THE DEVELOPMENT AND APPLICATION OF THE SIGNATURE AS AN IDENTIFICATION METHOD IN THE SOUTH AFRICAN LAW

by

MELANIE-JANE ROBINSON

submitted in partial fulfilment of the
requirements for the degree of

MAGISTER LEGUM

in the Faculty of Law
at
Vista University

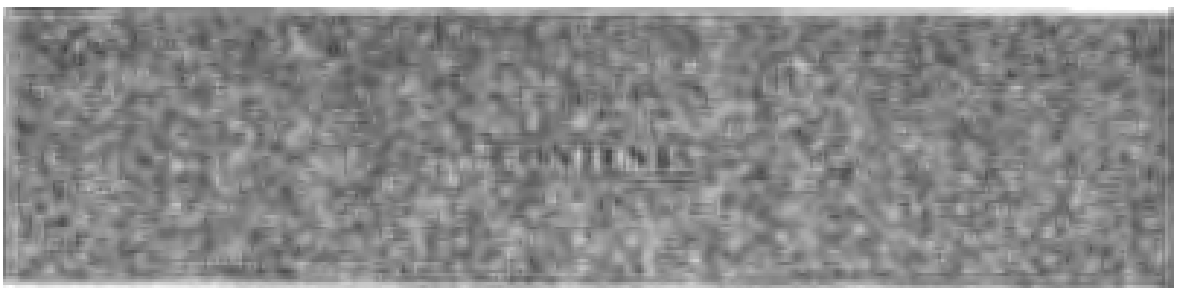
SUPERVISOR: **ADV.N BOHLER-MULLER**

1 July 2002

ACKNOWLEDGEMENTS

My heartfelt gratitude to the following without whom this research would never have occurred:

- My colleague, mentor and good friend, Professor Teresa Schwellnus for your invaluable input, guidance, help and encouragement.
- John, my partner, for your sacrifice, patience, loyal support and enthusiasm.
- My supervisor, Adv. Narnia Bohler-Muller, for your willingness, help and professional guidance.
- My parents, sister, Makulu and friends for your ongoing support, love and above all encouragement.
- The National Research Foundation (NRF, South Africa) for the financial assistance towards this research. Opinions expressed and conclusions arrived at, are those of myself, the author, and are not necessarily to be attributed to the National Research Foundation.
- UPE Research Committee for the financial help in the form of a Postgraduate Bursary, with special thanks to Mr R. Ncwadi.
- Mrs A Bohler, for your willingness to edit this dissertation upon such short notice.



SUMMARY

Whilst a signature is not a formality in our law in order for a valid and binding transaction to be concluded, it is invariably appended to identify the signatory, affirm the signatory's intention to append his/her signature and in so doing bind the signatory to the contents of the document.

South African law has rarely found it necessary to define what is meant by a signature, never legislating it but rather dealing with it on an *ad hoc* basis. New signature methods are dealt with analogously with the ways in which traditional manuscript signatures have previously been treated by our law.

Section A deals with the traditional manuscript signature with regards to the form it assumes as well as the functions it must fulfil. The uses of the traditional signature and its areas of application are identified. It is established that a signature does not have to be a signatory's name but can take the from of a mark, be it a seal, rubber stamp and so on, as long as it is made with the intention of signifying assent to the document. The traditional manuscript signature has played an extensive role in banking law and an extensive discussion is thus necessary.

As our society becomes less reliant on paper, businesses have been slow to embrace electronic commerce which in part is due to the perception that electronic commercial transactions are not secure. However, the increasingly widespread use of electronic communications demands a reassessment of what constitutes a valid signature.

Section B examines the forms of the electronic signature. An orientation of such forms is necessary to provide the reader with a general introduction into what constitutes an electronic signature before embarking on a lengthy discussion of each form, namely PINs and passwords, biometric identification and digital signatures.

PINs and passwords serve to identify and bind the signatory and are thus deemed to be electronic signatures. A heavier reliance is thus placed on the functions that they perform.

Biometric identification, as a form of electronic signature, refers to the automatic identification of an individual based on his/her physiological or behavioural traits, in an electronic environment. Biometrics is a recent technological advancement which is gaining more impetus daily. Each biometric technology is discussed, including fingerprinting, hand geometry and keystroke dynamics, as well as their performance as a technology and their respective applications. It is felt that these technologies have the ability to impinge on a person's basic fundamental rights. This latter constitutional aspect thus forms an integral part of the discussion and analysis.

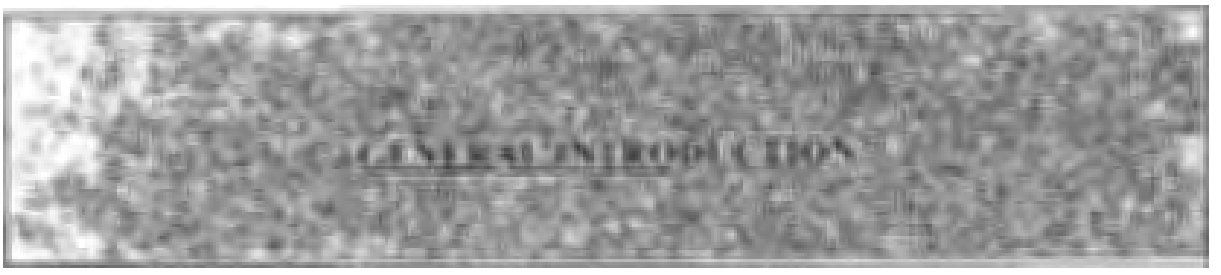
Digital signatures provide a secure means of concluding transactions over the Internet, while ensuring the integrity and authenticity of the information to which they correspond. It serves the same purpose as a traditional signature in that it allows the recipient of a digitally signed communication to determine whether the communication was changed after it was digitally signed. Thus the recipient knows the communication came from the sender albeit that it takes a different form. As it is also a relatively new technology, a detailed discussion is expedient and a multidisciplinary approach has to be adopted. The way in which a digital signature operates, as well as where it comes from (cryptography) is discussed to assist the reader in understanding the difficult technological concepts. The areas of application areas are extensively investigated as South Africa has no legislation regulating electronic commerce and thus has to rely on existing legislation. An investigation is made into how these laws (which relate to the physical world) can be used to regulate cyberspace.

Thus the development of the law relating to traditional manuscript signatures and other forms of signature, used for hard copy documents, is examined, tracing the move in judicial and legislative thinking from an approach that basically placed emphasis on *form* to one which is more reliant on the *function* which a signature performs.

Section C deals with an examination of electronic signature law as a vehicle for advancing electronic commerce, already applied in various foreign countries. Herein the viability of electronic commerce legislation in South Africa is explored, and the approach which should be adopted in South Africa in order to ensure that it does not stifle e-commerce is analysed. In March 2002, the South African legislature introduced the Electronic Communications and Transaction Bill of 2002, which attempts to regulate such issues. Mention is made of the Bill throughout this dissertation and it is foreseen that such reference is necessary as it is in all likelihood to be passed as legislation, despite contentious objections.

In this dissertation the conclusion is reached that a signature, as a legal concept, bears no relationship to the popular understanding of a name on paper in the signatory's own handwriting. A signature is not a 'thing', but a process. If that process produces sufficient evidence that a person has adopted a document as his/her own, and that document before the court is the same document to which the process was applied, then the document has been signed in legal terms. It is irrelevant whether the result of the process is a visible name, symbol, or a logical alteration of information content, as long as it provides sufficient evidence of the transaction.

ALL RESEARCH HEREIN HAS BEEN CONDUCTED UP TO AND INCLUDING 1 JULY 2002



1.1 GENERAL INTRODUCTION AND EXPOSITION OF THE PROBLEM

Signing a document is a fundamental legal act, so much so that every commercial document of any importance is signed. However, the signature as a legal artefact has received very little analytical attention in South Africa.

A signature may be examined on the basis of assessing whether or not the signature has the requisite *form*; and/or, by means of considering the *functions* which a signature must perform. The fundamental function of a signature amounts to evidencing three issues, namely: the signatory's identity, the signatory's intention to sign, and the signatory's adoption of the contents of the document so signed. Essentially, a signature amounts to no more than a method whereby assent to the contents of a document are confirmed by the signatory.

Traditionally, a signature has been applied using ink, or some alternative means of marking a document. A *signature* has never been clearly defined in South African law and, in circumstances where a new method of signing has arisen, the matter has been dealt with analogously and on an *ad hoc* basis such as when the courts consider signing by means of marks and rubber stamps.

The courts have recognized several other methods of appending a valid traditional signature, ranging from initials, to marks and seals, to the adoption of printed names and the use of rubber stamps, thereby endowing the word *signature* with a wide interpretation. A *signature* could thus refer to any mark placed on the document with the intention of *identifying* the signatory, as long as a direct link between the signatory and

his/her signature is established. Thus the courts have focused largely on the form of the signature.

The traditional (or manuscript) signature finds application in various legally relevant spheres in South Africa. Further, signature, as a concept, has been rendered diverse through the many definitions, or lack thereof, in the numerous fields in which it operates.

It is thus pertinent to examine and trace how the definition or form of a signature in its contemporary areas of application has been developed and interpreted, as well as to examine the functions of a traditional signature and its application in these various fields.

The re-orientation brought about by the introduction of computer-based technologies into the human experience has rendered reliance on paper cumbersome and expensive. Transactions have become largely paperless, providing no *corpus mechanicum* upon which the signature can be written and fixed. What is acceptable as a signature has changed to suit the means of doing business, which perforce takes into account advances in technology. Furthermore, modern global transactions have rendered the traditional signature impractical.

In consequence, a need has arisen for the development of a mechanism whereby businesses can transmit electronic messages which carry legally binding signatures that enable institutions and individuals to transact and enter into binding contracts entirely by electronic means. Technology has developed an electronic signature to provide for electronic transactions which effectively replaces/supplements the traditional signature.

Although the use of paper is being reduced, a signature is still needed, albeit electronic. Whatever the manner of affixing a *signature* to a document, it must achieve the core functions of *identifying and binding the signatory to the contents of the document* (be it stored electronically or in a physical form).

A reassessment of the concept of a *signature* is thus necessary since transactions have become largely paperless, thereby placing a heavier reliance on the function of the signature, rather than the form.

This research will critically examine the electronic signature technologies (such as PINs and passwords, biometric identification and digital signatures) and their capability of complying with the functional requirements in South African law, thereby establishing legally valid and legally enforceable signatures. An in-depth technology-orientated approach will be adopted as certain forms of the electronic signature are relatively new and require detailed explanation.

In South Africa, there is no existing legislation pertaining to electronic and traditional signatures. It is apparent that these new technologies have caused novel challenges and demands, and, for the development of the South African economy, adaptation was and is still required in several fields, specifically the law and its relation to these new technologies. Recently, however, there has been a move, internationally, toward the legal recognition of an electronic signature as a signature, in that there exists no apparent bar to this recognition on the basis of the *form* and *function* of this type of signature. Whatever mark (*form*) is used to indicate a signature, be it letters, characters, symbol[illegible] codes of an electronic record, they may be deemed a signature, provided they can be reliably linked to the signatory and, therefore, identify and bind that signatory to the contents of the document. A comparative approach in respect of the above is both necessary and expedient in order to ascertain whether South Africa should develop and extend existing laws or create new legislation pertaining to the aforegoing. Emphasis will be placed on the Electronic Communications and Transaction Bill of 2002 that was recently introduced by the South African legislature in an attempt to regulate electronic commerce.

