A "SIGN" OF THE TIMES: A BRIEF CONSIDERATION OF THE VALIDITY OF E-SIGNATURES IN AGREEMENTS AND AFFIDAVITS IN SOUTH AFRICAN LAW

Ciresh Singh
LLB LLM PhD
Associate Professor, University of South Africa

SUMMARY

The evolution of technology has changed business practices all over the world. Owing to technological and e-commerce developments, businesses can now transact with each other instantaneously across borders. The digitalisation of commerce and other traditional working methods has created a new "digital age" in human history. Digitalisation has taken over many economic activities and industries and is slowly finding its way into the legal system. Several businesses are now concluding commercial transactions and contracts electronically. Electronic signatures have consequently become essential tools for concluding legal agreements and conducting other daily business and legal practices. These new innovations have brought into question the legal validly of these transactions, and in particular the legitimacy and security of electronically signed documents.

1 INTRODUCTION

Advancements in technology have not just changed but totally transformed the way we communicate both socially and formally. Technology has made it possible for us to interact with one another from different parts of the globe. It is difficult to imagine the world today without technology. The Internet, social media, online shopping and emails have become a common part of everyday life. Technology has created and continues to create a new economic landscape, revolutionising the global economy,[1] and transforming the way we live.

[1] See Van der Merwe, Roos, Eiselen, Nel, Erlank and Mabeka *Information and Communications Technology Law* 3ed (2021) ch 6; Gereda "The Electronic Communications and Transactions Act" in Thornton, Carrim, Mtshaulana and Reyburn *Telecommunications Law in South Africa*: (2006) ch 6 263; Coetzee "The Electronic Communications and Transactions Act 25 of 2002, Facilitating Electronic Commerce" 2004 3 *Stellenbosch Law Review* 501.

The digital revolution has occurred so rapidly that its character and implications from a business and legal perspective have not yet been fully understood.[2] The age of digitalisation has changed the way we interact with one another, and from a legal perspective it has changed the way contracts and other legal and commercial transactions are concluded. Through technology, electronic contracting has become fluid and borderless and now enables traders to do business and conclude valid agreements across borders and national frontiers.[3] Most business transactions can now be performed electronically, from anywhere in the world and at any time. The growth in e-commerce has created numerous advantages for business, such as reduced paperwork and lower commercial transaction costs. However, one of the biggest challenges has always been reliability, safety concerns, and lack of clarity and understanding as to the legal validity of using e-contracts and e-signatures.[4]

In South Africa, the use of technology in the legal sphere was initially slow; in particular, there was much scepticism on the use of e-signatures in agreements and in court documents such as affidavits. Accordingly, this contribution aims to consider the legal validity of e-signatures and electronically signed documents, such as in contractual agreements and affidavits. This task is undertaken in seven parts. Parts one and two serve as an introduction and background to the topic. Part three analyses the concepts of the traditional "wet-ink" signature and the "electronic" signature, as well as their respective validity in South African law. Part four considers the concept of an electronic signature in more detail and understands the different forms of e-signature. Parts five and six respectively consider the different legislative and judicial principles governing e-signatures. This is undertaken by discussing the different Acts, Rules and case law concerning the concept of electronically signed agreements and affidavits. Part seven serves as a conclusion to this article and provides brief recommendations on how more clarity can be established on the advancement of e-signatures in South Africa.

Signatures have become an integral part of daily life and are well established in commercial and legal practice. A signature serves to consent to or confirm an agreement or legal document and is thus a vital feature in finalising a transaction. Technology, such as e-signatures, is increasingly being used in modern-day activities. The traditional wet-ink signature differs significantly in form and application from an electronic signature. Therefore,

---

2 Gereda in Thornton *et al Telecommunications Law in South Africa* 263.

3 See Coetzee "The Convention on the Use of Electronic Communications in International Contracts: Creating an International Legal Framework for Electronic Contracting" 2006 18 *South African Mercantile Law Journal* 245 246; Singh "You've Got Mail: Have Electronical Communications Become the New Registered Mail" 2022 Q1 *Without Prejudice*; Srivastava and Koekemoer "The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview" 2013 21(3) *African Journal of International and Comparative Law* 427; Berman "International Divergence: The Keys to Signing on the Digital Line – The Cross Border Recognition of Electronic Contract Signatures" 2001 28 *Syracuse Journal of International Law and Commerce* 125.

4 Srivastava and Koekemoer 2013 *African Journal of International and Comparative Law* 427–429. There are various forms of electronic signature, such as passcodes and pins. For purposes of this article, only an electronic signature similar to the traditional written form used on paper is considered.

it is paramount that the laws relating to e-signatures be clear to ensure confidence and consistency with their use. Accordingly, the overall purpose of this contribution is to determine whether South Africa's current laws allow for the electronic signing of an agreement and affidavit and consider whether there is a need for a paradigm shift to allow for the more regular and confident use of e-signatures in South Africa.

2 BACKGROUND

Since the turn of the millennium, as a result of great technological advancements, many countries across the world were prompted to create or develop their e-commerce laws and build new legal frameworks for this emerging digital sector. In response to these changes, the United Nations Commission of International Trade law (UNCITRAL) developed the "Model Law on Electronic Commerce 1996" and the "Model Law on Electronic Signatures 2001".[5] These Model Laws were an early response by the international community to some of the uncertainties of e-commerce.[6] Most importantly, the UNCITRAL Model Laws provided a guideline to lawmakers around the world on how to frame their e-legislation.[7]

In South Africa, the Electronic Communications and Transactions Act[8] (ECTA) is the primary legislation governing digital communications.[9] The Act aims to address the world of e-commerce and establish legal principles to govern digitally concluded contracts and transactions in South Africa. The Act also deals with issues such as accreditation, authentication, access to e-services and consumer protection, and provides a legal framework for the legality of data messages and e-signatures.[10] The main objectives of ECTA are to promote, facilitate and regulate electronic communications and transactions.[11] The UNCITRAL Model Law on Electronic Commerce formed the foundation of ECTA. One of the underlying principles of the Model Law that was adopted by ECTA was the "functional equivalence principle". This principle recognises that electronic communications will be given the same legal recognition and be the functional equivalent of paper-based communications.[12]

---

5 See also Coetzee 2006 *SAMLJ* 246 and Eiselen "Fiddling with the ECT Act – Electronic Signatures" 2014 17(6) *Potchefstroom Electronic Law Journal* 2805.

6 See Van der Merwe *et al Information and Communications Technology Law* ch 6, 164 and UNCITRAL "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods" (2009) https://digitallibrary.un.org. The UNCITRAL recognised the uncertainty that may arise from the widespread growth of e-commerce and responded to this challenge by publishing the Model Laws.

7 Eiselen 2014 *PELJ* 2807.

8 25 of 2002.

9 See Van der Merwe *et al Information and Communications Technology Law* ch 2. ECTA was the product of a due diligence report on e-commerce legal issues in 1999. This report led to the *Discussion Paper on Electronic Commerce* (1999) which eventually led to the promulgation of ECTA on 2 August 2002.

10 Coetzee 2004 *Stellenbosch Law Review* 502–503. See also webinar by Lexis Nexis presented by Maggs *Legal in the Digital Age* (15 March 2022) www.lexisnexis/webinars.

11 See s 2 of ECTA, and Coetzee 2004 *Stellenbosch Law Review* 502.

12 See the Model Law on Electronic Commerce: Guide to Enactment: Part E. The Guide to Enactment discourages national laws from imposing stringent requirements on electronic

Despite the advanced technological objectives of ECTA, South African law has moved at an intermediate pace in advancing its legal environment into the digital age. Currently, most court processes are still burdened by a paper overload, and a walk through any South African regional and district court, or attorney's office will reveal a barrage of court files, printers and papers. This suggests that the move to the digital age has been slow, and despite the technological facilities available in South Africa to advance the digital process, these devices have generally not been effectively used.[13] The sluggish growth in technology in South Africa's legal system was, however, accelerated by the recent worldwide coronavirus outbreak. In South Africa, requirements on social distancing, travel restrictions and related Covid lockdown measures resulted in many commercial and legal documents being signed and concluded electronically. Moreover, technology was used to deliver documents electronically and even conduct judicial trials virtually. The emergence of the worldwide coronavirus pandemic brought to light the importance of technology and the ability to sign and conclude agreements and transactions electronically. The move to digitisation, using electronic signatures to endorse transactions, has consequently become a valuable and necessary tool to conclude agreements and sign court documents such as affidavits, dispensing with the need for physical face-to-face interaction. This approach has, however, sparked much debate around the legality of these contracts and affidavits, and in particular, the validity of e-signatures. The following sections consider the concept of an e-signature and determine whether an e-signature is validly recognised in South African law.

