LAW SOCIETY
OF SOUTH AFRICA

Electronic Signatures for South African Law Firms

Guidelines: October 2014

Drafted for the
Law Society of South Africa
by Mark Heyink

Electronic Signatures for South African Law Firms

LSSA Guidelines

VERSION 1.0

MARK HEYINK

Attorney, Notary & Conveyancer
Specialising in Information Law

LAW SOCIETY OF SOUTH AFRICA

Electronic Signatures Guideline 2014

Foreword

Please read this foreword carefully.

This guideline has been compiled for the Law Society of South Africa primarily as a tool to assist attorneys in familiarising themselves with the understanding of electronic signatures.

This guideline is not intended and must not be construed as establishing any legal obligation. Neither is the guideline intended, nor must it be construed, as providing legal advice.

Signatures are intuitively understood by lawyers and lay persons alike. Their functions have become well established in commercial practice and it is extremely infrequently that, aside from questions of fraud, issues relating to signatures have to be decided upon in legal proceedings.

Electronic signatures and manuscript signatures differ considerably in form and manner of application. This Guideline addresses the difference in form between manuscript and electronic signatures and how in functions that are the equivalent of those inherent in manuscript signatures may be established by using electronic signatures properly.

Copyright

Chapter 1

1. INTRODUCTION

1.1 The use of signatures is ubiquitous and prevalent in our modern life in a myriad of ways. What is interesting is that in the author's lecturing on the subject, when attendees are asked how many times they may have signed their name during a particular day, almost without fail the answer is with reference only to manuscript signatures. This, despite the fact that many of them will have initiated tens and in some cases hundreds of electronic communications over the same period. In many very instances these communications will have been signed by the author or originator of the communication.

1.2 Signatures have been part of our written communications over thousands of years. As a consequence manuscript signatures are universally understood both in business and from a legal perspective and the need to define the meaning and functions of signature and its legal implications has been limited.

1.3 The advent of electronic communications, in which the use of manuscript signatures is redundant, has made it necessary to reconsider the nature and functions of electronic signatures in their various forms. In view of the considerable predominance of written communications being electronic and the importance of signatures in our communications, we need to re-examine how the functions of electronic signatures mirror the functions of manuscript signatures.

1.4 The author's experience is that there is widespread ignorance of the implications of use of electronic signatures, the different forms of electronic signatures and how they ensure the reliability of the signature itself and the integrity of electronic information signed by way of an electronic signature. Unfortunately, this ignorance is not confined to lay people and there are very few attorneys properly equipped to deal with the issues arising from the use of electronic signatures in their different forms.

1.5 This paper seeks to provide an understanding of:

- the function of signatures, whether manuscript or electronic;
- how electronic signatures in their different forms may provide "functional equivalence" (and are in certain cases superior) to manuscript signatures;
- how digital signatures work; and
- the evidential implications of the use of electronic signatures.

1.6 This Guideline also seeks to remove the confusion that has been created by the drafters of the Electronic Communications and Transactions Act ("the Act") in their failure to follow international principles defining electronic signatures and also to highlight the consequence of this failure. In doing so it is hoped that the Guideline will assist attorneys in understanding the very different approach taken by the drafters of the Act to the international principles and practices governing the use of electronic signatures.

1.7 Finally, this Guideline will deal with the importance of electronic signatures to members of the legal profession;

- in protecting the confidentiality of communications, as we are bound by the rules of our profession to do; and

- the profession's prospective dependency on information systems requiring the authentication of the identity of originators of communications (for instance eService and eFiling in our courts, e-Cadastre, electronic deeds registration systems and other electronic communications with government and private institutions where the signature of attorneys, conveyancers and notaries may be required).

1.8 It is stressed that in dealing with electronic signatures the issue of information security and how it applies to the use of electronic signatures is of fundamental importance. To that degree the Guideline on Information Security for South African Law Firms published by the LSSA is supplementary to this Guideline.

Chapter 2

2. THE FUNCTIONS OF SIGNATURE

The aim of this chapter is to assist the reader in understanding:

- The primary functions of a signature, which include evidencing the:
  - Identity of the signatory;
  - Intention of the signatory to sign; and
  - Adoption of the writing signed by the signatory.

Primary Function

2.1 Professor Chris Reed, the Head of the Information Technology Law Unit - Queen Mary & Westville College, London, in an article entitled "What is a Signature", identifies three primary functions of a signature recognised in commercial practice and in English law. Professor Reed concludes that English courts are prepared, at least in the case of hard copy documents, to accept signatures made in any manner that provide evidence of:

- The identity of the signatory;
- That the signatory intended a signature to be his or her signature; and
- That the writing or text to which the signature is associated is adopted or approved by the signatory.

2.2 It is submitted that the same principles apply to the use of manuscript signatures in South African law.

Secondary Function

2.3 In addition to the primary functions, Professor Reed also notes that there are secondary functions of signatures, which include the validation of some forms of administrative action and the protection of consumers. These issues are dealt with later.

The American Bar Association

2.4 The American Bar Association ("ABA") in its "Guideline to Digital Signatures" states:

> *"A signature is not part of the substance of a transaction but rather of its representation or form. Signing writings serve the following general purposes:*
>
> - **Evidence** – a signature authenticates a writing by identifying the signer with a signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer;
> - **Ceremony** – The act of signing a document calls to the signer's attention the legal significance of the signer's acts and thereby helps to prevent inconsiderate engagements.

- **Approval** – Approval, in certain contexts defined by law or custom by way of signature, expresses the signer's approval or authorisation of the writing, or the signer's intention that it has legal effect."

2.5 While the wording differs, what is immediately evident is that the functions contemplated by Professor Reed and the purposes stipulated in the ABAs "Digital Signature Guidelines" correlate closely. The issue of "identification" and "evidence" correlate with one another, the "intent of the signatory" and "ceremony" correlates with one another, and the issue of "adoption" and "approval" correlate with one another.

2.6 The ABA also identifies, as one of the purposes of signature, the function of "efficiency and logistics". It indicates that this function imparts a sense of clarity and finality to the transactions and may lessen the subsequent need to enquire beyond the face of the document. Professor Reed sees this as a secondary purpose which he describes as "a validation of an administrative action".

Uncitral Model Law on Electronic Signatures

2.7 The "Uncitral Model Law on Electronic Signatures Guide to Enactment 2001" ("the Uncitral Signature Guide") also deals with the function of signatures. It identifies the following functions traditionally performed by signature in a paper-based environment:

> *"… to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate the person with the content of the document."*

2.8 The Uncitral Signature Guide continues:

> *"It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed. For example a signature might attest to: the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing); the intent of a person to associate itself with the content of a document written by someone else; the fact that the time when a person had been at a given place."*

2.9 Again, in principle, there is no deviation from Professor Reed's hypothesis.

2.10 It is submitted that the same principles apply to signature in South African law.

Reliance on Signatures

2.11 Against this background a signature is evidence of the functions intended to be achieved by the signature. Essentially a signature will, on the face of it (sometimes supplemented by information associated with the signature), absent evidence to the contrary, be regarded by our courts as evidence that these functions were intended by the signatory.

