2, 3 and 6.

through a deed of transfer[88] or lease document. The matters are therefore regulated by the same statutes which require interrelated procedures to effect the transfers.

Lesotho regulates the transfer of immovable property or interests in immovable property through the Deeds Registry Act (DRA),[89] Deeds Registry Regulations (DRR),[90] Land Act,[91] Land Regulations[92] and where the statutes are silent, through common law.

6.4.1 The role of signature in transfer of immovable property and interest in the immovable property

The law requires the signature formality several times in the stages of the transfer of immovable property identified below.

6.4.1.1 Application for Commissioner of Land's consent

Parties who propose to transfer or dispose of immovable property must sign an application for consent of a Commissioner of Lands (Commissioner) for the transferee to occupy or use the property.[93] The application shall contain, among others, a description of the transaction; particulars of the land; particulars of the parties to the transaction and any documents the Commissioner may call for.[94] In practice, a legal practitioner of the parties sends the consent application form to the Commissioner who sends the response back to the legal practitioner.

6.4.1.2 Execution of a Deed of transfer of immovable property

After parties acquire the Commissioner's consent, they have to draft, execute and register a deed of transfer.[95] To do so, the transferor must sign a power of attorney by which they authorise a legal practitioner, conveyancer or notary public (legal practitioner) to pass, cede or cancel a deed on their behalf.[96] The power of attorney should be attested to by two

[88] Allen West *Conveyancing Practice Guide* 4 ed (2015) 22.
[89] 12 of 1967.
[90] 52 of 1967.
[91] 8 of 2010.
[92] 21 of 2011.
[93] Section 16 (2) & 24 (2) of the DRA; s 36 of the Land Act; & Regs 9 (1) (a), (c), 30 (1) & 46 (1) (c) of Land Regulations.
[94] Regulations 46 & 30 (3) of Land Regulations. For example, see Regs 9 (1) (f) & 46 (1) of the Land Regulations, s 30 (2) (c) of the Land Act and the Land Administration Authority 'Application for a lease' available at '*http://www.laa.org.ls/index.php?option=com_k2&view=item&layout=item&id=13&Itemid=119,* accessed on 5 September 2016.
[95] Section 16 (2) of DRA & Reg 30 of the Land Regulations. The application for transfer of immovable property in a rural area is made to an allocating party, not a Commissioner of Lands (Reg 29 of Land Regulations).
[96] West op cit note 88 at 27-28.

competent witnesses.[97] The parties to the transaction should also submit affidavits with their correct personal particulars.[98] The legal practitioner shall then draft the deed relating to immovably property.[99] He/she shall initial every alteration in the document and sign all pages if the document is contained in separate sheets.[100]

The deed of transfer is then executed by the owner of immovable property or a legal practitioner authorised by a power of attorney in the presence of the Registrar.[101] It is not compulsory for the party to sign their full name; an identifiable mark will be satisfactory.[102] The Registrar then attests his/her signature.[103]

6.4.1.3 Registration

The DRA states that '[e]very deed or agreement transferring rights in or to immovable property shall be registered in the deeds registry.'[104] The Registrar effects registration when he/she appends his/her signature to deeds or documents he/she executes or attests.[105] Any agreement registered contrary to the provisions of the DRA is null and void.[106]

Further the DRR stipulates the manner and form for filing the deeds. That is, they should be bound by book binders.[107] After this the deeds can subsequently be inspected by members of the public.[108]

The purpose of registration is 'to protect the real rights of those persons in whose names such rights are registered in the Deeds office.'[109] It also provides a public record that

[97] Section 52 of DRA. Alternatively a Magistrate, District Administrator, Justice of the Peace or Commissioner of oaths can attest to a power of attorney.
[98] West op cit note 88 at 30. The affidavits are evidence that the parties qualify to hold title to land as required by s 6 of the Land Act and Reg 30 (2) of the Land Regulations.
[99] Regulation 30 of DRR.
[100] Regulation 30 of DRR.
[101] Section 17 (1) of the DRA.
[102] Bridget Walker *Conveyancing* 3 ed (1998)161.
[103] Section 17 (1) of the DRA.
[104] Section 16 (1) of the DRA. Transfer or disposal of land allocated in rural areas that is not subject to a lease is to be recorded by an allocating authority in the register of allocations; the allocating authority is to notify the Commissioner of the transfers (Reg 30 (5) & (7) of Land Regulations). See also ss 9 (4), 12 (1), ss 34 (5) & 42 (3) of the Land Act.
[105] Section 11 of the DRA. The Registrar shall also attach his/her seal to deeds or documents executed and attested by him/her (s 4 (3) of DRA). For deeds or documents not executed by him/her but lodged for registration, the Registrar shall append his/her signature to a deed registration endorsement.
[106] Section 16 (6) of the DRA.
[107] Reg 46 (1) of the DRR; Section 9 (c), (n) & (o) of the DRA.
[108] Section 8 of the DRA.
[109] *Frye's (Pty) Ltd v Ries* 1957 (3) *SA* 575 at 583; Section 5 (w) of the DRA.

evidences transfer of ownership in immovable property or rights in immovable property such as a mortgage or lease.[110]

6.4.1.4 Analysis

The law requires the signature formality in transfers of immovable property or rights in immovable property 'to prevent uncertainty, disputes and malpractices in transactions relating to land.'[111] A signature achieves these purposes if a signer employs it to identify themselves and to express their intent with respect to information in a document they sign. For instance, a transferor and transferee's signature of an application for consent to a Commissioner serves to prove the identity of the parties. It also reflects the transferor's intent to transfer an identifiable piece of immovable property at a stated price to the transferee, and the transferee's intent to accept the immovable property under the terms stated in the form he/she signs. Therefore signature in these transactions serves the purposes of *identification*, *attribution*, *assent* and *authentication.*[112]

It is argued that an e-signature that meets the standard of CUECIC can be used to sign documents in transfer of immovable property transactions or rights thereof. This will be more effective if the state introduces an electronic conveyance (e-conveyance) system.[113] To illustrate, an appointed legal practitioner can download the consent form which is already available in electronic form from the Land Administration Authority (LAA)'s[114] webpage. They can fill in the form electronically and attach the identity documents of parties to the

[110] Radha Vasudevan 'Changed governance or computerized governance? Computerized property transfer processes in Tamil Nadu (India)' 2006 available at *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4085521,* accessed on 15 August 2016 at 102.

[111] *Wilker v Kohler* 1913 AD 135; *Clements v Simpson* 1971(3) SA 1 (A) at 7A-B. Seamus Keating 'Digital signatures and the electronic transfer of land' (2013) 7 *Masaryk University Journal of Law and Technology* 49 at 51; GB Bradfield *Christie's Law of Contract in South Africa* 7ed (2016) 129; Heinrich Schulze, Roshana Kelbrick & Tukishi Manamela *General Principles of Commercial Law* 8 ed (2015) 96. The most common forms of fraud in immovable property transactions are forgery of signatures, wrongfully persuading one to sign relevant documents and identity theft (Rouhshi Low 'From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System' (2009) 21 *Bond Law Review* 107 at 108; National Association of Realtors 'Moving Towards an Electronic Real Estate Transaction: The Electronic Signature – Legal Overview (U.S.)' 2010 available at *http://www.realtor.org/sites/default/files/handouts-and-brochures/2010/E-Signature-Whitepaper-2010-08-01.pdf,* accessed on 26 August 2016).

[112] Van der Merwe et al op cit note 47 at 163.

[113] See for example England's Land Registration Act of 2002 Chapter 9 which enables implementation of e-conveyance.

[114] A Lesotho organisation responsible for issuing land leases, registration of deeds of transfer, mortgages and so on (Sections 4 & 5 of the Land Administration Authority Act 9 of 2010).

transaction. For instance, they may attach to the form scanned passports, identity cards, or drivers licence as identity documents.[115] They can then attach an electronic agreement to transfer or deed of sale by the parties, or where it is in paper format, scan and attach the transfer agreement to the form. Where necessary, the legal practitioner can draft electronic affidavits (e-affidavits) in support of the application form, have the deponents take an oath and then sign the e-affidavit with their e-signatures by, for instance, typing their names into the e-affidavit or adding a scanned signature the e-affidavit. Further, the legal practitioner can draft an electronic power of attorney which authorises him/her to execute a deed of transfer on the parties' behalf.

Subsequently, the legal practitioner can show the parties to the transaction the consent form together with all the documents for their approval. He/she can do so, for example, by displaying the documents on a computer screen for their acceptance. Alternatively, the legal practitioner can email the e-communication to the parties. To do so, he/she can use accessible online authentication systems that show the origin of a message and protect its integrity such as encryption of an email message by Microsoft Outlook.[116] If the parties agree with the contents of the documentation, they can sign the form and power of attorney on screen with their e-signatures by typing their names into the documents or use an electronic pen on a signature pad.[117]

Regarding the requirement that a party's signature to a power of attorney must be attested by two witnesses, the views of the UNCITRAL Model Law on Electronic Commerce (MLEC) and CUECIC are evoked. The MLEC realised that 'there exist requirements that combine the traditional handwritten signature with additional security procedures such as the confirmation of the signature by witnesses.'[118] With the view that a document should not be denied legal value if it was not authenticated in a manner designed for the paper world,

[115] See UETA which states that scanned documents qualify as electronic records (§2 Comment 6; David E Ewan, John A Richards & Margo H K Tank 'It's the Message, Not the Medium! Electronic Record and Electronic Signature Rules Preserve Existing Focus of the Law on Content, Not Medium of Recorded Land Title Instruments' (2005) 60 *The Business Lawyer* 1487 at 1492). Where available, parties may attach biometric measures such as fingerprints to verify their identity (Thomas R, Griggs L & Low R 'Electronic conveyancing in Australia: is anyone concerned about security?' (2014) 23 *Australian Property Law Journal* 1 at 6).

[116] Alternatively, they can put the message in the form of a password protected attachment attached to an email message to protect its integrity, or use metadata to verify that the integrity of a message is intact and so on. See part 2.9.11 above for further alternative methods available for online authentication.

[117] See the Pennsylvania electronic real estate transactions explained by Tim Mekeel 'Home Sales: Forget the Paper' *Lancaster new era* (Pa) (Nov 13, 2006) at Al *available at* 2006 WLNR 19776240 cited in fn 244 of Michael E Doversberger 'Conveyancing at a crossroads: the transition to e-conveyancing applications in the U.S. and abroad' (2010) 20 *Indiana International & Comparative Law Review* 281 at 305.

[118] Para 54 of Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996) (Guide to MLEC) in part 4.3.3 above.

MLEC established that a document is 'authenticated with sufficient credibility' if a method is used to identify the originator of a message and show their approval towards the content of a message.[119] CUECIC subsequently amended the signature function that it must show a signer's intent towards the e-communication instead of their approval as witnesses do not sign to approve of e-communication but to show their association with it.[120] With this in mind, it is suggested that the requirement that witnesses attest to a party's signature of a power of attorney can be carried out by having two people present in the room at the same time when the transferor/transferee sign the documents on screen with their e-signatures. Thereafter, the witnesses may sign the e-documents with their e-signatures such as a scanned signature or use an electronic signature pad. Technologies such as meta data and time stamps will assist in showing the date and time when the witnesses attested the parties' signatures or when deponents and practitioners signed e-affidavits. For example, a word document can be customized to show date and time a document is created or modified.[121]

Subsequently, the legal practitioner will need to sign the e-documentation as well before he/she sends it off to a Commissioner. The method they use to sign should be as reliable as is appropriate for the purposes for which the e-communication is made.[122] Among the factors which determine the appropriateness of an e-signature is 'the nature of their trade activity… [and] the kind and size of the transaction involved. [123] Immovable property transactions are the largest and most significant transactions in people's lives as they affect the most important possessions one can have – they involve high financial stakes.[124] Because of the significant nature of immovable property transactions, they require secure and reliable authentication methods. Consequently, it is proposed that LAA should develop guidelines as to which authentication methods are better suited for a legal practitioner's signature of the compiled documentation.[125]

---

[119] Para 56 of Guide to MLEC; Tana Pistorius "'Nobody knows you're a dog': The attribution of data messages" (2002) *SA Merc LJ* 737 at 744.

[120] Article 9 (3) (a) of CUECIC & Para 160 Explanatory note on CUECIC in part 4.5.2 above; see also part 5.6.3.3 above.

[121] TechRepublic 'Automating dates and times in a Word document' available at *http://www.techrepublic.com/blog/microsoft-office/automating-dates-and-times-in-a-word-document/,* accessed on 25 July 2017; See part 5.6.3.3 above.

[122] Article 9 (3) (b) (i) of CUECIC.

[123] See part 4.5.2 above & Para 162 of Explanatory note on CUECIC.

[124] Doversberger op cit note 117 at 281.

[125] See for example Ontario's Regulatory Registry 'Considering the security of electronic agreements of purchase and sale: Electronic Commerce Act, Possible e-signature regulation' 2014 available at *http://www.ontariocanada.com/registry/view.do?postingId=17022&language=en,* accessed on 28 August 2016.

6.4.1.4 .1 Guidelines on e-signature in transfer of immovable property or rights in it

When an authority that deals with e-conveyancing develops guidelines on the appropriate e-signatures legal practitioners should adopt for e-conveyance, they should bear in mind that e-signatures/authenticating technologies have differing levels of security.[126] For example, guidelines can recommend that the legal practitioner use a SeS or an ordinary e-signature in conjunction with metadata. These two systems have the advantage of providing online security as they can reflect changes made to the signed e-communication; they can both secure the integrity of the e-communication.[127]

For one, LAA can develop guidelines that advise a legal practitioner to sign the e-documents with an ordinary e-signature technology that shows their identity and intent with respect to the contents of the e-documents and to send them to the Commissioner of Lands on a secure conveyancing LAA network.[128] The network may be secured in different ways. For example, it may be accessible only to parties involved in e-conveyancing or may be secured by Transport Layer Security (TLS) technology which encrypts communication between computer servers.[129] Upon arrival of the e-documentation, the Commissioner will grant his consent, sign it with an ordinary e-signature and email the entire package to the Registrar on the secure LAA network. Upon receipt, the Registrar will verify the integrity of the e-communication by use of metadata where the information was not sent on an encrypted network. If the metadata is unchanged,[130] the Registrar will sign it with their ordinary e-signature to execute and register the deed. As previously indicated, metadata used in support of an ordinary e-signature can perform the functions of a seal.[131] Hence the deed of transfer or lease will be registered as required by law.

Where the e-signature is subject to doubt, the signer can present evidence of facts to prove that the e-signature was used to meet the basic functions of identifying a signer and indicating his intention regarding the e-communication signed. Alternatively, evidence can

[126] Simone Franks *The Capricious Relegation of Offers to Purchase to Invalid Electronic Transactions by the Electronic Communications and Transactions Act 25 of 2002* (unpublished LLM dissertation, University of Cape Town, 2004) 47; AO Orifowomo & JO Agbana JO 'Manual signature and electronic signature: significance of forging a functional equivalence in electronic transactions' (2013) 24 *International Company and Commercial Law Review* 357 at 361.
[127] See part 5.6.3.3 above; Sharon Christensen 'Electronic Land Dealings in Canada, New Zealand and the United Kingdom: Lessons for Australia' (2004) 11 *Murdoch University Electronic Journal of Law* 37.
[128] Sharon D Nelson and John W Simek 'Encrypting sensitive emails now a no-brainer' (2016) 41 *Montana Lawyer* 18.
[129] See also part 2.9.11 above.
[130] From when the e-communication left the Commissioner's computer.
[131] See part 5.6.3.3 above.

prove that a signature was as reliable as appropriate in the circumstances. These include evidence of unaltered meta data, an encrypted communication network and so on.[132]

The soft law can permit a legal practitioner to use alternative e-signature methods in conveyancing. The practitioner may attach their digital signature based on PKI to the documents where available, then email the documents to the Commissioner on an LAA network. The Commissioner will subsequently confirm that the content of the application is unaltered by verifying the digital signature.[133] After confirming this and granting their consent, the Commissioner will attach their digital signature based on PKI to the consent form with and supporting e-documentation, then send them to the Registrar of Deeds for registration. The Registrar will also verify the Commissioner's digital signature. Then the Registrar will attach his/her digital signature based on PKI to the Deed. This way, the Registrar will have executed and sealed the e-deed, hence the deed will be fully registered as required by law.[134]

The soft laws may require that parties to the transaction be granted a unique barcode which allows them to check the progress of their application, but make no alterations to it. LAA's act of recommending the digital signature based on PKI or use of an ordinary e-signature supported with metadata in e-conveyance can reduce society's concern for fraud.[135]

Subsequently, the Registrar can copy the registered e-deed and its supporting documents onto an electronic storage medium such as a memory stick and hand it over to the transferor and transferee and relevant stakeholders. The Registrar and the parties can then store the documentation as an electronic record (e-record).[136]

---

[132] See part 4.3.3 above.

[133] Jacques Vos 'Using European legislation & electronic means in Cross-border conveyancing' 1 January 2014 5th Annual Publication *European Land Registry Association* available at *http://www.elra.eu/using-european-legislation/*, accessed on 22 August 2016; see part 2.9.10.2 above.

[134] See the Vancouver-based OneMove Technologies Inc., an e-conveyance system whereby an agent fills a form for transfer of immovable property, pushes a 'submit button' and title is transferred (Eric Shackleton 'Software Tames Tangle of Paperwork' *The Canadian Press* 11 July 2008 available at *http://www.theglobeandmail.com/real-estate/software-tames-tangle-of-paperwork/article4221434/*, accessed on 29 August 2016). See also Scotland's Automated Registration of Title to Land (ARTL) system which allows an authorised conveyancer to electronically register deeds by simply answering questions online instead of filling in application forms (Alistair Rennie, Michael Samuel & Roger Mackenzie 'The age of e-conveyancing?' 2001 *The Journal of the law society of Scotland* available at *http://www.journalonline.co.uk/Magazine/46-6/1000947.aspx*, accessed on 29 August 2016).

[135] Other alternative methods that ensure that the ordinary e-signature was as reliable as appropriate in the circumstances include the sending an encrypted email message with Microsoft Outlook or Zipcorp, or sending the email with the e-communication as an attachment to an email that is locked with a password (See part 2.9.11 above).

[136] See s 21 of the SADC ML on retention of records which does not prohibit this contention; s 21 of the Lesotho Bill. Where a digital signature based on PKI was used to sign the deed, the Registrar's office can verify its intergrity each time the need arises or on a periodic basis. Where the Registrar used an ordinary e-signature, metadata can be periodically checked to verify that the e-record remains unaltered. See also the Uniform Real

It is worth noting that there is a problem of electronic archaeology whereby modern software may not open e-documents created ten years ago or less with 100% accuracy.[137] But as previously reflected, one of the currently available standards that may deal with the issue and best archive e-documents is the Portable Document Format (PDF).[138] On the other hand, it has been suggested that where an e-record has to be archived for long periods of time such as ten years or more, it can be refreshed by transferring it to a new storage medium on a periodic basis to avoid technology obsolescence.[139] Hence the Registrar may store an e-deed in the form of PDF and/or refresh its storage from time to time. Alternative to the Registrar's storage of an e-deed as an e-record, the Registrar can print the e-deed, attach a seal to it and file it in paper format.

It is argued that if the Lesotho Bill would extend e-signatures to transfer of immovable property transactions, then it would support and promote the objectives of the Land Act.[140] The Act is aimed at facilitating swift acquisition and transfer of rights in immovable property, thereby facilitating efficiency in land transactions.[141] It encourages people to use their rights in immovable property for economic purposes, and improve the land market with more players who have leases.[142] Accordingly, the law's denial of extension of e-signature regulation to contracts transferring immovable property will 'hinder utilization of land as an economic asset.'[143] This is contrary to the objectives for promulgation of the 2010 Act, while extension of e-signature regulation will facilitate the Land Act objectives.

Nonetheless, paper and online conveyance can run concurrently from a state's introduction of an e-conveyance system until concerns on e-conveyance are ironed out. Consequently, parties will have a choice of which mode of conveyance they prefer.[144]

The MLEC and MLES recognise the use of e-signatures in leases. Leasing forms part of the commercial activities within their scope of application.[145]

Property Electronic Recording Act (URPERA) of 2004, a USA guideline available at *http://www.uniformlaws.org/shared/docs/real%20property%20electronic%20recording/urpera_final_apr05.pdf* , accessed on 16 January 2017. It gives clerks/registrars the authority to receive, record, archive and retrieve e-documents on real property transactions (s 4)

[137] Van der Merwe et al *Information* op cit note 47 at 136.

[138] Van der Merwe et al *Information* op cit note 47 at 136. See also the Open Document Format (OPF) and Open Office XML (OOXML) which may be suitable for archiving electronic documents.

[139] Sedona Guidelines op cit note 43 at 38.

[140] See Statement of Objects and Reasons of the Land Act 2010 Government Notice 45 of 2010.

[141] Ibid at Para 3.

[142] Ibid.

[143] Ibid at Para 3.1.

[144] Rennie et al 'The age of e-conveyancing?' op cit note 134.

[145] Article 1 of the MLEC & Art 1 of the MLES.

UETA entertains use of e-signature in real estate agreements between parties as well. It differentiates the efficiency of paper documents in an agreement of real estate from the effect of the agreements to third parties.[146] It notes that there is nothing exceptional about characteristics of transfer of immovable property transactions as compared to other transactions, hence no need to exclude them from e-contracting. [147]

It is recommended that SADC member states should conduct substantial research on how e-conveyance can be actualized. Extensive consultations with relevant stakeholders should be conducted. Factors that should form part of the research project will include decisions on which e-signature methods will be appropriate for e-conveyance transactions;[148] which of the e-documents will need to be printed and kept in paper form; the form in which electronic deeds will be stored and their time of storage,[149] and; who will bear risk of loss.[150] They should study how other states operate e-conveyance systems as well in order to learn and borrow from their strategies.[151] Lesotho has taken the first step in the right direction by availing consent forms and Cadastral Maps on its LAA website.[152] It is observed that there is a shortage of new academic literature on the subject in the SADC region, so rigorous research is necessary.[153] It should also be noted that the successful implementation of an e-conveyance system depends on the economic, political, social and cultural circumstances of each state.[154]

---

[146] UETA notes that the challenge of e-transacting will be encountered when the agreements are to be filed for effect on third parties. It proposes that while states tackle the issue of electronic filing they may file a piece of paper to perfect rights against a third party (See § 3 of UETA Comment 9 (3)).

[147] § 3 of UETA Comment 9 (3) & 7; National Association of Realtors op cit note134 .

[148] Keating op cit note 111 at 55.

[149] Christensen op cit note 127.