3 THE SIGNATURE

3 1 The traditional "wet-ink" signature

A full and detailed consideration of the history of the signature goes beyond the scope of this contribution. For purposes of this article, it is of value to note that the concept of a signature has been in existence for several millennia. The earliest relic of a signature was noted during Antiquity (3100 BCE), when Egyptians and Sumerians used markings on clay tablets to validate their identity. During the Middle Ages, Romans began using marks and other symbols on letters and contracts, as a sign of identification. By the seventeenth century, owing to the growth of business and industry, several countries such as England and the United States of America, passed legislation determining that certain contracts would only be valid if they were

transactions that are not required by paper-based transactions. Imposing stringent requirements on electronic transactions would have the effect of stifling e-commerce, which is detrimental to the concept of innovative business. The stringency of standards applied to electronic communications must be in accordance with those applied to paper-based communications. See also Van der Merwe *et al Information and Communications Technology Law* ch 2, and Papadopolous and Snail *Cyberlaw@SA III: The Law of the Internet in South Africa* 3ed (2012) 318.

13 Singh "Signed, Sealed and Delivered (Electronically): Embracing the Digital Takeover: A Brief Consideration of Electronic Signing and Delivery in South Africa" 2022 33(4) *Stellenbosch Law Review* 618 620.

signed by the contracting parties.[14] Accordingly, over the centuries the signature has developed into an important tool in business and modern life, as it is a source of authenticating one's identity and consent.

The word "sign" originates from the Latin word "*signum*" which means "mark". Over the years, legal academics and courts have formulated several propositions in an attempt to define the concept of a "signature". Similarly, the Oxford English Dictionary has provided several varying definitions for the word signature.[15] The most common proposition is that a "signature" is the signatory's name or mark, written in their own hand, on a paper document.[16] The most comprehensive definition of a signature was provided in *Putter v Provincial Insurance Co*,[17] in which the court found that any mark made by a person for the purpose of attesting the document, or identifying it as their act, is their signature thereto.[18]

According to this definition, a signature can fulfil a number of functions. First, it identifies the signatory as a party to the contract. Secondly, it expresses their intention to be bound by the contract; and, thirdly, it testifies to the true content of the agreement.[19] Consequently, in order for a signature to be valid in terms of South African common law:

a) the name or mark of the person signing must appear on the document;
b) the person signing must have applied it themselves; and
c) the person signing must have intended to sign the document.[20]

The UNCITRAL Model Law on Electronic Signatures Guide to Enactment 2001 deals with the function of signatures and provides that the functions traditionally performed by signature in a paper-based environment are to: identify a person; provide certainty as to that person's involvement in the act of signing; and associate the person with the content of the document. In essence, the primary functions of a signature are to confirm identification and intention. It naturally follows that if an e-signature can perform the same functions as a paper-based signature it should also be valid in law.[21]

---

14 See the English Statute of Frauds Act 1677.

15 Mason *Electronic Signatures in Law* 4ed (2016) 64.

16 *Harpur v Govindamall* 1993 (4) SA 751 (AD) 756–757. See also Kulehile *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* (PhD thesis, University of Cape Town) 2017 16.

17 1963 (3) SA 145 (W).

18 *Putter v Provincial Insurance Co supra* 148.

19 See Coetzee 2004 *Stellenbosch Law Review* 513; Mason *Electronic Signatures in Law* 65; Schellekens *Electronic Signatures: Authentication Technology From a Legal Perspective* (2004) 59–69. Mason and Schellekens identify seven functions of a signature, namely, identification; authentication; authorisation; integrity; originality; cautionary function; and attribution.

20 See Wong "Understanding Electronic Signatures in South Africa" (2018) https://dommisseattorneys.co.za/blog/understanding-electronic-signatures-in-south-africa/ (accessed 2023-02-01); Eiselen 2014 *PELJ* 2808.

21 See Heyink *Electronic Signatures for South African Law Firms: LSSA Guidelines* (2014) ch 2.

3 2 The electronic signature

As indicated above, one of the first forms of a signature was noted by the Egyptians. Another early form of the signature was in the Roman Empire when kings used a waxed sealed stamp on the envelope of letters. This was followed by the quill and papyrus and then by the modern-day and well-known handwritten signature using pen and paper.[22] Accordingly, over the centuries, the signature has evolved, and, as we experience the fourth industrial revolution, it only seems natural that the signature will now be developed by technology.[23]

It should be recognised that electronic documents need to be signed in the modern age, just as paper documents do. Hence, the effect of an e-signature in the online world needs to equate to a traditional "wet-ink" signature offline.[24] It follows that if an e-signature complies with the requirements and functions of a traditional signature, it should be deemed valid in law.[25] E-signatures are created using various electronic methods, and can be applied to a wide range of documents. The primary difference between a traditional wet-ink signature and an electronic signature is the nature of the act of signing. In the case of a traditional wet-ink signature, the signature is applied by the hand of the signer upon a manuscript, whereas an e-signature is applied by the use of digital software and other technical mechanisms. It is not always possible to "see" the person signing a document in the online world, hence the importance of ensuring that the person applying an electronic signature is authorised to do so.[26]

A large body of law and academic writing has recognised e-signatures.[27] Today, an electronic signature is widely recognised as the digital and functional equivalent of a handwritten signature.[28] As indicated, the functional equivalence principle, based on the UNCITRAL Model Law on Electronic Commerce and Model Law on Electronic Signatures, was heavily relied on in the drafting of ECTA.[29] As a result, several sections in ECTA have entrenched the position that an electronic signature is the functional

---

22 See webinar by Findlay *The Validity of Electronic Signatures and Cybersecurity* (23 October 2020) https://www.youtube.com/watch?v=JHfszr2KrVw (accessed 2024-01-05). See also webinar by Findlay, Singh, Hartman and Fourie "*Quo Vadis: Affidavits in the Digital Age*" (1 December 2021) https://lnkd.in/gaTZAnHW (accessed 2024-01-05).

23 Findlay https://www.youtube.com/watch?v=JHfszr2KrVw. See also Kulehile *An Analysis of the Regulatory Principles of Functional Equivalence and Technology Neutrality in Lesotho and SADC* 30–37.

24 See Schellekens *Electronic Signatures* 15 and Findlay *What You Need to Know About E-Signatures in South Africa: Think Twice Before You Sign* (2023).

25 See Eiselen 2014 *PELJ* 2808, and *UNCITRAL Model Law on Electronic Signatures* Part Two par 53–54, which provides that the minimum requirements for an e-signature are identity, authenticity, and integrity. See also Smedinghoff *Online Law: The SPA's Legal Guide to Doing Business on the Internet* (1997). Smedinghoff contends that e-signatures perform all the functions of a traditional signature, and in addition provide more security from fraud.

26 Schellekens *Electronic Signatures* 15.

27 See Van der Merwe *et al Information and Communications Technology Law* ch 2, and Papadopolous and Snail *Cyberlaw@SA III: The Law of the Internet in South Africa* 318.

28 See Findlay *What You Need to Know About E-Signatures in South Africa: Think Twice Before You Sign*.

29 See Heyink *Electronic Signatures for SA Law Firms* ch 2.

equivalent of a wet-ink signature.[30] For example, section 12 of ECTA recognises data as the functional equivalent of writing or evidence in writing by giving data messages the same legal validity as messages written on paper. It states that a requirement under law that a document or information be in writing is met if the document or information is in the form of a data message, and is accessible in a manner useable for subsequent reference to a person who either wants to rely on the existence of a particular agreement or for record purposes.[31]

Section 13 of ECTA deals with the validity of e-signature and provides:

> "(1) Where the signature of a person is required by law, that requirement in relation to a data message is met only if an advanced electronic signature is used.
> (2) Subject to subsection (1) an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.
> (3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if
> (a) a method is used to identify the person and indicate the person's approval of the information communicated; and
> (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.
> (4) Where an advanced electronic signature has been used, such signature is regarded as having created a valid electronic signature and to have been applied properly, unless the contrary is proved."

The words "electronic signature" or "e-signature" signify the concept of a signature that is conveyed by the application of a computer or computer-like device.[32] As with the traditional wet-ink signature, several attempts have been made by academia to define the concept of an electronic signature. Some have defined it as "anything in electronic form that can be used to demonstrate a signing entity intended their signature to have legal effect".[33] Others have described it 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".[34]

Section 1 of ECTA defines an "electronic signature" as:

> "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature."[35]

---

30 See ss 12, 13 and 22 of ECTA. See also art 11 of the *Model Law on Electronic Signatures*.

31 See Gereda *Telecommunications Law in South Africa* 270 and Snail "Electronic Signatures in South Africa" 2009 *De Rebus* 51.