2.12 Thus, if a purported signatory disputes that he or she is in fact the signer of a document and successfully provides evidence that the signature was not his or hers (the signature is a forgery), then clearly the "identity" function is not met and the elements of intent normally attributed to the signature would be absent.

2.13 In certain instances the signatory may admit that the signature was made by him or her but deny that the signature was intended as a signature (that it was merely an autograph), alternatively, deny that

the signature approves of or adopts the contents of the writing with which it is associated. In this instance, the nature of the writing will in many cases provide evidence extrinsic to the signature or supplementary thereto, which will assist the court in determining the signatory's intention.

2.14 We have developed practises which mitigate against a signatory disputing that the text or writing that him or her signed has been changed subsequent to signature. For instance, it is common practice if there are amendments in text, to initial pages of a document which has been signed to ensure that they cannot be replaced by different pages, and in some cases ruling through blank spaces to ensure that no further text can be added.

2.15 Some electronic signatures, typically known as digital signatures, can be applied to ensure that any change in the electronic text which has been signed cannot be altered. Any attempt to alter the text will be detected. To this extent digital signatures are superior to manuscript signatures in ensuring that the writing that is adopted or approved by the signatory can always be shown to have maintained its integrity. To this degree digital signatures more than meet the functional equivalence test. Digital signatures are dealt with in greater detail in Chapter 6 of this Guideline.

2.16 Thus, in determining what electronic signature would be appropriate for use in different circumstances, we can consider the functions that may be important in the application of the signature applicable to manuscript signatures. By applying the functional equivalence test, which is the foundation upon which the "Uncitral Model Law on Electronic Commerce" and "Unictral Model Law on Electronic Signatures" are based and, which were heavily relied upon in the drafting of the Electronic Communications and Transactions Act, we can determine what form of electronic signature would be appropriate in differing circumstances. The principal of "functional equivalence" is dealt with in greater detail in Chapter 4 of this Guideline.

Chapter 3

3. FORM OF SIGNATURE

The aim of this chapter is to assist the reader in understanding:

- That the form of a manuscript and an electronic signature are significantly different;
- That the difference in form between an electronic signature and a manuscript signature does not necessarily affect the function of the signature; and
- Requirements which entrench form may exclude the use of electronic signatures.

Manuscript Signatures

3.1 A manuscript signature is achieved by affixing a unique mark made by a signatory (which may or may not in itself identify the signatory) to physical media (typically paper).

3.2 In doing so the signature irrevocably changes the media by impregnating it with another substance (typically ink) and changing the structure of the media itself, for example impressing or breaking fibres on the paper.

3.3 Often the form of signature indicates the function and the reliance which we may place on the signature. In most instances extrinsic evidence which is a requirement of the "form" of the signature does not necessarily constitute part of the signature itself. For instance, it is a fact that many signatures do not, on the face of the signature, identify the signatory. In certain instances the signature is supplemented by the signatory's name (cheques are a good example) and possibly other information relating to the signatory. In instances where a person signs on behalf of a juristic person (by its nature a juristic person is unable to sign), the name of the juristic person would usually be indicated in a manner associated with the signature. In many instances, the fact that the signatory has signed in a representative capacity and has the authority to do so on behalf the juristic person, is also indicated.

3.4 These differing "forms" of signature incorporating evidence associated with and extrinsic to the signature are intended to enhance the evidential weight of the signature.

Examples

3.5 It may be helpful to demonstrate issues relating to "form" by way of examples that are common place in our use of signatures.

3.6 Typically we require that signatures be in ink to ensure that evidence of the signature is not easily removed. The fact that a signature may be in pencil does not detract from its legal efficacy, but the evidential weight that we place in a signature being persistent and ensuring that it cannot be easily erased or changed, underpins the requirement often insistent on, that a signature be in ink.

3.7 In certain instances signatures take on an additional evidentiary importance and legal requirements relating to the form of the signature have been established.

3.8 An example of the form of signature being dictated is the familiar attestation or commissioning of affidavits. Statutory rules are to be complied with in a proper attestation of an affidavit by a

commissioner of oaths. Typically to evidence that these rules have been followed, we provide additional wording associated with the commissioner's signature, which are intended to evidence that the oath or affirmation was properly administered. In addition we require that the full names and details as well as the address of a commission of oaths are also indicated and associated with the signature of the commissioner of oaths. This will also allow the commissioner to be called to give evidence if the affidavit is disputed.

3.9 A notary public is bound by similar regulation. Before admission a notary public of the High Court of South Africa has to satisfy certain regulatory requirements and qualify him or herself by passing an examination which tests the candidate's knowledge of notarial practice. Much of a notary's training is focused on providing the notary with a clear understanding of the evidentiary value that subsists in certifications or attestations which may be executed by the notary.

3.10 The trust which our courts place in the actions of notaries stems from the nature of the office and the fact that it can be reliable assumed that the practices required of the notary are faithfully and consistently applied.

3.11 The form that a notary public's signature takes is usually supplemented by risk management mechanisms intended to safeguard both the signature/s of the party/ies to the document as well as its text. This is because of the high levels of trust that we place on documents signed by or executed before a notary public. In this regard a seal or notarial impression may be used. The seal or the impression irrevocably change the nature of the paper in that they either impregnate the paper with ink, alternatively alter the paper by breaking the fibres so that the impression cannot be changed or removed.

3.12 In cases where the notary public may not place a seal or an impression on every page on voluminous documents, these documents may be bound and the notary public's seal applied in a manner which, if the binding were to be tampered with, would require the breaking of the seal. This would evidence that the integrity of the bundle of documents had been compromised.

3.13 Bodies of law have developed relating to the use of signatures where signatures and the text associated with signatures takes on specific legal significance. This is true in the case of negotiable instruments which rely heavily on the form of a signature placed on a negotiable instrument.

3.14 So too, our law requires a particular form to be followed in signing a Will. Every page of a Will must be signed in full by the testator or testatrix as well as the witnesses. In addition all of the parties must be present and actually witness the signatures of one another being applied. The reason for this form of signature is to establish an evidentiary risk management mechanism. As a Will is, by its nature, inchoate until the testator or testatrix die, it would not be possible for the testator or testatrix to give evidence as to their intention. Therefore this mechanism is intended to strengthen evidence that the testator or testatrix signed the Will and to ensure that there are witnesses who can at least testify to this fact.

3.15 Against this background and in particular the fact that our case law accepts that any mark, regardless of its functionality, will be regarded as a signature if the requisite intent is present, emphasises the purely evidentiary nature of signatures.