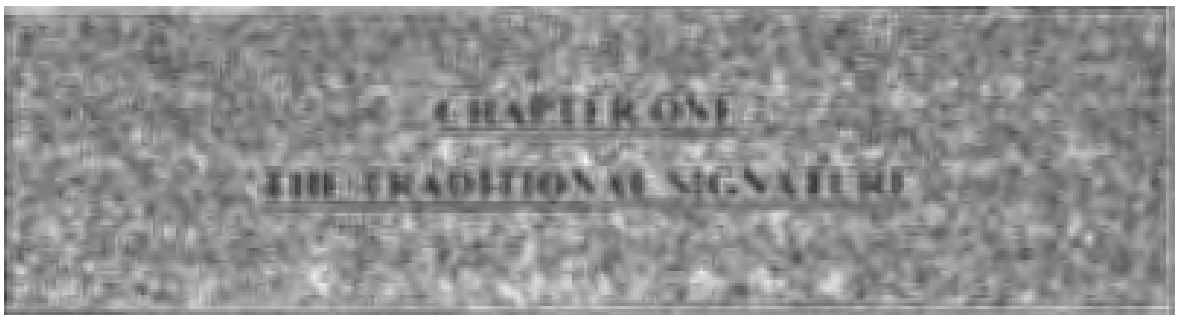
1.2 METHODOLOGY

The development and application of the signature in South Africa will be analysed as well as recent technological advances in this field. This dissertation contains three sections. Section A entails a full discussion of the traditional signature, identifying the functions it performs as well as the numerous forms that the traditional signature has assumed in its various areas of application, thereby extending/developing the concept *signature*. Section B amounts to a detailed discussion of the forms of the electronic signature and their respective applications, indicating the development that has taken place. In South Africa, there is no existing legislation pertaining to electronic commerce, specifically in respect of electronic signatures and, consequently, no formal definition of an electronic signature. Section C deals with various foreign legal systems that have implemented electronic signature legislation as well as the viability of such legislation in South African law.

An analytical multidisciplinary approach will be followed in this dissertation in that both legal and computer technological fields will be investigated. A comprehensive review of extensive existing literature will be the key methodological route. A comparative approach will be both necessary and expedient as they are yet to implement legislation in respect of the above in South Africa.

SECTION A

THE TRADITIONAL SIGNATURE



1.1 INTRODUCTION

The majority of legally and commercially significant documents require one or more signatures to be added to them for this significance to manifest itself. Consequently, a signature is a concept of fundamental legal importance, since signing a document is a fundamental legal act.[1]

Essentially, a signature amounts to no more than a method whereby assent to the contents of a document are confirmed by the signatory.[2] A traditional handwritten (or manuscript) signature is the most widely used and accepted method of identification[3] and authentication[4] for all transactions.[5]

---

1 Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

2 Mallesons Stephen Jaques Solicitors *The PenOp Signature: An Australian Legal Perspective* <http://www.biometrics.org> (1999-09-12).

3 Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm>(2000-08-17) defines identification as: "the association of data with a particular principal, where a principal is an identity having one or more distinguishing identifiers associated with it". Polemi holds that because transactions have become more complex, the original need for identification has moved from being social to economic. The first means of identification were names (surnames in particular) that were used in Britain in 1066. In 1300 passports were known to English law and in 1538 parish priests during the reign of Henry VIII kept registers of births, deaths and marriages for identification purposes.

4 Authentication is generally the process used to confirm the identity for a person or to prove the integrity of specific information - American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14).

5 Frazer Plastic and Electronic Money (1985) 156. Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 59 note that "the signature is still a relatively recent phenomenon – first legally recognized in France by the Ordannances de Moulins of 1566 and of Saint-Germain-en-Loye of 1667 ... being ... dependant on the generalization of alphabetization ...".

The manuscript signature supplies the required authentication in respect of paper documents.[6] Buys[7] notes that a paper document consists of four components, namely the sheet of paper, some physical representation of the information, information in respect of the issuer/originator, and the written signature to verify the authenticity of the aforegoing.

Reed[8] suggests that the law might test the validity and effectiveness of a signature in two ways: by assessing whether or not the signature has the requisite *form*; alternatively, by means of considering the *functions* which a signature must perform.

1.2 THE FORM OF THE SIGNATURE

A signature is not part of the substance of a transaction, but rather a representation or part of the form of a transaction.[9]

To date, there is no universally accepted definition of the concept *signature*. The word *signature* may mean a person's name or initials used in signing.[10] Poullet[11] defines a signature as "the manual writing by a specific individual of his name whereby he expresses his will to be bound by writing".

---

6 Smuts *A Survey of Information Authentication Techniques* (1994) 11 South African Computer Journal 84 84.

7 Buys (Ed) Cyberlaw@SA (2000) 131.

8 Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

9 American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14). Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 26 state that with the advent of electronic commerce (e-commerce), one of the fundamental requirements of securing online transactions is by way of an electronic signature, namely the digital signature, and submit that in the absence of South African Internet legislation, the law should have regard to the substance rather than the form of a signature.

10 Sykes (Ed) The Concise Oxford Dictionary of Current English (1984) 983.

11 Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 60.

However, the word *signature* has been given a wide interpretation.[12] A *signature* could thus refer to any mark placed on the instrument with the intention of identifying the signatory.[13]

The American Uniform Commercial Code (UCC)[14] defines *signed* as including "any symbol executed or adopted by a party with the present intention to authenticate a writing". It is thus evident that a signature can be used as a means of both *identification* and *authentication*. It not only identifies a specific individual but can also serve to authenticate a document by verifying the individual's identity, thereby preventing unauthorized use.[15]

In consequence, the traditional signature must establish a direct link between a person and their signature, hence the signature must express the signatory's will to be bound.[16]

1.3 THE FUNCTIONS OF THE SIGNATURE

A signature is deemed valid if it performs the functions that the law requires of it.[17] As mentioned above, a signature is a concept of fundamental importance in relation to legally binding transactions.

---

[12] Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 165; Malan and Pretorius Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law (1997) 99.

[13] Malan and Pretorius Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law (1997) 99.

[14] UCC art 1-201. For the corresponding position under South African law, see s 1 of the Wills Act 7 of 1953 (as amended), as well as *Ex Parte Singh* 1981 1 SA 793 (W), *Jhajbhai v The Master* 1971 2 SA 370 (D) and *Ex Parte Goldman and Kalmer* 1965 1 SA 464 (W) in paragraph 1.4.1.

[15] See Polemi *Review and Evaluation of Biometric Techniques for Identification and Authentication - Final Report* (summary) <http://www.cordis.lu/infosec/src/stud5fr.htm> (2000-08-17); Frazer Plastic and Electronic Money (1985) 156.

[16] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 60.

[17] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

In *Jurgens v Volkskas*,[18] Hoexter JA stated:

> " The function of a signature is to signify that the writing to which it pertains accords with the signatory. It conveys an attestation by the person signing of his approval and authority for what is contained in the document; and that it emanates from him."[19]

The manuscript signature on a signed writing serves the following general functions:

Firstly, the purported signature will be valid if it provides **evidence** of authentication of the document by the purported signatory.[20] A signature authenticates the writing by **identifying** the signer with the signed document. Poullet[21] opines that the signature authenticates both the physical presence of the (authoritative) signer as well as his/her will to be bound to the contents of the document. Therefore, when the signer makes a mark in a distinctive manner, that writing becomes attributable to the signer.[22] The identity of the signatory is the most crucial aspect to be evidenced by a signature, since where a document bears a traditional handwritten signature, it will suffice to adduce evidence of the purported signatory's normal signature and its similarity to the signature on the document. The signatory's intention to sign must also be evident from the signature employed, as well as the signatory's intention to authenticate and approve the document so signed.[23] Thus, signing one's signature "involves a mental element ... it is this that distinguishes it from the mere writing of the name".[24]

---

[18] 1993 1 SA 214 (AD).

[19] 1993 1 SA 214 (AD) 220E.

[20] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[21] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 62.

[22] Perillo *The Statute of Frauds in the light of the Functions and Dysfunctions of Form* 43 Fordham L.Rev. 39 48-64 (1974) as cited in American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14). A handwritten signature creates probative evidence in part because of the chemical properties of ink that make it adhere to paper, and because the handwriting style is unique to the signer.

[23] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[24] As per Slade LJ *Central Motors (Birmingham) Ltd v PA Wadsworth & Another (Trading as Pensagain)* (1982) 133 NLJ 555, Court of Appeal (Civil Division), as cited in Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

Secondly, the act of signing makes a signer aware of the legal significance of his/her act, thereby preventing inconsiderate engagements and holding that signatory liable for his/her transaction (the **ceremonial** function).[25]

Thirdly, where the law requires a party's signature,[26] that signature expresses the signer's **approval or authorization** of the writing, or the signer's intention that it has legal effect.[27]

And fourthly, a signature on a written document usually provides **clarity and finality** to the transaction, thereby lessening the need to inquire beyond the face of a document.[28]

Reed[29] suggests certain subsidiary functions of a signature, being the **validation of official action**, in that signatures are generally required for documents certifying or recording the decisions of judicial bodies, and **consumer protection**, specifically in respect of standard-form contracts, whereby the consumer's signature shows that the other party to the transaction has supplied the consumer with the required information, and the consumer has agreed to the terms of the standard-form contract.[30]

---

[25] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14). This "ceremonial" function also acts as a "cautionary" function.

[26] For example, a signature made on a written contract customarily indicates the signer's assent. A signature on the back of a cheque is customarily taken as an endorsement.

[27] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14).

[28] Perillo *The Statute of Frauds in the light of the Functions and Dysfunctions of Form* 43 Fordham L.Rev. 39 48-64 (1974) as cited in American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14) makes an analogy with the form of a legal transaction to minting of coins, which make their metal and weight content apparent without further examination. Clarity and finality provided by a form provides good evidence.

[29] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[30] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21) concludes that the secondary effect of a signature is manifest by means of its primary function as evidence of identity and agreement.

To facilitate the abovementioned general functions of a signature, the following attributes are apparent:[31]

i. signer authentication: a signature should identify the person who signed a document, and should be difficult for another to reproduce; and

ii. document authentication: a signature should indicate what is signed, making it impracticable to falsify or alter the signed matter or the signature without detection;[32] and

iii. affirmative act: affixing a signature should be an affirmative act which provides the ceremonial and approval functions of a signature and ensures that a legally consummated transaction is established; and

iv. efficiency: a signature and its creation and verification processes should provide assurance of the authenticity of both signatory and document, at minimum cost and resources.[33]

In consequence of the aforegoing, it is apparent that a signature should identify a person and associate that person with the content of the document, express the will to be identified *ex* the document (rendering the *animus signandi* of the signatory apparent), evidence the signatory's acceptance of liability, as well as perform a socially recognized ritual which is indicative of deliberation, commitment and resolve.[34]

---

[31] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14).

[32] A traditional (paper) signature identifies the document less than perfectly. Usually it appears below what is signed and the physical dimensions of the paper are relied upon to indicate alteration. However, these mechanisms are not sufficient to prevent difficult factual questions from arising.

[33] Digital signature technology apparently surpasses paper technology in all these attributes. See Section B: Chapter 3.

[34] Buys (Ed) Cyberlaw@SA (2000) 131; Mallesons Stephen Jaques Solicitors *The PenOp Signature: An Australian Legal Perspective* <http://www.biometrics.org> (1999-09-12); Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 62.

1.4 APPLICATIONS OF THE TRADITIONAL SIGNATURE

The traditional (or manuscript) signature finds application in various legally relevant spheres in South Africa. Further, signature, as a concept, has been rendered diverse through the many definitions, or lack thereof, in the numerous fields in which it operates.

It is thus pertinent to examine how the definition or form of a signature has been developed and interpreted, as well as to examine the functions of a traditional signature and its application in various fields.

1.4.1 THE LAW OF SUCCESSION

Previously the Wills Act[35] failed to give particular content to the words *sign* and *signature*, yet these two words appeared in practically every section. The Act, however, requires a will to be signed at the end thereof[36] and on every other page[37] by the testator, or by some other party in his presence and by his direction, which signature is to be made or acknowledged in the presence of two witnesses,[38] who must then also sign anywhere on the last page.