[150] Rod Thomas, Rouhshi Lowd & Lynden Griggs 'Land Fraud and Inappropriate Dealings in an Electronic Environment: An Australian and New Zealand Perspective' (12-13 July 2012) The 11th Australasian Property Law Teachers Conference National University of Singapore, Singapore *http://eprints.qut.edu.au/51014/* at 13. For more factors that require consideration, see Eugene Clark 'E-Conveyancing in Australia: An Important Step Along the Journey to E-government' (2011) 21 *Journal of Law, Information and Science* 62.

[151] For instance, see the Pennsylvania e-conveyance system emulated in the proposed e-conveyance structure for Lesotho above (Mekeel op cit note 117); See Ontario, Canada's e-conveyance system provided by Teranet (Christensen op cit note 127); the New Zealand e-conveyance system called Landonline (About Landonline available at *https://forms.landonline.govt.nz/about-landonline/security.asp,* accessed on 29 August 2016); and the South African Electronic Deeds Registration System (e-DRS) Policy Document approved by the Chief Registrar of Deeds on 12 June 2009.

[152] LAA 'Mapping' available at *http://www.laa.org.ls/index.php?option=com_k2&view=item&layout=item&id=2&Itemid=133,* accessed on 5 September 2016.

[153] Anthea P Amadi-Echendu, Magaret Phillips & Kudakwashe Chodokufa 'International E-Conveyancing Strategies: Lessons for South Africa' (2014) 10 *Mediterranean Journal of Social Sciences* 237 at 242.

[154] Richard Wu 'Land Registration Act 2002 of England: lessons on title registration reform for China' (2011-2012) 4 *Tsinghua China Law Review* 62 at 82; JF Whittal 'The potential use of cellular phone technology in maintaining an up-to-date register of land transactions for the urban poor' (2011) 14 *Potchefstroomse Elektroniese Regsblad* 162 /194.

The goal is for employment of e-signature and e-conveyance systems to find 'an appropriate balance between usability and security.'[155]

It is therefore concluded that an e-signature that meets CUECIC's standard can perform functions of signature in transfer of immovable property transactions or rights thereof. However, e-conveyance systems may need to be put in place and soft laws for such developed to enable the use of e-signatures and the e-transactions to take place. The next section looks into use of e-signatures in documents of title.

6.5 Documents of title

A document of title is '[a] written description, identification, or declaration of goods authorizing the holder … to receive, hold, and dispose of the document and the goods it covers.'[156] It is a written document which confers or proves ownership of property.[157] Documents of title include title deeds,[158] bill of lading,[159] warehouse receipts[160] and delivery orders.[161] Documents of title facilitate commercial transactions as a holder of the document can use it as security to obtain a loan from a financial institution, or can transfer the property with it.[162] Among documents of title listed above, only delivery orders are relevant in the case of Lesotho.[163]

---

[155] Doversberger op cit note 117 at 300; Clark op cit note 150 at 83.
[156] Bryan Garner (ed) *Black's Law Dictionary* 10ed (2014).
[157] See Business Dictionary 'Document of title' available on *http://www.businessdictionary.com/definition/document-of-title.html*, accessed on 6 September 2016.
[158] BusinessDictionary defines a title deed as a '[l]egal document (instrument) executed and acknowledged under the seal and in the presence of a notary, evidencing the right of ownership to a property described therein' available at *http://www.businessdictionary.com/definition/title-deed.html*, accessed on 7 September 2016.
[159] A bill of lading is 'a receipt of goods delivered to and received by a ship, signed by the person who contracts to carry them, or his agent, normally the master of the ship, and stating the terms of the contract of carriage under which the goods have been so delivered and received. During the period of transit and voyage the *bill of lading* is, by the law merchant, recognised as the symbol of the goods described in it, and the endorsement and delivery of the *bill of lading* operates as a symbolic delivery of the goods' (*Words and Phrases Legally Defined* 2ed available at *http://www-mylexisnexis-co-za.ezproxy.uct.ac.za/Index.aspx*, accessed on 6 September 2016).
[160] Warehouse receipts are 'certificates, issued by warehouse operators to depositors, which provide proof of ownership on a certain commodity deposited in a particular warehouse' (Antonaci L, Demeke M & Vezzani A Scientific paper No 9B *The Challenges of Implementing Price and Production Risk Management in Sub-Saharan Africa* (2015) Ulysses at 6).
[161] This is a 'written order to deliver goods, directed to a warehouseman, carrier, or other person who ordinarily issues warehouse receipts or bills of lading' (Garner op cit note 156).
[162] The FreeDictionary 'Document of title' available at *http://legaldictionary.thefreedictionary.com/document+of+title*, accessed on 6 September 2016.
[163] First, Lesotho is a landlocked country and as a result it does not have legislation relating to bills of lading. Secondly, a warehouse receipt system does not apply in Lesotho. A warehouse receipt system is an agricultural development system which requires farming and agricultural trade (USAID Southern Africa 'The Southern Africa Trade hub: Supporting Regional Food Security through Enhanced Agricultural Supply Chains' Slide 6 available at *www.satradehub.org*, accessed on 4 September 2016 & Antonaci et al op cit note 160 at 6). However, the agricultural sector of Lesotho is challenged as only 10 percent of its land is arable due to its

The Customs and Excise Act[164] together with its Regulations[165] regulate delivery orders in Lesotho. The Act provides that an officer in a state warehouse should decline to deliver goods in their custody unless they get proof that the person claiming the goods is lawfully entitled to them.[166] Consequently, an importer must present to the officer in possession of goods, a delivery order granted to him by the Director of Customs and Excise which authorises delivery of the goods to him/her (importer).[167] The Customs and Excise Regulations reiterate this requirement, but make the owner's submission of a delivery order optional. They state that a copy of a bill of entry will also be sufficient for one to claim delivery of goods.[168] In addition, the Act authorises the Minister to permit the owner to remove certain goods from a customs and excise warehouse after issuing the owner a prescribed/approved certificate, invoice or other certificate under regulations.[169] Therefore a delivery order is not mandatory for delivery of goods in Lesotho; instead, a bill of entry serves the same purpose – to grant a person a right to receive goods from a warehouse. In practice, the Lesotho Revenue Authority (LRA), an authority that deals with customs and excise, uses a bill of entry for these purposes.

Signature comes into play three times in a bill of entry. First, the officer of an authorised storage place shall endorse the copy of the bill of entry or other release document

---

mountainous terrains. This combined with severe land degradation and rising costs of seeds and fertilizers has made Lesotho's agricultural production low, failing to meet the country's needs and insufficient for export trade purposes (New Agriculturist 'Country profile – Lesotho' available at *www.new-ag.info,* accessed on 4 September 2016). Hence Lesotho does not have a warehouse receipts system and a regulatory framework for its operation. Nonetheless, warehouse receipts do apply in certain Sub Saharan Africa countries such as Zambia, Tanzania (Antonaci et al op cit note 160 at 7), Malawi (USAID *Highlights from the Field: Malawi Encouraging a Warehouse Receipt System (WRS) - first steps* (November 2011)), Kenya, Ethiopia, Uganda, South Africa and Madagascar (USAID *ICT to enhance warehouse receipt systems and commodity exchanges in Africa* (2011) 2). Warehouse receipts can either be in paper or in electronic documents signed with e-signatures (USAID 'ICT' ibid at 3 & USAID ibid slide 8). Hence they do not warrant discussion in this study. Thirdly, it is argued that a lease in Lesotho is not a document of title. In terms of s107 of the Constitution of Lesotho of 1993 and s 4 of the Land Act 2010, land in Lesotho belongs to the Basotho nation and is held in trust by the King. LAA administers the land for the King. As a result, lease holders in Lesotho acquire only the rights of use and enjoyment of the land for the duration of the lease period. When a lease expires, the land reverts to its owner, the nation. This means that a lease in Lesotho does not confer ownership; instead, it is simply a document that conveys interest in land as the state leases the land to a lease holder. MT Tlale *Property regulation in South Africa: Paving the way for regulation in Lesotho* (unpublished dissertation for LLM degree, North-West University 2014) 6-7. Although the leaseholder can deal with the property in the lease such as sublet, sell or mortgage it, they cannot do so without the consent of the Commissioner of lands, LAA because they do not have ownership rights to the land. Leases are discussed in the previous heading on conveyance of interests in immovable property, and will not form part of this discussion on documents of title. Further, title deeds in Lesotho are in respect of land and are encompassed in the discussion in part 6.4 above.

[164] 10 of 1982.

[165] Legal Notice 126 of 1984.

[166] Section 16 (2) of the Customs and Excise Act 1982.

[167] Section 39 (2) Act 1982.

[168] Regulation 12 (1) of the Customs and Excise Regulations .

[169] Section (4) (a) of the Customs and Excise Act 1989.

by signing and date stamping it before any action can be taken on the document.[170] Secondly, where an owner removes goods from a customs and excise warehouse with a certificate approved by the Minister, they should submit to the Director a valid bill of entry together with a declaration signed by the prescribed person.[171] Lastly, where an owner of goods intends to transfer ownership in the goods kept in a state warehouse, the transferor must submit to the Director a new bill of entry for re-warehousing on a prescribed form and a declaration of transfer, which is signed and dated by both the transferor and the transferee.[172]

Although the Lesotho Bill expressly excludes documents of title from e-communications and e-signature provisions, it is argued that its provisions are superseded by events. In August 2014, LRA engaged in a pilot project on automated bills of entry called Customs Procedures and Automation Project.[173] Under this project, a trader (owner of property) or a clearing agent, acting on behalf of a trader electronically lodges an e-bill of entry with LRA for clearance, instead of submitting it physically at LRA. When LRA clears the e-bill of entry, it changes the status of the bill of entry in its system to show that a trader is now authorised to declare goods in a warehouse. The trader receives a message that the bill of entry is cleared. LRA gives the trader and the warehouse officer access to the system, thus they can view the changing status of the bill of entry on LRA's database.[174] Parties involved in the submission, clearance and issuance of bill of entry communicate on a secure LRA network called Asycudaworld (AW) computer system of custom data.[175] AW uses a strong, wide-ranging declaration process that applies the European Single Administrative Declaration as a standard form.[176] Only limited persons have access to the network.[177]

Due to the system's operation, the need for an officer of a warehouse to endorse a bill of entry before action is taken on it falls away. So does the need for an owner to send signed documentation to the Director where they want to remove property from a customs and excise warehouse or to transfer ownership of property in warehouse to another person. All that is required is for the owner to send a new bill of entry with the transferee's names to LRA for clearance. This is since under the Automated system, LRA accepts a typed name of

[170] Regulations 12 (5) & (6) of the Customs and Excise Regulations.
[171] Section 40 (3) (a) & (b) of the Customs and Excise Act 1982.
[172] Regulation 37 of the Customs and Excise Regulations.
[173] This was part of an LRA umbrella project named Pilot Customs Modernisation Program.
[174] Interview with Mr. Lefielo Lefielo Manager Clearance Hub Lesotho Revenue Authority Maseru 11 April 2017.
[175] Lesotho Revenue Authority 'National rollout customs automated procedures' available at *ww.lra.og.ls,* accessed on 11 April 2017.
[176] Lesotho Revenue Authority 'Asycuda' available at *ecustoms.lra.org.ls,* accessed on 11 April 2017. The standard declaration form is also used in the SADC region.
[177] Lesotho Revenue Authority 'Information for traders' available at *ww.lra.og.ls,* accessed on 11 April 2017.

the person who lodges the bill of entry as sufficient proof of the owner of property or their agent. Additionally, LRA looks at the letterhead on invoices submitted by the lodging party together with the bill of entry in support of identity verification.[178] The pilot project was conducted with success in the Maputsoe border post for a period of a year. Subsequently, LRA rolled out the system to six major ports of entry in Lesotho during 2015 and 2016. It is currently operative in seven ports.[179]

Due to the success of the LRA automated customs project, the Customs and Excise Act 1982 and other relevant statutes are currently undergoing legal review to accommodate the modern methods. One of the results of the review is the Customs and Excise (Effective date of Customs Automation) Notice.[180] This statute was released by Parliament in February 2016. It authorises the use of an e-bill of entry in certain ports of entry where goods are imported or exported for commercial purposes.[181] It states that the e-bill of entry shall be accessed through an access code supplied by the LRA Commissioner General, and submitted to the commissioner electronically.[182] One of the issues discussed in the legal review is whether the statutes should request a specific e-signature for e-bills of entry. But currently a typed name, a letterhead in an e-invoice and an access code are accepted as sufficient proof of identity in an e-bill of entry. It follows that the Lesotho Bill's exclusion of bills of entry from its application is retrograde contrary to its spirit of facilitating e-commerce.

Electronic documents of title have a few benefits. They save time and administrative costs, reduce chances of error and if appropriate methods are applied, can increase security levels, hence be free from fraud.[183] It is recalled that an e-record can provide a similar level of security to paper with respect to paper functions, but is more reliable in identifying a source and content of data.[184]

It is noted that CUECIC excludes documents of title from its scope of application. It states that the repercussions of unauthorised copies of title documents are so immense that mechanisms are required that can guarantee that the documents cannot be copied – solutions which are yet to be created.[185] It is argued that mechanisms for securing non-duplication of

[178] Interview with Mr Lefielo op cit note 174.
[179] LRA 'National rollout customs automated procedures' op cit note 175.
[180] Legal Notice 10 of 2016.
[181] Section 3 (2) of the Customs Automation Notice.
[182] Section 3 (1) of the Customs Automation Notice.
[183] John Livermore & Krailerk Euarjai 'Electronic Bills of Lading and Functional Equivalence' 1998 (2) *Journal of Information, Law and Technology* available at *http://elj.warwick.ac.uk/jilt/ecomm/98_2liv/*, accessed on 2 September 2016.
[184] Paragraph 16 of Guide to MLEC.
[185] Para 80 of Explanatory note on CUECIC.

bills of entry are already operational in Lesotho as illustrated above. Moreover, the SADC Model law and other SADC states do not exclude documents of title from application of e-signature provisions due to their realisation that documents of title can be electronic and apply e-signatures. As a result, it is submitted that the Lesotho Bill's exclusion of documents of title from e-signature application is superfluous.

6.6 Indentures, declaration of trusts or power of attorney

An indenture is 'a deed or elaborate contract signed by two or more parties.'[186] It also refers to '[a] document such as a mortgage or deed of trust, which provides for security for a financial obligation and which sets forth essential terms such as interest rate and due date or maturity date.'[187] An indenture therefore includes among others, mortgage bonds,[188] notarial bonds,[189] and deeds of trust.[190] The role of signature in indentures is discussed below.

6.6.1 Signature in creation and execution of indentures

Mortgage bonds and notarial bonds are regulated by the DRA and DRR. Signature plays a role in several stages in the creation and execution of a mortgage bond. First, a mortgage bond must bear an endorsement signed by a legal practitioner, a notary public or conveyancer (legal practitioner) that indicates that it was prepared by a legal practitioner.[191] Secondly, the legal practitioner should initial all pages of the endorsement and bond and any alterations made on the documents.[192] Thirdly, there must be a power of attorney that authorises an agent to pass, amend, cede or cancel the mortgage on behalf of the mortgagor, which must be attested by two competent witnesses.[193] The consent of a proper authority is necessary to create the bond.[194] The mortgagors submit these documents to the Registrar, whereby the

[186] Garner op cit note 156 .
[187] YourDictionary 'Indenture defined' available at *www.yourdictionary.com>indenture*, accessed on 27 April 2016; See Garner op cit note 156 for the different kinds of indentures.
[188] A mortgage registered on immovable property of a debtor (mortgagor) or their surety, gives the creditor (mortgagee) a limited real right to the debtor's property as security pending payment of the debt. See (AJ van der Walt & GJ Pienaar *Introduction to the Law of Property* 7 ed (2016) 296).
[189] See A notarial bond means 'a bond attested by a notary public hypothecating movable property generally or specially' (ss 2 (1) of the DRA).
[190] A 'trust exists when property is to be held or administered by one person on behalf of another or for some purpose other than his own benefit.' (Garner op cit note 156).
[191] Regulation 30 of DRR.
[192] Regulation 30 of DRR.
[193] Section 52 of the DRA. Alternatively it may be attested by a Commissioner of oaths, a Magistrate or Justice of the Peace.
[194] Section 28 (1) of the DRA.

mortgage bond is executed by the owner or an authorised legal practitioner in the presence of the Registrar.[195] The Registrar then attests and registers the mortgage bond.[196]

Regarding notarial bonds, the DRA states that the Registrar shall register notarial bonds.[197] However, a notary public shall attest to a notarial bond before its registration, failing which, the Registrar will not have it registered.[198] The notarial bond is registered when its entry is made in the appropriate register of the Deeds registry.[199] A trust on the other hand will be valid if it reflects the intention of a settlor.[200] However, the law does not require signature in the creation or execution of a trust.[201]

It is submitted that an e-signature can apply in the execution of indentures. For example, a legal practitioner can draft an endorsement which indicates that they are the person who drafted an electronic mortgage bond (e-mortgage bond) together with other e-documents. They can then show the e-communication to parties to the mortgage and their witnesses. These people will subsequently click on an "I accept" icon as an indication that they agree to the contents of the endorsement and e-mortgage bond.[202] The legal practitioner can then sign the endorsement and the e-mortgage bond with any e-signature technology that meets CUECIC's requirements. They can email the e-documents to the Registrar for registration on a secure network.[203] The Registrar can further sign the bond with an e-signature for registration purposes. As indicated earlier, a digital signature based on Public Key Infrastructure[204] or ordinary e-signature supported with metadata can provide online security and therefore protect the integrity of e-documents by indicating if any changes were effected on the documents.[205] Hence the legal practitioner and Registrar will be free to use either of the signatures. Subsequent to this, the legal practitioner can hand over the e-

[195] Section 28 (2) of DRA.
[196] Section 5 (f) of the DRA; Reg 28 (2) of the DRR.
[197] Section 5 (i) of the DRA.
[198] Section 40 (2) of the DRA.
[199] Section 40 (8) of the DRA.
[200] Garner op cit note 156 .
[201] See the Friendly Societies Act of 1882; Trustee Investment in Basutoland Securities Proclamation 62 of 1950; Charities Trust Act 24 of 1975; Workmen's Compensation Trust Fund Regulations LN 42 of 1985 & Lesotho Unit Trust Act 8 of 2003.
[202] Arvin Sahakian 'E-Signatures Will Change the Mortgage and Real Estate Industry' April 2015 available at *https://www.besmartee.com/blog/e-signatures-will-change-the-mortgage-and-real-estate-industry,* accessed on 26 September 2016.
[203] Sahakian ibid.
[204] Sahakian ibid.
[205] See parts 2.9.10.1 & 5.6.3.3 above.

mortgage bond on a memory stick, Compact Disk (CD)[206] or send it to parties to the mortgage in PDF on a secure network.

CUECIC and UETA maintain that a notary public can notarise e-communication with an e-signature.[207] To do so, the notary public simply has to be present in the same room with the parties to the bond. The notary will then verify the identities of the parties, verify that they understand and attest to what they are about to sign, witness the signers' sign the notarial bond with their e-signatures, then sign the electronic notarial bond themselves with their e-signature as indication that the signers signed it in his/her presence. It is noted that the SADC ML and the ECT Act of South Africa do not exclude indentures from e-signature application.

Electronic indentures have several advantages. For instance, they save time of processing; reduce costs[208] of couriering documents between involved parties for review of the documentation; they are easily available to parties to the mortgage hence the parties can quickly detect errors on the documentation such as misspelt names and correct them; they save paper; they are therefore efficient as money lenders such as banks finance borrowers more speedily; and they enable lenders to trail track dated and time stamped activities that took place in concluding the mortgages.[209]

6.6.2 Power of attorney

A power of attorney is 'an instrument granting someone authority to act as agent or attorney-in-fact for the grantor.'[210] The law's requirement of written and signed proof of an agent's authority to take action is necessary to avoid disputes on whether the person who signed a contract for another (principal) indeed had the authority to act for that principal.[211] The Registrar is to register powers of attorney.[212] They do so by signing the deeds registry endorsement in respect thereof.[213] For application of an e-signature in a power of attorney, reference is made to part 6.4.1.4 above.

---

[206] Sahakian ibid. Alternatively, the legal practitioner can communicate the e-mortgage bond to the parties to the morgage through email and use any of the available online authentication methods previously discussed in part 2.9.11 to provide document security.
[207] See part 5.6.3.3 above.
[208] James Cain, Matt Levorchick, Alan Matuszak, Allan Pohlman, & Douglas Havelka 'eLoanDocs: Riding the Tide of Technology Without Wiping Out' (2015) 36 *Communications of the Association for Information Systems* 759 at 760.
[209] Sahakian op cit note 202.
[210] Garner op cit note 156.
[211] *Gugu & Ano v Zongwana & others* [2014] 1 ALL SA 203 [25].
[212] Sections 5 (t) of the DRA.
[213] Sections 11 (1) of the DRA.

The above discussion shows that the Lesotho Bill should not exclude indentures or power of attorneys from application of e-signature provisions. As previously indicated, e-documents can be archived for long periods of time.[214] These proposals for storage of e-records must not preclude the Registrar from printing the documents on paper for filing purposes if they chose to.

6.7 Conclusion

This chapter reflects that an e-signature which meets the standard set by CUECIC can fulfill the purpose of a handwritten signature in the creation and execution of wills, transfer of immovable property or rights in immovable property, more so if e-conveyancing is practiced, in indentures and powers of attorney, and in documents of title. As a result, it is submitted that the laws are not justified in excluding an e-signature from their application in these transactions. Nonetheless, the study shows that an e-signature cannot meet the purpose of endorsement by a signature in negotiable instruments. Hence the law's exclusion of e-signature application in these matters is justified.

[214] See the Sedona Guidelines and PDF in part 6.4.1.4.1 above.

CHAPTER SEVEN: RECOMMENDATIONS AND CONCLUSION

7.1 Introduction

This study examined how the Southern African Development Community (SADC) and Lesotho e-signature instruments apply the principles of functional equivalence and technology neutrality to effectively regulate e-signatures in e-transactions. This chapter reviews the study and summarises the key findings and concludes with recommendations for adequate e-signature regulation.