3.16 It is submitted that while they may be significantly different in form and application, appropriate electronic signatures, and particularly digital signatures, provide at least the equivalence in the function of manuscript signatures. Thomas J. Smedinghoff, in his book "Online Law", asserts that digital signatures of electronic information are capable of fulfilling all of the functional requirements of

manuscript signatures used on physical media. Digital signatures are dealt with in greater detail in Chapter 6 of this Guideline.

Exceptions in the ECT Act

3.17 In dealing with the sphere of application of the Act, Section 4(4) provides that the Act must not be construed as giving validity to any transactions mentioned in Schedule 2. The list in Schedule 2 is remarkably short and each of the exceptions is dealt with below.

3.18 **Alienation of Immovable Property.** The first exception is that of an agreement for the alienation of immovable property as provided for in the Alienation of Land Act 1981. In this instance it is submitted that the form of signature is no different to any other agreement and that the intention of the legislature in making this exclusion is based merely on the importance of transactions relating to immovable property and the relative value that these transactions typically have to the participants in the transaction. It is predicted that in time when our eCommerce economy matures the reality that electronic transactions properly signed using digital signatures are at least, if not more, secure than traditional agreements using manuscript signatures, will be recognised and this exception will be removed.

3.19 **Long Leases.** The next exception is that of long leases of immovable property in excess of twenty years. The same sentiments addressed above relating to agreements of immovable property apply.

3.20 **Wills and Codicils.** The regulation of signature of Wills has already been dealt with. It is clear that the functions of integrity of the text of the will and the certainty of the identity of the signatory can be achieved as effectively electronically as it can in manuscript form. Indeed, while not common place, “video wills” have been accepted by courts in other jurisdictions on the basis that they are accepted to be a reflection of the true intent of the testator or testatrix. In our digital age whether the electronic record is text or whether it is an image makes little difference to the electronic certification and encryption that can be applied to the record. Indeed, for many, being able to personally express themselves to their families by way of a digital record will be extremely attractive. In an indirect way, recognition of video remands, accepted by our Department of Justice, creates a precedent for the acceptance of video or digital records. As long as the function of the integrity of the record and the direct association of the record with the originator (the testator or testatrix) can be established there would appear to be no logical or legal reason why digital Wills should not be accepted in our law. I predict that in time the use of electronic technologies for the purposes of a Will, will become as commonplace as a written Will signed manually is today.

3.21 **Bills of Exchange.** The final exception relates to the Bills of Exchange Act. In this instance, as the law relating to bills of exchange is dependent to a large degree on paper artefacts and the form of signature being, as it is, extremely important, it is difficult to conceive how electronic signatures may be applied. In any event cheques, the most prevalent form of bills of exchange, are disappearing rapidly and banking institutions have developed electronic equivalents to the paper-counterparts governed by the Bills of Exchange Act. In this regard it is predicted that in time, probably sooner rather than later, Bills of Exchange, as we know them, will disappear and this Act will become redundant.

Chapter 4

4. FUNCTIONAL EQUIVALENCE

The aim of this Chapter is to assist the reader's understanding of:

- The Fact that manuscript signatures and electronic signatures, while different in form, can address the same functions; and
- The functional equivalence principle which defines the law governing electronic signatures.

Introduction

4.1 In chapters 2 and 3 of this guideline the functions of a signature were dealt with and the differences in the form of signature and the importance of these differences from a legal perspective were discussed. Having established that it is the function of a signature and not necessarily its form which is in most cases the determining factor as to its efficacy from a legal perspective, it is necessary to consider the principle of functional equivalence, which is fundamental to the Uncitral Model Laws on Electronic Signatures and Electronic Commerce, and on which the Electronic Communications and Transactions Act is based.

4.2 Again it is emphasised that the functions evidencing identity, the signatory's intent and adoption of the writing signed, do not have to be identical. In fact in many instances the functions inherent in electronic signatures, particularly in digital signatures, are significantly superior from both an evidentiary and a security perspective. However, where we use electronic signatures, the functions that we require the signature to perform must not fall short of what we require of manuscript signatures.

Uncitral Model Law on Electronic Signatures

4.3 In establishing the background on the functions of signatures and general remarks on electronic signatures the Uncitral Model Law on Electronic Signatures refers to the Uncitral Model Law on Electronic Commerce and the work that had been done relating to the functions of signatures in a commercial context.

4.4 In moving on to discuss digital signatures and other electronic signatures the Model Law on Electronic Signatures states:

> *"In discussing the desirability and feasibility of preparing the new Model Law and in defining the scope of uniform rules for electronic signatures, Uncitral has examined various electronic signature techniques currently being used or still under development. The common purpose of those techniques is to provide* ***functional equivalence*** *to-*
>
> *(a) handwritten signatures; and*
>
> *(b) other kinds of authentication mechanisms used in a paper based environment (eg. Seals or stamps)."*

Emphasis is added by the author.

American Bar Association Guideline to Digital Signatures

4.5 While not being based on the functional equivalence principle as expressly as is the case in the Model Laws, the American Bar Associations Guideline to Digital Signatures (published before the Model Laws) recognises the concept of functional equivalence. In the introduction to the Guidelines it is stated:

*"These guidelines seek to establish a safe harbour- a secure computer based **signature equivalent** – which will-*

(1) minimise the incidence of electronic forgeries,

(2) enable and foster the reliable authentication of documents in computer form,

(3) facilitate comments by means of computerised communications, and

(4) give legal effect to the general import of the technical standard for authentication of computerised messages."

Emphasis added by the author.

4.6 In the same way as we use manuscript signatures differently, in many cases consciously taking into account the nature and importance of the document signed and of the signature itself, so too are there many different variations of electronic signatures that may be appropriate in differing circumstances.

4.7 These distinctions are recognised in 13.3 of the ECT Act:

13(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if -

(a) a method is used to identify the person and to indicate the person's approval of the information communicated; and

*(b) **having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated."***

Emphasis added by the author.

4.8 From a business, legal and evidentiary perspective it is therefore necessary to understand the functionality provided by differing electronic signatures. For instance, does the electronic signature identify the signatory. If accountability and non-repudiation are an important function sought in the use of the signature it would be necessary that it can be established that the electronic signature fulfils this function. If the integrity of electronic information signed using the electronic signature is important, the function of being able to ensure that any change in the text is detectable and would be immediately evident would be an important consideration. If confidentiality of the information while communicated or stored is an important function, the ability to encrypt and decrypt messages using an electronic signature may come to the fore.

4.9 Electronic signatures, digital signatures and advanced electronic signatures are dealt with in greater detail in Chapters 5, 6 and 7 of this Guideline.