The permissibility of signing by means of a *mark* necessitated our courts[39] to distinguish between a mark and a signature. In the *Ex Parte Goldman and Kalmer*[40] case, the court examined this distinction and the word *signature* was afforded a wide meaning for this

---

35 Wills Act 7 of 1953.

36 Section 2 (1)(a)(i) of Act 7 of 1953.

37 Section 2 (1)(a)(v) of Act 7 of 1953.

38 Section 2 (1)(a)(ii) of Act 7 of 1953.

39 *Ex Parte Goldman and Kalmer* 1965 1 SA 464 (W).

40 *Ex Parte Goldman and Kalmer* 1965 1 SA 464 (W) 469.

purpose.[41] In the cases of *Ex Parte Singh*[42] and *Jhajbhai v The Master*,[43] the court reaffirmed the approach adopted in the *Goldman* case by applying the wide interpretation of *signature*; however, emphasizing the requisite *intention* of the testator in conjunction herewith to be present.

Opposed to this interpretation of the words *sign* and *signature*, the court in *Dempers and others v The Master and others*[44] and *Mellvill and Another NNO v The Master and Others*[45] applied the ordinary and popular interpretation, that is applying the common colloquial meaning. The conclusion in both cases was that initialing did not constitute a signature.

Section 1 of the Wills Act[46] was amended however so as to define a *signature* as follows:

> "'sign' includes the making of initials and, only in the case of a testator, the making of a mark, and 'signature' has a corresponding meaning."[47]

The legislature, in doing so, confirmed the application of the broad definition given to the concept *signature*.

Yet, immediately prior to this amendment, the court in *Harpur v Govindamall*[48] referred to the *Mellvill*[49] case with approval.

---

41 De Waal *et al* Law of Succession (1996) 46.

42 1981 1 SA 793 (W).

43 1971 2 SA 370 (D).

44 1977 4 SA 44 (SWA).

45 1984 3 SA 387 (C).

46 Act 7 of 1953.

47 Section 2 (c) of The Law of Succession Amendment Act 43 of 1992.

48 1993 4 SA 751 (A).

49 1984 3 SA 387 (C).

Only a testator may sign a will by means of a *mark*, such as a cross, thumbprint, rubber stamp or seal-ring impression. Where a testator signs by means of a mark, certain additional requirements are to be met.[50] In the case of *Goldman*,[51] the court construed the term *mark* in the narrow sense, while emphasizing the testator's intention to, in fact, write his/her name or initials. However, in consequence of the amendments effected by Act 43 of 1992, a mark should be something other than initialing.[52]

Hutchinson[53] believes that the term *signature* should be interpreted in the wide sense so as to include, among others, abbreviated signatures, incomplete signatures, fingerprint signatures, illegible signatures, stamped/typed signatures, signature affixed by seals, as well as signatures of nicknames, incorrect/misspelled names. Sonnekus[54] extends this to include video testimony, which appears to obviate the need for the traditional signature.

Hutchinson[55] notes further that whichever interpretation is applied, the fundamental fact remains that every signature consists of two essential elements, being *form* (the physical element) and *animus signandi* (the mental element) or the intention to sign. Consequently, according to Hutchinson,[56] "whatever form the signing takes, if it was not intended as a signature, it cannot be legally effective as such".

---

50 Section 2 (1)(a)(v) of Act 7 of 1953. If a will is signed by the testator by the making of a mark or by some other person in the presence and by the direction of the testator (which appears to sufficiently constitute a signature), a Commissioner of Oaths must certify that he/she has satisfied him/herself as to the identity of the testator and that the will so signed is the will of the testator and that each page of the will, excluding the page on which he appends his certificate, is also signed anywhere on the page.

51 1965 1 SA 464 (W).

52 De Waal *et al* Law of Succession (1996) 48.

53 Hutchinson *Signatures, Marks and the Wills Act of 1953* 1981 Acta Juridica 101 107-112.

54 Sonnekus *Videotestamente Naas Skriftelike Testamente* 1990 TSAR 114 114.

55 Hutchinson *Signatures, Marks and the Wills Act of 1953* 1981 Acta Juridica 101 107-112.

56 Hutchinson *Signatures, Marks and the Wills Act of 1953* 1981 Acta Juridica 101 102.

Consequently, the initial strict reliance upon the form of a testator's traditional manuscript signature as a means of identification was departed from so as to create an atmosphere facilitative of any acceptable mark (even by some other person in the testator's presence and by his/her direction), provided that such a mark is accompanied by the requisite intention, thereby promoting a development in form, as well as a heavier reliance on function.

Thus, the Amending Act[57] has shifted the bias to validate (rather than to invalidate) wills, and has given preferential emphasis to intention over form.

1.4.2 FOREIGN DOCUMENTS

The traditional signature plays an important role in the authentication of foreign documents. Rule 63(1) of the Supreme Court Rules[58] defines *authentication* as "when applied to a document, the verification of any signature thereon". Rule 63(2) states that the document is to bear the signature and seal of a diplomatic or consular official, or government official charged with the authentication of documents. Rule 63(2)(e) holds that, in respect of certain countries,[59] the signature or seal of a notary public ... ves to authenticate the document.

Thus, in terms of Supreme Court Rule 63, certain foreign documents will be deemed sufficiently authenticated for use within South Africa if they are authenticated by the signature and seal of either:

i. a relevant designated consular official; or
ii. a consular agent of the United Kingdom; or

---

[57] The Law of Succession Amendment Act 43 of 1992.

[58] The Supreme Court Act 59 of 1959.

[59] Namely the United Kingdom, Swaziland, Botswana, Lesotho, Northern Ireland and Zimbabwe.

iii. any government authority in a foreign place charged under the law of that nation with the authentication of documents; or

iv. any notary public, who is certified by a person referred to above as competent to authenticate documents; or

v. a notary public of the United Kingdom and Northern Ireland, Swaziland, Lesotho, Botswana or Zimbabwe; or

vi. a commissioned officer in the South African National Defence Force in respect of a document executed by any person on active service.[60]

Since South Africa's adoption of the Hague Convention's abolition of the requirement of diplomatic or consular legalisation of foreign public documents, which impacts on the requirements for executing public documents in one contracting nation for use in another contracting nation, another option has arisen by means of which a party may authenticate documents for use in another nation. A single formality is now required, namely the attaching of a certificate[61] by the designated official of the specific contracting nation to the document containing the signature to be authenticated, setting out the details of the signatory and of the designated official, and bearing the stamp or seal of his/her office.[62] Such South African designated officials include Magistrates, Registrars of the various High Courts, and any persons so designated by the Departments of Justice and of Foreign Affairs.[63]

The use of a certificate or counter-signature in respect of the above thus verifies the initial signatory's identity, as well as the requisite intention to be bound. However, the words "any signature" is not defined in the Supreme Court Rules, and this omission engenders uncertainty in respect of the form of a signature.

---

[60] Monaghan *Who Says the Signature's Genuine?* (1997) 5:2 Juta's Business Law 53 53.

[61] Which certificate must be placed on the document itself, be in the shape of a square with sides a minimum of nine centimeters long, and be clearly entitled "Apostille".

[62] Monaghan *Who Says the Signature's Genuine?* (1997) 5:2 Juta's Business Law 53 53.

[63] Sher *Authentication and Legalization of Foreign Documents* 1998 (May) De Rebus 30 31.

Thus, the signature's role in verifying the veracity of foreign documents, both in- and outside of South Africa, remains unaltered, despite contemporary methods of authenticating documents outside the parameters of the said Rules.

1.4.3 THE LAW OF CONTRACT

Kerr[64] notes that a

> "contract is formed when the parties who have the requisite intention and who comply with the requirements of the law agree together, or, in certain cases, appear to have the requisite intention and appear to agree together."

Thus, the intention of the parties is of fundamental importance, as the parties themselves, or their agents, establish the contractual legal bond. This has been apparent since Roman law times, as per Ulpian's[65] view that "(i)n stipulations and other contracts we always follow that which the parties intended".

This approach has been adopted by the South African courts, almost *verbatim*, as per Potgieter JA in the case of *Jonnes v Anglo-African Shipping Co*:[66]

> "In the interpretation of a contract the general rule is that the court should determine what the true intention of the parties was."

Kerr[67] further opines that the *intention of the parties* implies that there is a minimum of two parties to the contract, and that it is their agreement or, as Kerr[68] notes (quoting Pothier), their *concurrence of intention*. Consequently, a party is bound because, based on

---

[64] Kerr The Principles of the Law of Contract (1998) 41.

[65] D 50.17.34, as quoted in Kerr The Principles of the Law of Contract (1998) 3.

[66] *Jonnes v Anglo-African Shipping Co (1936) Ltd* 1972 2 SA 827 (A) 834D. See further *Collen v Rietfontein Engineering Works* 1948 1 SA 413 (A).

[67] Kerr The Principles of the Law of Contract (1998) 4.

[68] Pothier Obligations: A Treatise on the Law of Obligations or Contract par 4 as quoted in Kerr The Principles of the Law of Contract (1998) 4-5.

his/her intention, an offer made by this party has been accepted, or, in response to a question, this party makes a promise to another, which promise may be legally binding.

Thus, consensus is a prerequisite for the establishment of a contractual bond, which consensus necessitates communication between the parties, as set out by Mackeurtan, who was quoted with approval by Holmes JA in *Swart v Vosloo*:[69]

> "There must be an agreement of the minds of the parties, mutually communicated, with the intention of contracting ... in other words a *concursus animorum animo contrahendi.*"

Sharrock[70] further illustrates this point by stating that:

> "the law proceeds from the general premise that both parties must be of the same mind and intention before a contract will come into existence ... there must be a union of wills of the parties or ... the parties must have reached *consensus ad idem.*"

A few contracts[71] may be created without any indication of acceptance, whereas, generally, the acceptance of a contract must be manifested. The usual method of accepting a contract is by the use of spoken or written words.

In the case of *Goldblatt v Fremantle*,[72] Innes CJ held (in respect of oral contracts) that "any contract may be [orally] entered into; writing is not essential to contractual validity." Whereas where writing and/or signing are rendered prerequisites for a contract, either by the parties themselves or by legislation, then such prerequisites must be met for the contract to come into existence.[73]

---

[69] *Swart v Vosloo* 1965 1 SA 100 (A) 104H.

[70] Sharrock Business Transactions Law (1989) 50.

[71] Purely gratuitous contracts and others of no great significance.

[72] 1920 AD 123 128.

[73] Kerr The Principles of the Law of Contract (1998) 130.

Should it be required that the proposed contract be reduced to writing, it is generally intended that the express terms to be agreed to will be recorded in a written format, either in an unsigned document,[74] or recorded in writing and signed by the requisite signatories.[75]

The South African legislature has established *writing* as a requirement in various statutes[76] and, consequently, the legislature's intention must be ascertained, since the legislature intends divergent things in the various statutes, regardless of the fact that the wording used is similar. However, subtle differences in wording do not necessarily imply any difference in intention, as the requirements that a document be *signed* and that a document be *reduced to writing* both imply that the document must be *signed*.[77] Thus, generally, in terms of the South African law of contract, a written contract by necessary implication must be signed, thereby endowing the signature with evidentiary as well as identificatory relevance. However, *what amounts to a signature* requires qualification.

Sharrock[78] states that a party may sign by appending any mark of their choice. Thus it is not required that this party's surname be written in full, as initials, a cross, a rubber stamp of a company[79] or a thumb-print, which, together with the requisite intention to depict the name of the signatory, will satisfy the requirement of signing.

---

74 Such as a telex message.

75 Kerr The Principles of the Law of Contract (1998) 130.

76 Alienation of Land Act 68 of 1981, the Credit Agreements Act 75 of 1980, the Property Timesharing Control Act 75 of 1983, Formalities in Respect of Leases of Land Act 18 of 1969, the Rent Control Act 80 of 1976, Participation Bonds Act 65 of 1981, Security by Means of Moveable Property Act 57 of 1993, Copyright Act 98 of 1979 and Trade Marks Act 194 of 1993.