7.2 Summary of findings

7.2.1 Traditional signatures and e-signatures

Chapter two of this study discussed the concept of signature in contracts and the purpose of the signature formality, which is to promote certainty, prevent fraud and provide evidence of a contract.[1] The chapter found that traditional signatures have several functions and different forms, but their primary function is authentication. Moreover, function of a signature takes prevalence over the form of signature.[2] Again it found that there are hierarchies of document authentication procedures offline which serve to verify that a state of affairs exists. These authentication methods give documents more legal credibility when tested in court.[3] What is more, traditional signatures are prone to risks of fraud and malpractice, but factual evidence helps determine the truthfulness of a signature.[4]

Additionally, chapter two found that there are several forms of e-signature technologies and new authentication technologies emerge at a fast rate. The e-signature technologies differ in their ability to perform functions of the traditional signature. They also differ in their accessibility and security levels. Like traditional signatures, e-signatures are susceptible to risk and manipulation,[5] but there are several online authentication methods which can curb the vulnerability of e-signature technologies by reflecting the origin of a

[1] Part 2.2 above.
[2] Parts 2.5 & 2.6 above.
[3] Part 2.8 above.
[4] Part 2.7 above.
[5] Parts 2.9.1 to 2.9.10 above.

document and preserving its integrity.[6] Thus, it is possible for e-signatures to meet the purposes of a traditional signature if their shortcomings are adequately addressed.

7.2.2 Functional equivalence, technology neutrality and effective law

Chapter three of this study explored principles of ICT regulation, namely functional equivalence and technology neutrality in the context of e-signatures. It also explored principles that guide a lawmaker in drafting effective ICT laws. The chapter found that a functionally equivalent e-signature rule must provide the online user with a similar level of protection or have the same legal effect as a rule that regulates signature in offline contracts.[7] A rule should be functionally equivalent in both legal terms and practicability.[8] Moreover, a rule will achieve functional equivalence if it addresses the effects of people's conduct or their mental state at the time of engaging in conduct, and not the means of carrying out conduct.[9]

The chapter further found that e-signature rules should be technology neutral. A rule is technology neutral if it is non-discriminatory of e-signature technologies and addresses the effects of signature and not the means of making a signature. A technology neutral rule also promotes equivalence between offline and online spheres, enables innovation of new technologies and is able to withstand technology developments.[10] It also found that soft law can complement e-signature laws where necessary to assist users in the proper application and understanding of e-signatures.[11]

Furthermore, the chapter found that a law is effective if it achieves its social aims. It will achieve its aim if it is understood by its subjects and is stable over time. But if a law is drafted with detailed precision, is over-complex and changes frequently to keep up with technology developments, it will not achieve its aim.[12] The legitimacy of such a law is compromised.[13] Lastly, a rule's effectiveness is measured by its capacity to attract and maintain participants.[14] The chapter concludes that adequate e-signature regulation must be functionally equivalent and technology neutral to be effective.

---

[6] Part 2.9.11 above.
[7] Part 3.2.3.2 above.
[8] Part 3.2.3.2.1 above.
[9] Part 3.2.5 above.
[10] Part 3.3.3 above.
[11] Part 3.3.6 above.
[12] Part 3.4.1 above.
[13] Part 3.4.2 above.
[14] Part 3.4.2 above.

7.2.3 UNCITRAL instruments on e-signature regulation

Chapter four examined relevant UNCITRAL instruments and their interpretation of functional equivalence and technology neutrality in e-commerce for e-signature regulation. According to the research, the MLEC holds that:

- a lawmaker should create criteria (a rule) which will enable the data message to enjoy the same level of legal recognition as paper documents which perform a similar function, to promote offline and online equivalence.[15]
- a functionally equivalent rule should not be stricter or less strict than an offline rule.
- a technology neutral regulation encompasses the principle of non-discrimination of e-communication technologies and non-discrimination between online and offline communication.
- a technology neutral regulation should accommodate both current and future technologies.[16]
- criteria for the legal recognition of a data message where law requires signature is that the method should be used to identify a signer and reflect their approval of data, and the method should be as reliable as appropriate in the circumstances.[17]
- any e-signature technology is sufficient to meet the law's requirement of signature if it meets the criteria, but the question whether it was as reliable as appropriate is a matter of evidence.
- the reliability levels of e-signatures differ and their use depends on the purpose of each transaction.

The chapter found that relevant authorities can provide guidelines on the differing levels of e-signature reliability appropriate for different transactions, on the forms of evidence sufficient to proof reliability and on presentation of the evidence in proceedings.

Additionally, chapter four found that UNCITRAL's second instrument, the MLES:

- sets out a technical reliability standard to be met by e-signature technologies in order to have legal effect. But the standard favours, among currently available technologies, the digital signature based on PKI.

[15] Part 4.3.2.1 above.
[16] Part 4.3.2.2 above.
[17] Part 4.3.3 above.

- does not prohibit parties to prove the reliability of an e-signature through other means apart from its technical reliability standard.
- adopts a hybrid approach of technology specific and technology neutral e-signature regulation.[18]
- clarifies that not all e-signature technologies which identify a person represent the legal notion of signature. Instead, an e-signature technology should also be capable of indicating a signer's approval of information for it to have legal effect equivalent of a signature.[19]

Moreover, chapter four found that UNCITRAL's latest instrument, CUECIC, provides the best interpretation of functional equivalence and technology neutrality principles through its criteria for the legal recognition of a signature in e-communications. This is because:

- it adds an alternative reliability standard to the MLEC's criteria of e-signature recognition by stating that the method of signature is reliable if it is factually proved to show the identity and intent of a party.[20]
- it shows that reliability of an e-signature is not guaranteed by high technology methods alone, but by other surrounding factors.
- again, if the identity and intention of the signer is not disputed, the e-signature should not be denied on the basis that it was not as reliable as appropriate.
- its requirement that a method of signature must be used to reflect a signer's intent regarding information rather than their approval of information facilitates use of ordinary e-signatures for authentication of e-documents.[21]
- it therefore promotes equal treatment of online users to offline users more effectively.
- legislative instruments designed in line with CUECIC will be cost effective, practicable[22] and likely to be effective in removing hurdles to the use of e-signatures and promoting e-commerce.

[18] Part 4.4.3 & 4.4.5 above.
[19] Part 4.4.3 above.
[20] Part 4.5.2 above.
[21] Part 4.6 above.
[22] Part 4.6 above.

7.2.4 Assessment of SADC and Lesotho instruments

Based on the foundations set by previous chapters, chapter five assessed the Lesotho Bill and SADC ML's application of functional equivalence, technology neutrality and principles of effective law making in e-signature regulation. Regarding technology neutrality, it found that: although the instruments' definition of a SeS is open enough to accommodate other technologies, among currently available e-signature technologies, its features favour the digital signature based on PKI. This introduces a technology specific aspect to the definition.[23]

Furthermore, the instruments treat the SeS as superior to the ordinary e-signature by granting it certain presumptions, contrary to principles of technology neutrality. However, it found that the lawmaker can create presumptions on the use of e-signature that are technology neutral and have a functional equivalent effect without making the SeS superior to other e-signatures. Further, the Lesotho Bill's prescribed use of a SeS where law requires signature addresses conduct of signing instead of effects of signing contrary to the purpose of technology neutral regulation.[24]

Once more, chapter five found that the instruments' prescribed use of SeS for different hierarchies of document authentication favours the SeS contrary to technology neutrality. This is not the position offline. Offline laws do not prescribe use of a specific form of traditional signature for document authentication. It found that ordinary e-signature technologies that meet CUECIC's standard can perform the functions of document authentication if there is evidence to show their reliability. Soft law may provide guidance on the use of e-signatures for document authentication as is done in the USA.[25]

Again, the chapter found that the instruments' SeS may fail to accommodate future e-signature technologies which do not meet features of a SeS yet are reliable and cost effective. This will limit the instruments' sustainability.[26]

Thus, the Lesotho Bill's SeS provisions limit the technology neutrality of the instrument, and are sometimes technology specific. In other words, the Lesotho Bill adopts the hybrid approach. It aligns more with the MLES rather than with CUECIC. On the contrary, the SADC ML is more technology neutral and aligns with CUECIC due to

[23] Part 5.6.1 above.
[24] Part 5.6.3.1 & 3.3.3.1.1 above.
[25] Part 5.6.3.3 above.
[26] Part 5.6.3.4 above.

recognising any e-signature as sufficient to meet the law's requirement of a signature if it meets CUECIC's criteria. Nonetheless, the SADC ML's prescription of use of the SeS for document authentication and presumptions on the SeS limit its technology neutrality. By contrast, the Lesotho Bill's provisions on ordinary e-signatures are technology neutral.

Regarding functional equivalence, chapter five found that the Lesotho Bill's provisions on a SeS do not create a functional equivalent of a hand written signature because: they prescribe use of a SeS where law requires signature contrary to CUECIC's criteria of functional equivalence; they disregard relevant functions and reliability standards of e-signature sufficient for e-signature recognition identified by CUECIC and look to features of a technology for e-signature recognition instead; and they are not feasible in practice.[27] On the other hand, it found that the Lesotho Bill's e-signature only meets the functions of signature required by CUECIC, but is silent on reliability standards an e-signature is to meet.

With respect to proof of reliability of e-signatures, chapter five found that the Lesotho Bill and SADC ML consist of rules on admissibility and assessment of evidential weight of e-evidence[28] which will assist in the proof of the reliability of e-signatures. It found that the USA uses factual evidence including e-evidence to prove the reliability of e-signatures in proceedings and that the Model law in electronic evidence applies the same approach.[29] It found that if the Lesotho Bill enables the reliability of an e-signature technology to be proved with factual evidence like the USA and Model law on electronic evidence, it will comply with CUECIC's reliability standards and provide a functionally equivalent effect. However, the chapter found that the ECTA and Lesotho Bill make no provisions for how e-evidence is to be collected, stored or presented in proceedings.

On the other hand, the SADC ML's provisions on e-signature align with CUECIC's criteria of functional equivalence. However, it does not expressly provide for CUECIC's alternative e-signature reliability standard namely that a method of signature will be reliable if proved by itself or with facts to identify and show the intent of a signer. Again, the SADC ML's provisions on a SeS in document authentication fall short of applying functional equivalence.

With respect to effectiveness, chapter five found that the Lesotho Bill's provisions on the SeS will inhibit it from achieving its social aim of increasing use of e-signature and

[27] Part 5.9.2 above.
[28] Part 5.9.3 above.
[29] See part 5.9.3.2 above.

enhancing the growth of e-commerce by removing barriers to e-transactions resulting from uncertainties in signature requirements. This will be caused by the SeS' potential incomprehensibility to its subjects, its potential instability resulting from regular amendments and its failure to meet its subjects' needs for lack of technology neutral and a functionally equivalent effect.[30] However the Lesotho Bill's provisions on ordinary e-signatures may help it achieve its aim provided it is amended and adds that the ordinary e-signature should meet CUECIC's reliability standards.

On the other hand, the chapter found that if implemented in domestic law, the SADC ML is more likely to be effective due to its recognition of an e-signature that meets CUECIC's criteria where the law or parties to a transaction require signatures.[31] Otherwise its provisions on the SeS will have a minimal effect on its effectiveness.

Additionally, chapter five, in comparing South Africa, the EU and the USA, found that the USA closely aligned with the study's proposed principles of e-signature regulation. Just like the Lesotho Bill, South Africa and the EU adopted a two tier-approach of technology neutral and technology specific provisions which hold an SeS, AeS and QeS as superior to ordinary e-signatures. Consequently, they are ineffective in promoting the use of e-signatures in e-commerce where law requires signature.[32] Contrariwise, the USA's legal instruments adopted a technology neutral approach on e-signature regulation. They do so by granting equal legal recognition to all e-signature technologies in all activities. Thus they effectively promote e-signature use.

7.2.5 Transactions excluded from e-signature application

Lastly, chapter six examined whether the Lesotho Bill and SADC ML are justified to exclude certain transactions from application of e-signature provisions in terms of functional equivalence and technology neutrality. It found that an e-signature that meets the criterion of CUECIC supported with accessible technologies that ensure its reliability such as metadata, can meet the purposes and functions of signature in some of the matters. These include wills and codicils,[33] the sale, disposition, alienation and conveyance or transfer of immovable property or rights in immovable property transactions, long lease agreements,[34] documents of

[30] Part 5.10 above.
[31] Part 5.10 above.
[32] Part 5.10.4 above.
[33] Part 6.2 above.
[34] Part 6.4 above.

title[35] and indentures.[36] The challenge of filing and archiving of electronic records such as e-deeds of transfer can be met with storage of the e-records in Portable Document Format (PDF) or the transfer of an e-record to a new medium on a periodic basis.[37] For transfer of immovable property or rights in immovable property transactions it is advisable that the Lesotho Land Administration Authority establish an e-conveyance system to facilitate use of e-signatures in the e-transactions.

Nonetheless, chapter six found that an e-signature cannot meet the functions of signature in negotiable instruments for want of the negotiability function.[38] Despite the findings, the chapter noted that the submissions are tentative pending further research on whether the Lesotho Bill is justified to exclude application of its provisions on the recognition and effect of e-communications and on e-transactions, from the discussed matters.[39] The section below makes recommendations that address the obstacles identified in the instruments.

7.3 Recommendations

The findings of this study show that the Lesotho Bill and the SADC ML do not adequately align with the principles of technology neutrality and functional equivalence in their regulation of e-signatures. As a result, the instruments' effectiveness in facilitating the use of e-signature and consequently enhancing the growth of e-commerce will be limited. The following recommendations will assist the Lesotho Bill and SADC ML to adequately regulate e-signatures.

First, the Lesotho Bill should recognize an ordinary e-signature that meets CUECIC's standard as sufficient where law requires signature. It should adopt E-SIGN's position which prohibits regulatory bodies from developing laws that grade e-signature technologies. The differing reliability levels of an e-signature set by CUECIC can ensure that the e-signature is secure and appropriate for each transaction, hence meets the law's requirement of signature.

It is recommended that to facilitate proof of the reliability of an e-signature in an e-document, the instruments' should adopt the UETA and the Model law on electronic signatures' approach on proof of e-signatures. That is, they should expressly provide that they permit parties to produce any form of relevant evidence which will be given due evidential

[35] Part 6.5 above.
[36] Part 6.6 above.
[37] Part 6.4.1.4.1 above.
[38] Part 6.3.2.3 above.
[39] See s 5 (2) of the Lesotho Bill.

weight to show that an e-signature is that of a signer and was used to authenticate a document, hence prove the reliability and validity of e-signatures. This will help them closely align with CUECIC's criteria.[40]

Secondly, the Lesotho Bill and SADC ML should remove presumptions which favour an SeS. They should further adopt UETA's provision that does not give the presumption of attribution to a specific e-signature technology but maintains that an e-signature is an act of a person who made it. Whether an e-signature attributes a signer can be proved by showing the efficacy of a security process used to connect the person to the e-communication. It is therefore recommended that relevant authorities must develop soft laws that guide parties on how to prove the efficacy of a security process used. Thus, where the attribution, validity or proper application of an e-signature is disputed, parties must adduce evidence whose evidential weight will help prove the disputed issues.

Alternatively, the Lesotho Bill and SADC ML can maintain the concept of presumptions relating to e-signature. But the lawmaker must 'reformulate' the presumptions to ensure that they are technology neutral and have a functional equivalent effect.[41]

Thirdly, the Lesotho Bill and SADC ML should amend their sections that prescribe the use of a SeS where law requires document authentication. They should recognise e-signature technologies that meet CUECIC's criteria as sufficient for document authentication instead. Similar to the USA, relevant authorities must develop guidelines which assist users on how to authenticate documents with e-signatures of a high reliability level, but yet are practicable. The soft law may also provide that if a security method such as identifying words, numbers, or encryption can be used to prove that an e-signature attached to e-communication is attributable to a certifying officer, the e-communication is deemed certified. But the soft law's aim must be to ensure that an e-signature used for authentication is accessible, reliable and can reflect manipulation. Where the ordinary e-signature is subject to challenge in document authentication, it will be proved by either of the reliability tests set out in art 9 (3) (b) of CUECIC. Thus the e-signature will be proved with factual evidence as it is done when the authenticator's handwritten signature is disputed in a paper document.

Fourthly, where the law requires additional information for document authentication, the guidelines must indicate how the requirements should be met online. This lesson is learnt from the USA. For instance, where a law requires an Apostille in document authentication,

[40] See part 5.9.3.2 above.
[41] See part 5.6.2 above.

the guidelines may state that the authenticating officer must type the contents of the Apostille into the document, sign it with an ordinary e-signature and email it on an encrypted network, or send it as a password locked attachment to an email, or verify that metadata of the e-communication remained unchanged after communication. The soft law will consequently guide e-commerce users on use of measures that will help ensure that the integrity of their e-communication or e-signature is intact, hence provide accessible reliable document authentication without imposition of an SeS.[42]

It is recommended that the Lesotho LAA develop an e-conveyance system and soft laws to facilitate use of e-signatures in transfer of immovable property or rights in immovable property transaction.

Moreover, if the Lesotho Bill and SADC ML do not make the SeS mandatory in e-commerce, the instruments will be more effective due to their improved functional equivalence and technology neutrality. The laws' subjects will understand their provisions on e-signature, comply with them due to their practicability and increase their use of e-signatures. Hence the instruments will achieve their social aim of enhancing the growth of e-commerce. Possible suggestions for draft legislative provisions of the Lesotho Bill and SADC ML are attached herein to provide guidance to the legislature upon improvement of the instruments.[43]

If the Lesotho Bill and SADC ML implement the above recommendations, online regulation of e-signatures will have a similar effect to offline regulation. The instrument's subjects will not have to rely on a specific impracticable e-signature technology to fulfil the laws' requirement of signature or document authentication. But the instruments will facilitate use of accessible reliable e-signatures that can authenticate e-communication and show forgery and manipulation, hence perform the purposes of signature in a contract. Like the offline world, the instruments will require the use of evidence where an e-signature is disputed. This said, identified areas for future research are listed below.

7.4 Suggestions for further research

Four areas are identified for further research to promote the growth of e-commerce in the public interest. First, the Lesotho Bill and SADC ML wrongly excluded their e-signature provisions from wills, transfer of immovable property and rights in immovable property

[42] See part 5.6.3.3 above.
[43] See Recommended draft legislative provisions attached herein.

transactions, indentures and documents of title. However, it is imperative that further research is conducted on whether the Lesotho Bill is justified by excluding these transactions from application of its provisions on legal recognition and effects of e-communication and its provisions on e-transactions in terms of functional equivalence and technology neutrality.[44] The reason is that other provisions are inter-related with an e-signature, hence the recommendations regarding the instruments' exclusion of the transactions from e-signature application cannot be definite until its exclusion of the transactions from the other provisions is explored. Subsequent to further research, holistic recommendations can be made on whether the lawmaker should extend e-signature and other excluded provisions to the excluded transactions.

Secondly, e-evidence will play a significant role in proving the reliability of e-signatures if the Lesotho Bill adopts CUECIC's criteria on regulation of signatures. Hence research must be conducted on appropriate methods required to collect, store and present the e-evidence in proceedings.

Thirdly, since one of the recommendations in this study is that e-conveyance should be actualised in Lesotho, further research should be conducted on development of risk allocation rules in e-conveyance. Lastly, further research is to be conducted on how an e-signature is to meet the negotiability function in negotiable instruments online. This is so that the Lesotho Bill and SADC ML can extend their e-signature provisions to negotiable instruments.

[44] These sections include legal recognition of e-communications and writing, formation and validity of contracts, variation by agreement, time of dispatch and receipt of e-communications, place of dispatch and receipt of e-communications, time of contract formation, automated transactions and input errors.

REFERENCES

Books

Adams C & Lloyd S *Understanding PKI: Concepts, Standards, and Deployment Considerations* 2 ed (2002) Addison-Wesley, USA.

Baldwin R, Cave M & Lodge M *Understanding Regulation: Theory, Strategy, and Practice* 2ed (2012) Oxford University Press, New York.

Baumer D & JC Poindexter *Cyberlaw and e-commerce* (2002) McGray-Hill, New York.

Bhana D, Bonthuys E & Nortje M *Student's Guide to the Law of Contract* 3 ed (2013) Juta & Co Ltd, Claremont.

Bradfield G & Lehmann K *Principles of the Law of Sale & Lease* 3 ed (2013) Juta & Co, Cape Town.

Brazell L *Electronic Signatures and Identities Law and Regulation* 2 ed (2008) Sweet & Maxwell, London.

Buys R & Cronje F *Cyberlaw@SA II: The law of the internet in South Africa* 2 ed (2004) Van Schaik, Pretoria.

Chander A *The electronic silk road: how the web binds the world together in commerce* (2013) New Haven, London: Yale University Press.

Chissick M & Kelman A *Electronic Commerce: Law and Practice* 3 ed (2002) Sweet & Maxwell, London.

Christie J O *Conveyancing Practice Guide* 3 ed (2008) LexisNexis, Durban.

Christie JO & Allen West *The Conveyancing Practice Guide* 4 ed (2015) LexisNexis, Durban.

Colonna L *Legal implications of data mining* (2016) Tallinna Raamatutrükikoda, Tallinna.

Davidson A *The Law of Electronic Commerce* (2009) Cambridge University Press, Australia.

De Vaujany F, Mitev N, Lanzara GF, Mukherjee A (eds) *Materiality, Rules and Regulation: New Trends in Management and Organization Studies* (2015) Palgrave Macmillan, UK.

Eastlake DE & Niles K *Secure XML: The New Syntax for Signatures and Encryption* (2002) Pearson Education.

Edwards L & Waelde C (eds) *Law and the internet: A framework for electronic commerce* 2ed (2000) Hart Publishing, UK.

Farrand JT *Contents of a Conveyance: Registered and unregistered land* (1963) Oyez Publications, London.

Feno J & Nielson R *Legal Aspects of Electronic Commerce* (2001) Jurist-og Okonomforbundets, Denmark.

Ferguson N, Schneier B & Kohno T *Cryptography Engineering Design Principles and Practical Applications* (2010) Wiley Publishing, Indianapolis.

Ferguson N & Schneier B *Practical Cryptography* (2003) Wiley Publishing Inc, Indiana.

Fouche M, Collier-Reed DW, Haupt F, Jones M , Van As HJ *Legal Principles of Contracts and Commercial Law* 8 ed (2015) LexisNexis, Durban.

Forder J & Svantesson D *Internet and e-commerce law* (2008) Oxford University Press, Australia.

Fransman M *The New ICT Ecosystem Implications for Policy and Regulation* (2012) Cambridge University Press, New York.

Fuller L *The Morality of Law* (1964) New Haven & London, Yale University Press.

Garner B (ed) *Black's Law Dictionary* 10ed (2014) Thomas Reuters, USA.

Garner B (ed) *Black's Law Dictionary* 9ed (2004) Thomas Reuters, USA.

Gering L & Tobias DG *Handbook on the law of negotiable instruments* 3 ed (2007) Juta & Co (Pty) Ltd, Cape Town.