Chapter 5

5. ELECTRONIC SIGNATURES

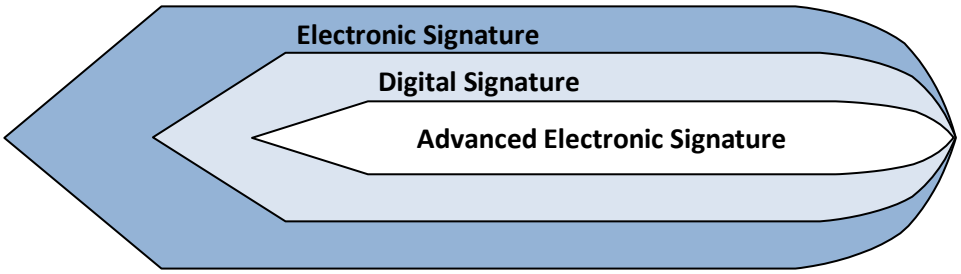
The aim of this Chapter is to assist the reader's understanding of:

- What the term "electronic signatures" embraces;
- How electronic signatures provide the functional equivalent of manuscript signatures; and
- Limitations on electronic signatures that are not digital signatures or advanced electronic signatures.

Introduction

5.1 As is the case with manuscript signatures, electronic signatures may fulfil the different functions we attribute to manuscript signatures, depending on the nature of the electronic signature.

5.2 The definition of "electronic signature" is all encompassing and includes digital signatures (not defined or mentioned in the ECT Act) and advanced electronic signatures. As the diagram immediately below illustrates, an electronic signature incorporates both digital signatures and advanced electronic signatures but may be neither of those. A digital signature is always an electronic signature but may not be an advanced electronic signature. An advanced electronic signature is always a digital signature and is by definition an electronic signature.



5.3 The further distinctions between digital signatures and advanced electronic signatures are dealt with in greater detail in Chapters 6 and 7 of this Guideline.

Electronic Signature

5.4 The ECT Act defines "electronic signature" as:

> *"electronic signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature;"*

5.5 The Uncitral Model Law on Electronic Signatures defines "electronic signature" a little differently:

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

5.6 While the Model Law emphasises the functions of signature, the intent of the two definitions is, in essence, the same and allows a simple electronic signature (without additional criteria associated with digital or advanced electronic signatures) to be used in the vast majority of the instances where records are now electronic and in which we would have used manuscript signatures were the same records on paper.

5.7 Based on the above definitions an electronic signature may not necessarily facilitate strong evidence of the identity of the signatory, the protection of the integrity of the text signed, or that it has been adopted by the signatory. Alternatively, they may have very stringent mechanisms linking the identity of the signatory to the signature, protecting the integrity of the text, and evidencing the adoption of the text by the signatory. Thus electronic signatures may lie anywhere along a continuum from the least reliable of electronic signatures to those that are regarded as the most reliable.

Identity

5.8 Manuscript signatures may, but do not necessarily, provide evidence of the identity of the signatory. In many instances evidence of the identity of a signatory is provided by supplementary writing immediately associated with the signature. For instance, in most agreements the name of the signatory is inserted adjacent to the signature provision, alternatively included in the agreement in such a way that the identity of the signatory is clear. Another example would be the fact that the names of signatories are clearly printed on cheques and, absent any arrangements to the contrary, only the named signatory may then sign the cheque.

5.9 In the vast majority of cases in electronic communications the typed name of the signatory constitutes the signature. In these instances the signatory's name is easily readable and the identity of the signatory is clear. In some cases the signature may just simply be by way of the initials of the persons, but typically the communication itself will also provide evidence of the identity of the signatory. For instance in eMail, the identity of the originator of the eMail is typically evident from the eMail address. Thus, for the most part, electronic signatures in this form (although they may have no security or possibly have limited forensic value) are superior to manuscript signatures and fulfil the functional equivalence test.

5.10 Nonetheless, in the same manner as our law recognises a mark intended to be a signature as a signature, so too with electronic signatures, something other than the person's name may be used and if it is intended to be used as a signatory would be a valid electronic signature. In these circumstances the deficiencies in identifying the signatory that exist with non-legible signatures may also be present with electronic signatures. Further, from a forensic perspective, the electronic signature would be less susceptible to providing proof that it is the signature of the purported signatory as would be the case with manuscript signatures, which could be subject to evaluation by handwriting experts.

5.11 The difficulties of evidence and proof described in the paragraph above do not however detract from the validity of electronic signature in this form. If it was intended by the signatory to be used as a signature it is the signatory's signature in our law. In the overwhelming majority of instances in electronic communication this form of signature is used and would be recognised by our law to be valid unless it is disputed.

5.12 It is also true that electronic signatures may have evidence and security which would not necessarily render the electronic signature a digital or advanced electronic signature, but nonetheless provide the type of reliability and integrity sought in terms of Section 15 of the Electronic Communications and Transactions Act in dealing with evidence. In assessing the weight of the evidence in legal proceedings a

court is obliged to take into account all relevant factors in determining whether the signature was valid or not.

5.13 Attention is also drawn to the rather common misconception that a manuscript signature which has been scanned and has been attached or placed in a document constitutes an electronic signature. The scanned image may well be an electronic signature, but the governing factor is whether the signatory intended that the scanned signature in fact be used as a signature. Absent this intention it cannot be regarded as the signatory's signature.

5.14 In digital signatures or advanced electronic signatures, typically the requirement of a Certification Authority will be that the full names of the signatory are contained in certificates issued by that Certification Authority. Again, in this regard electronic signatures in the form of digital or advanced electronic signatures are superior to manuscript signatures and fulfil the functional equivalent requirement upon the developing jurisprudence of electronic signatures is based.

Intent to Sign

5.15 As with manuscript signatures we have to rely on extrinsic evidence to determine whether the intent of the signatory is present. This evidence may be derived or inferred in many different ways, depending on the nature of the electronic communication or record. It may simply be the direct association with a signature and its immediacy to text or a part of text to which it is associated. In less formal communications the intent of the signatory may be more difficult to establish but in most formal communications, records or agreement this task is relatively easy and unless the application of the electronic signature (in the same manner as with a manuscript signature), is disputed it is submitted that there is little to choose between how we would infer the intent of a signatory using a manuscript signature or a signatory using an electronic signature.

Adoption of the Contents of Information Signed

5.16 As with the issue of intent, in most cases we would turn to extrinsic evidence to establish whether the information, whether in paper and text or electronic form, has been adopted, confirmed or agreed to by the signatory. Often this is relatively straight forward but disputes occur typically when a signatory disputes the content on the basis that it has been changed and is not the content intended to be signed.

5.17 In the paper and text environment we have developed measures to protect against unauthorised amendment. Among these are ruling through pages that are blank to prevent the addition of information and initialling each page to ensure that different pages may not be inserted. In addition, the mere physicality of the document and the relative ease with which amendments can be detected, provides an inherent protection.