32 Kulehile *An Analysis of the Regulatory Principles of Functional Equivalence and Technology Neutrality in Lesotho and SADC* 27–28.

33 See Mason *Electronic Signatures in Law* 199.

34 See Blythe "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 3.

35 "Data" is defined broadly by ECTA to include electronic representations of information in any form (s 1 of ECTA). See also s 11(1) of ECTA, which provides that information is not without legal force and effect merely on the grounds that it is wholly or partially in the form

The Model Law on Electronic Signatures defines "electronic signature" as:

> "data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."

From the above definitions, it can be seen that for a signature to be recognised as a valid electronic signature, the signature must comply with the criteria of "intention" and "relationship" in that there must be a "relationship" between the document and the signature, and the person must have "intended" it to be his signature.[36] Generally, an electronic signature is perhaps better capable of fulfilling these requirements than paper-based documentation, as the electronic signature process creates an electronic audit trail and certificate that clearly identifies the intention and relationship, and evidences any tampering with the signatures. In most instances, the audit trail will be able to identify the individual applying the signature and provide the date, time and place at which the signature was applied.

The key issue and concern with e-signatures is the evidence required in proving the identity of the signer and confirming that the document has not been altered. Consequently, the main challenge with the implementation of e-signatures in place of wet-ink signatures has always been the hesitancy among businesses to adopt such technology and process, and concerns over the validity, cybersecurity and court approval or acceptance of the use of e-signatures in contracts and affidavits.[37] Several commentators have pointed out that there are many advantages to using digital signatures instead of wet-ink signatures.[38] In particular, it is much easier to identify the signatory of an e-signature than a signatory of a wet-ink document, as an e-signature will always provide a crypto-authentication or audit trail and digital track record of the signing process. One of the biggest challenges with the traditional signature is forgery. E-signatures provide a mechanism to curb forgery, as an audit trail creates a digital signing ceremony or event and provides evidence of the date, time, place and signatories of the document, thereby confirming that the signing was done correctly. In comparison, wet-ink signatures require evidence from forensic handwriting experts, witnesses or co-signees of a document to prove the authenticity of the signature.[39] Furthermore, wet-ink signatures are much easier to forge than electronic

of a data message. Accordingly, "data" is given the same legal status as conventional paper information. See also s 22(1) of ECTA.

36 See Wong https://dommisseattorneys.co.za/blog/understanding-electronic-signatures-in-south-africa/ and Eiselen 2014 *PELJ* 2809–2810.

37 See also webinar by Summers, Pearson and Podbielski "Commissioning Affidavits Over Video" https://www.tech4law.co.za/courses-on-offer/webinar/commissioning-affidavits-over-video-tech-talk-legal/ (accessed 2022-12-13), wherein Summers indicates that although South Africa does not have a great amount of e-legislation, courts have been very pragmatic with the use of technology in the law.

38 See Smedinghoff *Online Law*; Heyink *Electronic Signatures for SA Law Firms* ch 5; and Findlay *The Validity of Electronic Signatures*.

39 See Heyink *Electronic Signatures for SA Law Firms* ch 5; Kulehile *An Analysis of the Regulatory Principles of Functional Equivalence and Technology Neutrality in Lesotho and SADC* 23, and Summers *et al* webinar, wherein Podbielski provides legal examples of fraudulent signatures, and comments that wet-ink signatures can easily be falsified and have many flaws.

signatures, as once an e-signature is placed on a secure uneditable document, the document locks and is unable to be tampered with, and detects when tampering has occurred.[40] Moreover, a digital certificate can be produced confirming the date, time and place of the signature, which is not possible with a wet-ink signature. For these reasons, it can be argued that e-signed documents are much more secure than paper-based ones.

Although e-signatures are increasing being used, Schedule 2 read with section 4(4) of ECTA specifically provides for four instances where an electronic signature would not be valid. These exclusions are:

a) the conclusion of an agreement for the alienation (disposal) of immovable property as provided for in the Alienation of Land Act 68 of 1981;
b) the conclusion of a long-term lease agreement of immovable property in excess of 20 years as provided for in the Alienation of Land Act;
c) the execution of a bill of exchange as defined in the Bills of Exchange Act 34 of 1964; and
d) the execution, retention and presentation of a will or codicil as defined in the Wills Act 7 of 1953.

It must however be noted that, with the rapid growth of e-commerce, many of the transactions excluded may soon be allowed to be signed electronically. There have already been several cases where courts have allowed for the e-signing of the above-mentioned exclusions.[41] If such exclusions are removed, the use of e-signatures may become more widely recognised and acceptable in South Africa.

4 FORMS OF E-SIGNATURE

Electronic signatures can manifest in a variety of forms, all of which may demonstrate the intention of the signer to authenticate data.[42] As indicated above, the term "electronic signature" is generally used to denote the generic concept of a signature brought about by use of a computer or computer-like device. South African law provides for two categories of electronic signature in ECTA, namely, "standard electronic signatures" and "advanced electronic signatures". This two-tiered approach to e-signatures is important as ECTA recognises both simple and technologically advanced e-

[40] Findlay *The Validity of Electronic Signatures*. Findlay makes reference to the 2002 movie "Catch Me If You Can", which depicts the real-life story of Frank Abagnale who was infamous for forging signatures on paper-based documents.

[41] See *MacDonald v The Master* 2002 (5) SA 64 (O) and Cornelius "Condonation of Electronic Documents in Terms of Section 2(3) of the Wills Act" *TSAR 2*003 210, which discusses instances where a court may allow electronic documents when considering a will. In respect of wills and codicils, there is an increasing trend among testators to create video recordings of their wills and last wishes. See also Snyman "To Use Electronic Signatures or Not to Use Electronic Signatures, That Is the Question?" https://heroldgie.com/using-electronic-singatures/ (accessed 2023-02-07); and *Borcherds v Duxbury* 2021 (1) SA 410 (ECP) wherein the court found that a sale agreement relating to immovable property that was signed using an e-signature was valid, as the signature was applied with the intention of forming a binding contract.

[42] See Mason *Electronic Signatures* 197 for a distinction between electronic and digital signatures.

signatures.[43] A standard e-signature can be used whenever *parties to an agreement* require a signature to validate a contract. However, when the *law* requires a signature, only an advanced electronic signature can be used to validate the agreement. These two forms of e-signature are discussed further below.

4 1 Standard electronic signatures

Standard electronic signatures can be applied to documents that do not require special legal requirements. Standard electronic signatures include digital or scanned signatures. An example would be using an electronic NotePad or SmartPhone to sign a document or merely printing, signing and scanning the document.[44] A standard electronic signature can be used where a signature is required by the parties to an agreement, and they do not specify the type of electronic signature to be used. In this instance, section 13(3) of ECTA provides that,

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

Essentially, a standard electronic signature can be described as an ordinary signature that is used for signing standard documents, such as email or letters, that require mid-level authentication or assurance. However, there may be circumstances where a more secure and reliable signature needs to be used, and which requires a high-level of authentication or assurance; in such cases, an "advanced electronic" signature is required.

4 2 Advanced electronic signatures

There are instances where an electronic signature other than a standard electronic signature may be required. This will include circumstances where the law requires that an agreement or document be in writing and signed.[45] In such instances, the document can only be signed with an "advanced electronic" signature as defined by ECTA. In other words, if a signed written document is a legal requirement for a transaction, that transaction will only be valid if an "advanced electronic" signature is used.[46] Accordingly, there is a need for standard electronic signatures to be distinguished from advanced electronic signatures. The main difference between a standard electronic

---

43 See Snail 2009 *De Rebus* 51.

44 Singh "Sign on the Digital Dotted Line: Evaluating the Legal Validity of Electronically Signed Document" 2021 *De Rebus* 20.

45 For e.g., the Companies Act 71 of 2008 requires that certain transactions be signed (see ss 12, 13, 30, 51, 58, 73, 77 and 101). In such instances, only an advanced e-signature can be used to conclude a valid transaction. See Van der Merwe *et al Information and Communications Technology Law* 129–130; and Christianson "Advanced Electronic Signatures" 2012 *De Rebus* 40.

46 Coetzee 2004 *Stellenbosch Law Review* 505; Gereda *Telecommunications Law in South Africa* 270.

signature and an advanced electronic signature is that the latter is endorsed with an accreditation by an accreditation authority.[47]

Section 13(1) of ECTA states that

> "where the law requires a signature to be used the requirement is only met in relation to a data message if an advanced electronic signature is used."

Section 1 of ECTA defines an "advanced electronic signature" as

> "an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37."