Gibson JTR *South African Mercantile and Company Law* (2003) Juta & Co Ltd, Lansdowne.

Guest AG *Chalmers and Guest on Bills of Exchange, cheques and promissory notes* 17 ed (2009) Sweet & Maxwell, London.

Hart HLA *The Concept of Law* (1961) Clarendon Press, Oxford.

Havenga P & Havenga M (eds) Hurter E, Kelbrick R, Manamela E, Manamela T, Schulze H & Stoop P *General Principles of Commercial Law* 7 ed (2010) Juta & Co Ltd, Claremont.

Hawthorne L & Pretorius C J *Contract Law Casebook* 3 ed (2010) Juta & Co Ltd, Cape Town.

Hofman J, Johnston D, Handa S & Morgan C et al (eds) *Cyberlaw: A Guide for South African's doing business online* (1999) Ampersand Press, Cape Town.

Holliday A *Doing and Writing Qualitative Research* 3 ed (2016) SAGE Publications, London.

Hornby A S *Oxford Advanced Learner's Dictionary of Current English* 7 ed (2005) Oxford University Press.

Houghton Mifflin Company, *The American Heritage: Dictionary of the English Language* 5 ed (2011) Houghton Mifflin Company, USA.

Hutchison D (ed), Pretorius CJ (eds), Du Plessis J, Eiselen S, Floyd T, Hawthorne L, Kuschke B, Maxwell C, Naudé T & De Stadler E *The Law of Contract in South Africa* 2ed (2012) Oxford University Press Southern Africa (Pty) Ltd, Cape Town.

Jager T *Alienation of Land* (1982) Juta & Co Ltd, Cape Town.

Jamneck J (ed), Rautenbach C (ed), Paleker M, Van der Linde A & Wood-Bodley M *The Law of Succession in South Africa* 2ed (2012), Oxford University Press, Southern Africa.

Joubert DJ *General Principles of the Law of Contract* (1987) Juta & Co Ltd, Kenwyn.

Kahn E *Contract and Mercantile Law: A Source Book* 2 ed (1988) Juta & Co Ltd, Cape Town.

Kerr A J *The Principles of the Law of Contract* 6 ed (2002) Butterworths, Durban.

Kirchberger C *Cyberlaw in Sweden* 2ed (2014) Kluwer Law International, The Netherlands.

Kirton J J & Trebilcock M J (eds) *Hard Choices, Soft Law: Voluntary Standards in Global Trade, Environment and Social Governance* (2004) Ashgate Publishing Company, USA.

Koops B, Lips M, Prins C and Schellekens M (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One-Liners* (2006) TMC Asser Press, The Hague The Netherlands.

Lowe M J, Dale M O, Kock A, Froneman SL & Lang A J G The South African Notary 6 ed (1987) Juta & Co Ltd, Cape Town.

Lötz D J, Nagel C J & Joubert E P *Specific Contracts in Court* 3 ed (2010) Lexis Nexis, South Africa.

Malan FR, Oelofse AN, de Vos W, Pretorius JT & Nagel CJ *Provisional Sentence on Bills of Exchange, Cheques and Promissory Notes* (1986) LexisNexis, South Africa.

Malan FR, Pretorius JT & Du Toit SF *Malan on Bills of Exchange, Cheques and Promissory notes in South African Law* 5 ed (2009) LexisNesis, Durban.

Marshall McLuhan & Quentin Fiore *The medium is the message* (1967) Bantam Books, New York.

Mason S *Electronic Evidence* 3 ed (2012) LexisNexis, United Kingdom.

Mason S *Electronic Signatures in Law* 4ed (2016) University of London, London.

Mason S & Seng D *Electronic Evidence* 4 ed (2017) University of London, United Kingdom.

Morton JC & Hutchison SC *The Presumption of Innocence* (1987) Carswell, Toronto.

Nagel et al *Business Law* 5 ed (2015) LexisNexis, South Africa.

O'Neill M *Web Services Security* (2003) McGraw-Hill, Inc New York, USA.

Papadopoulos S & Snail S (eds) *Cyberlaw@SAIII: The Law of the internet in South Africa* (2012) Van Schaik, Johannesburg.

Piper F and Murphy S *Cryptography: A Very Short Introduction* (2002) Oxford University Press, Oxford.

Polanski PP *Customary Law of the Internet: In the Search for a Supranational Cyberspace Law* (2007) TMC Asser Press, The Hague.

Rakotsoane F *Writing a scholarly Research proposal* (2012) Morija, Lesotho.

Reed C & Angel J *Computer Law: The Law and Regulation of Information Technology* 6 ed (2007) Oxford University Press, Oxford.

Reed C *Making Laws for Cyberspace* (2012) Oxford University Press, United Kingdom.

Ridley D *A step-by-Step Guide for students* (2009) SAGE Publications Ltd, London.

Saith A & Vijayabaskar M *ICTS and Indian economic development Economy, Work, Regulation* (2005) SAGE Publications, New Delhi.

Savin A *EU Internet Law* (2013) Edward Elgar Publishing Limited, UK.

Savona EU (ed) in *Crime and Technology New Frontiers for Regulation, Law Enforcement and Research* (2004) Springer.

Schellekens M H M *Electronic Signatures: Authentication Technology from a Legal Perspective* (2004) TMC Asser Press, The Hague The Netherlands.

Schulze H, Kelbrick R, Manamela T, Stoop P, Manamela E, Hurter E, Masuku B & Stoop C *General Principles of Commercial Law* 8 ed (2015) Juta & Co (Pty) Ltd, Claremont South Africa.

Schwenzer I (ed) *Commentary on the UN Convention on the International Sale of Goods (CISG)* 4 ed (2016) Oxford University Press Oxford, Oxford.

Schwikkard P J & Van der Merwe S E *Principles of evidence* 4 ed (2016) Juta & Co, Cape Town.

Sharrock R *Business Transactions Law* 9 ed (2017) Juta & Co Ltd, Cape Town.

Simpson AWB *A History of the Common Law of Contract: The Rise of the Action of Assumpsit* (1987) Clarendon Press, Oxford.

Smith GJH *Internet Law and Regulation* 4ed (2007) Sweet & Maxwell, London.

Smith RE *Authentication from Passwords to Public Keys* (2002) Addison-Wesley, USA.

Sookman BB *Computer, Internet and electronic commerce terms: Judicial, legislative and technical definitions* (2009) Thomson Reuters Canada Limited, Ontario.

Southwood BR *Essential Judicial Reasoning in Practice and Procedure and the Assessment of Evidence* (2015) LexisNexis (Pty) Ltd, Durban.

Stumer A *The presumption of innocence: Evidential and human rights perspectives* (2010) Hart Publishing, United Kingdom.

Ubena J *How to regulate information and communications technology? : a jurisprudential inquiry into legislative and regulatory techniques* (2015) Jure, Stockholm.

Van der Merwe D (ed), Roos A, Pistorius T & Eiselen S *Information and Communications Technology Law* (2008) Lexis Nexis, Durban.

Van der Merwe D (ed), Roos A, Pistorius T, Eiselen S & Nel S *Information and Communications Technology Law* 2ed (2016) Lexis Nexis, Durban.

Van der Merwe FE *Notarial Practice* (2001) Butterworths, Durban.

Van der Merwe S, Van Huyssteen LF, Reinecke MFB & Lubbe GF *Contract: General Principles* 3 ed (2007) Juta & Co Ltd, Cape Town.

Van Der Merwe SWJ, Van Huyssteen LF, Reinecke MFB & Lubbe GF *Contract General Principles* 4 ed (2012) Juta & Co, Cape Town.

Van der Walt AJ & Pienaar GJ *Introduction to the Law of Property* 7 ed (2016) Juta & Co Ltd, Cape Town.

Van Huyssteen LF & Maxwell CJ *Contract Law in South Africa* 3ed (2014) Kluwer Law International, The Netherlands.

Van Huyssteen LF, Lubbe GF & Reinecke MFB *Contract General Principles* 5 ed (2016) Juta & Co, Cape Town.

Vithal R & Jansen J *Designing your first research proposal* (2010) Juta & Co Ltd.

Walker B *Conveyancing* 3 ed (1998) Blackstone Press Limited, London.

Weijers H *Made in Africa: A discussion on the role of law in absorptive capacity in African software industries* (2014) Oisterwijk: Wolf Legal Publishers.

West A *Conveyancing Practice Guide* 4 ed (2015) LexisNexis, South Africa.

Wright B & Winn J *The Law of Electronic Commerce* 3 ed (1999) Aspen Law & Business.

Xanthaki Helen *Drafting Legislation: Art and technology of rules for regulation* (2014) Hart Publishing, Oxford.

Zeffertt DT & Paizes AP *The South African Law of Evidence* (2009) LexisNexis, Durban.

Chapters in Books

Batroff P, Chinea G, Harstmann T, Jonas K & Moedeker J 'A pilot of a QoS-A ware wireless Back-Haul Network for rural areas' in Popescu-Zeletin R, Jonas K, Rai IA, Glitho R and Villafiorita A (Eds) *e-Infrastructure and e-Services for developing countries* (2011) Springer.

Botha J 'Negotiable Instruments' in Fouche MA (ed), Botha J, Collier-Reed D, Haupt A, Ncube CB, Schonwetter T, Van As HJ *Legal Principles of Contracts and Commercial Law* 8 ed (2015) LexisNexis, Durban.

Collier D 'Machine-generated evidence and related matters' in Schwikkard et al *Principles of Evidence* 3 ed (2008) Juta, Cape Town.

Breyer S 'Typical Justifications for Regulation' in Baldwin R, Scott C & Hood C (eds) *A Reader on Regulation* (1998) Oxford University Press, New York.

Chinkin C 'Normative Development in the International Legal System' in Dinah Shelton (ed) *Commitment and compliance: the role of non-binding norms in the international legal system* (2003) Oxford University Press, Oxford UK.

Collier D W 'Electronic evidence and related matters' in Schwikkard P J & van der Merwe S E *Principles of evidence* 3ed (2012) Juta, South Africa.

Collier-Reed D 'Breach of contract and remedies' in Collier-Reed D & Lehmann K *Basic Principles of Business Law* 2ed (2010) LexisNexis, Durban.

De Jager J 'Electronic evidence' in Schwikkard P J & Van der Merwe S E *Principles of evidence* (2016) Juta & Co, Cape Town.

Diver C S 'The Optimal Precision of Administrative Rules' in Baldwin R, Scott C & Hood C (eds) *A Reader on Regulation* (1998) Oxford University Press, New York.

Gereda S L 'The Electronic Communications and Transaction Act' in Thornton L, Carrim Y, Mtshaulana P & Reburn P (eds) *Telecommunications Law in South Africa* (2006) STE Publishers, Johannesburg.

Herek G M 'Developing a Theoretical Framework and Rationale for a Research Proposal' in Willo Pequegnat, Ellen Stover & Cheryl Boyce (eds) *How to Write a Successful Research Grant Application: A Guide for Social and Behavioral Scientists* 2 ed (2011) Springer, USA.

Hofman J & De Jager J 'South Africa' in Stephen Mason (ed) *Electronic evidence* 3ed (2012) LexisNexis, United Kingdom.

Hofmeyr G Y S 'Execution of Wills or Testamentary Form' in Corbett MM, Hofmeyr GYS & Kahn E *The Law of Succession in South Africa* 2 ed (2001) Juta Law, Lansdowne.

Koops B J 'Should ICT regulation be neutral-technology' in Koops BJ, Lips M, Prins C and Schellekens M (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One- Liners* (2006) 77 TMC Asser Press, The Hague The Netherlands.

Lehmann K 'The formation of a valid contract' in Debbie Collier-Reed & Karin Lehmann *Basic Principles of Business Law* 2ed (2010) LexisNexis, Durban.

Magnusson Sjoberg C 'Managing electronic signatures' in Ruth Nielsen, Soren Sandfeld Jakobsen & Jan Trzaskowiski (eds) *EU Electronic commerce Law* (2004) Djof Publishing, Copenhagen.

Mason S, Freedman C & Patel S 'England and Wales' in Stephen Mason *Electronic Evidence* 3 ed (2012) LexisNexis, United Kingdom.

Nielsen R 'Horizontal versus Vertical Regulations: Regulative Imperatives for the information market' in Stanley Greenstein (ed) *Vem Reglerar informationssamhallet?* (2010) Jure AB, Stockholm.

Ramberg C 'Contracting on the internet – Trends and challenges for law' in Peter Seipel (ed) *Law and Information Technology: Swedish Views* (2002) Stockholm.

Reed C 'Old wine in new bottles: Traditional transactions in the internet environment' in Reed C *Internet law: Text and materials* 2ed (2004) Cambridge University Press, UK.

Reed C 'On the internet, nobody knows you're a dog: identity and identification' in Reed C *Internet Law: Text and Materials* (2000) Butterworths, London.

Schafer B & Mason S **'**The characteristics of electronic evidence in digital format' in Stephen Mason *Electronic evidence* 3ed (2012) LexisNexis, United Kingdom.

Schellekens M 'What holds off-line, also holds on-line?' in Koops B J, Lips M, Prins C and Schellekens M (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One-Liners* (2006) 51, TMC Asser Press, The Hague The Netherlands.

Schwerha IV JJ, Bagby J W & Esler B W 'United States of America' in Stephen Mason *Electronic Evidence* 3ed (2012) Lexis Nexis, United Kingdom.

Journal Articles

Aalberts A A & van der Hof S 'Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication' (2000) 7 *EDI L Rev* 1.

Abbott K W & Snidal D 'Hard and Soft Law in International Governance' (2000) 54 *International Organization* 421.

Aguilar G C & Ortega J L B 'United Nations Convention on the Use of Electronic Communications in International Contracts (E-CC)' (2014) 18 *Vindobona Journal of International Commercial Law & Arbitration* 41.

AHIMA e-HIM Workgroup: Best Practices for Electronic Signature and Attestation. 'Electronic Signature, Attestation, and Authorship (Updated)' (2009) 11 *Journal of AHIMA* 80.

Alba M 'Electronic Commerce Provisions in the UNCITRAL Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea' (2009) 44 *Texas International Law Journal* 387.

Alba M 'Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions' (2014) 47 *Creighton Law Review* 387.

Allen R J 'How presumptions should be allocated: burdens of proof, uncertainty, and ambiguity in modern legal discourse' (1994) 17 *Harvard Journal of Law & Public Policy* 628.

Amadi-Echendu A P Phillips M & Chodokufa K 'International E-Conveyancing Strategies: Lessons for South Africa' (2014) 10 *Mediterranean Journal of Social Sciences* 237.

Andrade D E 'Is the pen mightier than the electronic signature?' (2005) December *De Rebus* 26.

Ashouri A, Bowers C & Warden C 'The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts' (2014) 11 *Digital Evidence and Electronic Signature Law Review* 115.

Bambauer D E 'Schrodinger's Cybersecurity' (2015) 48 *UC Davis Law Review* at 819.

Barofsky A 'The European Commission's Directive on Electronic Signatures: Technological "Favoritism" Towards Digital Signatures' (2000) 24 *B C Int'l & Comp L Rev* 145.

Barry G 'Stratford Digital democracy: Anderson v Bell & the expansion of electronic signatures in election law' (2013) *Utah Law Review OnLaw* 46.

Basu A & Muylle S 'Authentication in E-Commerce' (2003) 46 *Communications of the ACM* 159.

Bayer-Pacht E 'The computerization of land records: how advances in recording systems affect the rationale behind some existing chain of title doctrine' (2010-2011) 32 *Cardozo Law Review* 337.

Bechini U 'Bread and donkey for breakfast: How IT law false friends can confound lawmakers: An Italian tale about digital signatures' (2009) 6 *Digital Evidence and Electronic Signature Law Review* 80.

Bennett S C 'Electronic signatures in New York: an update on recent developments' (2013) 85 *New York State Bar Journal* 44.

Beyer C W & Hargrove C G in 'Digital Wills: Has the Time Come for Wills to join the Digital Revolution?' (2007) 33 *Ohio NUL Rev* 865.

Bhattacharyya D, Ranjan R, Alisherov FA & Choi M 'Biometric Authentication: A Review' (2009) 2 *International Journal of u- and e-Service, Science and Technology* 13.

Biddle C B 'Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace' (1997) 34 *San Diego L Rev* 1225.

Bing J 'Norwegian case LB-2006-27667' (2008) 5 *Digital Evidence and Electronic Signature Law Journal* 134.

Birnhack M 'Reverse engineering informational privacy law' (2013) 15 *Yale Journal of Law and Technology* 24.

Blythe S E 'Lithuania's Electronic Signature Law: Promoting the Growth of Secure E-commerce Transactions' (2007) 8 *Barry Law Review* 23.

Blythe S E 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce with Enhanced Security' (2005) 11 *Richmond Journal of Law and Technology* 1.

Boddery S S 'Electronic wills: drawing a line in the sand against their validity' (2012) 47 *Real Property, Trust and Estate Law Journal* 197.

Bohm N 'Watch what you sign!' (2006) 3 *Digital Evidence & Elec Signature L Rev* 45.

Boss A H 'Searching for Security in the Law of Electronic Commerce' (1999) 23 *Nova Law Review* 585.

Boss A H 'The evolution of commercial law norms: lessons to be learned from electronic commerce' (2008-2009) 34 *Brook J INT'L L* 673.

Browne MN & Bouzat F 'The contingent ethics of market transactions: linking the regulation of business to specific forms of markets' (2011-2012) 6 *Charleston L Rev* 163.

Brownsword R 'Regulating Human Genetics: New Dilemmas for a New Millennium' (2004) 12 *Medical Law Rev* 14.

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

Cain J, Levorchick M, Matuszak A, Pohlman A & Douglas Havelka D 'eLoanDocs: Riding the Tide of Technology Without Wiping Out' (2015) 36 *Communications of the Association for Information Systems* 759.

Case Reviews (2006) 2 *SACJ* 257.

Castellani L G 'An assessment of the Convention on the limitation period in the international sale of goods through case law' (2013) 58 *Villanova Law Review* 645.

Castellani L G 'Related international instruments and organizations: an assessment of the Convention on the limitation period in the international sale of goods through case law' (2013) 58 *Villanova Law Review* 645.

Castellani L G 'The role of UNCITRAL texts in promoting a harmonized legal framework for cross-border mobile payments' (2013) 8 *Washington Journal of Law, Technology & Arts* 265.

Chik W B '"Customary internet-ional law": Creating a body of customary law for cyberspace. Part 2: Applying custom as law to the Internet infrastructure' (2010) 26 *Computer Law & Security Review* 185.

Christensen S 'Electronic Land Dealings in Canada, New Zealand and the United Kingdom: Lessons for Australia' (2004) 11 *Murdoch University Electronic Journal of Law* 37.

Christensen S, Mason S & O'Shea K 'The international judicial recognition of electronic signatures - has your agreement been signed?' (2006)11 *Communications Law* 150.

Christianson G 'Advanced Electronic Signatures' 2012 November *De Rebus*.

Clark E 'E-Conveyancing in Australia: An Important Step Along the Journey to E-government' (2011) 21 *Journal of Law, Information and Science* 62.

Cleary E W 'Presuming and Pleading: An Essay on Juristic Immaturity' (1959) 12 *Stanford Law Review* 5.

Coetzee J 'The Convention on the Use of Electronic Communications in International Contracts: Creating An International Legal Framework for Electronic Contracting' (2006) 18 *SA Merc LJ* 245.

Coetzee J 'The Electronic Communications and Transactions Act of 2002: Facilitating Electronic Commerce' 2009 *Stellenbosch Law Review* 502.

Colja O D 'Case note: Republic of Slovenia, Case citation I Up 505/2003' (2007) 4 *Digital Evidence and Electronic Signature Law Review* 97.

Collier D 'e-Mail and SMS contracts: Lessons from the Labour Court' (2008) 16 *Juta's Bus L* 20.

Collier D 'Evidently not so simple: Producing computer print-outs in court' (2005) 13 *Juta's Business Law* 6.

Connolly C & Ravindra P 'International eCommerce regulation: First UN Convention on e-commerce finalised' (2006) 22 *Computer Law & Security Report* 31.

Cornelius S 'Condonation of Electronic Documents in terms of Section 2(3) of the Wills Act 7 of 1953' 2003 *Tydskrif vir die Suid-Afrikaanse Reg* 208.

Çoruhlu Y E, Demir O 'E-government services on foundation immovable properties' (2015) 33 *Journal of Engineering and Natural Sciences* 233.

Craig C J 'Technological Neutrality: Recalibrating Copyright in the Information Age' (2016) 17 *Theoretical Inquiries Law* 601.

Curry S 'Washington's Electronic Signature Act: an anachronism in the new millennium' (2013) 88 *Washington Law Review* 559.

Dempsey J X 'Creating the Legal Framework for ICT Development: The Example of E-Signature Legislation in Emerging Market Economies' (2003) 1 *Information Technologies & International Development* 39.

Doversberger M E 'Conveyancing at a crossroads: the transition to e-conveyancing applications in the U.S. and abroad' (2010) 20 *Indiana International & Comparative Law Review* 281.

Eckfeldt B 'What does RFID do for the customer?' (2005) 48 *Communications of the ACM* 77.

Eiselen S 'Electronic Commerce and the UN Convention on Contracts for the International Sale of Goods (CISG) 1980' (1999) 6 *EDI L Rev* 21.

Eiselen S 'Fiddling with the ECT Act – electronic signatures' (2014) 17 *PER / PELJ* 2805.

Eiselen S 'The UNECIC: International Trade in the Digital Era' (2007) 2 *PER* 1.

Elliott K J in 'The notarial seal - the last vestige of notaries past' (1997-1998) 31 *The John Marshall L Rev* 903.

Ellison C & Schneier B 'Ten risks of PKI: What you're are not being told about Public Key Infrastructure' (2000) 16 *Computer Security Journal* 1.

Escudero-Pascual A and Hosein I 'The Hazards of Technology Neutral Policy: Questioning Lawful Access to Traffic Data' (2004) 47 *Communications of the ACM* 77-82.

Ewan D E, Richards J A, and Tank M H K 'It's the Message, Not the Medium! Electronic Record and Electronic Signature Rules Preserve Existing Focus of the Law on Content, Not Medium of Recorded Land Title Instruments' (2005) 60 *The Business Lawyer* 1487.

Ewelukwa N 'Is Africa Ready for Electronic Commerce? A Critical Appraisal of the Legal Framework for Ecommerce in Africa' 2011 (13) *European Journal of Law Reform* 550.

Faerber C N 'Being there: the importance of physical presence to the notary' (1997-1998) 31 *John Marshall L Rev* 749.

Fan J & Tao Y 'Negotiable Instruments, in Particular Bills of Exchange in Macau, China' (2007) 2 *Journal of International Commercial Law and Technology* 84.