5.18 In the electronic environment, where electronic signatures which do not incorporate the ability to "lock" or encrypt the information signed in a manner that any amendment would be detectable, the protections, based on the physicality of paper and text will not be present. Who and when an unauthorised amendment may have been made is very often difficult, if not impossible, to establish. In this regard the integrity of paper documents incorporating the physical protections that we have developed to prevent unauthorised amendment, are superior to those in the electronic environment.

5.19 The proposition of the superiority of manuscript signatures and the safeguards we employ in paper and text is however only true if electronic signatures do not provide safeguards, which are inherent in digital and advanced electronic signatures that can be used to protect the integrity of electronic

information. These functions allow a signatory to "lock" the content of an electronic communication or record, so that any change to the document of whatever nature will be detectable and caution the recipient of the communication, or a reader, that an amendment has been made and the document is not the same as the document signed by the signatory. This functionality is dealt with in Chapters 6 and 7 of this Guideline.

Conclusion

5.20 Thus, in the vast majority of cases electronic signatures can provide us with a functional equivalent of manuscript signatures and initials. In the same way that we have learned to protect important information and documents containing the information by the use of signatures and other mechanisms that the importance of the document may dictate requires protections, so do digital signatures and therefore advanced electronic signatures provide us with at least an equivalent to those functions and in most cases are significantly superior.

Chapter 6

6. DIGITAL SIGNATURES

This chapter seeks to assist the reader's understanding of:

- **Signatures that may be regarded as reliable;**
- **What constitutes a digital signature;**
- **The advantages of digital signatures; and**
- **The law relating to digital signatures.**

Introduction

6.1 While the Act does not specifically mention or refer to digital signatures, they constitute an extremely important feature of our electronic communications and transactions landscape.

6.2 In his authoritative book "Online Law" Thomas J. Smedinghoff states:

> *"Digital signatures are one of the most promising information security measures available to satisfy the legal and business requirements of authenticity, integrity, non-reputability and writing and signature. To meet these requirements, however, digital signature technology must be supported by certain institutional and legal infrastructures as well as other cryptographic measures."*

6.3 The author goes on to say:

> *"A digital signature is an electronic substitute for a manual signature and serves the same functions as a manual signature and more."*

6.4 Digital signatures have been viewed as of significant importance by the American Bar Association which has (as long ago as 1966) published a Digital Signature Guideline describing legal infrastructures for certification authorities and secure electronic commerce.

6.5 In doing so the approach adopted by the American Bar Association was markedly multi-disciplinary. In addition, submissions and contributions were also made by experts in other jurisdictions. The guideline remains a seminal description of both the commercial and legal implications of the use of digital signatures and the underlying institutional framework which promotes the reliability of digital signatures.

American Bar Association

6.6 The American Bar Association defines a digital signature in far more technical terms than Smedinghoff, as:

> *"A transformation of a message using an asymmetric crypto system and a hash function such that a person having the initial message and the signers public key can accurately determine:*
>
> *(1) Whether the transformation was created using the private key that corresponds to the signers public key; and*

(2) Whether the initial message has been altered since the transformation was made."

Uncitral Model Law on Electronic Signatures

6.7 The Uncitral Model Law on Electronic Signatures does not define "digital signature" but the guideline discusses digital signatures relying on public key cryptography in some depth and it is clear that digital signatures conforming to the standards and infrastructure which govern public key infrastructures will fulfil the criteria established in Article 6 of the Model Law and against which an electronic signature may be considered to be reliable.

6.8 It is clear that a digital signature falls within the definition of electronic signatures in the ECT Act and the Uncitral Model, a digital signature properly used within a PKI infrastructure fulfils all the functional requirements of a manuscript signature and is superior to a manuscript signature in several ways.

How Do Digital Signatures Work

6.9 Digital signatures are based on what is referred to as asymmetric encryption. Two keys (which are large numbers produced using a series of mathematical formulae applied to prime numbers) are created. The keys are such that algorithmic functions relate the keys to one another but, depending on the length of the keys, it is computationally infeasible for one key to be derived using the other key. It is believed that given the computing power available in the world, it would take more than one thousand years to derive one key from another where the keys comprise a key length of 2,048 bits.

6.10 The two keys are described as a public key and a private key. The public key is generally accessible to those persons wishing to authenticate the identity of a person using a private key, alternatively decrypt messages which have been encrypted using the private key. The private key on the other hand is accessible solely to the person to whom it is issued and is used for the signing of messages to allow the signatory's identity to be authenticated and to encrypt or lock messages which may be decrypted using the public key.

Hash Function

6.11 In addition to the key pair another process fundamental in creating and verifying digital signatures is a "hash function".

6.12 This is a mathematical process which compresses the electronic message into a message digest or "fingerprint" which is represented by a hash value.

6.13 The hash is significantly smaller than the message but is substantially unique to it and any change to the message invariably produces a different hash value. The different hash value allows the detection of any tampering with the original message. Even the insertion of a spacebar would change the hash value significantly and allow the parties to a message signed using mechanisms incorporating a hash function, to establish whether the integrity of the message has been compromised.

The Application of Digital Signatures

6.14 To enable the signature of an electronic message, the signatory first will delimit what parts of the message are to be signed. The hash function will then be applied to the message using a hash value. Software under the control of the signatory is then used to transform the hash value into a digital signature using the signatory's private key.

6.15 Typically the signature will form part of the electronic communication but it can be maintained and communicated separately. However, the signature cannot be operated in a manner which disassociates it from the message which is to be signed, as the message itself is used to create the hash function with which the signature is associated.

6.16 The diagrams below viewed in conjunction with paragraphs 6.9 to 6.15 will assist the reader in understanding how digital signatures work.