77 Kerr The Principles of the Law of Contract (1998) 130.

78 Sharrock Business Transactions Law (1989) 72.

79 Such rubber stamp must bear the name of the company; alternately, a party may append the name of the company and then sign their own name and indicate that they are signing as a representative of the company.

Kerr,[80] on the basis of South African case law, notes that:

> "a signature takes the form of a person's name, written by him on the document. But this ... is not the only way ... [as] ... [a]ny mark on a document made by a person for the purpose of attesting the document, or identifying it as his act is ... his signature thereto."[81]

In the case of *In re Trollip*,[82] De Villiers CJ noted that if a mark suffices as a signature, then *a fortiori* initials too suffice, and further "it is no more necessary to sign one's surname in full than it is to sign one's Christian names in full".

Kerr notes further that the appending of a thumb-print amounts to a signature, per Fleming DJP:[83]

> "(S)igning is achieved by making a mark or marks intended to represent the relevant person, if the making of the mark is done with the function of making the document an act of the writer, of signifying the assent of the party to that which is embodied in the document."

The signature must *prima facie* indicate that the signature refers to the document as a whole, thus it is not necessary for the signature to be appended at the end of the document, or on each page thereof. However, in practice, this has become customary. Yet, only once all material terms have been added may the document be signed. Should later additions or amendments be effected, then these necessitate further signing by the relevant parties.[84]

Where a place has been provided for the parties' signatures as a token of execution, then the signatures are to be appended there. It is not necessary to include the date and place of

---

[80] Kerr The Principles of the Law of Contract (1998) 95.

[81] Per Coleman AJ in *Putter v Provincial Insurance Co Ltd and Another* 1963 3 SA 145 (W) 148.

[82] *In re Trollip* (1895) 12 SC 243 246.

[83] *Chisnall and Chisnall v Sturgeon and Sturgeon* 1993 2 SA 642 (W) 645E-G.

[84] Sharrock Business Transactions Law (1989) 73.

signing, or have witnesses, but again practice has rendered these requirements customary for purposes of proof.[85]

The avoidance of liability on the basis of absence of consensus by a contracting party who has signed the relevant document enjoins the maxim *caveat subscriptor*, since by signing, the signatory established the reasonable impression of the intention to be bound by and to the terms contained therein. Further, the fact that it is apparent to the other contracting party that the signatory cannot or has not read the document which bears his/her signature, has led our courts to regard this other party as justified in assuming that the signatory is satisfied to be bound to the terms of the contract embodied in the document he/she has signed, whatever these may mean to him/her.[86]

In consequence, when one appends one's signature to a document, one is bound to the terms contained therein, since "(i)t is a sound principle of law that a man, when he signs a contract, is taken to be bound by the ordinary meaning and effect of the words which appear over his signature".[87]

Thus, the role of the signature in the South African law of contract is significant, as a signature, in addition to identifying the contracting party, also binds the signatory to the terms thereof. Yet, the law of contract neglects to define the *form* of the signature. However, the use of a mark[88] is not prohibited, and therefore it seems that the law of contract is as amenable to development, as far as the concept *signature* is concerned, as the aforegoing areas are.

---

[85] Sharrock Business Transactions Law (1989) 72.

[86] Sharrock Business Transactions Law (1989) 51-52.

[87] Kerr The Principles of the Law of Contract (1998) 97.

[88] The South African law of contract avoids imposing stringent prerequisites for the validity of a mark, as opposed to, for example, the Wills Act 7 of 1953.

1.4.4 THE LAW OF NEGOTIABLE INSTRUMENTS

In terms of Section 21 of the Bills of Exchange Act[89] no person will be liable[90] as drawer, acceptor or indorser of a bill if he has not signed it as such.

A negotiable instrument relies on formal requirements, including a signature, in order to be negotiated with "ease, rapidity, and minimal interruption".[91]

A negotiable instrument must thus be signed by the drawer or maker thereof. However, the Act fails to define a signature, nor does it prescribe any form of signature.[92]

Malan[93] suggests that a signature refers to *any mark*, be it a person's full name and surname, or initials and surname, or initials alone, or merely a mark, placed on the instrument with the intention of identifying the signatory.

---

89 Act 34 of 1964.

90 See also, for example, the UCC s3-401 (1990) (a person is not liable on an instrument unless the person signed it).

91 American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14).

92 The South African Law Commission Project 50: Investigation into the Payments System in South African Law (1994) 505 included various suggestions in respect of amendments to the Bills of Exchange Act 34 of 1964, including (under the heading *Signature as requirement for liability: s 34*) that a signature may be made in handwriting or typescript or by way of sealing, stamping, symbol, facsimile, perforation or other means.

93 Malan and Pretorius Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law (1997) 99.

Nicholas AJA held in *Harpur v Govindamall*,[94] that the words *sign*[95] and *signature*, (which the court deemed not to be technical or legal terms) must be given their ordinary, popular meaning, which, in ordinary and unqualified usage, means signature by name *or* mark.

This decision was echoed in *Navidas v Essop*,[96] where the court stated that a signature is undefined and may amount to any mark whereby the endorser signifies his/her willingness to be bound.[97]

In *Morton v Copeland*,[98] the court held that a signature does not necessarily mean writing a person's Christian and surname, but any mark which identifies it as the act of the party.

In the case of *Associated Engineers Co Ltd v Goldblatt*,[99] the court held that it was

> "prepared to accept that the official stamp of a company may be regarded as the equivalent of the company's signature, provided that such stamp was placed on the instrument by one acting with due authority and with intent to bind the company."

In *Goodman v J Eban Ltd*,[100] Evershed MK noted that one may sign by: "...impressing upon the document, one's name or 'signature' so as personally to authenticate the document".

---

94 1993 4 SA 751 (AD) 756-7.

95 Is derived from the Latin word *signum* (mark). Malan and Pretorius Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law (1997) 99 are of the opinion that it should be interpreted to mean the placing of a mark on the document identifying or representing the person signing.

96 1994 4 SA 141 (AD) 156.

97 See also *In re Trollip* (1895) 12 SC 243 246; *Goodman v J Eban Ltd* 1954 1 QB 550 (CA) 557; *Van Niekerk v Smit* 1952 3 SA 17 (T) 25.

98 (1855) 16 CB 517 535.

99 1938 WLD 139 142.

100 1954 1 QB 550 (CA) 557.

In terms of Section 95(1) of the Bills of Exchange Act, the authorized sealing with the seal of a corporation is sufficient and deemed to be equivalent to the signing or indorsement of any instrument or writing required by the Act to be signed, and Section 95 (2) of the Act endows a computer-printed signature of an authorized signatory, upon a warrant voucher or post office cheque, with the legal consequence of a signature.

Consequently, a *signature* means any mark – be it a person's full name and surname, or his/her initials and surname, or only his/her initials, or a stamp, or seal or other mechanical means to place his/her signature, whether as a facsimile or otherwise – placed on the instrument with the intention of *identifying* the signatory and *binding* him/her to the contents thereof.[101]

The law of negotiable instruments holds the concept *signature* as one of fundamental importance, in consequence of a signature's ability to perform three distinct functions,[102] in relation to those negotiable instruments regulated by the Bills of Exchange Act,[103] which distinct functions impact on validity, liability and negotiation. These functions are as follows:

i. Validity Function: Section 87(1)[104] states that, in respect of a promissory note, the unconditional written promise is to be signed by the maker. Thus, the signature of the maker[105] is a prerequisite for the creation of a **valid** promissory note.[106] As regards a bill of exchange or a cheque, which is defined as a particular kind of bill of exchange, the

---

[101] Malan and Pretorius Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law (1997) 99.

[102] Apart from and yet in addition to its basic function *vis-à-vis* identifying the signatory and expressing his/her intention to be bound.

[103] Act 34 of 1964.

[104] Act 34 of 1964.

[105] Alternatively, the signature of some other party by or under the maker's authority.

[106] Gering Handbook on the Law of Negotiable Instruments (1997) 35.

drawer must sign the unconditional order in writing.[107] Consequently, the signature of the drawer is required for the creation of a valid bill of exchange or valid cheque.[108] Thus, a signature is required for validity, as well as to confirm the identity of the signatory.

ii. Liability Function: Signature exists as but one of the requirements for incurring **liability** as a party to a valid cheque, promissory note or bill of exchange, and Section 21[109] states that no person is liable as drawer, acceptor or indorser of a bill of exchange if he/she has not signed as such. However, it is not necessary for a party to sign in his/her own name, since the signature may be that of another party who has the authority to so sign.[110] Should the signature be an assumed name, the signatory will be liable on the bill or promissory note as if he had signed his own name.[111] A signatory may limit personal liability by means of adding words to his signature, indicating that he signs for or on behalf of a principal, or in a representative capacity, should such signatory be endowed with the actual authority to so sign. The absence of such actual authority will render the signatory personally liable.[112] Hence, this function serves to identify the signatory, while also rendering the signing party liable.

iii. Negotiability Function: An instrument payable to order is **negotiated** by the indorsement of the holder completed by delivery, which indorsement is required to be written on the instrument, and signed by the indorser.[113] Thus, a promissory note payable to a named payee or his/her order requires the signature of that payee for it to function as a negotiation of the note to another party, which party would then be rendered the holder

---

[107] Section 2, read with s 1, of Act 34 of 1964.

[108] Gering Handbook on the Law of Negotiable Instruments (1997) 35.

[109] Act 34 of 1964.

[110] Section 95 (1) of Act 34 of 1964.

[111] Section 21 (a) of Act 34 of 1964.

[112] Section 24 (1), and the proviso thereto, of Act 34 of 1964; Gering Handbook on the Law of Negotiable Instruments (1997) 37.

[113] s 29 (3) and s 30 (1) of Act 34 of 1964.

of the instrument.[114] The payee's signature consequently performs functions in respect of negotiation, as well as in respect of liability, as the transfer of the instrument constitutes the transferee as the holder of the note, and the payee will be liable as the indorser of the note.[115] However, should the maker of a promissory note indorse the instrument, his/her signature as indorser will operate to render the instrument a valid promissory note (validity), the maker liable as indorser (liability), and the party to whom the maker indorses the note thereby becomes the holder thereof (negotiation).[116]

Thus, a signature on a bill can constitute the bill, guarantee its payment and effect its transfer.

Certain forms of negotiable instruments, for example, cheques and bills of exchange, are regarded as liquid documents. The holder of a **liquid document**, which entails a document signed by the debtor wherein he acknowledges his indebtedness in a fixed and determinate sum of money, may sue for provisional sentence, based on the defendant's signature on that liquid document. Nestadt J held in *Colee Investments v Papageorge*[117] that "the receipt of a liquid document is one of the few compensations which a creditor derives from his agreement to accept payment by cheque instead of in cash". Harms[118] states that the most frequently found documents in provisional sentence proceedings before our courts are cheques, bills of exchange, promissory notes, acknowledgements of debt and mortgage bonds. In such proceedings, it is presumed that the defendant had the capacity to incur liability, that the signature on the instrument was appended by the defendant with the intention of being rendered the drawer or indorser, that the instrument was delivered by the defendant with the intention of contracting on it and the debtor's undertaking is founded upon reasonable cause. The plaintiff is to prove that the

[114] Gering Handbook on the Law of Negotiable Instruments (1997) 36.

[115] Gering Handbook on the Law of Negotiable Instruments (1997) 37.

[116] Gering Handbook on the Law of Negotiable Instruments (1997) 37-38.

[117] 1985 3 SA 305 (W) 308I.

[118] Harms Civil Procedure in the Supreme Court (1995) Sections H2-H4.

instrument is valid *per se* and that the defendant (or his/her agent) signed the instrument.[119]

The plaintiff's attempt to obtain judgment in such a manner may be frustrated by the defendant successfully disputing an essential fact of the plaintiff's cause of action, or that an additional element of the cambial obligation is missing, or that he/she is not liable for some other reason. Specifically, the defendant may aver that he/she did not realise that what he/she was signing was a cheque, thus the defence of *non est factum*,[120] wherein the signature of a party whose mind fails to accompany that signature is rendered a nullity.[121]

It is apparent from the aforegoing that the signature plays a role in various negotiable instruments, which will now be expanded upon.