Faria J A E 'e-Commerce and International Legal Harmonization: Time To Go Beyond Functional Equivalence?' (2004) 16 *SA Merc LJ* 529.

Faria J A E 'The United Nations Convention on the Use of Electronic Communications in International Contracts—An Introductory Note' (2006) 55 *International and Comparative Law Quarterly* 689.

Faria J A E 'Uniform law and functional equivalence: diverting paths or stops along the same road? thoughts on a new international regime for transport documents' (2011) 2 *Elon Law Review* 1.

Felstiner A 'Grappling with online work: lessons from cyberlaw' (2011-2012) 56 *Saint Louis University Law Journal* 209.

Forder J 'The inadequate legislative response to e-signatures' (2010) 26 *Computer Law & Security Review* 418.

Fridman G H L "The Necessity for Writing in Contracts within the Statute of Frauds" (1985) 35 *University of Toronto Law Journal* 43.

Fry P B 'Introduction to the Uniform Electronic Transactions Act: principles, policies and provisions' (2000-2001) 37 *Idaho Law Review* 237.

Fuchs C & Horak E 'Africa and the digital divide' (2008) 25 *Telematics and Informatics* 99.

Gabriel HD 'United Nations Convention on the use of electronic communications in international contracts and compatibility with the American domestic law of electronic commerce' (2006-2007) 7 *Loyola Law and Technology Annual* 1.

Garrie D & Borden R 'Encryption for lawyers' 2016 *Business Lawyer Today* 1.

Gasser U 'Regulating Search engines: Taking Stock and Looking ahead' (2005-2006) 8 *Yale LJ & Tech* 201 - 234.

Gervais D J 'Towards a New Core International Copyright Norm: The Reverse Three-Step Test' (2005) 9 *Marquette Intellectual Property Law Review* 1.

Grant J K 'Shattering and moving beyond the Gutenberg paradigm: The dawn of the electronic will' (2008) 42 *University of Michigan Journal of Law Reform* 105.

Graux H 'Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union' (2013) 8 *Journal of International Commercial Law and Technology* 110.

Graux H 'Rethinking the E-signatures Directive: on laws, trust services, and the digital single market' (2011) 8 *Digital Evidence and Electronic Signature Law Review* 9.

Greenberg B A 'Rethinking Technology Neutrality' (2016) 100 *Minnesota Law Review* 1495.

Gregory J D 'Implementing the electronic communications convention' (2008-2009) 18 *Business Law Today* 43.

Gregory J D 'Legislating Trust' (2014) 12 *Canadian Journal of Law and Technology* 1.

Guadamuz A and Rens A 'Comparative analysis of copyright assignment and licence formalities for open source contributor agreements' (2013) 10 *SCRIPTed* 207.

Gunther O & Spiekermann S 'RFID and the perception of control: The consumer's view' (2005) 48 *Communications of the ACM* 73.

Hain M 'Making Law far away from Kitchen Tables: Imposing Trusts regardless of Formalities' (2014) *Oxford University Undergraduate Law Journal* 55.

Hart D K 'Form & substance in Nancy Kim's *wrap contracts*' (2014-2015) 44 S*outhwestern Law Review* 251.

Hawkins R J 'Dysfunctional Equivalence: The New Approach to Defining "Postal Channels" Under The Hague Service Convention' (2007) 55 *UCLA Law Review* 205.

Hays M J 'The E-SIGN Act of 2000: The triumph of function over form in American contract law' (2000 – 2001) 76 *Notre Dame L Rev* 1183.

Hildebrandt M 'Legal protection by design: objections and refutations' (2011) 5 *Legisprudence* 223.

Hill R ‘The internet, its governance, and the multi-stakeholder model’ (2014) 16 *Info* 16.

Hofman J ‘Electronic evidence in criminal cases’ (2006) 3 *SACJ* 257.

Hughes B ‘The rise of electronic discovery’ (2012) *De Rebus* 24.

Hughes J ‘The Internet and the Persistence of Law’ (2003) 44 *BCL Rev* 359.

Hultmark C ‘European and U.S. Perspectives on Electronic Documents and Electronic Signature’ (1999) 14 *The Tulane European and Civil Law Forum* 123.

Hutchison C J ‘Technological Neutrality Explained & Applied to CBC v. SODRAC’ (2015) 13 *Canadian Journal of Law and Technology* 101.

Jacobs J & Lambrechts L ‘Valid or not? General principles for challenging a will’ (2013) 535 *De Rebus* 30.

Jain A, Hong L & Pankanti S ‘Biometric Identification’ (2000) 23 *Communications of the ACM* 91.

Jones G ‘Failings in the Treatment of Electronic Signatures’ (2003) 1 *Hertfordshire Law Journal* 101.

Kadir R ‘Are form requirements a hurdle to electronic commerce?’ 6.6 (2012) *Advances in Natural and Applied Sciences* 831.

Kahn R A & Silverberg DJ 'From Mount Sinai to Cyberspace: Making Good E-business Records' (2001) 57 *Business Lawyer* 431.

Kamecke U & Korber T ‘Technological neutrality in the EC regulatory framework for electronic communications: a good principle widely misunderstood’ (2008) 29 *European Competition Law Review* 330.

Kartau K & Saldu K ‘The purchase and sale of registered immovable property: stages of the registration process carried out by notaries and ensuring the effecting of transactions’ (2001) 10 *Juridica* 685.

Keating S ‘Digital signatures and the electronic transfer of land’ (2013) 7 *Masaryk University Journal of Law and Technology* 49.

Keller B P ‘Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property’ (1997-1998) 11 *Harvard Journal of Law & Technology* 401.

Kennedy D ‘Form and Substance in Private Law Adjudication’ (1976) 89 *Havr L Rev* 1685.

Kierkegaard SM ‘E-contract formation: U.S. and EU perspectives’ (2007) 3 *Shidler J L Com & Tech* 12.

Kirby C A 'Defining Abusive Software to Protect Computer Users from the Threat of Spyware' (2005-2006) 10 *Computer L Rev & Tech J* 287.

Kirby M D 'Medical Technology and New Frontiers of Family Law' (1987) 1 *Australian Journal of Family Law* 196.

Kisswani N M & Al-bakri A A 'Regulating the use of electronic signatures given the changing face of contracts' (2010) 7 *Macquarie J Bus L* 53.

Koger J L 'You Sign, E-SIGN, We all fall Down: Why the United Sates Should Not Crown the Marketplace As Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Law and Contemporary Problems* 491.

Koops B J 'Should ICT regulation be neutral-technology' in Bert-Jaap Koops, Miriam Lips, Corien Prins and Maurice Schellekens (eds) *Starting Points for ICT Regulation: Deconstructing Pevalent Policy One- Liners* (2006) TMC Asser Press, The Hague 51.

Kresse J R 'Privacy of Conversations over Cordless and Cellular Telephones: Federal Protection under the Electronic Communications Privacy Act of 1986' (1987) 9 *Geo Mason UL Rev* 335

Krige M 'Using the internet for business purposes' (1998) *Juta's Business Law* 130.

Lefebvre G 'Electronic Data Interchange and the New Civil Code of Quebec' (1998) *J of Business Law* 300.

Lessig L 'The Path of Cyberlaw' (1995) 104 *Yale LJ* 17.

Lillie S 'Will E-SIGN force states to adopt UETA?' (2001-2002) 42 *Jurimetrics* 21.

Lim K H, Leung K, Sia CL and Lee MKO 'Is eCommerce boundary-less? Effects of Individualism- Collectivism and Uncertainty Avoidance on Internet shopping' (2004) 35 *Journal of International Business Studies* 545.

Liu S & Silverman M 'A Practical Guide to Biometric Security Technology' (2001) *IT Pro* 27.

Llewellyn K N 'Meet negotiable instruments' (1944) XLIV *Columbia Law Review* 299.

Low R 'From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System' (2009) 21 *Bond Law Review* 107.

Macdonald E 'Dispatching the dispatch rule? The postal rule, email, revocation and implied terms' (2013) 19 *European Journal of Current Legal Issues* 1.

MacNeil H 'From the Memory of the Act to the Act Itself. The Evolution of Written Records as Proof of Jural Acts in England, 11th to 17th Century' (2006) 6 *Arch Sci* 313.

Magnusson Sjoberg C & Norden A 'Managing electronic signatures: Current challenges' 47 *Scandinavian Studies in Law* 79.

Manyathi-Jele N 'Electronic wills discussed at FISA conference' (2014) 547 *De Rebus* 9 at 10.

Martin CH 'The Electronic Contracts Convention, the CISG, and New Sources of E-Commerce Law' (2008) 16 *Tulane Journal of Int'l & Comp Law* 467.

Martin C H 'The UNCITRAL electronic contracts convention: will it be used or avoided?' (2006) 17 *Pace International Law Review* 261.

Martin J W 'I Want To Sign An Electronic Will' (2009) *The Practical Lawyer* 61.

Mashaw J L 'Administrative Due Process: The Quest for a Dignitary Theory' (1981) 61 *Boston University Law Review* 885.

Mason S & Bromby M 'Response to *Digital Agenda for Europe*: Electronic identification, authentication and signatures in the European digital single market. Public consultation' (2012) 3 *European Journal of Law and Technology* 1.

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

Mason S 'The international implications of using electronic signatures' (2005) 11 *CTLR* 160.

Matwyshyn A M 'Technology, Commerce, Development, Identity' (2007) 8 *Minn JL Sci & Tech* 515.

Maxwell W J & Bourreau M 'Technology neutrality in internet, telecoms and data protection regulation' (2015) 21 *Computer and Telecommunications Law Review* 1.

Mazzotta F G 'Notes on the United Nations Convention on the use of electronic communications in international contracts and its effects on the United Nations Convention on contracts for the international sale of goods' (2006-2007) 33 *Rutgers Computer & Technology Law Journal* 251.

McBarnet D & Whelan C 'The Elusive Spirit of the Law: Formalism and the Struggle for Legal Control' (1991) 54 *Modern Law Review* 848.

McBarnet D 'Law, Policy, and Legal Avoidance: Can Law Effectively Implement Egalitarian Policies?' (1988) 15 *Journal of Law and Society* 113.

Melnychuk K 'One Click Away: The Prospect of Electronic Wills in Saskatchewan' (2014) 77 *Saskatchewan Law Review* 27.

Menon S 'Policy impediments to media convergence: an exploration of case studies from South Africa and India' (2008) 12 *International Journal of Communications Law and Policy* 313.

Mik E ‘Certainty at last? A "new" framework for electronic contracting in Singapore’ (2013) 8 *Journal of International Commercial Law and Technology* 160.

Mik E ‘Contracts Governing the Use of Websites’ (2016) *Singapore Journal of Legal Studies* 70.

Mik E ‘Evaluating the Impact of the UN Convention on the Use of Electronic Communications in International Contracts on Domestic Contract Law--The Singapore Example’ (2010) 28 *Chinese (Taiwan) Yearbook of International Law and Affairs* 43.

Mik E ‘The Unimportance of being "electronic" or – popular misconceptions about "Internet contracting" ’ (2011) 19 *International Journl of Iaw and Information Technology* 324.

Mitchell P ‘Demystifying media neutrality’ (2003) 10 *Journal of Database Marketing* 303.

Moringiello J M & Reynolds W L ‘From Lord Coke to Internet Privacy: The Past, Present and Future of the Law of Electronic Contracting’ (2013) 72 *Maryland Law Review* 452.

Moringiello J M, Reynolds W L ‘Survey of the law of cyberspace: electronic contracting cases 2005-2006’ (2006) 62 *Business Lawyer* 195.

Moses L B ‘Understanding Legal Responses to Technological Change: The example of *In Vitro* Fertilization’ (2004-2005) 6 *Minn J L Sc & Tech* 505.

Nelson S D & Simek J W ‘Encryption made easy: The basics of keeping your data secure’ 2016 *Oregon State Bar Bulletin* at 2.

Nelson S D and Simek JW ‘Encrypting sensitive emails now a no-brainer’ (2016) 41 *Montana Lawyer* 18.

Njotini M N ‘Evaluating the position of information or data in the law of property’ (2015) *Stell LR* 220.

O’Gorman L ‘Comparing Passwords, Tokens, and Biometrics for User Authentication’ (Dec 2003) 91 *Proceedings of the IEEE* 2021.

O’hara E A ‘Choice of law for internet transactions: the uneasy case for online consumer protection’ (2005) 153 *University of Pennsylvania Law Review* 1883.

Orifowomo A O & Agbana J O ‘Manual signature and electronic signature: significance of forging a functional equivalence in electronic transactions’ (2013) 24 *International Company and Commercial Law Review* 357.

Ottosen A M ‘Case Note Denmark Case Citation U.2006.1341V’ (2007) 4 *Digital Evidence and Electronic Signature Law Review* 99.

Overby B A 'UNCITRAL Model Law on Electronic Commerce: Will Cyberlaw be Uniform? An Introduction to the UNCITRAL Model Law on Electronic Commerce' (1999) 7 *Tulane J of Int'l & Comp L* 219.

Palmer B C 'Disparate impact of electronic signature legislation on indigent Californians' (2005) 36 *McGeorge Law Review* 697.

Papadopoulos P 'Electronic Wills with an Aura of Authenticity: *Van der Merwe v Master of the High Court and Another*' (2012) 24 *SA Mercantile LJ* 93.

Pappas C W 'Comparative US and EU approaches to e-commerce regulation: Jurisdiction, electronic contracts, electronic signatures and taxation' (2002-2003) 31 *Denver Journal of International Law and Policy* 325.

Perillo J M 'The Statute of Frauds in Light of the Functions and Dysfunctions of Form' (1974) 43 *Fordham L Rev* 39.

Pidcock B C 'Cross-border fraud: Bridging global protection disparity through international cooperative efforts' (2008-2009) 17 *Currents International Trade LJ* 78.

Pistorius T '"Nobody knows you're a dog": The attribution of data messages' (2002) *SA Merc LJ* 737.

Pistorius T 'Click-Wrap and Web-Wrap Agreements' (2004) 16 *SA Merc LJ* at 570.

Pistorius T 'Contract formation: a comparative perspective on the Model Law on Electronic Commerce' (2002) XXXV *CILSA* 129.

Pistorius T 'Developing countries and copyright in the information age: The Functional Equivalent Implementation of the WCT' (2006) 9 *PER/PELJ* 149/197.

Pistorius T 'Formation of Internet Contracts: An Analysis of the Contractual and Security Issues' (1999) 11 *SA Merc LJ*.

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) XXXIX *CILSA* 178.

Polanski PP 'International electronic contracting in the newest UN Convention' (2007) 2 *Journal of International Commercial Law and Technology* 112.

Pooe A & Labuschagne L 'Factors impacting on the adoption of biometric technology by South African banks: An empirical investigation' (2011) 15 *Southern African Business Review* 119.

Prosser T 'Regulation and Social Solidarity' (2006) 33 *Journal of Law and Society* 364.

Rajab A 'Technology Neutrality' (2009) 14 *Lex Electronica* 1.

Ramokanate L L 'The Lesotho electronic transactions and electronic commerce bill: will it replace the common law of contract as we know it?' (2015) 22 *Lesotho Law Journal* 117.

Raymond A H & Lambert J B 'Technology, e-commerce and the emerging harmonization: the growing body of international instruments facilitating ecommerce and the continuing need to encourage wide adoption' (2014) 17 *International Trade and Business Law Review* 419.

Reed C 'Online and Offline Equivalence: Aspiration and Achievement' (2010) 18 *International Journal of Law and Information Technology* 248.

Reed C 'Taking Sides on Technology Neutrality' (2007) 4 *SCRIP T-ed* 263.

Reiniger T & Francoeur J R 'Justice and sheriff: practical and authoritative methods for the electronic issuance of officially certified documents in the United States' (2010) 7 *Digital Evidence & Electronic Signature Law Review* 42.

Ries D G & Simek J W 'Encryption made simple for lawyers' (2013) 56 *Res Gestae Indiana Bar Journal* 1.

Roland S E 'The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?' (2001) 35 *Suffolk University Law Review* 625.

Rosas R 'Comparative Study of the Formation of Electronic Contracts in American Law with references to International and Mexican Law' (2004-2005) 8 *Newcastle L Rev* 79.

Rosett A 'Critical Reflections on the United Nations Convention on Contracts for the International Sale of Goods' (1984) *Ohio State LJ* 265.

Ross C M 'Probate – *Taylor v. Holt*: The Tennessee Court of Appeals Allows a Computer Generated Signature to validate a Testamentary Will' (2004-2005) 35 *U Mem L Rev* 603.

Saba Jr J D 'Internet Property Rights: e-Trespass' (2001-2002) 33 *St Mary's LJ* 367.

Sandberg H 'Real estate e-conveyancing: vision and risks' (2010) 19 *Information & Communications Technology Law* 101.

Schlechtriem P 'Recent Developments in International Sales Law' (1983) 18 *Israel Law Review* 309.

Schmidt A 'Radbruch in Cyberspace: About Law-system Quality and ICT Innovation' (2009) 2 *Masaryk University Journal of Law and Technology* 195.

Schoeman-Malan L, Du Toit F, Van der Linde A & Faber J 'Section 2(3) of the Wills Act 7 of 1953: a retrospective and critical appraisal of some unresolved issues' 2014 *Acta Juridica : South African Law of Succession and Trusts- the past meeting the present and thoughts for the future* 78.

Schultz E E 'The gap between cryptography and information security' (2002) 21 *Computers & Security* 674.

Shaffer G C & Pollack M A 'Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance' (2010) 94 *Minnesota Law Review* 706.

Skeen 'Proposed Alterations' (1992) 109 *SALJ* 138.

Smedinghoff T J 'The Legal Challenges of Implementing Electronic Transactions' (2008) 41 *Uniform Commercial Code Law Journal* 1.

Smedinghoff T J & Bro R H 'Moving with change: electronic signature legislation as a vehicle for advancing e-commerce' (1999) 17 *Marshall Journal of Computer & Information Law* 723.

Smedinghoff T J 'Challenges to privacy, integrity, and security in a borderless world: it's all about trust: the expanding scope of security obligations in global privacy and e-transactions law' (2007) 16 *Michigan State Journal of International Law* 1.

Smith S E 'The United Nations Convention on the Use of Electronic Communication in International Contracts (Cuecic): Why It Should Be Adopted and How It Will Affect International E-Contracting' (2007-2008) 11 *SMU Science and Technology Law Review* 133.

Snail S & Hall N 'Electronic Wills in South Africa' (2010) 7 *Digital Evidence & Elec Signature L Rev* 67.

Snail S & Matanzima S 'Electronic wills – beyond the MacDonald v The Master decision' 2011 *Without Prejudice* 61.

Snail S 'Electronic Signatures in South Africa' (2009) August *De Rebus* 51.

Sorieul R, Clift JR, & Estrella-Faria JA 'Establishing a Legal Framework for Electronic Commerce: The Work of the United Nations Commission on International Trade Law (UNCITRAL)' (2001) 35 *The International Lawyer* 107.

Srivastava A & Koekemoer M 'The legal recognition of electronic signatures in South Africa: A Critical Overview' (2013) 21 *African Journal of International and Comparative Law* 427.

Srivastava A ‘Legal understanding and issues with electronic signatures – an empirical study of large businesses' (2008) 35 *Rutgers Computer & Technology* LJ 42.

Stern J E ‘The Electronic Signatures in Global and National Commerce Act’ (2001) 16 *Berkeley Technology Law Journal* 391.

Stitilis D, Petrauskas R, Rotomskis I ‘The implementation of public e-services for immovable property contracts in Lithuania: legal aspects’ (2006) 1 *Journal of International Commercial Law and Technology* 80.

Stratford B G ‘Digital democracy: Anderson v. Bell & the expansion of electronic signatures in election’ 2013 *Utah Law review OnLaw* 46.

Sundt C ‘PKI – Panacea or Silver Bullet?’ (2000) 5 *Information Security Technical Report* 53.

Swales L ‘The Regulation of electronic signatures: Time for Review and Amendment’ (2015) 132 *SALJ* 257.

Tasneem F ‘Electronic Contracts and Cloud Computing’ (2014) 9 *Journal of International Commercial Law and Technology* 105.

Theophilopoulos C ‘The admissibility of data, data messages, and electronic documents at trial’ 2015 *TSAR* 461.

Thomas LM ‘Abandoned Frozen Embryos and Texas Law of Abandoned Personal Property: Should There Be a Connection’ (1997-1998) 29 *St Mary’s LJ* 255.

Thomas R, Griggs L, & Low R ‘Electronic conveyancing in Australia: is anyone concerned about security?’ (2014) 23 *Australian Property Law Journal* 1.

Thompson M ‘The neutralization of harmony: the problem of technological neutrality, east and west’ (2012) 18 *Boston University Journal of Science & Technology Law* 303.

Tribe L H ‘Perspectives on *Bakke*: Equal Protection, Procedural Fairness, or Structural Justice?’ (1979) 92 *Harvard Law Review* 864.

Tsai H ‘Media neutrality in the digital era: a study of the peer-to-peer file sharing issues’ (2005) 5 *Chicago-Kent Journal of Intellectual Property* 46.

Tussey D ‘Technology matters: the courts, media neutrality, and new technologies’ (2004-2005) 12 *J Intell Prop L* 427.

Tussman J & tenBroek J ‘The Equal Protection of the Laws’ (1949) 37 *California Law Review* 341.

Urs Gasser, Jonathan Zittrain, Robert Faris & Rebekah Heacock Jones 'Internet Monitor 2014: Reflections on the Digital World' (2014-17) *The Berkman Center for Internet & Society Research Publication* 138.

Van der Hof S 'The Status of eGovernment in the Netherlands' (2007) 11 *Electronic Journal of Comparative Law* 1.

Van der Merwe D 'How standards (such as XML) accomplish electronic authentication in web services' 2005 *Obiter* 665.

Van der Merwe D 'The current legal position regarding digital evidence (and XML as a possible solution)' (2010) 73 *THRHR* 81.

Van der Merwe D 'XBRL and the law: legal implications of markup languages' 2011 *THRHR* 418.

Van Eeden L 'Document security and electronic signatures' (2011) 4 *Enterprise Risk* 19.

Vassil D Zhivkov S J D 'Warehouse receipts: a roadmap for the harmonization of trans-pacific law and practice' (2016) 33 *Arizona Journal of International & Comparative Law* 191.

Vihials I B 'Electronic mass procurement by means of "web technology": basic options in its regulation' (2013-2014) 20 *ILSA Journal of International & Comparative Law* 373.