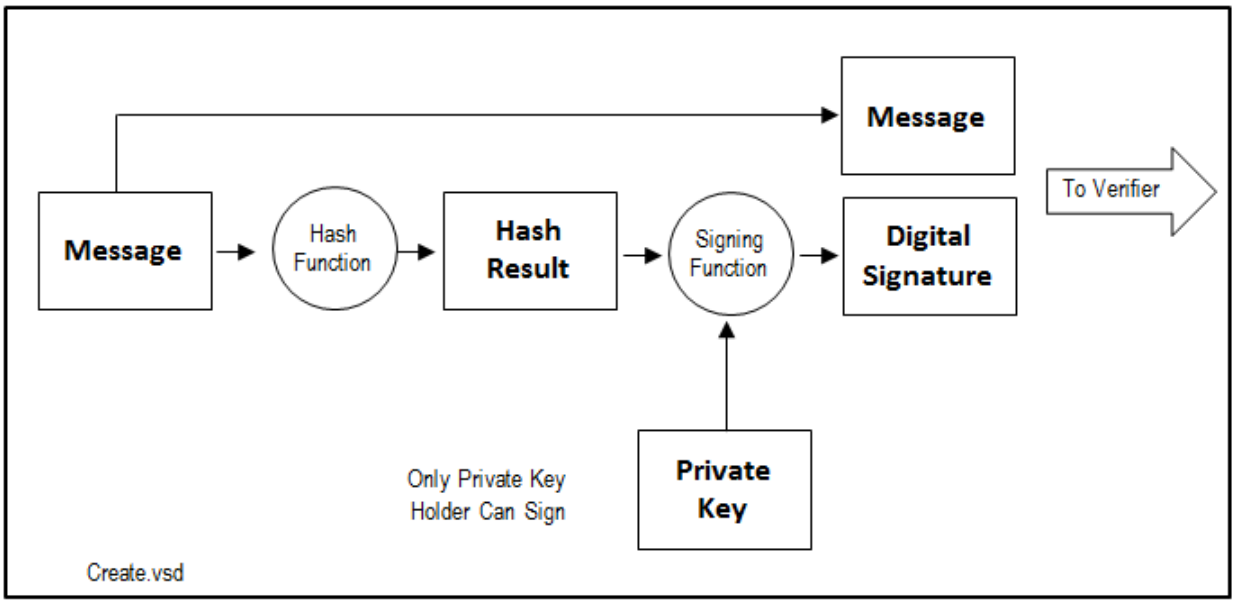


Figure 1 : Digital signature creation

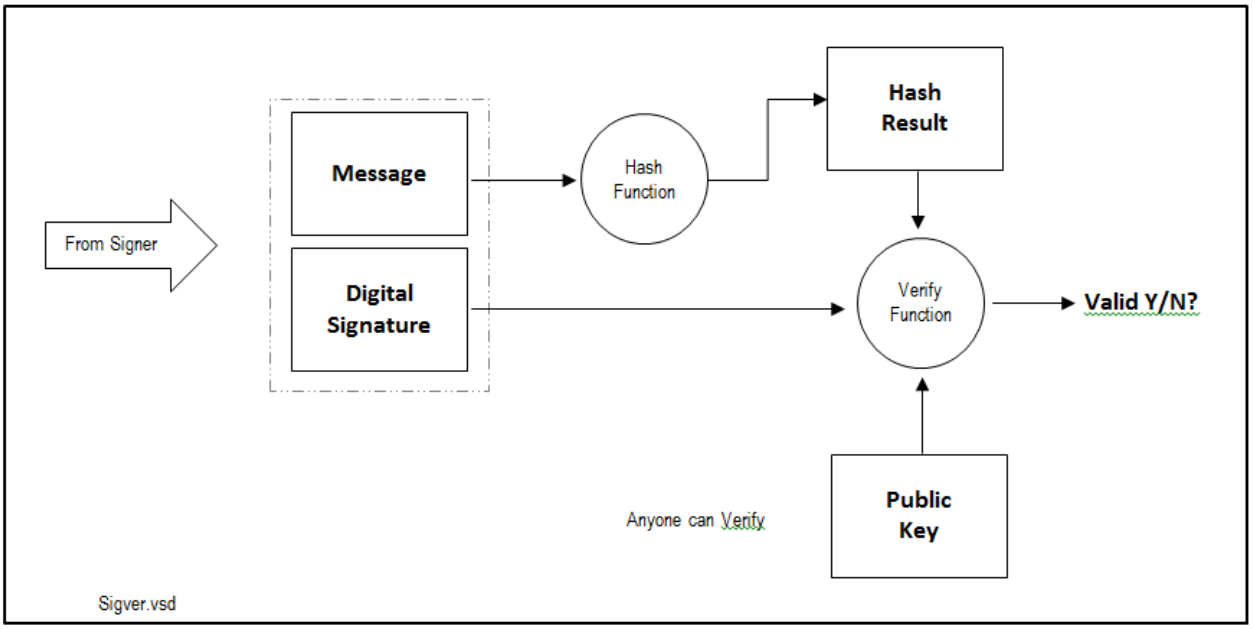


Figure 2 : Verification of a digital signature

Chapter 7

7. ADVANCED ELECTRONIC SIGNATURES

The aim of this chapter is to assist the reader's understanding of:

- **An advanced electronic signature as defined in the Act;**
- **The accreditation of products and services required for advanced electronic signatures; and**
- **Where advanced electronic signatures may/must be used.**

Introduction

7.1 An advanced electronic signature is a creature of statute, having been defined in the Act as follows:

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

7.2 In determining the criteria for accreditation, the accreditation regulations and the standards referred to in the Regulations have to be satisfied before accreditation can be granted. These standards are premised on the types of technologies and the policies and practices used in providing digital signatures.

7.3 Under the present law an advanced electronic signature cannot be anything but a digital signature. In the circumstances the provisions of Chapter 6 of this Guideline, describing digital signatures and their use, are relevant to understanding advanced electronic signatures.

Definitions

7.4 Three definitions are important in considering advanced electronic signatures. These are:

> *"**advanced electronic signature**" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37;*
>
> *"**authentication products or services**" means products or services designed to identify the holder of an electronic signature to other persons;*
>
> *"**authentication service provider**" means a person whose authentication products or services have been accredited by the Accreditation Authority under section 37 or recognised under section 40;*

7.5 In addition to the definitions quoted above Chapter VII of the ECT Act, entitled "Authentication Service Providers" requires that the Director General must act as the Accreditation Authority and employees of the Department (of Communications) as deputy accreditation authorities and officers.

7.6 Accreditation is defined in Chapter VI as the *"recognition of an authentication product or service by the Accreditation Authority"*.

Accreditation

7.7 The wording relating to accreditation is, with respect, confusing. It provides that the Accreditation Authority accredits the authentication products and services in support of electronic signatures. Neither the signatures themselves or the parties using the products and services to provide advanced electronic signatures are actually accredited.

7.8 The resolution of this confusion is not assisted by the Certificates of Accreditation granted to date by the South African Accreditation Authority to the only two providers of advanced electronic signatures accredited at the time of writing this Guideline, LawTrust Third Party (Pty) Limited and the South African Post Office. The relevant provision states:

> *"The authentication product/service used in support of an electronic signature is hereby accredited as an advanced electronic signature."*

7.9 The certificates of accreditation allow for the description of the authenticated products or service to be inserted, but in neither case has this been done.

7.10 Against this background the users of products or services in respect of which the certificates of accreditation have been granted have no idea from the Certificate of Accreditation what products and services have been accredited and whether they are in fact the products and services employed by the authentication service providers in providing advanced electronic signatures.

7.11 While the South African Accreditation Authority relies on the completion of audits by external experts, its failure to provide meaningful certificates that comply with the provisions of the Act betrays its lack of qualification and expertise in both the technologies necessary for advanced electronic signatures and as the body entrusted with accreditation.

7.12 Nonetheless, the fact remains that before accreditation is granted, applicants for accreditation are subject to strict auditing to ensure that they comply with the provisions of ISO21188-2006. In successfully satisfying the audit requirements, the applicants accredited will comply with the criteria and standards generally expected of the providers of reliable digital signatures. At least to this extent accreditation does provide strong assurance from both a commercial and a legal perspective of the reliability of the signatures issued by applicants certified by the accreditation authority.