1.4.4.1 THE ROLE OF THE SIGNATURE IN CHEQUES

A cheque must, per its definition, comply with certain elements of form so as to qualify as a cheque for purposes of the Bills of Exchange Act.[122] A cheque is defined[123] as "an unconditional order in writing, addressed by one person to a banker, signed by the person giving it, requiring the banker to pay on demand, a sum certain in money, to a specified person or his order, or to bearer".

---

[119] Sharrock Business Transactions Law (1996) 346.

[120] This defence is distinct from *forgery* since the forger merely denies his signature, whereas with *non est factum*, the defendant admits his signature but denies that his intention was coupled with the signature. In addition, the onus is upon the plaintiff to prove that the defendant's signature is genuine.

[121] Sharrock Business Transactions Law (1996) 350.

[122] Act 34 of 1964.

[123] s 1 of Act 34 of 1964, read with s 2.

A signature by the drawer is thus essential for the creation and validity of a cheque, and only the signature of the drawer has such a constitutive function (*contra* the signature of the drawee, which may amount to acceptance).[124]

A cheque comprises four relationships. Firstly, the contractual relationship between the drawee bank and the drawer, or the bank-customer relationship,[125] in terms of which it is incumbent upon the bank to effect payment from available funds in the drawer's account. This is generally accepted to be based upon a mandate, and each individual cheque drawn amounts to a specific mandate, flowing from the general contract of mandate. Secondly, the contractual relationship between the collecting bank and the payee, in terms of which it is incumbent upon the bank to collect payment on the payee's behalf on the cheque deposited for collection. Thirdly, the underlying debtor-creditor relationship between the drawer and payee. Fourthly, the tripartite agreement among the relevant banks and the Automated Clearing Bureau (Pty) Ltd (the ACB), in terms of which the Bureau's automated cheque-clearing facilities clears cheques deposited with the banks for collection.[126]

Ideally, the authenticity of the signature on the cheque should be verified (in consequence of the ever-developing methods of fraud jeopardizing the form of the signature). This verification could be effected in various ways:

i. the cheque could be sent physically or electronically by the ACB to the drawee bank for inspection; or
ii. an image of the cheque can be created by means of specialized equipment, which image is transmitted to the main frame computer of the drawee bank

---

[124] Malan Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law (1997) 97.

[125] This relationship may simultaneously be viewed as a debtor-creditor relationship. which is generally accepted to be based upon a *mandate*, and each individual cheque drawn amounts to a specific mandate, flowing from the general contract of mandate. See further Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 48.

[126] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 27-28.

where the cheques are inspected (which is known as *digital-image processing*); or

iii. equipment designed for this particular function may be utilized to authenticate the signature on the cheque by means of reading the magnetic code on the cheque so as to verify technical correctness; or

iv. the establishment of a system whereby cheques up to a certain value need not be examined for authenticity (but here the collecting bank would still be required to verify the technical correctness of the cheque).[127]

Thus, the essential roles of the signature are to identify the signatory and render same liable *ex* the instrument; however, due to the prevalence of fraud, such signature must now be checked and verified utilizing the abovementioned techniques.

1.4.4.2 THE ROLE OF THE SIGNATURE IN CHEQUE CARDS

Payment may also be effected by a cheque card, where a signature is a condition of such a card. This card is, alone, without value as a credit or debit card. However, such a card is guaranteed by the drawee bank to secure payment up to a predetermined maximum amount at any branch of the issuing bank, or at the branches of certain specified other banks.[128] The undertaking to pay is usually subject to the following conditions: that the cheque is drawn in settlement of one transaction which must not exceed the stated limit; that the cheque is signed in the presence of the payee, and the drawer's signature corresponds with that on the card; that the cheque is dated before the expiry date on the card; and that the cheque appears to be complete and regular on the face of it.[129] In South Africa, cheque cards do not appear to be in use, but some banks' credit cards used in conjunction with their cheques serve the function of cheque cards. They serve to

---

[127] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 38-40.

[128] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 189.

[129] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 34-35.

guarantee payment on the cheque, which entails that the bank guarantees payment on the cheque and that payment on the cheque can thus not be countermanded.[130]

Consequently, the signature on a cheque card serves to identify the drawer by verifying the signature on the cheque, as well as to authenticate the transaction, while further providing a guarantee-function.

1.4.4.3 THE ROLE OF THE SIGNATURE IN TRAVELLERS' CHEQUES

Travellers' cheques are yet another method of effecting payment wherein a signature exists as a condition for the validity and completion of the instrument. However, no legal concept thereof exists with its own definition and legal consequences. Generally, a traveller's cheque consists of either an order to, or a promise by, the issuing institution, requiring this institution to pay the traveller or his/her order, which order or promise is usually qualified by the insertion of the words *when countersigned below with this signature.*[131]

In *S v Katsikaris*[132] the court felt that this phrase indicated that payment was to be made only if the countersignature was appended and it corresponded with the traveller's signature. Consequently, the instrument was rendered conditional as it relied on a countersignature for validity.

The majority of travellers' cheques are payable to a person or to their order, alternately to the traveller themselves or to their order. The traveller's name is to be signed in the payee's presence, which payee is to then compare the two signatures so as to confirm the traveller's identity.[133] Further, the traveller bears the risk if they append their

---

[130] Cowen & Gering The Law of Negotiable instruments in South Africa (1985) 270-271.

[131] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 50.

[132] 1980 3 SA 580 (A) 594F-G–595B-C.

[133] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 52; see Stassen *Legal nature of Travellers' cheques* (1978) 95 South African Law Journal 180 182-183.

countersignature before the instrument is lost or stolen. Thus, the countersignature serves as a method of identification, and it provides a measure of protection to both issuer and traveller.

Presently, all major banks have international banking accounts (*nostro accounts*) where the traveller's cheque is cleared electronically, which process negates these banks from presenting these instruments physically.[134] However, the traveller must cash the cheque at the paying institution, where the authenticity of the signature will be verified by the countersignature.

1.4.4.4 THE ROLE OF THE SIGNATURE IN POSTAL AND MONEY ORDERS

1.4.4.4.1 POSTAL ORDERS

The Post Office Act[135] defines a postal order as "a postal order issued under this Act or by any postal authority for payment under this Act".[136] Postal orders may be issued in South Africa for payment in any country as determined by the Postmaster-General.

The sender of a postal order is required to pay a specific sum to the Postmaster, plus the prescribed commission thereon, prior to a postal order being issued. The Postmaster then date-stamps the postal order, signifying the postal order's date of issue, which date is of significance as the Postmaster will not make payment on a postal order after three months

---

[134] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 53.

[135] Act 44 of 1958. The conditions pertaining to postal orders are contained n regulations promulgated in accordance with the enabling provisions in the Post Office Act 44 of 1958, that is, RK 608 in GN6429 of 29/04/1960 as amended by R2416 of 21/12/1973, R825 of 19/10/1979, and R1899 of 12/09/1980.

[136] De Beer *Die Effek van die Kruising van Poswissels met Besondere Verwysing na die Regsposisie van die Poskantoor* (1987) De Jure 285 288 is of the opinion that a postal order does not amount to either a bill of exchange, a promissory note nor is it a negotiable instrument.

from the last day of the month of issue. However, the issuer is required to inscribe the name of the payee upon the postal order prior to dispatching the same.[137]

For payment to be effected on an uncrossed postal order, the payee must enter his/her signature in the space provided upon the postal order, and then prove his/her identity or authority before he/she may claim payment on behalf of the stipulated payee. If a postal order is crossed, payment has to be effected through a bank. For payment to be effected on a postal order that is crossed generally, the drawee bank may not pay it to any person other than a banker. If it is a special crossing, then the banker on which it is drawn may not effect payment to any person other than the banker to whom it is crossed. However, the bank would also require a signature from the receiver for identification.

Should the payee be unable to sign, their mark is to be attested to by a witness before a post office official. In terms of Rule 12, the signature of the recipient is to correspond in all respects with the name on the postal order, but the Postmaster-General may consent to payment if convinced that the person who signed the postal order is the person whose signature appears on the order.[138]

The post office may refuse payment of a postal order should this order contain evidence of alterations or deletions, and if the order is not signed before a post office official, the post office official to whom the order is presented for payment may require it to be re-signed in his/her presence. If sufficient grounds exist indicating that the person claiming payment is in fact not entitled to payment then, despite all the formal requirements being complied with, the post office still has a discretion to refuse payment.[139]

---

[137] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 59.

[138] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 59.

[139] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 60.

The requirement that a signature be appended prior to effecting payment fails to serve as a pre-payment control measure, since no specimen signature is on record for purposes of comparison.

Hence, a duly authorized person may with relative ease sign the order to correspond with the name on the postal order, and, consequently, crossing the postal order fails to distance the payee from the institution of payment. Thus, the efficacy of payment is not affected should a bank collect payment of a postal order.[140]

A signature is thus a constitutive element of the postal order. However, its effectiveness is diminished as no confirmatory counter-signature is present to identify and verify the signatory. Consequently, a party's signature and proof of identity serve to obtain payment on the instrument, and as such, this system is open to abuse.

Further, it is evident that a mark may, in certain instances, amount to a signature, if attested to by a witness in the presence of a postal official; hence, it seems that this application is as amenable to development, as far as the concept *signature* is concerned, as the aforegoing areas are.

It is evident that heavier reliance is placed upon the function element of the signature since, even if the order is signed, the post office retains the discretion to refuse accepting the form of the signature should sufficient grounds exist indicating that the person is not entitled to payment.

[140] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 62.

1.4.4.4.2 MONEY ORDERS

A money order is similarly described in terms of the Post Office Act[141] as "money order issued under this Act or by any postal authority for payment under this Act".

The payee is to sign their name in the space provided therefor on the order, except should payment be effected through a bank. The payee must also prove his/her identity and/or authority before payment will be made to him/her. Should the payee be unable to sign, his/her mark is to be attested to by a witness before a post office official. The signature is to correspond in all respects with the name on the money order. Additionally, the claimant must provide the name of the sender.[142]

Rule 7 states that once all the aforegoing requirements have been met, payment will not be made if the official, on good cause, believes the person claiming payment on the money order is not actually entitled thereto. However, the Postmaster-General holds a discretion to consent to payment on the order allegedly signed by the payee, and may require this payee to sign again in his/her presence.[143] A money order that is damaged, spoilt, altered or indicative of deletions can be refused payment by the Postmaster.[144]

The dispatcher of a money order holds a discretion in respect of supplying the name of the payee, and, as the bank does not receive the advice, it cannot confirm the identity of the person claiming payment upon the money order. Consequently, the crossing of a money order impacts directly upon the sanctity thereof, and the opportunity for forgery

---

[141] Section 1 of Act 44 of 1958. As with a postal order, a money order also fails to amount to a bill of exchange, a promissory note, nor a negotiable instrument - Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 63. The conditions pertaining to money orders are also contaned in regulations promulgated in accordance with the enabling provisions in the Post Offcie Act, that is RK 609 in GN 29/04/1960.

[142] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 64.

[143] r 15.

[144] r 16.

and unauthorized signatures is expanded. Schwellnus[145] opines that the crossing of money orders should be eradicated, and the payment thereof statutorily confined to the post office.

As above, a signature amounts to a constitutive element of a money order, and proves to be more effective than a signature on a postal order, since the recipient thereof must know the name of the sender, as well as be able to sign the name indicated on the postal advice in order to identify and verify that signatory. All the particulars must coincide with those on the postal advice; however, this proves ineffective for banks, as they are not provided with the postal advice in the cases of crossed money orders.