In order to be valid, an "advanced electronic signature" must meet the following requirements:

a) it must be uniquely linked to the signatory;
b) it must be capable of identifying the signatory;
c) it must be created using means that are under the signatory's sole control; and
d) it must be linked to other electronic data in such a way that any alteration to the said data can be detected.[48]

In practical terms, an advanced electronic signature is an electronic signature created with a digital certificate that results from a process which has been accredited by the South African Accreditation Authority, following a face-to-face identification. The criteria and standards for accreditation are set in the Regulations to the Act.[49] To date, there are only two accredited providers, namely the South African Post Office and LAWTrust.[50] This is problematic given the lack of efficiency and poor service from the Post Office, and the prohibitive costs of LAWTrust's signatures. In addition, the standards for accreditation are onerous and costly, and some argue that the costs of compliance with the standards result in South Africa having the world's most expensive advanced electronic signature.[51]

There has thus been much criticism on South Africa's advanced signature provisions. In addition to the burdensome administrative process and excessive costs of obtaining accreditation and signature, many academics argue that ECTA's provisions requiring an advanced electronic signature undermines the principle of technological neutrality.[52] Technological

---

47 See s 1 of ECTA. The authority for accreditation is held by the Department of Communication.

48 See s 38(1) of ECTA.

49 See also ss 37, 38 and 40 of ECTA.

50 See Singh 2021 *De Rebus* 20; and Gereda *Telecommunications Law in South Africa* 283. See also lawtrust.co.za.

51 See Heyink *Electronic Signatures for SA Law Firms* ch 7.

52 See Srivastava and Koekemoer 2013 *African Journal of International and Comparative Law* 430; Berman 2001 *Syracuse Journal of International Law and Commerce* 149; Snail "Electronic Contracts in South Africa: A Comparative Analysis" 2008 2 *Journal of Information, Law & Technology* 1–24; Swales "The Regulation of Electronic Signatures: Time for Review and Amendment" 2015 132(2) *South African Law Journal* 257 270). Swales argues that users should have the liberty to decide which type of technology they wish to use. Technologically prescriptive law has the potential to stifle the growth of e-commerce by restricting newer technologies from being used. Likewise, Snail suggests that

neutrality is an e-commerce principle that requires legislation to be non-prescriptive of technology, and is one of the underlying principles of e-commerce. The principle of technological neutrality proposes that law should not discriminate against or favour the use of any particular type of technology. The Model Laws do not prescribe any form or type of e-signature to be used, and advanced electronic signatures are not mentioned under the Model Laws. Thus, it has been argued that the accreditation requirement in ECTA for advanced electronic signatures violates the principle of technological neutrality and goes against the objects of the Model Laws.[53]

Conversely, others submit that advanced electronic signatures are necessary as they ensure a secure and protected environment, as they have several safeguards that authenticate the security of the signature. The accreditation requirements for these signatures serve as a safeguard against fraud and allow for a higher degree of security than standard e-signatures.[54] Accordingly, unlike standard electronic signatures, advanced electronic signatures are given special evidentiary advantages and are rebuttably presumed to be valid. Some commentators submit that an advanced electronic signature is the most secure signature available worldwide, and indicate that the cryptography behind an advanced electronic signature makes it mathematically infeasible to tamper with, as evidence of tampering will be shown – for example, by sending a warning.[55] Most advanced electronic signatures make use of a public key infrastructure (PKI), which uses two keys and an authorised cryptography provider to verify the authenticity of the signature.[56] A digital certificate confirms that the security,

South Africa should remove the stringent requirements for advanced electronic signatures and adopt a technology-neutral approach, while still providing a high level of security.

53 See Faria "E-Commerce and International Legal Harmonization; To Go Beyond Functional Equivalence?" 2004 16 *South African Mercantile Law Journal* 529, Swales 2015 *SALJ*; Srivastava and Koekemoer 2013 *African Journal of International and Comparative Law* 444. It is also noted that while the European Council Directive 1999/93/EC on electronic signatures allows for the use of advanced electronic signatures, it does not require accreditation for signatures to be valid. The EC Directive promotes technological neutrality in Recital 4 by viewing accreditation as a barrier to the development of commerce. Swales submits that the accreditation approach adopted by South Africa is cumbersome and onerous and is not in line with international standards.

54 See also Barofsky "The European Commission's Directive on Electronic Signature: Technological 'Favoritism' towards Digital Signature" 2000 24(1) *Boston College International and Comparative Law Review* 145.

55 See Department of Public Service and Administration *Electronic Signatures Guidelines* version 1.10 (12 February 2019) https://www.dpsa.gov.za/dpsa2g/documents/egov/2019/Electronic%20Signature%20Guidelines%20for%20the%20Public%20Service%20%20final.pdf (accessed 2024-01-05) par 4; Christianson 2012 *De Rebus* 40.

56 S 32(2) of ECTA provides that no person may provide cryptography products or services in the Republic until certain details, as required by the Act, are registered. In terms of Accreditation Regulation, a service provider of advanced electronic signatures must comply with the SANS 21188 PKI minimum standards. PKI involves the encryption of electronic messages. The encrypted data messages become the signature, which uniquely links the signatory to the message. In order for these messages to be decrypted, one would need to be in possession of a public key or private key. The document is signed with a private key and the recipient of the document will only be able to view the document if he enters the corresponding public key. See also ss37 and 38 of ECTA; Van der Merwe *et al Information and Communications Technology Law*; Christianson *De Rebus*; Kulehile *An Analysis of the*

integrity and identity of the signatory are upheld. This will usually also involve a face-to-face verification mechanism, which may also authenticate, *inter alia*, the biometrics, such as the fingerprints or iris scan of the signatory; and/or a pin or password belonging to the signatory. It is submitted that thumbprint verification can usually be used in addition to an e-signature to authenticate the identity of an individual, as most electronic devices such as cellphones and notepads already have such scanning ability.[57] An advanced electronic signature is a digital certificate-based signature that illustrates mechanisms to ensure security and integrity, and confirms the identity of the signer. Consequently, an advanced electronic signature is deemed reliable in law and is accepted as *prima facie* proof of its validity.[58]

Section 18 of ECTA, entitled "Notarisation, acknowledgement and certification" provides:

> "(1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached to, incorporated in or logically associated with the electronic signature or data message.[59]
>
> …
>
> (3) 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 an advanced electronic signature."

In South Africa, an advanced electronic signature is required for signing as a notary and/or commissioner of oaths.[60] Thus, it is submitted that an advanced electronic signature may be used for the signing of an affidavit and other court documents. The challenge with affidavits is the requirement that the documents be commissioned "in the presence of a commissioner of oaths". Regulations 1, 2 and 3 under the Justices of the Peace and Commissioners of Oaths Act[61] provide that the deponent shall sign the declaration in the presence of the commissioner of oaths. It is submitted that this requirement could be fulfilled electronically with the use of a video-conferencing system such as WhatsApp, Skye, Microsoft Teams or Zoom. Thus, the signing and commissioning of an affidavit could be done online via a video conference in which the deponent and the commissioner of oaths

Regulatory Principles of Functional Equivalence and Technology Neutrality in Lesotho and SADC 42–49, for a deeper analysis of cryptography and PKI.

57 UNCITRAL *Promoting Confidence in Electronic Commerce.* See also Bharvada "Electronic Signatures, Biometrics and PKI in the UK" 2002 16(3) *International Review of Law, Computers and Technology* 269.

58 See s 13 of ECTA.

59 See also Bechini and Gassen "Á New Approach to Improving Interoperability of Electronic Signatures in Cross Border Legal Transactions" 2008-2009 17(3) *Michigan State Journal of International Law* 703; Srivastava and Koekemoer 2013 *African Journal of International and Comparative Law* 430–440; Swales 2015 *SALJ* 257–270.

60 See Van der Merwe *et al Information and Communications Technology Law* ch 5 128–134. See also *Massbuild v Tikon Construction* [2020] 6986-2017 (GJ), where the court found that the suretyship agreement that was signed electronically was not valid, as an advanced electronic signature was not used.

61 16 of 1963.

are able to identify each other, and the signing occurs in each other's "virtual" presence, thereby complying with the Justices of the Peace and Commissioners of Oaths Act.[62] The requirement that the signing must occur in the presence of the commissioner is to ensure that the commissioner is able to identify the signer. It is contended that this identification is achievable virtually, and proof can be evidenced by a video recording. Furthermore, it must be noted that the Act is now over 60 years old, and there is a need for its practices to be reviewed in light of technological advancements.