Criteria for Accreditation

7.13 The Act, in dealing specifically with electronic signatures, in the provisions of Section 38(1), are critical in understanding the requirements of an advanced electronic signature.

> *"38(1) The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—*
>
> *(a) is uniquely linked to the user;*
>
> *(b) is capable of identifying that user;*
>
> *(c) is created using means that can be maintained under the sole control of that user; and*
>
> *(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;*

(e) is based on the face-to-face identification of the user."

7.14 It is to be noted that these provisions, save for sub-section 38(1)(e) are materially the same as those contemplated in Article 6 of the Uncitral Model Law, which defines reliable signatures and the provisions of Directive 1999/93/EC of the European Parliament in its definition of an advanced electronic signature.

7.15 The only difference is the addition in Section 13(1) the ECT Act of the words:

"(e) is based on face to face identification of the user."

7.16 The issue of face to face identification is dealt with later in this Chapter.

7.17 It appears that it is at this juncture that the drafters of the ECT Act regrettably misdirected themselves. In the context of both the Directive and the Uncitral Model Law, reliable signatures as contemplated in the Uncitral Model Law and advanced electronic signatures, as contemplated in the Directive, are the same.

7.18 The drafters perverted this intention and caused considerable confusion in failing to recognise the difference between an "advanced electronic signature" and a "qualified certificate" as contemplated in the Directive. A qualified certificate is defined in the Directive as a certificate which meets the requirements laid down in Annexures 1 and 2 of the Directive, which are quoted in their entirety later in this Chapter.

7.19 The requirements for qualified certificates are the requirements which are mirrored to a large degree in the criteria for accreditation provided for in the ECT Act, which accreditation allows for the provision of advanced electronic signatures.

7.20 Thus it is clear that it would have been far better for the drafters to have properly followed the intent of the Directive. This would have allowed the generally accepted understanding of advanced electronic signatures (or reliable signatures as they are sometimes referred to) have applied to our law. Qualified signatures, in terms of the Directive and a general understanding of electronic signatures in Europe and in the United States, are those which are accredited similarly to the accreditation provided for in the ECT Act by national institutions.

7.21 Even the wording "advanced electronic signatures", being applied, as it is in the ECT Act, only to those signatures which are accredited, is misleading. It implies that these signatures are better and more reliable than other signatures. This is simply not true and in fact both the providers of advanced electronic signatures who have been accredited in South Africa use exactly the same technology for digital signatures as they would for advanced electronic signatures. The only difference is the procedural criterion which requires for face-to-face identification with advanced electronic signatures and this may not be required (although in many instances would be followed) in verifying the identity of a subscriber for a digital signature.

Criteria for Qualified Certificates

7.22 The requirements relating to qualified certificates are set out in Annexes I and II to the Directive, which state:

"ANNEX I

Requirements for qualified certificates

Qualified certificates must contain:

(a) an indication that the certificate is issued as a qualified certificate;

(b) the identification of the certification-service-provider and the State in which it is established;

(c) the name of the signatory or a pseudonym, which shall be identified as such;

(d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;

(e) Signature-verification data which correspond to signature-creation data under the control of the signatory;

(f) An indication of the beginning and end of the period of validity of the certificate;

(g) The identity code of the certificate;

(h) The advanced electronic signature of the certification-service-provider issuing it;

(i) Limitations on the scope of use of the certificate, if applicable; and

(j) Limits on the value of transactions for which the certificate can be used, if applicable."

"ANNEX II

Requirements for certification-service-providers issuing qualified certificates

Certification-service-providers must:

(a) demonstrate the reliability necessary for providing certification services;

(b) ensure the operation of a prompt and secure directory and a secure and immediate revocation service;

(c) ensure that the date and time when a certificate is issued or revoked can be determined precisely;

(d) verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued;

(e) employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also apply administrative and management procedures which are adequate and correspond to recognised standards;

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

(h) maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance;

(i) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(j) not store or copy signature-creation data of the person to whom the certification-service-provider provided key management services;

(k) before entering into a contractual relationship with a person seeking a certificate to support his electronic signature inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third-parties relying on the certificate;

(l) use trustworthy systems to store certificates in a verifiable form so that:

- *only authorised persons can make entries and changes,*
- *information can be checked for authenticity,*
- *certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained, and*
- *any technical changes compromising these security requirements are apparent to the operator."*

Accreditation Regulations

7.23 The Accreditation Regulations published by the Department of Communications are not dealt with in any depth in this Guideline, but it is important to note the Public Key Infrastructure (PKI) framework addressed in the Accreditation Regulations. The Accreditation Regulations are replete with references to PKI standards, definitions, practices and policies, including requirement for compliance with SANS21188-1006. Therefore, without considerably rewording it seems impossible that Accreditation Regulations can cater for any other services or technologies, which are not digital signatures.

SANS21188-2006 (Public Key Infrastructure for Financial Services – Practices and Policy Framework)

7.24 This South African National Standard, which mirrors the international organisational standard ISO21188:2006, provides the detail of what is required for the public key infrastructures and against which an applicant will be audited prior to accreditation. As the name of this Standard implies, it is in fact a Public Key Infrastructure that providers of advanced electronic signatures have to comply with to achieve accreditation.

7.25 The Standard is onerous and compliance extremely costly. The result is that in many instances adherence to the Standard will provide South Africa with the most expensive "advanced electronic signatures" (or if you will, "qualified certificates") in the world.

7.26 While having strong Standards which govern the reliability of signatures may be desirable, unfortunately the misguided efforts and the Department of Communications will now see South Africa falling outside of generally accepted developments relating to electronic signature infrastructures and the manner in which reliability of electronic signatures, and in particular digital signatures, is judged.

7.27 The pity of this is that it defeats one of the primary objectives of the ECT Act, and that is to ensure that our law is harmonised with international development.

Face to Face Identification

7.28 The feature which distinguishes digital signatures or reliable signatures from advanced electronic signatures as defined in our law is the element of face to face authentication. Section 38(1) was initially drafted without this element. However, Parliament was persuaded by the South African Post Office (SAPO) to include the provision. The argument advanced at the time was that SAPO had a greater footprint than any other entity in South Africa and were therefore best able to deal with the authentication of identity of applicants and link the applicants to digital certificates inherent in digital certificates.

7.29 While perhaps the intention of SAPO was honourably, it is also demonstrably self-serving. Regrettably SAPO has proved unable to deliver on its promises and at the time of writing, some 11 years after the promulgation of the Act, the face to face identification, and the ability to obtain an advanced electronic signature from any post office in the Republic of South Africa, remains a pipe dream.