The development of the concept *signature* to incorporate a mark, attested to by a witness in front of postal official, is accepted as a signature.

Greater reliance is placed upon the function element of the signature once again since, even if the instrument is signed, the post office retains the discretion to refuse accepting the form of the signature, should sufficient grounds exist indicating that the person is not entitled to payment.

[145] Schwellnus *Die effektiwiteit van die Handtekening as Identifikasiemiddel met Verwysing na Poswissels* (1992) Obiter 125 129.

1.4.4.5 THE ROLE OF THE SIGNATURE IN PAYMENT CARDS

The credit card and the debit card, and the variations thereof, are the most notable of the types of cards upon which payment may be made.[146]

1.4.4.5.1 CREDIT CARDS

Van Jaarsveld[147] broadly defines a credit card as

> "some document which, when produced to a relevant supplier, will constitute payment for purchases and thus enable the user to render himself liable to the issuer to reimburse him for all transactions entered into when using the card."

A credit card thus enables the holder thereof to acquire extended credit to a predetermined limit, and at a particular interest rate.[148]

A credit card will be either a charge card, or a bilateral credit card, or a trilateral credit card. A charge card's primary function is to facilitate payment, and involves no revolving credit, as the holder is generally required to settle his/her account monthly. A bilateral credit, or retail card, is issued by retailers for the exclusive use of their clients, and which identifies these clients as eligible for credit or services up to a certain limit. A trilateral credit card is issued by those institutions specialising in the issuing of these cards, where the holder may either be granted credit from date of purchase to date of account, or the holder may be entitled to elect whether to pay the entire outstanding balance in full or in installments at a prescribed rate of interest.[149]

---

[146] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 78.

[147] Van Jaarsveld *About Credit Cards and Liability* (XXXXI) 2 Codicillus 92 93, quoting Jones The Law Relating to Credit Cards (1989) 4.

[148] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 79.

[149] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 80-81.

The tripartite credit card encapsulates three distinct relationships. The first is that between the retailer/merchant and issuer, in terms of which a written agreement is concluded whereby goods and services are to rendered on the understanding that payment will be made to the retailer/merchant by the issuer. The second relationship exists between the issuer and the holder of the credit card, on the basis of which the use of the card is regulated by written agreement. The third relationship is between the retailer/merchant and the holder of the credit card, whereby (on the presumption that all the relevant requisite *essentialia* are present) a contractual relationship occurs as per the particular circumstances.[150]

A credit card amounts to a plastic card exhibiting the account holder's name, account number, expiry date and the name of the issuing institution. On the reverse of the card is a magnetic strip and a clear area wherein the cardholder is to sign his/her signature immediately upon receipt of the card from the issuing institution. The cardholder authorizes a transaction by signing a transaction slip/receipt. [151]

A credit card scheme necessitates a signature in three distinct instances: firstly, on the application form; secondly, on the reverse side of the credit card itself; and thirdly, on the credit card transaction slip. In the first instance, the signature binds the cardholder to the offer made to same by the card-issuing institution, thereby establishing a mandate. In the second instance, the reason for the requirement of a signature is unclear, as some authors suggest it serves as a precautionary measure to negate fraudulent use of the credit card, while others hold it serves an indentificatory role.[152] In the third instance, the majority of card-issuing institutions require a cardholder to sign a sales voucher when employing the credit card to effect payment. This is to render the cardholder liable in respect of the transaction, while simultaneously establishing a mechanism whereby the merchant may verify the signature on the card against that on the sales voucher, thereby ensuring that an

[150] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 82.

[151] Or by entering their secret personal identification number into the relevant technology provided.

[152] The latter view seems to be supported in practice, as merchants are responsible for verifying that the signature on the transaction slip is the same as that upon the credit card.

authorised party is using the credit card. It is thus used as an identification control mechanism, attempting to limit any potential damage. However, the efficiency of such is dependant on whether or not the cardholder has signed the reverse side of the credit card.[153]

The signature of the cardholder thus serves to protect the retailer/merchant who can verify the signature. Generally, the relationship referred to above between the cardholder and the issuing institution specifically elaborates as to signatures, especially as to whose signature will be accepted as a valid tender.[154] Added to this, the retailer/merchant must also confirm that the card has not expired, and that it does not appear on the list of invalidated credit cards. Once all these steps have been taken, the retailer/merchant is to complete a sales voucher in triplicate, exhibiting a summary of the transaction, the amount due, the name and account number of the cardholder and the retailer/merchant, and, lastly, the signature of the cardholder.[155]

1.4.4.5.2 DEBIT CARDS

A debit card operates in the same manner as a credit card, except that the account is to be maintained in credit, and this card may be used to draw cash, or purchase goods and services. A garage card is a particular type of debit card, presentable to retailers/merchants who display the appropriate garage card sign, generally garages and service stations. The cardholder's name and make and registration number of the motor vehicle may appear on the face of the card in embossed print. Each time the card is used in a transaction, and as per the cardholder's contract with the relevant issuing institution,

---

[153] Newman The Legal Implications of Credit Card Agreements in South Africa LLM Dissertation (1999) 51-53.

[154] Van Jaarsveld *About Credit Cards and Liability* (XXXXI) 2 Codicillus 92 94.

[155] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 83.

the cardholder is to sign a sales voucher, whereupon the issuing institution is authorized to debit the cardholder's account in favour of the retailer/merchant.[156]

The signature's role in respect of debit cards is the same as in credit cards above. However, according to the conditions of use of the debit card, the signature on the reverse of the card merely plays an identification role, as it must correspond with the signature on the transaction slip. The signature on the transaction slip is, however, used as an identification control mechanism, limiting potential damage, as payment can take place without it.

1.4.5 MISCELLANEOUS APPLICATIONS

A signature is capable of performing numerous other applications, according to the circumstances and/or the type of document signed. A signature may thus attest to the intention of the signatory to be contractually bound, or to indicate authorship, or to associate the signatory with the content of another's document,[157] or to certify copies of court records and thereby render these as admissible as evidence,[158] provided that such signature is appended to the document with the intention of establishing the identity of the signatory, and indicates his/her intention to be bound thereby.

[156] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 86-88.

[157] Buys (ed) Cyberlaw@SA (2000) 133.

[158] s 18 of the Supreme Court Act 59 of 1959.

1.5 CONCLUSION

The formal requirements for legal transactions, including the need for signatures, vary in different legal systems, as do the legal consequences of failure to cast the transaction in the required form. Although most legal systems have reduced formal requirements, sound practice still requires transactions to be formalised in such a way so that the parties are assured of validity and enforceability. Formalisation usually entails documenting the transaction on paper and signing/authenticating the paper.[159]

Whilst in South Africa a signature is generally not a required formality to establish a valid and binding contract, it is invariably appended to a document to identify the signatory, to affirm the signatory's intention to append their signature, and to indicate the adoption by the signatory of the contents of the document.

A general characteristic of the concept of a *signature* is the absence of a prescription in respect of the modality of signing. Initially, a traditional manuscript signature entailed personally signing one's name. However, due to differing circumstances (such as illiteracy), the various areas of application in law have accepted the wider interpretation of the concept *signature*, thereby facilitating the incorporation of divergent modes of signing. Thus, the courts have recognized methods ranging from initials to marks to seals to the adoption of printed names and the use of rubber stamps as valid traditional signatures.

Consequently, it seems that the form of a traditional signature should be a personal signature, that establishes a direct link between the signatory and his/her signature, thereby expressing the signatory's intention to be bound.

[159] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14).

The traditional signature, however, evinces certain critical inadequacies, such as susceptibility to forgery, as well as time and cost implications in respect of the visual comparison of the same.

A signature may thus be examined on the basis of its form, as well as the function that it performs. On the form basis, development has occurred per statute and case law to provide for the extension of the concept *signature* to encompass, for example, marks and seals. Yet, from the function aspect, the South African courts have tended to place more reliance on a signature fulfilling its functions. However, despite the immediately aforegoing, a signature must, at least, identify the signatory, and bind the signatory to the contents of the document.

SECTION B

THE ELECTRONIC SIGNATURE

1 ORIENTATION: FORMS OF THE ELECTRONIC SIGNATURE

In the previous chapter, it was discussed how a traditional signature may be applied and utilized to date, generally to document transactions on paper. Emphasis was on the form of the traditional signature which has extended and developed over time to include many more forms, besides the traditional manuscript signature.

However, the re-orientation brought about by the introduction of computer-based technologies into the human experience has rendered "reliance on paper cumbersome and expensive".[160] Transactions have become largely paperless, providing no *corpus mechanicum* upon which the signature can be written and fixed.[161] What is acceptable as a signature has changed to suit the means of doing business, which perforce takes into account advances in technology.[162] Thus, modern global mass transactions and trade have rendered the traditional signature impractical.[163]

Because of the aforementioned technological acceleration and consequent explosion in electronic commerce (or e-commerce), there is a demand for a new type of signature to effectively substitute the traditional signature. There is a need for the development of a mechanism whereby businesses may transmit electronic messages which carry legally binding signatures that enable institutions and individuals to transact and enter into binding contracts entirely by electronic means. The electronic signature ostensibly provides for this.

Although the use of paper is being reduced, a signature is still needed, albeit electronic. Whatever the manner of affixing a *signature* to a document, it must achieve the core

---

[160] Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 154.

[161] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 59.

[162] See Mallesons Stephen Jaques Solicitors *The PenOp Signature: An Australian Legal Perspective* <http://www.biometrics.org> (1999-09-12).

[163] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 60.

functions of *identifying and binding the signatory to the contents of the document* (be it stored electronically or in a physical form).[164]

It is apparent that these new technologies have caused novel challenges and demands, and, for the development of the South African economy, adaptation was and is still required in various fields, specifically the law and its relation to these new technologies.[165]

These modern computer and communications technologies have thus made it feasible, and in some cases essential, to employ methods of *signature* (such as an electronic signature) which differ from the traditional signature.[166]

Malan[167] notes that an electronic signature may exist in one of two forms: "it is either a personal identification number or code, often used in conjunction with a card, giving the user access to a system or computer; or a quality linked to a person, such as his fingerprint, retinal structure or voice ...".

Polemi[168] associates the signature with personal identification; that is, the association of a particular individual with an identity. Identification thus entails the determination and verification of an individual's identity. The goal of this is to protect a system against unauthorized use. To attain this goal, Polemi notes that personal identification is based on three premises: firstly, proof by knowledge (*knowledge-based personal identification*), such as passwords and PINs, where identity is based on what a person knows; secondly,

---

[164] See Mallesons Stephen Jaques Solicitors *The PenOp Signature: An Australian Legal Perspective* <http://www.biometrics.org> (1999-09-12).

[165] Visser *Banking in the Computer Age: The Allocation of Some of the Risks Arising from the Introduction of Automated Teller Machines* (1985) 102 South African Law Journal 646 646.

[166] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[167] Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 161.

[168] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm>(2000-08-17).

proof by possession (*token-based personal identification*), such as ATM and smart cards, where identity is based on possession of an object; and thirdly, proof by property (*proof by property personal identification*), such as fingerprints and retinal structures, where identity is measured by the human characteristics of an individual.

Smedinghoff and Bro[169] define an *electronic signature* in concise and generalized terms as:

> "a generic, technology-neutral term that refers to the universe of all of the various methods by which one can 'sign' an electronic record. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeros), they can take many forms and can be created by many different technologies. Examples of electronic signatures include: a name typed at the end of an e-mail message by the sender; a digitized image of a handwritten signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics); a secret code or PIN (such as that used with ATM cards and credit cards) to identify the sender to the recipient; a code or "handle" that the sender of a message uses to identify himself; a unique biometrics-based identifier, such as a fingerprint or a retinal scan; and a digital signature (created through the use of public key cryptography)."

It is apparent that a digital signature,[170] which involves the use of public-key cryptography, is also merely a form of an electronic signature.