5 E-LEGISLATION: LEGISLATIVE PROVISIONS PROMOTING E-SIGNATURES

5 1 International provisions

In view of the exponential growth of the Internet and e-commerce, international organisations have recognised the urgent need for uniform rules to be implemented to govern this growing sector. As a result, UNCITRAL developed two laws, namely the Model Law on Electronic Commerce 1996, and the Model Law of Electronic Signatures 2001. The main purpose of these Model Laws was to create a uniform set of international rules to govern e-commerce, promote the acceptance and efficiency of electronic mediums, create legal certainty by developing a safer legal electronic environment, and provide legal recognition for e-contracting and e-signatures.[63]

These Model Laws pursued the establishment of a functional equivalence approach that sought to allow electronic data to be recognised in the same manner as paper documents. This was promoted by article 5 of the Model Law on Electronic Commerce, which provides that "information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message." Article 7 of the Model Law on Electronic Commerce deals with e-signatures and reads as follows:

> "Where the law requires a signature of a person, that requirement is met in relation to a data message if:
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement."

Article 7 essentially provides that where e-signatures meet the criteria of technical reliability, they will be regarded as functionally equivalent to handwritten signatures. It further sets out general conditions under which

---

62 See *Gulyas v Minister of Law and Order* [1986] 4 All SA 357 (C), wherein the court held that "in the presence of" is analogous to "within eyeshot", in that the commissioner must be within eyeshot of the deponent to ascertain their identity and ensure the papers are correctly deposed.

63 See UNCITRAL *Model Law on Electronic Signatures With Guide to Enactment 2001* Part Two par 1–6. UNCITRAL went further to remedy the situation of international electronic contracting, and enacted the Convention on the Use of Electronic Communications in International Contracts. Adopted 23/11/2005; EIF: 01/03/2013.

electronic data can be regarded as authentic and enforceable, focusing on two of the main functions of a signature – namely, to identify the signer of the document, and to confirm the signer's consent to the contents of the document.

The Model Law on Electronic Signatures is based on article 7 of the Model Law on Electronic Commerce. The Model Law on Electronic Signatures was adopted in light of the increased use of e-signatures globally. The objectives of this Model Law are to encourage the use of electronic signatures and to promote equal treatment for all documents, whether they be in electronic or paper format. This Model Law focuses mainly on the roles or functions relating to public-key cryptography providers, which act as certification authorities for e-signatures.

Article 2 of the Model Law of Electronic Signatures defines an electronic signature as:

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

Article 6 of the Model Law on Electronic Signatures deals with the legal recognition of an e-signature and provides that an e-signature will be valid if it is reliable and appropriate for the purpose for which it was generated or communicated in light of all the circumstances. The Guide to Enactment to the Model Law on Electronic Signatures further sets out a number of legal, technical and commercial factors that should be taken into account when determining whether the method used for signing was sufficiently reliable and appropriate.[64] The Guide sets out practical standards that are required for technical reliability and legal effectiveness to be expected from the e-signature.

The Guide to Enactment makes it explicit that the Model Law only offers a framework within which laws can be structured, and that it is not intended to set out all the requirements that may be necessary to implement any given electronic signature law. It does not set out the rules and regulations that may be necessary to implement electronic signature techniques, nor does it deal with liability, leaving national laws to determine what liability a party may be subject to in accordance with applicable law. However, the Model Laws do set out criteria against which an adjudicator might assess the conduct of the parties.[65]

Several countries across the world have adopted the Model Laws and given recognition to the validity of e-signatures. In the United States, the Electronic Signatures in Global and National Commerce Act, also known as the E-Sign Act, and the Uniform Electronic Transactions Act, were enacted in 2000. These Acts provide legal recognition to electronic records, electronic signatures and electronic contracts.[66] Likewise, Australia (the Electronic Transactions Act 1999), Germany (the Electronic Signatures Act of 2001), Canada, (the Canadian Uniform Electronic Commerce Act), and

64 See the Guide to Enactment par 58–61.
65 Mason *Electronic Signatures* 101.
66 S 101 of the US E-Sign Act.

the United Kingdom (the Electronic Communications Act 2000) provide legal recognition to electronic signatures and transactions, and provide that a transaction may not be denied legal effect solely because of its electronic format. These countries have adopted the functional equivalence approach, which provides that if a law requires a record to be in writing, an electronic record satisfies the law.[67]

5 2 Domestic (South African) provisions

South Africa has followed the global trend in recognising the legality of electronic signatures, rendering the status of electronic signatures the functional equivalent of traditional wet-ink, pen-based signatures. ECTA, like most e-legislation in foreign countries, has followed the recommendations of the Model Laws. There are several sections in ECTA that confirm the validity of the electronic signature. Section 13(2) specifically confirms that an electronic signature cannot be denied enforceability merely because it has been given electronically or through data messages. Section 13(4) further provides that "where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved."[68] ECTA specifically states that an electronic signature is not without legal force and effect merely because it is in electronic form,[69] clearly confirming that electronic signatures are legally recognised in South Africa.[70]

In relation to credit agreements, the validity of electronic signatures is governed by section 2(3)(*b*) of the National Credit Act[71] (NCA), which provides:

> "If a provision of this Act requires a document to be signed or initialled by a party to a credit agreement, that signing or initialing may be effected by use of– ... an advanced or electronic signature as defined in the Electronic Communications Act, 2002 (Act No. 25 of 2002), provided that:
> (i) the electronic signature is applied by each party in the physical presence of the other party or an agent of the party; and
> (ii) the credit provider must take reasonable measures to prevent the use of the Consumer's electronic signature for any purpose other than the signing or initialing of the particular document that the consumer intended to sign or initial."

---

67 S 7 of the US Uniform Electronic Transactions Act. See also s 106 of the US E-Sign Act. The United States has adopted a minimalistic approach to e-signatures and defines an e-signature as 'any electronic sound or process logically associated with a contract or record and executed or adopted by a person with the intent to sign the record. The minimalistic approach has however been criticised as it allows for a low level of security and opens the door to fraud.

68 See also art 7 of the Model Law, which establishes the presumption that an electronic signature shall be treated as a handwritten signature where it meets the criteria of technical reliability.

69 See also ss 11(1), 13(2) and 14(1) of ECTA.

70 See s 15(4) of ECTA, which provides that a data message, such as an electronic signature, produced in any legal proceedings is admissible evidence and is rebuttable proof of the facts therein. This means that once a data message is produced in court it is presumed to be factually accurate. See also *Absa Bank Limited v Le Roux* 2014 (1) SA 475 (WCC).

71 34 of 2005.

Section 2(3) provides that when the NCA requires a document to be signed, that requirement is fulfilled if an electronic signature is used, provided that the electronic signature is applied in the physical presence of the other contracting party. This provision, however, does not specify a required form of signature (whether a standard or advanced electronic signature), nor does it specify that an electronic signature is required to be applied in the manner stated in section 2(3) for the validity of a credit agreement.[72] As seen with the provisions in the Justices of the Peace and Commissioners of Oaths Act, the NCA also requires that signatories of a document must be in the "physical presence of each other". Accordingly, it is debatable whether a credit agreement is valid if it is e-signed by both parties at different times and in different locations, and whether e-signing in the "virtual" presence of one of the contracting parties is acceptable. It is submitted that an amendment to the NCA may be required to establish clarity on these points.

Another key example of the use of and support for e-signatures in South Africa is the publication of the "Electronic Signature Guidelines" by the Department of Public Service and Administration in February 2019.[73] These Guidelines essentially recognise the development of e-services in the public sector and provide support for the use of e-signatures within public service departments. The Guidelines aim to provide a framework for evaluating the appropriateness of e-signatures and seek to enable greater adoption of e-signatures across governmental departments.[74] Its primary purpose is to provide guidance to governmental departments to deploy e-signatures and ultimately modernise the public sector. The Guidelines provide detailed steps to ensure the trustworthiness of e-signed documents and encourage public departments to establish policies and frameworks to incorporate the use of e-signatures in their business.

The above-mentioned legislative provisions and guidelines not only recognise the use of e-signatures but also provide the assurance that e-signatures have the same legal validity as wet-ink signatures. Accordingly, if an e-signature is used to conclude an agreement, provided all the essential requirements are met, neither party to that agreement can repudiate the contract purely on the ground that the contract was signed electronically, rather than on paper. The following section provides some examples of where an e-signature was used in legal documents.

6 JUDICIAL PRECEDENT ON E-SIGNATURES

6 1 E-signatures to conclude agreements

The following section discusses some of the most prevalent cases interpreting e-contracts and e-signatures in South Africa.

---

[72] See Warmback and Ebrahim "Electronic Signatures, Credit Agreements and the National Credit Act" (9 October 2020) www.wylie.co.za/Articles/Read/27/Electronic-Signatures-Credit-Agreements-and-the-National-Credit-Act (accessed 2023-02-14).

[73] See Department of Public Service and Administration https://www.dpsa.gov.za/dpsa2g/documents/egov/2019/Electronic%20Signature%20Guidelines%20for%20the%20Public%20Service%20%20final.pdf.