7.30 It also disqualifies from the realm of advanced electronic signatures other mechanisms of identification which may be as secure as face to face identification. The result is that in many instances where modern technologies allow for the positive identification of a potential user, these may (unless they can be shown to constitute a face to face identification) be excluded from electronic signatures capable of enjoying accreditation as advanced electronic signatures.

Review of the Law

7.31 It is submitted that our law will benefit from a review of the provisions relating to electronic signatures, and in particular advanced electronic signatures. The fact is that qualified signatures, the equivalent of what is intended by advanced electronic signatures in South Africa, failed in other jurisdictions and the recognition that governments will not control signatures (while they may require reliable signatures to be used by virtue of law) and that the market will determine the most suitable mechanisms of signature currently prevails.

7.32 If this is not addressed the danger exists that the unwary, using signatures which satisfy all of the functions of advanced electronic signature as defined in the Accreditation Regulations, may be disqualified from using alternative technologies.

7.33 Further, one of the most fundamental criteria in our modern world, and particularly in our modern commercial world, where dealings with all jurisdictions are required, is the harmonisation of our law. Our law of electronic signature as it stands does violence to generally accepted concepts of electronic signatures and advanced electronic signatures globally.

7.34 While not wishing to elaborate further on the failings of the ECT Act in this regard, it is believed that South Africa will benefit immeasurably from the review of the provisions relating to electronic signatures in the ECT Act, and a realignment to generally accepted international practice in this regard.

Chapter 8

8. THE IMPORTANCE OF ELECTRONIC SIGNATURES FOR ATTORNEYS IN SOUTH AFRICA

The aim of this chapter is to assist attorneys in:

- **Understanding the importance of electronic signatures in practice;**
- **The initiatives of the LSSA in the provision of advanced electronic signatures to attorneys;**
- **The importance of electronic signatures in the interaction with government departments; and**
- **How attorneys must commit themselves in embracing the use of electronic signatures.**

Introduction

8.1 There is little doubt that an attorney cannot function and complete his or her daily tasks without the use of signatures. Therefore, as we migrate from a paper and text environment to electronic environments, the necessity for understanding the implications of using electronic signatures and their functionality needs to be learnt until it becomes as intuitive as the use of manuscript signatures.

8.2 In our interaction with government institutions, the security provided by manuscript signatures and the way that manuscript signatures are required to be applied will be replaced by electronic signatures in the form at least of digital signatures and probably advanced electronic signatures. As this becomes an increasing reality, the need for the attorneys' profession to establish a Public Key Infrastructure framework facilitating the attorney's use of digital signatures and advanced electronic signatures, becomes more urgent.

8.3 It is also true that increasingly our clients will require the use of reliable signatures, ensuring the integrity and confidentiality of communications and records and authenticating the identity of the signatory.

The LSSA's Initiatives

8.4 The LSSA is currently investigating the establishment of a public key infrastructure facilitating the use of electronic signatures by attorneys. It has engaged with the only two service providers that have been accredited and are capable of providing advanced electronic signatures in South Africa at the time of writing. The reason is that under our law as it currently stands, advanced electronic signatures are required by law when dealing with the electronic communications and records which may in the future be used in our courts in legal proceedings. They will also be required in prospective eCadastre electronic registration systems which are being investigated by the Department of Land Affairs. So too will advanced electronic signatures be necessary to allow attorneys to communicate with the Master of the High Court once the development of electronic infrastructures and interfaces allow this.

8.5 However, the establishment of the proper use of advanced electronic signatures by attorneys will not happen overnight. An appropriate infrastructure must be developed to authenticate the identity and the credentials of an attorney acting in a particular capacity. For example an attorney may sign a

pleading but unless qualified as a conveyancer, it will not be competent for the same person to sign a deed being lodged in the Deeds Office. It is also important to highlight the attorney's duty of confidentiality and therefore the importance of ensuring confidentiality in electronic communications between attorneys and between attorneys and their clients. Without the provision of digital signatures within an appropriate Public Key Infrastructure this cannot happen.

8.6 In order to prepare properly for the facilitation of advanced electronic signatures in the future, pilot projects have been planned to enable an assessment of the advantages and potential difficulties of the use of advanced electronic signatures in electronic communication and information systems currently used by attorneys.

Laws and Rules

8.7 Currently laws, regulations and rules developed for use in paper and text environments may create barriers to the use of electronic signatures by attorneys. These too have to be considered and recommended amendments or alternatively parallel sets of rules considered and implemented to ensure that they are appropriate to the intended use of electronic communications and signature. This is one of the aims of pilot projects which are contemplated.

Registration Authority

8.8 From a perspective of advanced electronic signatures the face to face identification of attorneys needs to be carefully considered. Currently the Provincial Law Societies are custodians of databases relating to the information of attorneys, conveyancers and notaries public. It will be necessary to consolidate all of the databases into a single database for the purpose of providing information required in digital certificates which assure the identity of the signatory.

8.9 This will be investigated and dealt with in pilot projects contemplated by the LSSA.

Security

8.10 For many hundreds of years we have developed security measures around physical documents and manuscript signatures. The functional equivalent of these security measures have to be considered in moving into the electronic environment. This will place an obligation on attorneys to understand how to use signatures appropriately and the security measures that are essential to ensure that the functions that we commonly associate with manuscript signatures are inherent in electronic signatures.

8.11 Attorneys are urged to not only read the LSSA Guideline on Information Security, but to also learn and implement the control measures that are necessary to establish and maintain appropriate security in the electronic world of the information society.

Protection of Personal Information

8.12 The Protection of Personal Information Bill, once enacted, will be the first instance in our law that we are statutorily required to provide information security in providing the personal information of our clients. The use of electronic signatures (and associated encryption technologies) will significantly advance the security of our electronic communications and also the storage of information electronically.

Conclusion

8.13 As the world moves at an accelerated pace in its embrace of information and communications technologies, the importance of signatures in the life of an attorney will not diminish, it will simply change. The sooner attorneys both understand and begin to use electronic signatures correctly, the more likely they are to unlock the many advantages that electronic communications and information technologies hold for the profession.

Chapter 9

9. REFERENCES

To enable ease of reference to various documents in this regard, the following information is provided.

1. The ECT Act **http://www.info.gov.za/view/DownloadFileAction?id=68060**
2. Regulations published under the ECT Act **http://www.info.gov.za/view/DownloadFileAction?id=59987**
3. Uncitral Model Law on Electronic Signatures **http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf**
4. Uncitral Model Law on Electronic Commerce **http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf**
5. American Bar Association Guideline to Digital Signatures **http://apps.americanbar.org/favicon.ico**
6. European Union Directive on Electronic Signatures **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:EN:PDF**
7. SANS21188-2006 Standard (obtainable from Standards South Africa **Search results for: 'SANS 21188'** or eMail **sales@sabs.co.za** or **webstore@sabs.co.za**. Alternatively, telephone 012 428-6883/6128/6283 or the Call Centre at 0861 27 72 27)