Vua K P L, Proctorb R W, Bhargav-Spantzelb A, (Belin) Taib B L, Joshua Cookb J & Schultzc EE 'Improving password security and memorability to protect personal and organisational information' (2007) 65 *International Journal of Human-Computer Studies* 744.

Wahlgren P 'The Legitimacy Sphere: Between Law, Culture, Politics and Enforceability' (1999-2015) 56 *Scandinavian Studies in Law* 427.

Walden I 'Regulating Electronic Commerce: Europe in the Global E-conomy' (2001) 26 *European Law Review* 529.

Wang F F 'The incorporation of terms into commercial contracts: a reassessment in the digital age' (2015) 2 *Journal of Business Law* 87.

Wang M 'Do the regulations on electronic signatures facilitate international electronic commerce? A critical review' (2007) 23 *Computer law & Security Report* 32.

Wang M 'The Impact of Information Technology Development on the Legal concept – A Particular Examination on the Legal concept of 'Signatures'' (2007) 15 *Int'l JL & Info Tech* 253.

Wayman J L 'Fundamentals of Biometric Authentication Technologies' (2001) *International Journal of Image and Graphics* 93.

Wei CK & Suling J C 'United Nations Convention on the use of Electronic Communications in International Contracts - A new global standard' (2006) 18 *SAcLJ* 116.

Welinder 'Facing real-time identification in mobile apps & wearable computers' (2013-2014) 30 *Santa Clara High Tech LJ* 89.

Wells R B in 'The fog of cloud computing: fourth amendment issues raised by the blurring of online and offline content' (2009-2010) 12 *Journal of constitutional law* 223.

Whitaker R D in 'Rules Under the Uniform Electronic Transactions Act for an Electronic Equivalent to a Negotiable Promissory Note' (1999-2000) 55 *The Business Lawyer* 437.

Whittal J F 'The potential use of cellular phone technology in maintaining an up-to-date register of land transactions for the urban poor' (2011) 14 *Potchefstroomse Elektroniese Regsblad* 194.

Wiehl T 'Human and computerized facial recognition: comparison and constitutional analysis' (2013) VI *Northwestern Interdisciplinary Law Review* 95.

Winn J K 'The Emperor's new clothes: The shocking truth about digital signatures and Internet commerce' (2001) 37 *Idaho Law Review* 353.

Wiseman T A **'**Encryption, Forced Decryption, and the Constitution' (2015) 11 *A Journal of law and policy for the Information Society* 525.

Wittie R A & Winn J K 'Electronic Records and Signatures under the Federal E-SIGN Legislation and the UETA' (2000-2001) 56 *The Business Lawyer* 293.

Wood-Bodley M C 'MacDonald v The Master: computer files and the 'rescue' provision of the wills act' (2004) 121 *SALJ* 34.

Woods C B 'Commercial Law: Determining Repugnancy in an Electronic Age: Excluded Transactions Under Electronic Writing and Signature Legislation' (1999) 52 *Oklahoma Law Review* 411.

Wright B 'Eggs in Baskets: Distributing the risks of electronic signatures' (1997) 15 *John Marshall Journal of Computer and Information Law* 189.

Wright B 'Eggs in Baskets: Distributing the Risks of Electronic Signatures' (2001) 32 *UWLA L Rev* 215.

Wu R 'Land Registration Act 2002 of England: lessons on title registration reform for China' (2011-2012) 4 *Tsinghua China Law Review* 62.

Wylly P 'Evaluating the costs of technology neutrality in light of the importance of social network influences and bandwagon effects for innovation diffusion' (2015) 23 *NYU Environmental Law Journal* 300.

Zaba S 'Digital signature legislation: The first 10 years at 24' (2006) 11 *Information Security Technical Report* 18.

Internet Sources

'Account planning methods: The Media Neutral Idea' available at *account-planning-confessions.blogspot.com/.../media-supremacy-vs-media-neutrality.html,* accessed on 12 July 2015.

'An introduction to Contactless' available at *http://www.contactless.info/Introduction-to-Contactless.asp,* accessed on the 17 May 2014.

'Audit trail' available at *http://www.businessdictionary.com/definition/audit-trail.html,* accessed on 13 March 2017.

Baller S, Di Battista A, Dutta S, Lanvin B 'The Networked Readiness Index 2016' in *The Global Information Technology Report 2016* available at *http://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.1_2016.pdf,* accessed on the 21 July 2017.

'Electronic Signatures and Infrastructure (ESI): Policy Requirements for certification authorities issuing public key certificates' ETSI TS 102 042 V2.1.1 (2009-05) available at *http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.01.01_60/ts_102042v020101p.pdf,* accessed on 20 October 2014.

'Framework for Global Electronic Commerce' 1 July 1997 available at *http://www.ecommerce.gov/framewrk.htm,* accessed on 6 March 2014.

'ICT Policy for Lesotho: Policy Measures, Instruments and Initiatives' 2005 available at *http://research.businessonlybusiness.com/matrix.php?Electronic%20transactions%20of%20Lesotho,* accessed on 04 June 2013.

'Mozambique: Government Seeks to Curb Electronic Fraud' available on *http://allafrica.com/stories/201404030229.html,* accessed on 18 November 2014.

'Soft Law & Legal Definition' available at *definitions.uslegal.com/s/soft-law/,* accessed on 1 October 2016.

‘The ESIGN Act’ June 2011 available at *http://electronicsignature.com/esignact/,* accessed on 1 December 2015.

‘The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age’ A Project of the Sedona Conference Working Group on Best Practices for Electronic Document Retention & Production Second Edition November 2007 at 30 available at *file:///C:/Users/user/Downloads/Guidelines.pdf,* accessed 26 November 2015.

‘Timestamp’ available at *https://en.oxforddictionaries.com/definition/timestamp,* accessed on 13 March 2017.

‘UNCITRAL Model law on Electronic commerce (1996): Text – Guide to enactment status’ available at *www.uncitral.org,* accessed on 23 September 2016.

‘UNDP in Lesotho’ available at *http://www.ls.undp.org/content/lesotho/en/home/countryinfo.html,* accessed on 20 March 2016.

About Landonline ‘e-dealing’ available at *https://forms.landonline.govt.nz/about-landonline/benefits-services/edealing.asp,* accessed on 29 August 2016.

About Landonline available at *https://forms.landonline.govt.nz/about-landonline/security.asp,* accessed on 29 August 2016.

Advice from the Law Commission ‘Electronic Commerce: Formal Requirements in Commercial Transactions’ December 2001 para 3.37 available at *http://lawcommission.justice.gov.uk/docs/Electronic_Commerce_Advice_Paper.pdf,* accessed on 20 October 2014.

Africa Ranking ‘Top 10 most developed African countries’ available at *http://www.africaranking.com/most-developed-african-countries/5/,* accessed on 20 March 2016.

Amended Proposal for a European Parliament and Council Directive on a common framework for electronic signatures, COM (99) 195 final available at *http://aei.pitt.edu/13384/1/13384.pdf,* accessed on 25 November 2016.

American Society of Notaries ‘E-notarization’ available at *http://www.asnnotary.org/?form=enotary,* accessed on 16 January 2017.

Barlow J P ‘Declaration of Independence of Cyberspace’ 09 February 1996 Davos Switzerland available at

https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration, accessed on 03 May 2014.

Bianca M C & Bonell M J 'Commentary on the International Sales Law' (Milan: Giuffré) (1987) 103 available at *http://www.cisg.law.pace.edu/cisg/biblio/bonell-bb9.html,* accessed on 20 August 2015.

Black's Law Dictionary Free online legal dictionary 2 ed available at *http://thelawdictionary.org/telegram/,* accessed on 21 March 2017.

Bonell M J 'Article 9' in Bianca-Bonell Commentary on the International Sales Law, Giuffrè: Milan (1987) 103 available at *http://www.cisg.law.pace.edu/cisg/biblio/bonell-bb9.html,* accessed on 20 August 2015.

Brand New Technologies: Electronic Signatures and Security 'Electronic Signatures – Understanding Technology, Methods and Authentication' 17 May 2011 available at *http://us-cdn.creamermedia.co.za/assets/articles/attachments/34131_brand_new.pdf,* accessed on 12 May 2014.

Business Dictionary 'Document of title' available on *http://www.businessdictionary.com/definition/document-of-title.html,* accessed on 6 September 2016.

Business Dictionary 'bill of entry' available *http://www.businessdictionary.com/definition/bill-of-entry.html,* accessed on 8 September 2016.

Business Dictionary 'title deed' available at *http://www.businessdictionary.com/definition/title-deed.html,* accessed on 7 September 2016.

BusinessDictionary.com 'Notarised document' available at *http://www.businessdictionary.com/definition/notarized-document.html,* accessed on 25 November 2015.

BusinessDictionary.com available at *http://www.businessdictionary.com/definition/password.html,* accessed on 18 May 2014.

Cambridge Dictionary available at *http://dictionary.cambridge.org/dictionary/english/delivery-order,* accessed on 08 September 2016.

Chondrocoukis G & Lagou P 'Non Repudiation: Gap between Legislation and Practice' available at *http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.2154&rep=rep1&type=pdf*, accessed on 14 December 2015.

Company Overview of LAW Trusted Third Party Services (Pty) Ltd 2016 available at *http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=52341011*, accessed on 18 October 2016.

companySIG.com 'What exactly is an email signature' available at *http://www.companysig.com/what_is_an_email_signature.php*, accessed on 17 May 2014.

Criddle L 'What is social engineering?' available at *https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering*, accessed on 11 Decemer 2017.

Davies B 'A Guide To Property Transfer In South Africa' available at *http://www.chaseveritt.co.za/conveyancing*, accessed on 16 April 2016.

Davis D 'Compliance Defects in Public-Key Cryptography' Proceedings of the Usenix Technical Conference 10 March 10, 1997 available on *http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=EBDC2E05F435F95ABB068C453F46F618?doi=10.1.1.195.9905&rep=rep1&type=pdf*, accessed on 22 October 2014.

Department of Communications South African Government 20 June 2007 'South African Accreditation Authority on applications for accreditation of electronic signatures' available at *http://www.gov.za/south-african-accreditation-authority-applications-accreditation-electronic-signatures*, accessed on 8 March 2016.

Dictionary.com available at *dictionary.reference.com/browse/telegram*, accessed on 03 June 2014.

Dictionary.com available at *http://dictionary.reference.com/browse/alienation*, accessed on 20 March 2015.

Dictionary.com available at *http://dictionary.reference.com/browse/facsimile*, accessed on 04 June 2014.

DocuSign 'ESIGN Act & UETA' available on *https://www.docusign.com/esign-act-and-ueta*, accessed on 1 December 2015.

Drukker Solicitors 'Notarisation' available at *http://www.drukker.co.uk/publications/reference/notarisation/#.VlWwFHaDFBc,* accessed on 25 November 2015.

Dusick D M 'Writing the Theoretical Framework' BOLD Educational Software 2011 available at *http://bold-ed.com/framework.htm,* accessed on 03 May 2013.

Eliza M I K 'Contract Formation in Open Electronic Networks - Chapter 1 Introduction' Singapore Management University available at *http://works.bepress.com/elizamik/2,* accessed on 10 December 2013.

Eliza M I K 'From Clay tablets to AJAX: Replicating Writing and Documents in Internet Transactions' *Research Collection School of Law (Open Access) Paper 1069* 2012 available at *http://ink. library.smu.edu.sg/sol_research/1069,* accessed on 10 December 2013.

Ellipsis Regulatory Solutions 'Electronic Communications and Transactions Amendment Bill 2012' 2012 available at *http://mybroadband.co.za/vb/showthread.php/478510-Electronic-Communications-and-Transactions-Amendment-Bill-2012*, accessed on 18 November 2014.

Ellison C 'Improvements on Conventional PKI Wisdom' 1st Annual PKI Research Workshop – Proceedings held at NIST April 2002 available at *www.cs.dartmouth.edu/~pki02/,* accessed on 14 June 2014.

Ellison C M 'Establishing identity without certification authorities' paper presented at the 6th USENIX Security Symposium in San Jose 22-25 July 1996 available at *www.usenix.org/publications/library/proceedings/sec96/ellison.html,* accessed on 31 July 2014.

Encyclopaedia Britannica available at *www.britannica.com/EBchecked/topic/586267/telex,* accessed on 03 June 2014.

Ernst & Young Baltic AS 'Summary of the study: "usage of qualified electronic signature within Europe Union"', 2015 available at *https://mkm.ee/sites/default/files/summary_of_the_study_usage_of_qualified_electronic_signature_within_europe_union.pdf,* accessed on 5 January 2018.

EUR-Lex 'Access to European Union law - eSignature in the EU' available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24118,* accessed on 02 December 2015.

EUROPA ‘Legal Aspects of electronic commerce’ available on *europa.eu/legislation_summaries/information_society/other_policies/124204_en.htm,* accessed on the 22 June 2013.

European Commission ‘Digital agenda for Europe: A Europe 2020 Initiative’ available at *http://ec.europa.eu/digital-agenda/en/trust-services,* accessed on 02 December 2015.

European Commission ‘Internal market, Industry, entrepreneurship and SMEs’ available at *ec.europa.eu,* accessed on 01 May 2017.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, available at *http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R(01),* accessed on 14 December 2015.

European Union ‘The Euro’ available at *europa.eu,* accessed on 28 April 2017.

Extech Data System ‘RFID’s advantages & disadvantages explained’ 2008 available at *http://www.usingrfid.com/news/read.asp?Ic=s44325nx1433zg,* accessed on the 17 May 2014.

Forensicon ‘What is Metadata?’ 2016 available at http://www.forensicon.com/resources/articles/what-is-metadata/, accessed on 13 January 2016.

Forum of European Supervisory Authorities for Electronic Signatures ‘Public Statement on server based signature Services’ 17 October 2005 available at *http://www.ibls.com/internet_law_news_portal_view.aspx?s=sa&id=1364,* accessed on 14 December 2015.

Forum of European Supervisory Authorities for electronic signatures ‘Working paper on advanced electronic signatures’ 12 October 2004 available at *http://www.fesa.eu/public-documents/WorkingPaper-AdvancedSignature-20041012.pdf,* accessed on 14 December 2015.

Furber L ‘Custom and practice, and employment contract terms (implied and express terms)’ 21 October 2011 available at *https://www.crunch.co.uk/blog/small-business-advice/2011/10/21/custom-and-practice-and-employment-contract-terms/,* accessed on 21 August 2015.

Gondwe G Biztechafrica.com available at http://www.biztechafrica.com/article/malawi-drafts-new-ict-bill/7024/#.VGsTKyKUfeI, accessed on 18 November 2014.

Granger S 'Social Engineering Fundamentals, Part I: Hacker Tactics' 2001 available at *https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics,* accessed on 11 December 2017.

Gutmann P 'PKI: It's Not Dead, Just resting' available at *http://www.cs.auckland.ac.nz/~pgut001/pubs/notdead.pdf,* accessed on 16 February 2016.

Heyink M 'Electronic signatures for South African Law Firms Guidelines' 2014 Law Society of South Africa available at *http://www.lssa.org.za/upload/documents/LSSA%20Guidelines_Electronic%20Signatures%20for%20South%20African%20Law%20Firms_October%202014.pdf,* accessed on 3 January 2017.

HIM Body of Knowledge 'Electronic Signature, Attestation, and Authorship (2013 update)' available at *http://library.ahima.org/doc?oid=107151#.V7Xgmfl96Uk,* accessed on18 August 2016.

Ince D 'Dictionary of the Internet' 3 ed (2013) Oxford University Press, Online publication, accessed on 18 March 2016.

Investopedia available at *http://www.investopedia.com/terms/n/notarize.asp*, accessed on 26 November 2015.

Italy Agricultural products case available at *http://cisgw3.law.pace.edu/cases/040225i3.html*, accessed on 21 August 2015.

ITU 'About ITU' available on *http://www.itu.int/en/about/Pages/default.aspx,* accessed on 10 March 2016.

ITU 'Support for harmonization of the ICT Policies in Sub-Saharan Africa' 2015 available at *http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx,* accessed on 14 April 2015.

ITU in cyberwellness profile-Democratic Republic of Congo Report of 12 August 2014 available on at *http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Congo.pdf,* accessed on 18 November 2014.

ITU-T Recommendations 'Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks' available at *http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509,* accessed on 05 October 2016.

Johnson J M C 'Chapter 8: Consequences of and problems with electronic contracts' available at *reference.sabinet.co.za/webx/access/electronic_journals/medsor/medsor_n37_a9.pdf*, accessed on 24 June 2014.

Knowledge-Based Society and Role of Global Mapping, Conference Global Mapping G8 Okinawa, Okinawa Charter on Global Information Society, available on *http://www.dotforce.org/reports/itl.html* accessed on the 10 December 2013.

Kohnfelder L M *Towards a Practical Public Key Cryptosystem* (Bachelor of Science thesis, Massachusetts Institute of Technology, 1978) available at *http://groups.csail.mit.edu/cis/theses/kohnfelder-bs.pdf*, accessed on 19 May 2014.

Kongtcheu P 'Method and systems to facilitate online electronic notary, signatures and time stamping' 2004 available at *https://www.google.com/patents/US20040221162*, accessed on 26 November 2015.

Kuner C & Miedbrodt A 'Written Signature Requirements and Electronic Authentication: A Comparative Perspective' available at *http://www.kuner.com/data/articles/signature perspective.html*, accessed on 12 May 2014.

Kuner C 'German Consumer Association Denounces EU Draft Digital Signature Directive' 1998 available at *http://www.kuner.com/data/sig/verbrauc.htm, a*ccessed on 20 February 2014.

Kurbalija J 'Internet Governance and International Law' *Reforming Internet Governance: Perspectives from WGIG* at 113 available on *http://www.wgig.org/docs/book/Jovan_Kurbalija%20.pdf*, accessed on 12 November 2014.

LAA 'Mapping' available at *http://www.laa.org.ls/index.php?option=com_k2&view=item&layout=item&id=2&Itemid=133*, accessed on 5 September 2016.

Land Administration Authority available at *http://www.laa.org.ls/*, accessed on 15 August 2016.

Law Reacher 'Electronic Signatures Dissertation' available at *http://www.lawteacher.net/free-law-dissertations/electronic-signatures-dissertation.php*, accessed on 17 May 2014.

LawTrust ‘e4 Registration Authority Charter: Information security policy’ 2014 available at *https://www.e4.co.za/e4Website/docs/e4%20RA%20Charter%20(14-07-2015)-Signed.pdf,* accessed on 20 March 2016.

LawTrust Information Security Solutions ‘About Lawtrust’ available at *https://www.lawtrust.co.za/pages/about,* accessed on 14 January 2017.

LawTrust Information Security Solutions ‘eDNA’ available at *https://www.lawtrust.co.za/solutions/edna,* accessed on 14 January 2017.

LawTrust Information Security Solutions ‘Our solutions’ available at *www.lawtrust.co.za,* accessed on 14 January 2017.

LAWTrust Information Security Solutions available at *https://www.lawtrust.co.za/pages/electronic-signing-solutions,* accessed on 17 January 2017.

Lesotho Communications Authority ‘Our mandate’ available at *www.lca.org.ls,* accessed on 20 February 2017.

Lesotho Revenue Authority ‘Asycuda’ available at *ecustoms.lra.org.ls,* accessed on 11 April 2017.

Lesotho Revenue Authority ‘Information for traders’ available at *ww.lra.og.ls,* accessed on 11 April 2017.

Lesotho Revenue Authority ‘National rollout customs automated procedures’ available at *ww.lra.og.ls,* accessed on 11 April 2017.

Lessing I & Jani P ‘Just how much is your electronic signature worth?’ DLA Cliffe Dekker Hofmeyr August 2013 available at *http://www.lexology.com/library/detail.aspx?g=bdf66791-22d4-403d-92fd-a1abb726c9ac,* accessed on 12 May 2014.

Livermore J & Euarjai K ‘Electronic Bills of Lading and Functional Equivalence’ 1998 (2) *Journal of Information, Law and Technology* available at *http://elj.warwick.ac.uk/jilt/ecomm/98_2liv/,* accessed on 2 September 2016.

Louwman W ‘CROBECO: a future-proof system to support cross-border conveyancing’ 6 th Annual Publication 1 January 2015 available at *http://www.elra.eu/crobeco-a-future-proof-system-to-support-cross-border-conveyancing/,* accessed on 22 August 2016.

m.roo.net/, accessed on 22 July 2014.

Maxie E 'Digitized Signatures vs. Digital Signatures: A Complete Comparison' 2013 available at *http://www.signix.com/blog/bid/99443/Digitized-Signatures-vs-Digital-Signatures-A-Complete-Comparison,* accessed on the 17 May 2014.

McKinley H L 'SSL and T L S: A Beginners Guide' SANS Institute 2003 available at *file:///G:/%C2%A0/corrections%20material/SSL%20and%20TSL.pdf,* accessed on 20 December 2016.

Moses L B 'Recurring Dilemmas: The Law's Race to Keep Up With Technological Change' 2007 *University of New South Wales Faculty of Law Research Series* Paper 21 available at *http://law.bepress.com/unswwps-flrps/art21,* accessed on 21 February 2014.

Mutigwe C & Aghdasi F 'Research Trends in RFID Technology' 2007 available at *http://www.stitcs.com/en/rfid/rfidresearchtrends.pdf,* accessed on 29 November 2016.

Nassiri NN 'Signature verification using a third party authenticator via a paperless electronic document platform' 2005 available at *https://www.google.com/patents/US6904416,* accessed on 26 November 2015.

National Association of Realtors 'Moving Towards an Electronic Real Estate Transaction: The Electronic Signature – Legal Overview (U.S.)' 2010 available at *http://www.realtor.org/sites/default/files/handouts-and-brochures/2010/E-Signature-Whitepaper-2010-08-01.pdf,* accessed on 26 August 2016.

National Association of Secretaries of State National e-notarization Standards 2006 available at *http://www.asnnotary.org/img/NASS%20Natl%20Standards%20on%20ENotarization%20July%202006.pdf,* accessed on 16 January 2017.

Neville K 'The Art And Science Of The Email Signature' available at *http://www.smashingmagazine.com/2010/02/04/the-art-and-science-of-the-email-signature/,* accessed on 17 May 2014.

New Agriculturist 'Country profile – Lesotho' available at *www.new-ag.info,* accessed on 4 September 2016.

Nolan C 'The property registration process' 25 Nov 2015 available at *http://www.privateproperty.co.za/advice/property/articles/the-property-registration-process/587,* accessed on 16 April 2016.

OECD ‘APEC–OECD Integrated Checklist on Regulatory Reform’ available at *www.oecd.org/dataoecd/41/9/34989455.pdf*, accessed on 4 January 2018.