[74] Par 1.3 and 2 of The Guidelines.

6 1 1 Jafta v Ezemvelo KZN Wildlife [2008] 10 BLLR 954 (LC)

Jafta v Ezemvelo KZN Wildlife was one of the first major cases in South Africa to interpret ECTA. Although this case did not strictly deal with an e-signature, it did confirm the recognition and validity of electronic messages in South Africa.[75] The facts of the case are complex: in summary, Jafta attended an employment interview and was offered employment at Ezemvelo Wildlife. There were some negotiations about the exact start date of the contract; as a result, emails and SMSes were exchanged between the parties.[76] The main issue before the court was whether these e-communications amounted to an acceptance of the offer of employment.

Ezemvelo did not dispute that the sending of an email was an acceptable form of communicating the offer of acceptance. However, they claimed that they never received any emails from Jafta.[77] The court confirmed that the receipt of emails and SMSes were dealt with by ECTA. With regard to emails, it was settled that emails were an effective form of communication, and that an email sent by Jafta amounted to an acceptance of the offer of employment.[78] This email, however, was never successfully received by Ezemvelo, and therefore it was necessary to consider whether an SMS also amounted to an acceptance in terms of ECTA.

In making its decision, the court considered international law and foreign law. It was trite that several international and foreign law provisions recognise the validity of e-communications. E-communications law had become international and consequently had to be applied harmoniously and uniformly.[79] By adopting international principles, such as the Model Laws, South Africa had incurred a duty to implement the unification of international e-communications law. This had already been done by ECTA and was required to be implemented by the courts. Consequently, in terms of the Model Laws, data messages had to be given the functional equivalence of paper-based solutions, and courts had to give due evidentiary weight to data messages, and recognise that any agreements formed from data messages have full legal effect.[80] The court acknowledged that e-communications were now standard forms of transacting in the information age, and anyone seeking to exclude particular forms of communication had expressly to contract out of them.[81] The court accordingly found that by communicating with Jafta by SMS, Emvelo signalled that SMS was a valid mode for

---

75 See also Papadopoulos "Short Message Services And E-Contracting" 2010 31 *Obiter* 188.

76 *Jafta v Ezemvelo KZN Wildlife* [2008] 10 BLLR 954 (LC) par 5–8.

77 *Jafta supra* par 17–29. Expert IT evidence revealed that there may have been some technical virus safeguards that blocked Jafta's emails from being received by Ezemvelo.

78 *Jafha supra* par 37.

79 *Jafta supra* par 57.

80 *Jafta supra* par 72–73, referring to ss 15, 22 and 22 of ECTA, and Singapore High Court-Suit No 594 of 2003 *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*, and US *Shattuck v Klotzbach* 14 Mass.L.Rptr.360, 2001 WL 1839720 (Mass.Super) and *Rosenfeld v Zerneck* 4Misc.3d193. In these cases, the courts held that the typewritten names of the parties on an email constituted a valid signature.

81 *Jafta supra* par 98.

acceptance of their offer.[82] The court concluded that an SMS was an electronic communication in terms of ECTA, and therefore was a valid mode of communication for acceptance of the offer.

The *Jafta* decision was confirmed in *Mafika v SABC.*[83] In this matter, Mafika had sent an SMS to his employer confirming his intention to resign with immediate effect. The issue before the court was whether the SMS constituted a valid written resignation. In making its decision, the court considered section 12 of ECTA, which provides:

> "A requirement in law that a document or information must be in writing is met if the document or information is—
> (*a*) in the form of a data message; and
> (*b*) accessible in a manner usable for subsequent reference."

Accordingly, the court confirmed the finding in *Jafta* and confirmed that a communication by SMS is a communication in writing. Consequently, the court held that an SMS sent as a resignation amounted to a data message in terms of section 12 of ECTA.[84] The early *Jafta* and *SABC* cases confirmed the validity of emails and SMSes as valid forms of communication to conclude agreements and was the first step in recognising the validity of e-signatures. Importantly, the court in *Jafta* held if, in this modern age, one wishes not to use e-communications, one needs expressly to contract out of its use.[85]

6 1 2 FirstRand Bank t/a Wesbank v Molamugae [2018] ZAGPPHC 762

In *First Rand Bank v Molamugae,* the court considered the validity of an e-signature in a credit agreement. In this matter, Wesbank instituted action against Molamugae for the cancellation of an instalment sale agreement known as an "iContract" and the repossession of a motor vehicle.[86] The iContract was signed by the defendant online and electronically. A special watermark generated by the computer appeared on the iContract once the debtor accepted the terms and conditions by effecting his electronic signature.[87] The main issues before the court were whether an instalment sale agreement had been concluded in terms of the NCA, and whether the electronic signature was in compliance with ECTA.[88] In analysing section 2(3) of the NCA, the court held that the NCA does not provide for the form that the signature to the instalment sale agreement needs to take. As a

---

82 *Jafta supra* par 101.

83 [2010] 5 BLLR 542 (LC).

84 See also Manamela "'To Meet Is to Part': Resignation by SMS Constitutes Notice in Writing as Required by the Basic Conditions of Employment Act: *Mafika v SA Broadcasting Corporation Ltd: Case Comments*" (2011) 23 *SAMLJ* 521.

85 Papadopoulos 2010 *Obiter* 200.

86 *FirstRand Bank t/a Wesbank v Molamugae supra* par 6.

87 *FirstRand Bank t/a Wesbank v Molamugae supra* par 17.

88 *FirstRand Bank t/a Wesbank v Molamugae supra* par 27. The defendant contended that s 2(3) of the NCA was not complied with. In response, FirstRand pleaded that the agreement was completed and signed electronically by the defendant and that it constituted a valid agreement in terms of the NCA and ECTA.

result, it is quite possible for an electronic signature on the agreement to be in compliance with ECTA.[89] The court held further that in modern-day society with advanced technology, agreements are concluded without parties being in the physical presence of each other.[90] Consequently, the court found that an instalment sale agreement had been concluded electronically and was valid and binding.

On the basis of the wording of section 2(3) of the NCA and the court's interpretation in the *Molamugae* case, it is apparent that there is no prescribed form for the signing of a credit agreement that falls within the ambit of the NCA. Therefore, a credit agreement that is signed electronically, using a standard electronic or advanced electronic signature, will be valid and binding, having full force and effect in law, as if a manuscript hard copy had been signed.[91] The current legal position will prove favourable, particularly to financial institutions that seek to limit physical interaction, increase efficiency, be environmentally sustainable and keep up with the digital age.[92] Accordingly, it is submitted that the NCA needs to be amended to allow for the e-signing of documents, by removing the requirement that the parties must be in the physical presence of one another.

6 1 3 Spring Forest Trading 599 CC v Wildberry (Pty) Ltd 2015 (2) SA 118 (SCA)

Another example of judicial approval of electronic signatures is noted in the case of *Spring Forest Trading 599 CC v Wildberry (Pty) Ltd.*[93] In this matter, the Supreme Court of Appeal held that a signature affixed to an email constituted a valid electronic signature. The case dealt with the rental agreement of several car-washing mobile dispensing units. The agreement contained a non-variation clause providing that no variation or consensual cancellation would be effective unless reduced to writing and signed by both parties.[94] The court had to consider whether an exchange of emails between the parties discussing the cancellation merely recorded a negotiation, or whether the emails and footer e-signatures therein amounted to an agreement to cancel.[95] The Supreme Court confirmed that ECTA gives legal recognition to transactions concluded by email and held that the typewritten names at the end of the email correspondence between the parties constituted an electronic signature in terms of section 13(3) of ECTA.[96] The court found that the typewritten names of the parties at the foot of the emails, which were used to identify the users, constituted "data" that is logically associated with the data in the body of the emails, as envisaged in the definition of an "electronic signature". It therefore satisfied the

89 *FirstRand Bank t/a Wesbank v Molamugae supra* par 43.

90 *FirstRand Bank t/a Wesbank v Molamugae supra* par 44.

91 Warmback and Ebrahim www.wylie.co.za/Articles/Read/27/Electronic-Signatures-Credit-Agreements-and-the-National-Credit-Act.

92 Warmback and Ebrahim www.wylie.co.za/Articles/Read/27/Electronic-Signatures-Credit-Agreements-and-the-National-Credit-Act.

93 2015 (2) SA 118 (SCA).

94 *Spring Forest Trading supra* par 2–4.

95 *Spring Forest Trading supra* par 12.