The South African Electronic Communications and Transaction Bill[171] defines *electronic*[172] as a digital or other intangible form; and *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". [173] An *advanced electronic signature* (including a

[169] Smedinghoff & Bro *The Core Legislative Concern: Electronic and Digital Signatures* <http://www.profs.lp.findlaw.com/signatures/signature_2.html> (2000-12-20).

[170] Possibly the one type of electronic signature which has generated the most business, technical efforts and legislative responses.

[171] s 1 of the Electronic Communications and Transaction Bill of 2002.

[172] s 1 of the Electronic Communications and Transaction Bill of 2002.

[173] s 1 of the Electronic Communications and Transaction Bill of 2002.

digital signature) is defined as an " electronic signature which results from a process which has been accredited by the Authority ...".[174]

Section 13 of the Bill[175] notes that:

> "13. (1) Where the signature of a person is required by law, the 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 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.
> (4) Where an advanced 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.
> (5) Subsection (4) does not preclude any person from-
> *(a)* establishing the validity of an advanced electronic signature in any other way; or
> *(b)* adducing evidence of the non-validity of an advanced electronic signature."

It seems apparent that the Bill thus regards an electronic signature as a signature having legal force and effect, provided that the electronic signature is used by the signatory with the intention of creating a signature. Additionally, such a signature must identify the signatory, and indicate the signatory's assent.

Initially, an electronic signature was not deemed a signature that could be afforded the same legal status as a traditional signature, as it was construed to fall short of the expression of an individual's will to be bound by the writing, and, consequently, it was seen as merely conferring upon the user access to the system, without the defining of the resulting transactions. Also highlighted were further deviations from the traditional signature, such as the ability to make an exact copy of an electronic signature, the absence of criminal sanctions in respect of the forgery of an electronic signature, the possible absence of the element of personal creation by the signatory, and the capacity of a single individual to have multiple electronic signatures, as opposed to a single

[174] s 1 of the Electronic Communications and Transaction Bill of 2002.

[175] The Electronic Communications and Transaction Bill of 2002.

traditional signature. Further, the fraudulent use of an electronic signature may impugn liability to the card's owner or user, but this is not in consequence of the signature itself, but rather in consequence of the comprehensive agreements in respect of the card. Hence, it is not the signature itself that establishes liability, but the authorized use thereof. Yet, despite these reservations, it was believed that the term *electronic signature* could not be objected to, as the "access procedure that has succeeded has the same value as the (traditional) signature",[176] thus the word *signature* refers to both the means and the positive end. [177]

Recently, however, there has been a move toward the legal recognition of an electronic signature as a signature, in that there exists no apparent bar to this recognition on the basis of the *form* and *function* of this type of signature.

Whatever mark (*form*) is used to indicate a signature, be it letters, characters, symbols or codes of an electronic record, they may be deemed a signature, provided they can be reliably linked to the signatory and, therefore, identify and bind that signatory to the contents of the document.

Electronic signatures meet the law's *functional* requirements, but in a different way to that of the traditional signature. To establish the signatory's identity, both traditional and electronic signatures may rely on extrinsic evidence, and once identity has been established, the mere fact that the electronic signature has been affixed to the relevant document should raise the same presumptions as is the case for traditional signatures, that is the intention to sign, as well as to adopt the contents of the document. Yet, whereas the traditional signatory must be physically present when signing, electronic signatures may be signed by means of either: making a selection from a menu or clicking a button with the signature key that is stored on the signatory's computer; or by the application of

---

[176] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 63.

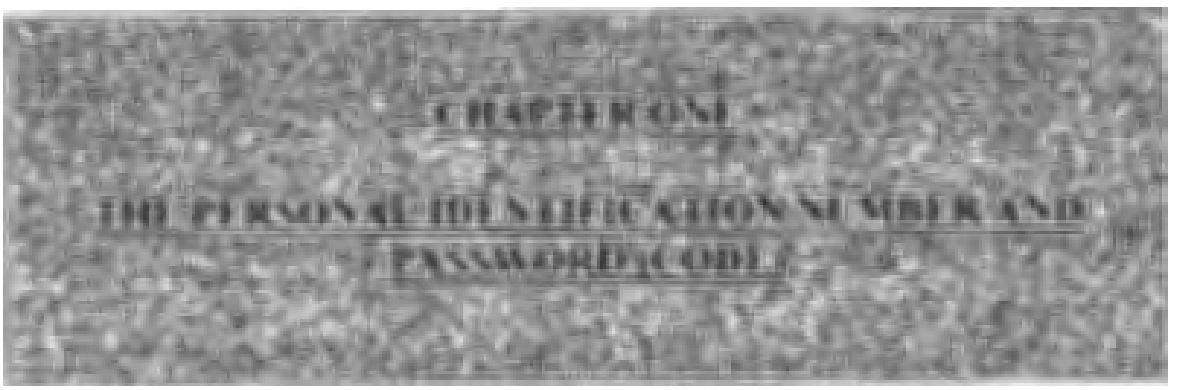
[177] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 62-65; Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 161-2.

signature software, wherein the signature key is located on a physical token which must be present before the said software can affix the signature.[178]

The aforegoing serves to elucidate that an electronic signature comprises any method of signing by electronic means wherein the affixation of a traditional signature upon paper is not a constituent element, as long as such electronic signature identifies the signatory and binds the same to the contents of the document.

In the following chapters, a detailed technologically-orientated approach will be adopted to consider the various forms which an electronic signature may assume, while noting the development in the field of the signature, and the signature's ability to be extended further *vis-à-vis* technology.

[178] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21); Anon *Is a Digital Signature Legal?* <http://www.salaw.co.za/library/digsigleg.htm> (2002-03-10).



1.1 INTRODUCTION

An electronic signature may exist as a personal identification number or a code (generally used in conjunction with a card which facilitates the user's access to a computerised system).[179] These personal identification methods may be token-based personal identification (this approach employs something physical which a person has to use to effect a personal identification, such as a smart card, credit card etc), and/or knowledge-based personal identification, which approach uses something known to the user to effect personal identification, such as a password or a personal identification number (PIN).[180]

1.2 PERSONAL IDENTIFICATION NUMBERS (PINS)

The implementation of electronic innovations, specifically the introduction of electronic transfer mechanisms, ushered in significant and far-reaching legal implications.

---

[179] Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 161.

[180] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm>(2000-08-17).

Electronic Funds Transfer (or EFT) has been defined by the US Electronic Funds Transfer Act of 1978[181] as follows:

> "The term 'electronic funds transfer' means any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorise a financial institution to debit or credit an account. Such term includes, but is not limited to, point-of-sale transfers, automatic teller machines, direct deposits or withdrawal of funds, and transfers initiated by telephone."

EFT is thus a generic term encompassing any transfer of funds in which electronic methods replace one or more steps in the process previously incorporating paper-based techniques.[182] EFT is distinct in that even the tangible system of value is done away with, specifically traditional commercial paper, and, by necessary implication, the traditional manuscript signature.[183]

EFT in its most popular form is the automated teller machines (ATM's), which has by its introduction, delivered manifold benefits[184] to both the various banking institutions as well as to their clients. The ATM is accessed by means of inserting a plastic card and then entering that card's personal identification number (PIN), whereupon the required balance enquiry, fund transfer, withdrawal or deposit is completed.[185]

Banks employ one of two possible approaches for the creation of the individual PIN. The first is that the PIN is generated by the bank with software that utilizes an algorithm together with certain data specific to the customer, resulting in either a four or six digit PIN, which is then delivered to the customer, and thereby eliminates the possibility of the

---

[181] Act 15 USC 1693.

[182] Including ATM's, the transfer of funds at point of sale, direct deposit/withdrawal of funds and transfers initiated per telephone.

[183] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 200.

[184] Banking services are ostensibly available 24 hours a day, 7 days per week, and the banks have been able to offer decreased transaction costs and reduce their paper consumption, as well as employ fewer tellers.

[185] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 198; Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 115.

bank's employees having sight of the PIN. The alternative approach is to allow the customer to select their own PIN, and this is usually based on some personally relevant sequence of numbers, or on an easily memorized sequence, for example 4321, or 123456. However, as this number is not generated by the bank, it must be logged against the customer's file, and is thus susceptible to anyone having access to this customer's file.[186]

Such a computerised banking system may be either on-line or off-line. In the off-line system, each transaction is recorded onto a tape, which tape is then delivered on a daily basis per courier to the financial institution for processing. Here the machine decrypts an encrypted version of the PIN from the magnetic stripe. The on-line system enables the financial institution to process transactions immediately. In this instance, the system verifies the PIN inserted by the customer by comparing it with the customer's PIN in the computer's master file. An algorithm is performed on a combination of the cardholder number and the PIN and the result is then compared with some predetermined value and if the result is correct, the cardholder is accepted as an authorized user. Usually, the customer is given three attempts to enter the PIN, upon failure whereof the machine will retain the card.[187]

The following seven steps are involved in a typical ATM transaction:

i. a plastic card is inserted into the ATM;

ii. a PIN specific to that card is entered into the ATM, providing the customer with access to their bank account;

iii. the ATM provides the customer with various options in respect of dealing with their account;

iv. the customer selects a specific option from those available;

v. the ATM may then request specific details pertaining to the transaction, which the customer then enters;

---

[186] Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 117.

[187] Arora Electronic Banking and the Law (1988) 113; Reed *Electronic Finance Law* (1991) 62; Schwellnus Die Aard en Rol van die Handtekening as Betalingsmagtiging LLM Dissertation (1991) 113; Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 107.

vi. the ATM displays the details requested, as well as a prompt for the customer to confirm the details and the selected option, whereupon the customer duly confirms by instructing the ATM to proceed;

vii. the ATM completes the transaction.[188]

The use of the traditional signature as a means of identification has thus largely been replaced by the PIN/card combination. To provide security against unauthorized withdrawals from an ATM, the customer is required to present an account card, and enter the card-/account-specific PIN, so as to gain access to the account through the ATM. However, despite this high-level of security, unauthorized access is still a real and ever-present threat to account integrity. A third party may acquire the legitimate card-owner's card and PIN, or the relevant bank's computer network may be accessed either on-line or off-line by unauthorized third parties, be they computer/electronic experts or the bank's employees. Thus, a need exists for an upgrade in ATM security, which presents itself as a system of user-authentication based upon unique personal characteristics.[189]

Electronic funds transfer at point of sale (EFTPOS) has been hailed as the "computer-age version of a cash transaction".[190] It facilitates retail payments to be made by the transfer of funds electronically from a customer's bank account to the retailer's bank account at the point of sale. Essential components of the EFTPOS system include electronic equipment installed in retail premises, magnetic strip plastic cards and their associated PINs, and an automated message transmission system linking the banks with the retailers.[191]

---

[188] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 199.

[189] Visser *Banking in the Computer Age: The Allocation of Some of the Risks Arising from the Introduction of Automated Teller Machines* (1985) 102 South African Law Journal 646 650. See Section B: Chapter 2.

[190] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 202.

[191] Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 116; Arora Electronic Banking and the Law (1988) 83; Goode Electronic Banking (1985) 11.

EFTPOS may exist as either a credit or a debit card transaction, distinguishable by the fact that a EFTPOS credit card transaction provides the cardholder with the option of paying the outstanding balance on the card in full or in installments, whereas payment in full is made immediately in respect of EFTPOS debit card transactions.[192]

A typical EFTPOS transaction would entail the following steps:

i. customer inserts the card into the card-reading terminal;
ii. customer enters a card specific PIN into the terminal;
iii. retailer enters details of transaction into terminal;
iv. information thus far entered is encrypted;
v. encrypted information is transmitted via a network to the relevant bank;
vi. customer's account with the bank is scrutinized so as to ascertain whether sufficient funds or credit facilities are available for the transaction;
vii. terminal prints a confirmation of the transaction;
viii. customer's account with the bank debited with the value of the transaction, and the retailer's account credited with same.[193]

Lawack[194] submits that the EFTPOS payment system is based upon mandate, as the customer instructs the bank by means of "swiping" the card and entering the PIN, thereby electronically transmitting a mandate to make payment, subject to sufficient funds or credit being available.