OECD ‘OECD Council Recommendation on Principles for Internet Policy Making’ 13 December 2011 at 6 available at *https://www.oecd.org/internet/ieconomy/49258588.pdf*, accessed on 26 November 2016.

OECD Expert Group ‘Defining and Measuring E-commerce’ 2001 available at *http://stats.oecd.org/glossary/detail.asp?ID=758*, accessed on 26 April 2013.

OMB Procedures and Guidance; Implementation of Government Paperwork Elimination Act 65 Fed Reg 25508-21 2 May 2000 in IT LAW available at *http://itlaw.wikia.com/wiki/Digitized_signature*, accessed on 17 May 2014.

Ontario News ‘Making Electronic Real Estate Transactions Easier, More Secure’ 2014 available at *https://news.ontario.ca/mag/en/2014/11/making-electronic-real-estate-transactions-easier-more-secure.html*, accessed on 26 August 2016.

Ontario's Regulatory Registry ‘Considering the security of electronic agreements of purchase and sale: Electronic Commerce Act, Possible e-signature regulation’ 2014 available at *http://www.ontariocanada.com/registry/view.do?postingId=17022&language=en*, accessed on 28 August 2016.

Oxford Dictionaries: Language matters, Oxford University Press 2014 available at*www.oxforddictionaries.com/definition/english/technology*, accessed on 6 March 2014.

Parry G C James-Moore M, Graves A P, & Altinok O ‘Legal aspects of electronic signatures’ 2008 available at *http://www.easysoft.nu/images/IDPIC/legal_Esignature.pdf*, accessed on 29 November 2015.

Pintsov L A & Pintsov D ‘Method for electronically endorsing check images US 7797250 B2’ 2010 available at *http://www.google.com/patents/US7797250*, accessed on 11 March 2015.

Prabhakar S, Pankant S & Jain A K ‘Biometric Recognition: Security and Privacy Concerns’ March/April 2003 *IEEE security & privacy* 33 available at *http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/PrabhakarPankantiJain_BiometricSecurityPrivacy_SPM03.pdf*, accessed on 23 November 2015.

Proposal for a decision of the European Parliament and of the Council on establishing a multi annual Community programme on promoting safer use of the Internet and new online technologies COM 2004 91 final available at *http://library.certh.gr/libfiles/PDF/PAPYR-1205-EU-PROPOSAL-SAFER-INTERNET-COM-2004-91-PP37-EN-acte_en.pdf,* accessed on 25 November 2016.

Reed C 'How To Make Bad Law: Lessons from the computing and communications sector' Research Paper 40/2010 Part 2 Queen Mary University of London School of Law Legal Studies available at *http://ssrn.com/abstract=1538527,* accessed on 15 January 2014.

Reed C 'What is a Signature?' (2000) 3 *The Journal of Information, Law and Technology* available at *http://elj.warwick.ac.uk/jilt/00-3/reed.html,* accessed on 02 May 2014.

Rennie A, Samuel M & Mackenzie R 'The age of e-conveyancing?' 2001 *The Journal of the law society of Scotland* available at *http://www.journalonline.co.uk/Magazine/46-6/1000947.aspx,* accessed on 29 August 2016.

Report from the Commission to the European Parliament and the Council - Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures (2006) available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0120,* accessed on 2 December 2015.

Rodríguez A M L 'Lex Mercatoria' University of Aarhus available at *http://law.au.dk/fileadmin/site_files/filer_jura/dokumenter/forskning/rettid/artikler/2020020046.pdf,* accessed on 19 August 2015.

Roessler T (ed) W3C Working Group Note 'Using XML digital signatures in the 2006 XML environment' 20 December 2006 available at *http://www.w3.org/TR/DSig-usage/#C14N11,* accessed on 22 October 2014.

Rose India Technologies Pvt Ltd 'What is eToken?' available at *http://www.roseindia.net/whatis/etoken.shtml,* accessed on 18 May 2014.

Rosenthal L H 'Metadata and Issues Relating to the Form of Production' (2006-2007) 116 *The Yale Law Journal* available at *http://www.yalelawjournal.org/forum/metadata-and-issues-relating-to-the-form-of-production,* accessed on 20 November 2015.

Rouse M 'Password' *http://searchsecurity.techtarget.com/definition/password*, accessed on 18 May 2014.

SADC 'South African Community Development: Towards a common future' available at *http://www.sadc.int/member-states,* accessed on 13 December 2015.

SADC: Towards a common future 'SADC Declaration on Information and Communications Technology (ICT)' 14 August 2001 available at *http://www.sadc.int/documents-publications/show/830,* accessed on 10 March 2016.

Sahakian A 'E-Signatures Will Change the Mortgage and Real Estate Industry' April 2015 available at *https://www.besmartee.com/blog/e-signatures-will-change-the-mortgage-and-real-estate-industry,* accessed on 26 September 2016

Samson M 'Stratton Oakmont, Inc. et al. v. Prodigy Services Company, et al' Internet Library of Law and court Decisions available at *http://www.internetlibrary.com/cases/lib_case80.cfm,* accessed on 10 December 2013.

Samuelson P, 'Five challenges for Regulating the Global Information Society' in Chris Marsden (ed) *Regulating the Global Information Society*, Routledge 2000 available at *http://www.sims.berkeley.edu/~pam/papers/5challenges_feb22_v2_final_.pdf,* accessed on 15 January 2014.

Seal Dictionary Definition available at *http://www.yourdictionary.com/seal,* accessed on 16 March 2016.Seltzer W 'Spitzer Suit Shows the Right Way to Fight Spyware' 28 April 2005 available at *http://www.eff.org/deeplinks/archives/2005_04.php*, accessed on 20 February 2014.

Shackleton E, '*Software Tames Tangle of Paperwork'* The Canadian Press 11 July 2008 available at *http://www.theglobeandmail.com/real-estate/software-tames-tangle-of-paperwork/article4221434/,* accessed on 29 August 2016.

SIGNiX '2014 E-Signature Trends: Security and Assurance Will Be King' 2014 available at *https://www.signix.com/blog/bid/108796/2014-E-Signature-Trends-Security-and-Assurance-Will-Be-King,* accessed on 5 January 2018.

Simpson Notaries available at *https://www.simpsonnotaries.com/notarized/,* accessed on 25 November 2015.

Skjærseth J B, Stokke O S & Wettestad J 'Soft Law, Hard Law, and Effective Implementation of International Environmental Norms' available at *http://www.fni.no/doc&pdf/JBS-OSS-JW-GEP-2006-3.pdf,* accessed on 11 November 2014.

Smart Card Alliance 'Contactless Smart Chip Technology: The Business Benefits' available at *http://www.smartcardalliance.org/publications-contactless-business-benefits/,* accessed on 20 May 2014 at 1 & 2.

Smith L 'The Introduction of E-Conveyancing 15 Sep 2010 available at *http://www.diyconveyance.co.uk/introduction-econveyancing.html*, accessed on 29 August 2016.

Southern African Customs Union Agreement 2002 available at *www.sacu.int*, accessed on 29 March 2017.

Spyrelli C 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) 2 *The Journal of Information, Law and Technology (JILT)* available at *http:/www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2.spyrelli/*, accessed on 16 January 2014.

Srivastava A 'Electronic Signatures: A brief review of the Literature' 605 available at *http://dl.acm.org/citation.cfm?id=1151469*, accessed on 28 November 2015.

Study on Cross-Border Interoperability of e-signatures (CROBIES) 2010 available at *file:///C:/Users/user/Downloads/KK0113059ENN_002.pdf*, accessed on 10 January 2016.

TechRepublic 'Automating dates and times in a Word document' available at *http://www.techrepublic.com/blog/microsoft-office/automating-dates-and-times-in-a-word-document/*, accessed on 25 July 2017.

TechTerms.com available at *http://www.techterms.com/definition/username*, accessed on 18 May 2014.

The European Commission 'Towards a new framework for Electronic Communications infrastructure and associated services' The 1999 Communications Review, COM (1999) 539 available at *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24216*, accessed on 25 November 2016.

The Free Dictionary available at *http://www.thefreedictionary.com/disposal*, accessed on 20 March 2016.

The FreeDictionary 'Document of title' available at *http://legaldictionary.thefreedictionary.com/document+of+title*, accessed on 6 September 2016.

Traverse Legal Attorneys and Advisors 'After Stratton Oakmont v. Prodigy: Section 230 of the Communications Decency Act Provides Blanket Immunity For Interactive Computer Service Providers' 2008 available on

http://tcattorney.typepad.com/digital_millennium_copyri/2008/07/after-stratton.html, accessed on the 10 December 2013.

Trochim, William M K *Philosophy of Research. Research Methods Knowledge Base* 2006 Colorado State University available at *http://pdf.aminer.org/000/248/418/quantitative_and_qualitative_measures_myths_of_the_culture.pdf, accessed on 03/05/2013.*

Tšiu T 'Minister launches HIPSSA project in Lesotho' Lesotho Communications Authority Press Release 29 March 2013 available at *www.lca.org.ls,* accessed on 03 March 2015.

TUC Work smart 'What is meant by custom and practice?' 2015 available on *https://worksmart.org.uk/work-rights/pay-and-contracts/contract-terminology/what-meant-custom-and-practice,* accessed on 21 August 2015.

Tyson J 'How Encryption Works' 2017 available at *http://computer.howstuffworks.com/encryption4.htm,* accessed on 10 January 2017.

UNCITRAL 'Status UNCITRAL Model Law on Electronic Commerce (1996)' 2015 available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html,* accessed on 18 August 2015.

UNCITRAL 'Status United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 2005)' available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html,* accessed on 19 August 2015.

UNCITRAL 'Status: UNCITRAL Model Law on Electronic Signatures (2001)' available at *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html,* accessed on 20 August 2015

UNCTAD 'UN list of Least Developed Countries' available at *http://unctad.org/en/Pages/ALDC/Least%20Developed%20Countries/UN-list-of-Least-Developed-Countries.aspx,* accessed on 20 March 2016.

Uniform Law Commission available at *http://www.uniformlaws.org/Act.aspx?title=Electronic%20Transactions%20Act,* accessed on 02 March 2016.

United Nations available at *http://www.un.org/en/member-states/*, accessed on 28 March 2017.

United Nations Commission on International Trade Law 'A Guide to UNCITRAL: Basic facts about the United Nations Commission on International Trade Law Davidson' 2013 available on *http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf*, accessed on 19 August 2015.

United Nations Information Service Press Releases UNIS/L/212 16 January 2015 available at *http://www.unis.unvienna.org/unis/en/pressrels/2015/unisl212.html*, accessed on 11 April 2015.

University of South California 'Organizing Your Social Sciences Research Paper' 2013 available at *http://libguides.usc.edu/writingguide*, accessed on 30 May 2013.

USAID Southern Africa 'The Southern Africa Trade hub: Supporting Regional Food Security through Enhanced Agricultural Supply Chains' Slide 6 available at *www.satradehub.org*, accessed on 4 September 2016.

USLegal.com 'Soft Law & Legal Definition' available at *http://definitions.uslegal.com/s/soft-law/*, accessed on 11 November 2014.

Vasudevan R 'Changed governance or computerized governance? Computerized property transfer processes in Tamil Nadu (India)' 2006 available at *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4085521*, accessed on 15 August 2016.

Vos J 'Using European legislation & electronic means in Cross-border conveyancing' 1 January 2014 5th Annual Publication *European Land Registry Association* available at *http://www.elra.eu/using-european-legislation/*, accessed on 22 August 2016.

Wade Publications CC 'The Lesotho Review: An overview of the Kingdom of Lesotho's economy, Information and Communications Technology' 2015 available at *www.lesothoreview.com*, accessed on 1 May 2017.

Watkins K United Nations Human Development Report 2005 available at *http://hdr.undp.org/sites/default/files/reports/266/hdr05_complete.pdf*, accessed 20 March 2017.

Weber RH 'Proliferation of "Internet Governance" ' 1 September 2014 GigaNet – Annual Symposium 1 available at *http://ssrn.com.abstract=2809847*, accessed on 21 January 2015 at 8.

Words and Phrases Legally Defined 2ed available at *http://www-mylexisnexis-co-za.ezproxy.uct.ac.za/Index.aspx*, accessed on 6 September 2016.

www.oxforddictionaries.com/definition/english/rubber-stamp, accessed on 02 June 2014.

Your Dictionary 'Indenture defined' available at *www.yourdictionary.com>indenture*, accessed on 27 April 2016.

Reports/ Discussion Papers & Guidelines

Alberta Law Reform Institute Final report no 96 *The creation of wills* (September 2009) Edmonton Alberta.

American Bar Association *Digital signature guidelines* (1996) Chicago, USA.

Antonaci L, Demeke M & Vezzani A Scientific paper No 9B *The Challenges of Implementing Price and Production Risk Management in Sub-Saharan Africa* (2015) Ulysses.

ChamberSign *Position paper in light of the review of the esignature framework* (October 2010).

Chilima D *Capacity support for the Agricultural Commodity Exchange for Africa Trust Final Program Report* (2012) Agricultural Commodity Exchange for Africa.

Dumortier J, Kelm S, Nilsson H, Skouma G, Van Eecke P *The legal and market aspects of electronic signatures* Interdisciplinary Centre for Law and Information Technology, Katholieke Universiteit.

European Commission *Proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market* COM (2012) 238 final, Brussels.

Irish Law Reform Commission *Documentary and electronic evidence CP 57 – 2009.*

ITU *Cyberwellness profile -Republic of Mozambique* (11 March 2015).

Lesotho Revenue Authority *Report from Performance Analysis and Strategy Management Office* (May 2013).

Mochebele M (ed) *The state of ICT in Key sectors: Business, Education, Health and Tourism Lesotho 2013* 2ed (2015) Lesotho Communications Authority.

Ndulo M Paper 60 *The Need for the Harmonisation of Trade Laws in the Southern African Development Community (SADC)* (1996) Cornell Law Faculty Publications.

OECD *Guiding Principles for Regulatory Quality and Performance* (2005).

Office of Management and Budget *Procedures and Guidance; Implementation of Government Paperwork Elimination Act 65 Fed Reg 25508-21* (2 May 2000) in IT LAW.

Ølnes J & Cook S O *Security and signature requirements for e-tendering systems and services* (16 August 2016) Direktoratet for forvaltning og IKT.

Polanski P P Paper 20 (BLED 2006 Proceedings) *Convention on E-Contracting: The Rise of International Law of Electronic Commerce?* (2006).

Singh A & Ramesh J (Report for Telecommunication Development Bureau) *Readiness assessment report to establish a national CIRT for Lesotho* (November 2012).

South African Law Reform Commission Discussion Paper 131 (Project 126) *The Review of the Law of Evidence* (2015).

Trubek D M, Cottrell P & Nance M Legal Studies Research Paper Series No 1002 *"Soft Law," "Hard Law," and European Integration: Toward a Theory of Hybridity* (2005) University of Wisconsin Law School.

USAID *Highlights from the Field: Malawi Encouraging a Warehouse Receipt System (WRS) - first steps* (November 2011).

USAID *ICT to enhance warehouse receipt systems and commodity exchanges in Africa* (2011).

Van der Haar Ilse TILEC Discussion Paper *Technology Neutrality; What Does It Entail?* (March 2007) Tilburg University.

Waggoner L W Working Paper no 174 (Public law and legal theory working paper series) *Uniform Probate Code authorizes notarized wills* (November 2009).

Presentations & Conference papers

Clarke R 'The fundamental inadequacies of conventional public key infrastructure' (27-29 June 2001) Paper presented at the 9th European Conference on Information System, Bled Slovenia.

Faber J 'Electronic wills and jurisdictional issues surrounding a "digital estate" ' (18 September 2014) The Fiduciary Institute of Southern Africa (FISA) 4th Annual Conference, Johannesburg.

Hurlburt W H 'Electronic Wills and Powers of Attorney: Has Their Day Come?' (2001) Paper delivered at the Proceedings of the Uniform Law Conference of Canada.

Johnssén G 'Time, space, and documents – Principles for e-government regulation' (2006) Proceedings of the 39th Hawaii International Conference on System Sciences.

Kamanga-Mafusire B ‘Presentation on Electronic Transactions and E-Commerce bill’ (15 & 16 July 2013) HIPSSA Project.

Magnusson Sjoberg C ‘IT Law for IT Professionals’ (2013) King’s College, London.

Makaya G ‘The Determinants of Regulatory Effectiveness in Liberalised Markets: Developing Country Experiences’ (2001) Annual Forum, Trade and Industry Policy Strategies, Johannesburg.

Mambi A ‘Overview of the e-transaction & e-communications Bill’ (4 - 8 March 2013) Workshop on Transposition of SADC Cyber-security Model Laws, HIPSSA Project.

Mezghani M ‘E-Commerce Readiness Study in the SADC sub-Strategy’ (16-17 April 2012) Validation workshop by UNECA and SADC, Balaclava Mauritius.

Motjolopane N ‘An Overview of the SADC Model Law on Electronic Transactions and Electronic Commerce’ (2013) Support for Harmonization of ICT Policies in Sub Sahara Africa (HIPSSA Project) workshop/conference on Transposition of SADC Cybersecurity Model Laws into national laws for Lesotho, Ministry of Communication, Science and Technology (MCST) Lesotho.

Motjolopane N ‘e-commerce: SADC Model Law on Electronic Transactions and Electronic Commerce’ (28 August 2013) 2nd Stakeholder Workshop HIPSSA Project.

Onumah G ‘Implementing Warehouse Receipt Systems in Africa Potential and Challenges’ (6-7 September 2010) Paper prepared for the 4th African Agricultural Markets Program Policy Symposium, organized by the Alliance for Commodity Trade in Eastern and Southern Africa (ACTESA) of the Common Market for Eastern and Southern Africa (COMESA) Lilongwe Malawi.

Thomas R, Lowd R & Griggs L ‘Land Fraud and Inappropriate Dealings in an Electronic Environment: An Australian and New Zealand Perspective’ (12-13 July 2012) The 11th Australasian Property Law Teachers Conference National University of Singapore, Singapore *http://eprints.qut.edu.au/51014/*.

Wang M ‘A Review of Electronic Signatures Regulations: Do They Facilitate or Impede International Electronic Commerce?’ (August 2006) Proceedings of the 8th International Conference on Electronic Commerce, Fredericton, Canada.

Theses

Chetty P *An analysis of electronic signature regulation in South Africa* (Master of Management Research Report, University of Witwatersrand, 2013).

Franks S *The Capricious Relegation of Offers to Purchase to Invalid Electronic Transactions by the Electronic Communications and Transactions Act 25 of 2002* (unpublished LLM dissertation, University of Cape Town, 2004).

Lawack-Davids V A *Aspects of Internet Payments Instruments* (unpublished LLD thesis, University of South Africa, 2000).

Lichaba M F *The Lesotho Electronic Transactions and Electronic Commerce Bill 2013: An Appraisal* (unpublished LLM dissertation, University of Pretoria, 2015).

Myburgh F E *Statutory Formalities in South African Law* (unpublished LLD thesis, Stellenbosch University, 2013).

Nangela D J *The Adequacy of the Tanzanian Law on E-commerce and Econtracting: Possible Solutions to be Found in International Models and South African Legislation* (unpublished LLD thesis, University of Cape Town, 2011).

Potgieter J M *The importance of the concept of "functional equivalence" for the South African approach to form and writing* (unpublished mini dissertation for LLM degree, Potchefstroomse Universiteit, 2002).

Tlale M T *Property regulation in South Africa: Paving the way for regulation in Lesotho* (unpublished dissertation for LLM degree, North-West University, 2014).