96 *Spring Forest Trading supra* par 24–27.

requirement of a signature and had the effect of authenticating the information contained in the emails.[97] The court held that if there is intention for the data to constitute a signature, and such data is attached to or logically connected with other data, then it amounts to an electronic signature. Accordingly, if the parties require a signature but have not agreed on the method, the signature requirement is met under ECTA if the electronic signature method used:

a) identifies the person;
b) indicates the person's approval of the information communicated; and
c) is reliable and appropriate for the purposes for which the information was communicated, having regard to the circumstances.[98]

The *Spring Forest* case essentially confirmed the principle that the affixing of one's name upon an email footer authenticates that email and the typed name constitutes a valid e-signature. Several foreign jurisdictions have confirmed the same principle.[99] This principle affirms the courts' acceptance of technological developments and further confirms the position that contracts can be signed and concluded electronically by email.

6 1 4 Global & Local Investments Advisors (Pty) Ltd v Fouché 2021 (1) SA 371 (SCA)

In this matter, Fouché had given a written mandate to Global to invest money on his behalf.[100] The mandate provided that all instructions must be given by fax or email with Fouché's signature. Fraudsters hacked Fouché's email and instructed Global to transfer money into a third person's account.[101] The emails from the fraudsters ended with the words "Thanks Nick / Regards Nick". Fouché claimed that this transfer was contrary to their mandate, as it did not bear his signature, either electronically or in manuscript form. The court held:

> [S]ince the mandate requires a 'signature' which in every day and commercial context serves an authentication and verification purpose. In order to be able to resort to s 13(3) of the ECT Act Global would have had to show that in terms of the mandate an electronic signature was required. The word 'electronic' is conspicuously absent from the mandate. The court below cannot be faulted for concluding that what was required was a signature in the ordinary course, namely in manuscript form, even if transmitted electronically, for purposes of authentication and verification. The instruction was not accompanied by such a signature and the court below correctly held that the

97 *Spring Forest Trading supra* par 28.

98 *Spring Forest Trading supra* par 18, referring to s 13 of ECTA. See also the Missouri case of *International Casings Group, Inc. v Premium Standard Farms, Inc* 358 F.Supp.2d 863 (W.D.Mo. 2005), 2005 WL 486784, where the court held that where an email includes the name of the sender in the header or at the bottom of the email, the act of pressing the send icon on a computer constituted the authentication of the document, and it was a valid electronic signature under the Missouri and North Carolina Electronic Transactions Act.

99 See *4 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); and *Faulks v Cameron* [2004] NTSC 61.

100 *Global & Local Investments Advisors (Pty) Ltd v Fouché supra* par 2.

101 *Global & Local Investments Advisors (Pty) Ltd v Fouché supra* par 3.

> funds were transferred without proper instructions and contrary to the mandate.[102]
>
> *Spring Forest* is distinguishable for the following reasons: The authority of the persons who had actually written and sent the emails was not an issue in that case as it is in the present case. The issue in that case was whether an exchange of emails between the contracting parties could satisfy the requirement imposed by them in the contract that 'consensual cancellation' of their contract be 'in writing and signed' by the parties. There was no dispute regarding the reliability of the emails, accuracy of the information communicated or the identities of the persons who appended their names to the emails. In the present case the emails in issue were in fact fraudulent. They were not written nor sent by the person they purported to originate from. They are fraudulent as they were written and dispatched by person or persons without the authority to do so. They are not binding on Mr Fouché.[103]

While the court in *Spring Forest Trading* found that an email signature amounted to a valid and binding electronic signature, in the case of *Global*, which dealt with payments made based on fraudulent emails, the court held that the mandate between the parties did not explicitly refer to an 'electronic signature' and found the signature and resultant transaction non-binding and invalid. Thus, the court in *Global* held that the email signature did not constitute a signature as required by the mandate between the parties.[104] According to this case, it is advisable that contracting parties explicitly agree to the use of electronic signatures and agree on the signing method to be used to comply with the requirements in ECTA.

6 1 5 FirstRand Bank Limited v Govender [2023] ZAGPJHC 610[105]

FirstRand Bank v Govender is one of the most recent cases involving an e-signature.[106] The facts of the case were fairly similar to *Molamugae,* in that Govender concluded a credit agreement with FirstRand for the purchase of a motor vehicle. The agreement was concluded electronically using FirstRand's iContract software. Govender defaulted on his payments in terms of the agreement and FirstRand thereafter initiated litigation and sought recovery of the vehicle.[107]

Govender denied concluding any electronic agreement with FirstRand and claimed that his brother-in-law had, without his knowledge and consent, concluded the agreement.[108] FirstRand Bank led evidence confirming that an iContract had indeed been concluded and that Govender had knowledge of

---

[102] *Global & Local Investments Advisors (Pty) Ltd v Fouché supra* par 14.

[103] *Global & Local Investments Advisors (Pty) Ltd v Fouché supra* par 16.

[104] See also *SN4, LLC, v. Anchor Bank*, FSB 848 N.W.2d 559 (Minn.App. 2014) before the Court of Appeals of Minnesota. In this case, the parties exchanged a series of emails relating to the sale and purchase of real estate. It was contended that the signature on the emails constituted a signed contract. The court rejected this argument and found that both parties explicitly agreed that they would enter into a written contract signed with manuscript signatures, hence an electronic email agreement was contrary to their intentions.

[105] See also *FirstRand Bank Limited v Silver Solutions 3138 CC* [2023] ZAKZPHC 26, wherein the court confirmed the validity of an e-signed agreement.

[106] This judgment was delivered on 1 June 2023.

[107] *FirstRand Bank Limited v Govender supra* par 1–4.

[108] *FirstRand Bank Limited v Govender supra* par 7, 20, 21, 22.

the agreement.[109] FirstRand showed that the iContract contained a watermark stamp in the middle of each contract page that proved that Govender signed the contract electronically. Prior to the e-signing, an SMS and email containing a link to the iContract was sent to Govender. Thereafter Govender received a One Time Pin, which allowed him access to the iContract. This entire process required Govender to produce his identity documents and other relevant documents after he entered the Pin, ensuring that he was the only one who would have access to the contract.[110]

On consideration of the evidence, the court concluded that the facts revealed that Govender had indeed concluded an e-contract and at all times had knowledge of its existence and validity. The court unequivocally confirmed that the validity of e-contracts and e-signatures was settled in South Africa by ECTA.[111] Accordingly, it was trite that a contract could be validly signed and concluded electronically.

6 2 E-signatures for signing as a deponent and commissioner of oaths on a court affidavit

In the recent cases of *FirstRand Bank v Briedenhann*,[112] *Knuttel v Shana*[113] and *Maluleke v JR Investments*,[114] the courts had to decide on the issue of whether a court affidavit could be signed and commissioned electronically, and whether the rules for commissioning could be relaxed under these circumstances. In *Knuttel* and *Maluleke*, the deponents to the affidavit had contracted the Covid-19 virus and this made it impossible for them to sign the affidavit in the physical presence of a commissioner of oaths. Accordingly, under the circumstances, the commissioner communicated with the deponent via WhatsApp video and the deponent signed the affidavit during the video call. Similarly, in *Briedenhann*, the applicant's affidavit had been deposed to electronically and was commissioned by way of a virtual conference. Referring to the case of *S v Munn*,[115] the courts in the above-mentioned cases confirmed that the requirement for physical face-to-face interaction was not peremptory and could be relaxed during commissioning. Consequently, the court held that the signing of the affidavit virtually was

[109] *FirstRand Bank Limited v Govender supra* par 11–15. FirstRand produced evidence of telephone recordings confirming Govender's knowledge of the agreement, and admission that he paid the instalments in terms of the agreement for over four years.

[110] *FirstRand Bank Limited v Govender supra* par 11.

[111] *FirstRand Bank Limited v Govender supra* par 24.

[112] *FirstRand Bank v Briedenhann* [2022] 3690 (ECG).

[113] *Knuttel NO v Shana* 2021 (JOL) 51059 (GJ) (unreported case no 38683/2020, 27 August 2021).

[114] *Maluleke v JR 209 Investments* [2021] 60330-2021 (GP) par 12. In this matter, the commissioner commissioning the affidavit filed a separate affidavit detailing the steps they took to ensure that there was compliance with the Justices of the Peace and Commissioners of Oaths Act.