Statutes

Lesotho

Access and Receipt of Information Bill 2000

Attesting Witnesses Act 22 of 1876

Authentication of Documents Proclamation No 2 of 1964

Bills of Exchange Proclamation 13 of 1912

Charities Trust Act 24 of 1975

Communications Act of 2011

Companies Act 18 of 2011

Criminal Procedure and Evidence (Amendment) Act 3 of 2001

Customs and Excise (Amendment) Act 3 of 1984

Customs and Excise (Effective date of Customs Automation) Notice 10 of 2016

Customs and Excise Act 10 of 1982
Customs and Excise Regulations Legal Notice 126 of 1984
Data Protection Act of 2011
Deeds Registry Act 12 of 1967
Deeds Registry Regulations 52 of 1967
Friendly Societies Act of 1882
Hire Purchase Act No 27 of 1974
Justices of the Peace and Commissioners of Oaths Proclamation 13 of 1945
Land Act 8 of 2010
Land Administration Authority Act No 9 of 2010
Land Regulations 21 of 2011
Lesotho Labour Code Order 24 of 1992
Mines and Minerals Act 4 of 2005
Partnership Proclamation of 1957
Proclamation 2B of 1884
Trustee Investment in Basutoland Securities Proclamation 62 of 1950
Wills Ordinance of 1845
Workmen's Compensation Trust Fund Regulations LN 42 of 1985

South Africa

Accreditation Regulations Government GN 29995 of 20 June 2007
Alienation of Land Act No 68 of 1981
Consumer Protection Act No 68 of 2008
Electronic Communications and Transactions Act No 25 of 2002
Electronic Communications and Transactions Amendment Bill (ECT Amendment Bill) GN 888 GG35821 of 26 October 2012
General Law Amendment Act No 50 of 1956
Labour Relations Act No 66 of 1995
Law of Succession Amendment Act No 43 of 1992
National Credit Act No 34 of 2005
Wills Act No 7 of 1953

International

2013 Nevada Revised Statutes: NRS 133.085

Act of Apr 29 2011 ch 183 2011 Wash Sess Laws 1377 (codified as amended WASH REV CODE § 19 34 231)

Australia Electronic Transactions Act 162 of 1999

Australia Northern Territory Wills Act of 2000

Convention on Cybercrime No 185 of 2001

Electronic Commerce and Information Act CCSM c ESS Part 2 of Manitoba

Electronic Signatures in Global and National Commerce Act of 2000

England's Land Registration Act of 2002

European Union Directive on Electronic Signatures 1999/93/EC

German Law Governing Framework Conditions for Electronic Signatures (Bundesgesetzblatt – BGB1. Teil I S. 876) of 21 May 2001

Statute of Frauds 1677 Chapter 154 *LRO 1/2002* Statute law of the Bahamas

Swedish Act on Qualified Electronic Signatures 2000

Swedish Qualified Electronic Signatures Act (SFS 2000:832)

Tennessee Code Ann § 1-3-105(30) 2003

Uniform Electronic Transactions Act 1999

Uniform Probate Code of the USA

Uniform Real Property Electronic Recording Act of 2004

Utah code ann §§ 46-3-101-104 (1996) repealed by 2006 Utah Laws chapters 21 § 13

Western Australia Wills Act of 1970

Cases

Lesotho

Construction and Allied Workers Union v Lesotho Brick And Pave and Another (Pty) Ltd [2011] LSLC 28

Lechesa v KPMG/Harley & Morris joint Venture and Others [2004] LSHC 88

Lesotho bank (1999) limited v Boliba multipurpose cooperative society C of A (CIV) No 43 of 2011

Lesotho Public Motor Transport (Pty) Ltd v Lesotho Bus and Taxi Owners Association [2015] LSHC 29

Lesupi & Ano v The Crown [2012] LSCA 8

Lisenyeho v Mahlomolatoki [1997] LSHC 16

Makhalane v Minister of Law & Constitutional Affairs [2013] LSLC 73

Marake v National University of Lesotho [2002] LSLC 10

Mota v Motokoa [2002] LSHC 7

Nedbank Ltd v Mendelow No & Another 2013 (6) SA 130 (SCA)

Ntsihlele v Lesotho Bank [2010] LSLC 32

Pheko v Mafeteng United Co-Operative Society [1985] LSCA 119

R v Mahase [1992] LSHC 51

R v Moahloli [1980] LSHC 39

R v Rammoneng [2002] LSCA 110

R v Sentle & Another [1988] LSCA 155

R v Thamae [2005] LSHC 24

Sebeko v Sebeko [2004] LSHC 91

Selebeng v Hlalele [2000] LSCA 106

Thamae v Crown [2005] LSHC 214

South Africa

Africa Solar (Pty) Ltd v Divwatt (Pty) Ltd 2002 (4) SA 681 (SCA)

Afrox Healthcare Bpk v Strydom 2002 (6) SA 21 (SCA)

Ariefdien v Soeker 1982 (2) SA 570 (C) 578

Associated Engineers Co Ltd v Goldblatt 1938 WLD 139

Avis v Verseput 1943 AD 331

Bekker v Naude en Andere 2003 (5) SA 173 (SCA)

Brink v Humphries & Jewell 2005 (2) SA 419

Chisnall and Chisnall v Sturgeon and Sturgeon 1993 (2) SA 642 (W)

Clements v Simpson 1971 (3) SA 1 (AD)

Conradie v Rossouw 1919 AD 279

Conroy v Coetzee 1944 OPD 207

Craib v Crisp 1984 (3) SA 594 (T)

De Bruin v Brink 1925 OPD 68 69

Dempers and others v The Master and others 1977(4) SA 44

Dlovo v Brian Porter Motors t/a Port Motors Newlands 1994 (2) SA 518 (C)

Du Plessis v Nel 1952 (1) *SA* 513 (A) 525H

Ex Parte Goldman & Kalmer 1965 (1) SA 464

Ex Parte Jackson No: In re estate Miller 1991 (2) SA 586

Ex Parte Singh 1981 (1) 793

Exdev (Pty) Ltd v Pekudei Investments (Pty) Ltd 2011(2) SA 282 (SCA)

First National Bank Ltd v Avtjoglou 2000 (1) SA 989 (C)

Firstrand Bank v Venter [2012] ZASCA 117

Fourlamel (Pty) Ltd v Maddison 1977 (1) SA 333 (A)

Fraser v Viljoen 2008 (4) SA 106 (SCA)

Frye's (Pty) Ltd v Ries 1957 (3) *SA* 575

George v Fairmead (Pty) Ltd 1958 (2) SA 465 (A)

Goldblatt v Fremantle 1920 AD 123

Golden Fried Chicken (Pty) Ltd v Yum Restaurants International (Pty) Ltd 2005 BIP 269 (T)/ [2005] ZAGPHC 311

Gugu & Ano v Zongwana & others [2014] 1 ALL SA 203

Harpur v Govindamall 1993 (4) SA 751

Hendrik Van der Merwe v The Master of the High Court 2010 (6) SA 544 (SCA)

Horty Investments v Interior Acoustics 1984 (3) SA 537

Hugo v Gross 1989 (1) SA 154 (C)

Jafta v Ezemvelo KZN Wildlife [2008] 10 BLLR 954 (LC)

Jhajbhai & others v Master and Ano 1971 (2) SA 370

John Barr & Co (Pty) Ltd 1967 (3) *SA* 292 (W)

Johnston v Leal [1980] 3 SA 927 (AD)

Jordaan v De Villiers 1991 (4) SA 396 (C)

Jurgens v Volkskas Bank 1993 (1) SA 214 (A)

Just Names Properties 11 CC v Fourie 2008 (1) SA 343 (SCA)

Khumalo & others v Holomisa (Case CCT 53/01) 2002 (5) SA 401

LA Consortium & Vending CC v MTN Service Provider (Pty) Ltd 2011 (4) SA 77 (GSJ)

Letsekga v The Master & others 1995 (4) SA 731

MacDonald v The Master 2002 (5) SA 64 Orange Freestate Provincial Division

Magwaza v Heenan 1979 (2) SA 1019 (A)

MAN Truck & Bus (SA) (Pty) Ltd v Dusbus Leasing CC 2004 (1) SA 454 (W)

Matanda v Rex 1923 AD 435 (B)

Mellvill & Another v The Master and Others 1984 (3) SA 387

Meter Motors (Pty) Ltd v Cohen 1966 (2) SA 735 (T)

Meyer v Roberts 1971 (1) SA 328

Navidas v Essop 1994 (4) SA 141 (A)

Ndlovu v Minister of Correctional Services [2006] 4 ALL SA 165 (w)

Nedbank Ltd v Mendelow No & Another 2013 (6) SA 130 (SCA*)*

Newell v Tarrant (2004) WL 741782

Northend v Ulbrick 1972 (1) SA 737

Novartis v Maphil [2015] ZASCA 111

Patel v Le Clus (Pty) Ltd 1949 TPD 30

Pillay and Another v Shaik and others [2009] 2 ALL SA 435 (SCA)

Pillay v Shaik 2009 (4) *SA* 74 (SCA)

Pretoria East Builders CC v Basson 2004 (6) SA 15 (SCA)

Putter v Provincial Insurance Co Ltd and Another 1963 (3) SA 145 (W)

Rockbreakers and Parts (Pty) Ltd v Rolag Property Trading (Pty) Ltd 2010 (2) SA 400 (SCA)

Rumarch Investment Holdings (Pty) Ltd v Old Fashioned Fish and Chips (Pty) Ltd North Gauteng High Court unreported case no 21168/2014 of 25 March 2015.

Sanop Petroleum v Pappadogianis 1992 (3) SA 234 (A)

Scheepers v Strydom 1989 (2) SA 778 (NC)

Senekal v Home Sites (Pty) Ltd 1950 1 SA 139 (W)

Smith v Walles 1985 (2) SA 189 (T)

South African Municipal Workers Union (SAMWU) v South African Local Government Bargaining Council and Others (DA7/2012) (2014) 35 ILJ 2824 (LAC) (13 February 2014)

South African Municipal Workers Union (SAMWU) v Rycroft NO [2009] ZALC 252

Spindrifter v Lester Donovan 1986 (1) SA 303 (A)

Spring Forest Trading v Wilberry [2014] ZASCA 178

Steyn v LSA Motors Ltd 1994 (1) SA 49 (A)

Van der Merwe NO v Hydraberg Hydraulics CC 2010 (5) SA 555 (WCC)

Van Niekerk v Smith 1952 (3) SA 17

Van Rooyen v Hume Mellville Motors (Edms) Bpk 1964 (2) SA 68

Van Vuuren v Van Vuuren (1854) 2 Searle 116

Van Wetten v Bosch 2004 (1) SA 348 (SCA)

Wilbery (Pty) Ltd t/a Ecowash v Springforest Trading 599 CC & Another (2994/2013) [2013] ZAKZDHC 37 (31 May 2013).*Wilken v Kohler* 1913 AD 135

International

Ardery v Smith 35 Ind App 94 73 NE 840

Ball v Dunsterville 100 ER 1038

Barwick v Govt Emp Ins Co Inc 2011 Ark 128 (2011)

Bassano v Toft [2014] EWHC 377 (QB)

Beatty v First Exploration Fund 1987 and Company, Limited Partnership 25 BCLR 2d 377 (1988) 385

Berdan v Berdan 103 P2d 622

Brantley v Wilson 2006 US Dist LEXIS 17722

Campaign Against Arms Trade v BAE Systems PLC [2007] ALL ER (D) 324 (Feb)

Central Motors (Birmingham) Ltd v PA Wadsworth & Another (Trading as Pensagain) (1982) 133 NJL 555 Court of Appeal (Civil Division)

Computer Sky Edv v Prime Medical Company Ltd Tel-Aviv Peace Court Civil Case 29488/04 (4 August 2004 unpublished Israeli case)

Cook In the Estate of (deceased). Murison v Cook & Another [1960] 1 ALL ER 689

Crestwood Shops v Hilkene 197 SW 3d 641 651 (Mo Ct App 2006)

Cubby Inc v CompuServe Inc 776 F Supp 135 (SDNY 1991)

Djordje Mitic v Eco Pro Australia Pty Ltd [2009] AIRC 503 (May 2009)

Dow Chemical Company v General electric 58 UCC Rep Serv 2d (CBC) 74 (E D Mich 2005)

Eastbourne Corporation v AG [1904] AC at 55

Edme v Internet Brands Inc 968 F Supp 2d 519 (2013), 41 Media L Rep 2696

Ellis v Smith 30 ER 205; 34 ER 666

Faulks v Cameron [2004] NTSC 61

First National Securities Ltd v Jones [1978] 2 ALL ER 221, CA

France v Dutton [1892] 2 QB 208

George A Ohl & Co v AL Smith Iron Works 288 US 170

Good Challenger Navegante SA v Metalexportimport SA [2004] 1 Lloyd's Rep 67

Goodman v Eban Ltd [1954] 1 ALL ER 763

Goodman v J Eban Ltd [1954] 1 QB 550

H Sayner and Joblink Plus Limited – re Termination of employment PR950280 [2004] AIRC 748 (30 July 2004)

Hellard v Money [2008] EWHC 2275 (Ch)

In re a Debtor (No 2021 of 1995) [1996] 2 ALL ER 345

In re Trollip 12 SC 243

International Casings Group Inc v Premium Standard Farms Inc 358 F Supp 2d 863 (W D Mo 2005)

Kevin C McMunigal v Kate E Bloch 2010 WL 4636549 (2010)

Lemayne v Stanley 83 ER 545

Lord Lovelace's Case W Jones 82 ER 140 270, 82 ER 141

Macdonald v Sun Life Assurance Company of Canada 2006 CanLII 41669 (ON SC)

McGuren v Simpson [2004] NSWSC 35

Morton v Copeland (1855) 16 CB 517

Naldi v Grunberg 2010 NY App Div Lexis 7173 (2010)

Newborne v Sensolid (Great Britain) Ltd [1954] 1 QB 45

Norwegian case LB-2006-27667, Borgarting appellate court, 20 August 2007

On Line Power Technologies Inc v Square D Co 2004 US Dist LEXIS 9655 (April 30 2004)

*Progressive **C**asualty Insurance Company v Estate of Jose Juan Palomera-Ruiz* 2011 WL 291137

R v Cowper (1890) 24 QBD 60, 533

Re Chalcraft's Goods [1948] P 222

Re Lemon's Goods (1896) 30 IrLTR 127

Rhodes v Peterson [1971] SC 56

Rioux v Coulombe (1996), 19 ETR (2d) 201, JE 97-263 (Quebec Sup Ct)

Rosenfeld v Zerneck 776 NYS 2d 458 (2004)

Sarl v Bourdillon 140 ER 79

Shattuck v Klotzbach 14 Mass L Rep 360 (Mass Super Ct 2001)

Shroyer v New Cingular Wireless Services Inc 498 F.3d 976

SM Integrated Transware Ltd v Schenker Singapore (Pte) Ltd [2005] 2 SLR 651, [2005] SGHC 58

Smith v Evans 95 ER 63

Stratton Oakmont v Prodigy 1995 WL 323710 (NY Sup Ct 1995)

Tassone v Kirkham [2014] SADC 134, 2014 WL 3889065

Taylor v Holt 134 SW3d 830, 834 (Tenn Ct App 2003)

Waddle v Elrod 367 SW 3d 217 (Tenn 2012)

Wilkens v Iowa Insurance Commissioner 457 N W 2d 1 (Iowa Ct App 1990)

DIAGRAM 1 ON ELECTRONIC SIGNATURES

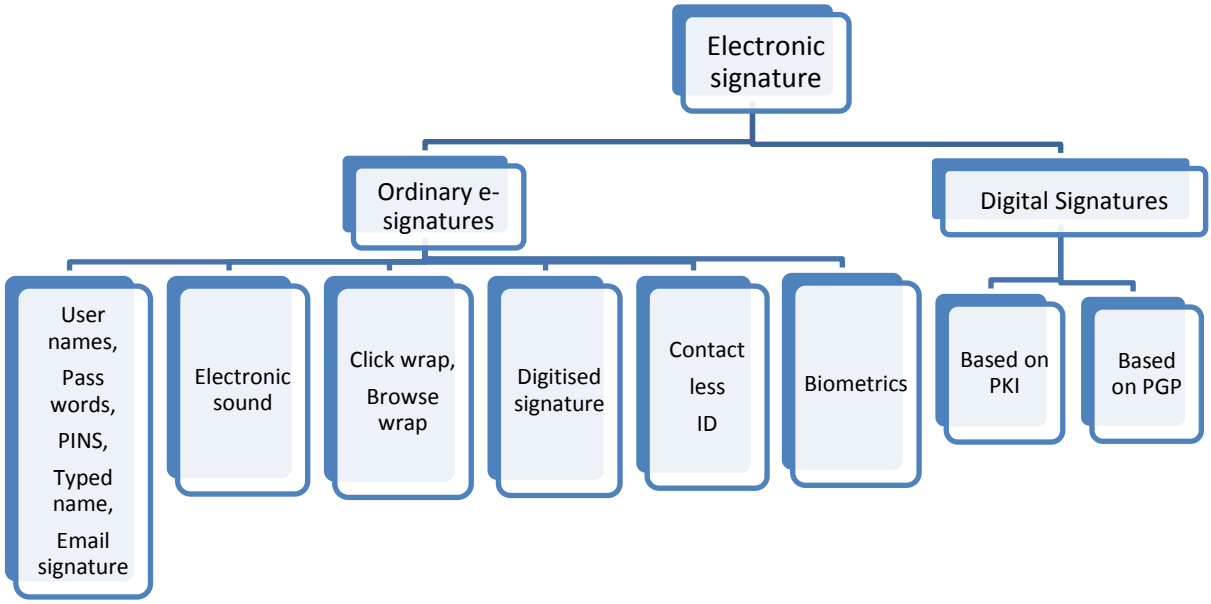

DIAGRAM 2: TABLE OF LEGISLATIVE INSTRUMENTS

The thesis examines the following legislative instruments and their adherence to proposed principles of e-signature regulation:

Legislation	**Technology neutral**	**Technology specific**	**Functionally equivalent**	**Not functionally equivalent**
SADC ML	1. Section 1 (11): definition of ordinary e-signature. 2.Section 7: recognises ordinary e-signatures when law or parties require signature.	1.Sections 1 (19) and 8 (1): definition of SeS. 2.Sections 8 (3): gives a SeS the presumption of validity and proper application. 3.Section 18: gives the SeS a presumption of attribution. 4.Sections 23 (1), (3) and 24 (3): require an SeS for document authentication.	1.Section 7 (1) and (2): any ordinary e-signature that meets functions of signature and is as reliable as appropriate will meet the law's requirement of signature. 2.Section 20: on admissibility and evidential weight of e-evidence.	1.Section 8 (3): gives a SeS the presumption of validity and proper application.
Lesotho Bill	1.Section 2: definition of ordinary e-signature and 'signed'. 2.Section 9 (2): recognises ordinary e-signatures.	1. Section 9 (1): prescribes use of the SeS where law requires signature and equates a SeS to a manuscript signature. 2. Section 2: Describes features of a SeS and	1.Section 2 and 9 (3) (a): on functions to be met by an ordinary e-signature and an SeS. 2.Section 20: admissibility and evidential weight of e-evidence.	1.Section 9 (1): prescribes SeS when law requires signature. 2.Section 9 (1) read with s 9 (3): Only an SeS is as reliable as appropriate to meet the law's

		prescribes the SeS where law requires writing. 3. Section 18 (2) gives an SeS a presumption of attribution. 4. Sections 23 (1), (3) and 24 (3) require a SeS for document authentication.		requirement of signature. 4. Section 9 (1) equates a SeS to a manuscript signature.
ECTA	1.Section 1: definition of ordinary an e-signature. 2.Section 13 (3): recognises ordinary e-signatures.	1.Section 13 (1): prescribes an AeS where law has not specified the e-signature it requires. 2. Sections 2, 37 and 38: requirements and features of the AeS. 3.Sections 18 (1) and (3): require an AeS for document authentication.	1.Section 13 (3) (a): functions of an ordinary e-signature. 2.Section 13 (3) (b): reliability level of an ordinary e-signature where parties require signature. 3.Section 15: admissibility and evidential weight of data messages.	1.Section 13 (4): grants an AeS a presumption of validity and proper application.
South Africa ECT Amendment Bill		1.Section 1 (u): definition of ordinary e-signature. 2.Section 1(b): definition of AeS. 3. Section 13 (4): gives the AeS		

		presumption of validity and proper application.		
EU Directive	1.Articles 5 (2): an ordinary e-signature should not be denied legal effect.	1. Article 2 (2): definition of an AeS. 2.Article 5 (1) (a): a QeS fulfils legal requirements of signature on data in the same way as a handwritten signature meets them in paper. 3. Article 5 (1) read with 2 (8) and (10): requirements of a QeS.		1. Article 5 (1) (a).
eIDAS Regulation	1. Article 3 (10): definition of ordinary e-signature. 2. Article 25 (1): recognises an ordinary e-signature. Article 3 (25) and 35 (1): give legal effect to any technology used as an e-seal.	1. Article 3 (11) and 26: definition of an AeS. 2.Article 25 (2): '[a] qualified electronic signature shall have the equivalent legal effect of a handwritten signature'. 3. Art 3 (12): provides that QeS means an AeS created by a 'qualified electronic signature creation device' that is	1. Article 3 (10): definition of ordinary e-signature.	1. Article 25 (2): equates a QeS to a handwritten signature.

		based on a 'qualified certificate for electronic signatures'.		
UETA	1. § 2 (8): definition of e-signature. 2. § 7 (a): ordinary e-signature not to be denied legal force. 3. § 7 (d): ordinary e-signature meets law's requirement of signature. 4. § 9 (a): an e-record or e-signature is attributable to a person if it was the act of the person. 5. § 11: an ordinary e-signature is sufficient for document authentication:		1. § 2 (8): defines ordinary e-signature 2. § 7 (d): an ordinary e-signature meets requirement of signature. 2. § 13: evidence of an e-signature or e-record not to be rejected due to its electronic form.	
E-SIGN	1. 15 USC § 7006 (2) & (5): definition of ordinary e-signature. 2. 15 USC §7001 (a) (1): an ordinary e-signature may not be denied legal effect.		1. 15 USC 7031 (a) (2) (C): parties to prove in proceedings that their authentication methods are valid.	1. 15 USC § 7004 (b) (2) (C) II: restricts regulation that requires unnecessary costs for use of e-records, instead requirements of offline and online must be equivalent.

	3.15 USC § 7001 (g): an ordinary e-signature is sufficient for document authentication.			

RECOMMENDED DRAFT LEGISLATIVE PROVISIONS

The suggested draft provisions below may assist the legislature improve e-signature regulations:

1. **For section 9 (1) of the Lesotho Bill** which reads 'Where a law requires the signature (manuscript) of a person, that requirement is met by a secure electronic signature.'
   It should adopt CUECIC's standard and read as follows:

   (1) If a law requires the signature of a person, that requirement is met in relation to an electronic communication if

   a. the method is used to identify the person and to indicate the person's intention in regard to the information communicated; and

   b. At the time it was used, the method used is either:
   (i) as reliable as appropriate for the purposes for which the information was communicated in light of all the relevant circumstances; or

   (ii) proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

The recommended wording effectively amends **section 9 (3)** of the Lesotho Bill which when read with section 9 (1) implies that only the SeS will be a reliable signature to meet the law's requirement of signature.

2. **Sections 8 (3) Lesotho Bill** and **SADC ML** read as follows: '[w]here a secure electronic signature has been used, the signature is regarded as being a valid electronic signature and having been applied properly, unless the contrary is proved'.
   And
   section 18 and 18 (2) of the SADC ML and Lesotho Bill respectively provide that:
   'A secure electronic signature is deemed to have been applied by the holder of the secure electronic signature, unless the contrary is proved.'

   The sections should read as follows:
   (1) An ordinary e-signature that is supported with metadata or other reliable evidence is attributable to the signer, and is presumed valid and properly applied, unless the contrary is proved.

Alternatively, consider the wording of § 9 (a) UETA: 'an e-record or e-signature is attributable to a person if it was the act of the person.'

3. **Section 2** of the Lesotho Bill defines an SeS as follows: ' "[S]ecure electronic signature" means a signature duly recognised in terms of subsection 8(1)'.

The Bill should delete the words 'duly recognised in terms of subsection 8(1)' from the definition.

4. **Sections 23 (1) of the Lesotho Bill & SADC ML** provide that**:**

'Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the secure electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or electronic communication.'

And

section 24 (3) of the Lesotho Bill & the SADC ML provide that:

'Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such a document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the secure electronic signature of the person by whom it is required to be sealed.'

The section to read as follows:

23. (1) If a law requires a signature or record to be notarised, acknowledged, verified, made under oath or a seal, the requirement is satisfied if an ordinary e-signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to, incorporated in or logically associated with the electronic signature or electronic communication.

(2) The e-signature method applied must either be:

(a) as reliable as appropriate in the circumstances for the purposes for which the information was communicated in light of all the relevant circumstances, or

(b) factually proven to identify the signer and their intentions; and

(3) The e-signature must be supported by another online authentication method.

5. **Sections 23 (3) of the Lesotho Bill & SADC ML** provide that**:**

   'Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of a secure electronic signature'.

   To read as follows:

   23 (3) If a security method can be used to prove that an electronic signature attached to e-communication is attributable to a certifying officer, the electronic communication is deemed certified.

   (4) "Security procedure" is a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, call back or other acknowledgment procedures.

6. **Section 9 (3):** See suggestion in point 1 above.

7. It is recommended that the above draft sections should be supported by a provision to the following effect:

   Parties to a transaction are to have the opportunity to prove in court or other proceedings that their authentication approaches and their transactions are valid.