[115] 1973 (3) SA 734 (NC). The court held that non-compliance with the regulations would not intrinsically invalidate an affidavit if there was substantial compliance with the formalities in such a way as to give effect to the purpose of obtaining a deponent's signature to an affidavit. See also Snyman and Matyeni "Solemnly Swearing Virtually" (3 March 2022) https://heroldgie.com/solemnly-swearing-virtually/ (accessed 2023-02-14).

valid, and found that there was substantial compliance with administering the oath.[116]

The three judgments mentioned are welcome findings by the courts, as not only do they confirm the courts' approval of the use of e-signatures, but they also allow for the commissioning of documents virtually, dispensing with the need for the parties to be in the physical presence of one another. This approach is indeed welcome in the digital era in which we live.[117] South Africa's legal system depends significantly on evidence being supplied by affidavits.[118] In practice, almost every court application requires a signed and commissioned affidavit. The traditional wet-ink signing of affidavits is extremely cumbersome, as the signing and commissioning process is costly and time-consuming.[119] The e-signing of affidavits could serve as an easier, faster and more cost-effective measure to undertake this exercise. In this regard, it is contended that the Justices of the Peace and Commissioners of Oaths Act should be amended by allowing for e-signing and e-commissioning of affidavits. It is noted that the Justices of the Peace and Commissioners of Oaths Act is 60 years old, and the Act needs amending to be brought in line with the current digital age.[120]

The above legal provisions and case law unequivocally affirms the validity of e-signatures in South African law. Most importantly, ECTA does not limit the operation of any law, nor does it compel anyone to use or submit information in an electronic form.[121] Gereda submits that the Act does not discriminate between paper and electronic documents, nor does it create a new way of doing business. ECTA does however facilitate, and gives legal recognition to, the new ways of doing business that are emerging through the evolution of technology.[122] In a country like South Africa, which has components of both a developing and developed society, the emergence of a digitalised economy could prove challenging to the public and private sector. Given this unique position, ECTA has done well to facilitate the use of electronic communications.[123]

---

116 See Steyn "Commissioning of Oaths in the 21st Century" 2021 *De Rebus* 9. See also the Canadian Superior Court of Justice case of *Rabbat v Nadon* 2020 ONSC 2933, where the court permitted the virtual commissioning of affidavits considering the restrictions owing to Covid-19.

117 Steyn 2021 *De Rebus* 9.

118 See Otzen and Brouwer "Remote Commissioning of Affidavits" 2020 *De Rebus* 22, referring to *Elchin Mammadov and Vugar Dadashov v Jan Stefanus Stander* (GP) (unreported case no 100608/15), which provided several steps for the commissioning of an affidavit virtually.

119 See *Quo Vadis* webinar https://www.youtube.com/watch?v=P81JYA4kffE, wherein Singh provides a summary of the signing and commissioning of a traditional wet-ink affidavit, *inter alia*, the need for the affidavit to be printed, travel arrangements to be made for commissioning, every page required to be initialled, and finally scanned and posted to the attorneys.

120 See *Quo Vadis* webinar, for comments by Fourie on the Justices of the Peace and Commissioners of Oaths Act. It is interesting to note that a recent poll by Lexis Nexis revealed that 98 per cent of legal professionals are in agreement about to having e-signatures in place for affidavits.

121 Gereda *Telecommunications Law in South Africa* 269.

122 Gereda *Telecommunications Law in South Africa* 270.

123 Gereda *Telecommunications Law in South Africa* 294.

7 CONCLUSION AND WAY FORWARD

In the introduction to this article, the question was posed whether e-signatures can be validly used to sign an agreement and court affidavit. This article has provided numerous examples of where the legislature and courts have accepted and embraced the use of technology and the validity of e-signatures in concluding agreements and signing affidavits. Furthermore, it is noted that South Africa has followed international trends by recognising e-signatures and adopting the principles in the Model Laws. In addition, South Africa has provided an extra level of security for e-signatures by requiring advanced e-signatures in instances where a high level of security is required.

Generally, courts are hesitant to acknowledge and adapt to fast-paced changes and this should be understood in the context that courts adhere to established procedures in order to promote legal certainty and justice.[124] Fortunately, South Africa's legislature and courts have moved smoothly in recognising the evolution of communication systems and technology. Moreover, in addition to judicial endorsement of e-contracts and e-signing, courts are steadily accepting technology into traditional court processes, and this is evidenced by the introduction of Caselines in Gauteng and the movement by several judges to hold trials and other proceedings virtually as opposed to in court.[125] During the height of the coronavirus pandemic that broke out in early 2020, an urgent directive was issued by the Judge President of the Gauteng Provincial Division to the effect that all cases were to be issued via Caselines. The outbreak of the virus prompted the escalated use of Caselines and also ignited the use of technology in the law by engaging in the service of documents via emails and the use of e-signatures. In 2023, it seems that this electronic process is slowly becoming the norm as more and more businesses and attorneys are using e-signing in their work process.[126]

While there has been some hesitancy in business to use e-signatures, ECTA, together with court jurisprudence and other legislation, has created certainty as to the validity of e-signatures. E-signatures are becoming an important part of commerce; thus, it is necessary for these forms to be properly regulated. Accordingly, it is submitted that some minor amendments are required to promote the use of e-signatures, and to create greater clarity on certain aspects, *inter alia*:

- *An amendment to the Justices of the Peace and Commissioners of Oaths Act to allow for signing and commissioning of documents electronically*: this can be done by inserting the phrase "virtual" in

---

[124] *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD) par 2.

[125] Caselines is a digital platform introduced by the North and South Gauteng High Courts in early 2020. Caselines essentially seeks to serve as a paperless case management system for the courts wherein all court documents such as pleadings, notices and applications can be filed, uploaded and shared. See https://www.judiciary.org.za and https://sajustice.caselines.com.

[126] See ss 27 and 28 of ECTA, which provide that any public body that *inter alia* creates and accepts the filing and retention of documents may perform such filing in the form of data messages. This section effectively allows the courts to perform their functions electronically.

sections 1-3 to read thus: "a deponent shall sign the declaration in the '*virtual or physical presence'* of the commissioner of oaths." Otherwise, this can be done in the Regulations to the Act by confirming that affidavits can be commissioned electronically in the virtual presence of a commissioner. The Act is over 60 years old and the Act and Regulations need to be reviewed holistically.

- *An amendment to section 2(3) of the NCA by allowing certain credit agreements to be signed electronically anywhere*: this can be done by removing the requirement that the agreement must be signed in the physical presence of one another.
- *Allowing more accreditation providers for advanced electronic signatures*: currently, LawTrust and the Post Office are the only accreditation authorities in South Africa. An adoption of more accreditation authorities will greatly assist in promoting the use of electronic signatures in business and the legal sector.[127] Furthermore, the strict criteria and prohibitive costs of accreditation may need to be reviewed and relaxed. While it is conceded that strict regulations need to be in place to ensure the reliability of e-signatures, the challenges in obtaining accreditation defeats the aim of ECTA to enhance technology adoption in South Africa and bring us in line with international developments. Furthermore, the accreditation requirements for advanced e-signatures need to be reconsidered as such provisions violate the principle of technological neutrality and are not consistent with international standards, and potentially inhibit foreign trade.[128]
- *A reconsideration of the exclusions in section 4 of ECTA*: it is recommended that a review should be undertaken of the prohibition of e-signatures for long-term leases, transactions relating to immovable property, and wills and codicils. (Bills of exchange have become redundant in South Africa and therefore the exclusion of bills is not relevant). In this modern age, it will not be long before all documents will be signed electronically. It is submitted that, provided face-to-face and other identification mechanisms are confirmed, documents relating to immovable property and wills should be allowed to be signed electronically. Although, it is recognised that these transactions are susceptible to fraud, it is recommended that safety mechanisms can be put in place by requiring that these transactions be signed using advanced electronic signatures. Such measures will provide security to the transaction and contracting parties, and will further expedite the administrative processes for these transactions.
- *Finally, an update of the Uniform Rules of Court to allow for greater use of e-signatures*: there does not appear to be any express provision in the Uniform Rules that allows for the use of e-signatures. It is

---

127 See Van der Merwe *et al Information and Communications Technology Law* 128–130. Ss 28 and 37 provide for requirements for an "accreditation authority". It is submitted that the Minister of Communications should promote more private e-commerce service providers to be registered as accreditation authorities.

128 See Faria 2004 *South African Mercantile Law Journal* 529. South Africa's accreditation requirements are stricter than those of other states; other countries do not require the compulsory accreditation for the validity of e-signatures. This lack of uniformity could pose a hurdle during trade.

recommended that specific rules be implemented to promote the use and acceptance of e-signatures and other digital mechanisms during court process.

In light of technological developments, South Africa will hugely benefit from a review of the provisions relating to electronic signatures. In conclusion, it is trite that the digital revolution is moving fast. Technology is changing the face of the law, and the South African legal system cannot afford to stand still. Accordingly, it is submitted that provided the inclusion of technology is imputed correctly into the legal system, there should not be any prohibition against e-signing. It is clear that e-signatures are fully valid in law. Given rapid technological developments, it will not be long before pen and paper will be items of the past – indeed, an “(e) sign” of the times.