As public policy requires of banks to establish as secure a payment system as possible, and the card/PIN combination have proved flawed as a secure means of establishing

---

[192] Van Jaarsveld *About Credit Cards and Liability* (XXXXI) 2 Codicillus 92 95.

[193] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 202; Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 116.

[194] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 114.

customer identification and authorization, is needs to be replaced by a more effective alternative.[195]

Le smart card[196] was invented in 1974 and amounts to a significant development in the EFTPOS field. Typically, a smart card is embedded with a microprocessor and a certain amount of memory,[197] and, upon issue by the bank, information is entered into some of this memory and then rendered tamper-proof. This memory also records all the transactions performed using the smart card. Thus, the smart card may act as an electronic bank account, as a predetermined value is recorded in the memory, representing available funds or a credit limit. Once this predetermined value has been exhausted, the smart card is simply recharged or replaced.[198]

When used in conjunction with a card-reading terminal, the retailer receives an electronic account number from which the transfer of funds as payment is requested either immediately, or at a later stage from the bank.[199]

The smart card/PIN-pad interaction facilitates the customer displaying *entitlement to use* the smart card, as would be the case with a magnetic stripe card, save for the fact that instead of the verification of *entitlement to use* being performed by the PIN pad or by the bank's computer network, the verification emanates from the smart card itself.[200]

---

[195] Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 117.

[196] Or *carte a memoire* (memory or "smart" card).

[197] Originally ranging from 8kB to 32kB.

[198] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 202; Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 117.

[199] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 202-203; Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 117.

[200] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 204.

The advantages of the smart card are that it stores transaction receipts in memory, provides a high level of security,[201] and may even serve as a universal debit card for use internationally as an electronic traveller's cheque.[202] Meiring[203] believes that the most beneficial application of the smart card is its off-line function, when it authorises its own transactions and confirms the cardholder's identity and credit balance without having to refer to the bank's mainframe, thereby not being susceptible to mainframe inaccessibility failure. A disadvantage is that, once loaded or charged with a certain value, this value ceases to earn interest.

The traditional signature thus plays no part in an EFTPOS transaction, and has been superceded by the PIN (in conjunction with a card), which PIN amounts to the constitutive element of the transaction. Thus, the card/PIN combination serves to identify the customer and authorise the transaction in an ATM withdrawal or an EFTPOS transaction, as distinct from the case of the drawer's signature on a cheque in the case of fraud. Here, should the bank pay a cheque which has been forged or bears an unauthorized signature, the customer may, with relative ease, discharge any burden of proof by means of a physical examination of the signature in question. Whereas, should the card/PIN be used fraudulently or without authorisation, the conditions of use of that specific card will usually stipulate that the bank is authorised to effect a debit against the customer's account for all withdrawals or transactions implemented by the use of the card/PIN. This is despite the fraudulent withdrawal by an unauthorized party, unless and until the customer has notified the bank[204] that the card has been lost or stolen, since any withdrawals allowed thereafter will, generally, be reimbursed by the bank.[205]

---

[201] The memory may be loaded with biometric data such as, for example, voice- or fingerprints. See Section B: Chapter 2 for more information.

[202] Visser *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189 204; Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 117.

[203] Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 117.

[204] Alternately, or in addition to, the customer proving that the withdrawal was made without the use of the relevant card/PIN.

[205] Meiring *ATM's and EFTPOS: Some Legal Considerations* (1987) Modern Business Law 115 116.

In addition to the aforegoing methods of electronic payment, the transfer of money between accounts is also possible per telephone, that is home- or office-banking.

The home-banking facility enables the customer to instruct the bank to effect a funds transfer from one account to another. The plastic card is not required, hence the identification of the customer becomes pivotal, and identification methods such as PINs and encrypted passwords are employed.[206]

Similarly, the telephone bill-paying mechanism enables access to certain banking services over the telephone. These services may include the payment of accounts, balance enquiries and the transfer of funds between accounts. A push-button or pulse telephone, together with an identification code (the PIN), enable the customer to instruct the bank, and pre-recorded verbal prompts guides the customer in providing the requisite information for the transaction, such as monetary amounts and account numbers.[207]

Office-banking services provide for certain transactions from the office of the business-entity concerned, and include intra-business transfers and third party payments. These transactions exist as either pre-formatted (per disks or magnetic tapes) or on a free-formatted basis, per smart card technology. Pre-formatted transactions establish a diskette security method wherein specially encoded disks identify the client to the bank, and include encrypted messages, signatory numbers and personal passwords; whereas free-formatted transactions enable transfers on a non-nominated basis by means of smart card technology. These free-formatted transactions involve the use of two cards, which digitally authenticate each other, and all messages communicated between the two cards are encrypted.[208] The signatory card is validated by a corporate card resident in the second reader, and then both the signatory and corporate card are validated at the host.

---

[206] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 128. See paragraph 1.3 below.

[207] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 129; Schwellnus Die Aard en Rol van die Handtekening as Betalingsmagtiging LLM Dissertation (1991) 124.

[208] For more of a detailed discussion regarding encryption, see Section B: Chapter 3.

Further, the presence within the second reader of a valid and corresponding corporate card is a precondition for an authorized signatory card to be inserted. The signatory card password, number of invalid attempts and accesses are controlled by the software resident on the card, as well as the fact that software on the computer will not allow the entry of a signatory number from the keyboard, as it has to be read from the signatory card.[209]

Thus, home, telephone and office banking incorporates the simultaneous application of several forms of an electronic signature, foregoing the use of a traditional signature, and, nevertheless, increasing security and certainty.

Van Jaarsveld[210] notes that a Code of Banking Practice was adopted by the Banking Council of South Africa in late 1999, and is based largely upon the Banking Code of the British Banker's Association. This Code is aimed at informing customers of, amongst other topics, the protection of confidentiality. The Code of Banking Practice states that the PIN is strictly confidential, and should never be disclosed to anyone, including an employee of the bank.[211] Despite the above Code and publicity campaigns by both the banks and the state, urging greater care, cards and their PINs are acquired by fraudulent third parties with relative ease.

Consequently, with current transactions such as ATM withdrawals, EFTPOS transfers, or home-banking conducted through the Internet, the initiating message or instruction is not carried in a permanent format, since it is expressed in a computer language, where the traditional handwritten manuscript signature has been superceded by an electronic key (the PIN) that authenticates the message.

1.3 PASSWORDS

[209] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 129-132.

[210] Van Jaarsveld *About Credit Cards and Liability* (XXXXI) 2 Codicillus 92 98.

[211] Van Jaarsveld *About Credit Cards and Liability* (XXXXI) 2 Codicillus 92 98.

As alluded to above, electronic signatures may also take the form of passwords (codes) as identification mediums. Passwords evince the characteristic aspect of *proof by knowledge*, in that the verifier knows the information in respect of the claimed identity, which information can only be known/produced by a principal with that identity.[212]

Proof by knowledge is the most common method of user authentication as a result of it's simplicity and ease of use, but this advantage suffers a defect in that passwords used are generally predictable, and computer programs may be used to detect more sophisticated passwords. In addition, the passage of passwords over networks renders these passwords susceptible to interception.[213]

Generally, there exists five categories of passwords:

i. group passwords – these are common knowledge to all users of a specific system;
ii. unique passwords – these are usually manually recorded on paper or in text files on the user's computer;
iii. non-unique passwords – these are used to confirm a claimed identity in cases where identification is based upon a long numerical and/or letter sequence stored on a card;
iv. continuously changing passwords – in systems where a list of passwords is maintained on the central system, a copy which is by necessity distributed to each user; and

[212] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[213] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

v. questionnaire passwords – a series of questions are posed to individual users, the answers to which distinctly identify them.[214]

The aforegoing amounts to a situation of minimum security, in that they are by no means impervious to a serious assault, and thus are required to be used in conjunction with additional security measures.[215]

Passwords are generally employed to identify the user by reference, but, as passwords are intangible mental objects, they can be exchanged or intercepted without any tangible loss. Consequently, the strength and trustworthiness of a password depends upon the behaviour of the user thereof.[216]

Successful password management may be achieved by accurately assessing the risk and predicting the correct balance between various possible environments, since a user with many passwords which are infrequently used may need to record these passwords, which activity compromises confidentiality; the use of a single password over an extended period increases the risk of such password being intercepted; and where a single password is employed at numerous services, such a password is shared with various persons, hence reducing confidentiality.[217]

There are three levels of risk, associated with three domains of password use. A *local password* is regarded as the most resilient form of password, since it is a secret shared between a user and a single machine, such as a smart card PIN or the boot password on

[214] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[215] These could range from PINs to smart cards to digital signatures to biometric identification. Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[216] Buys Cyberlaw@SA (2000) 144.

[217] Buys Cyberlaw@SA (2000) 144.

an individual's computer. A *closed domain password* is authenticated by the known administrator of your network, being received by the said administrator via a known and secure transport medium. A *public password* has the same characteristics of a closed domain password, save that the administrator and transport medium are unknown to the user.[218]

Basic suggestions for password use are that users should elect a password consisting of at least two words, preferably not English words, which password can easily be remembered by the user, and then construct a "pair" of words for each risk domain area frequented by the user. Finally, create a derivative of the base word pair for each instance required in various risk domains.[219]

Therefore with the use of passwords as a form of an electronic signature, individuals can establish their positive identity by claiming it, providing proof of that identity as well as authenticating the proof and thus the identity.

[218] Buys Cyberlaw@SA (2000) 145.

[219] Buys Cyberlaw@SA (2000) 146.

1.4 CONCLUSION

In consequence of the innovations in electronic technologies, a traditional signature can no longer be utilized, and, consequently, PINs, passwords and PIN/card combinations have been adopted which, so long as these identify and bind the signatory, are deemed to be electronic signatures.

PINs and passwords are rendered ineffectual as a result of various inherent drawbacks that negate the satisfaction of security requirements presently demanded by our highly inter-connected, information-orientated society.[220] These identification methods are incapable of differentiating an authorized person from an impostor who fraudulently acquires a token/knowledge of that authorized person. They are thus inadequate measures to combat counterfeiting. They suffer from a number of drawbacks, for example, tokens may be lost or stolen; PINS may be forgotten, guessed or intercepted by impostors.[221]

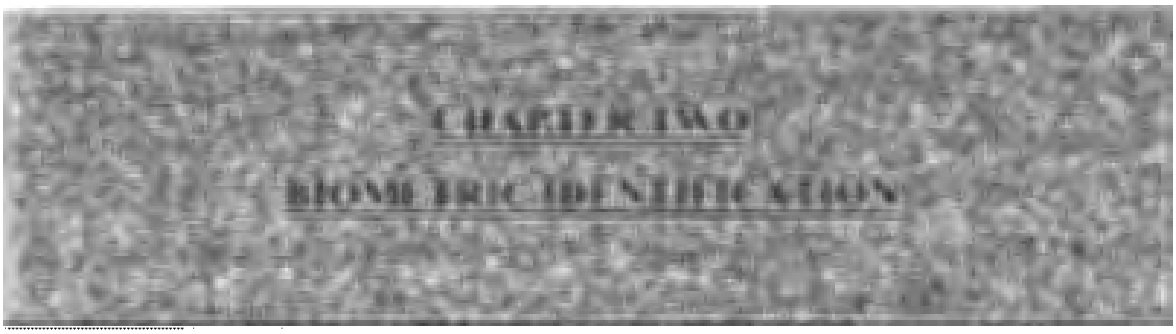
As these methods are not based on the inherent attributes of an individual, and they are incapable of satisfying the security requirements of an electronically inter-connected information society, additional and convenient security mechanisms are thus needed as our society becomes increasingly computer-dependant.[222]

---

[220] Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 161.

[221] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17), 25% of people write their PINs on their ATM cards.

[222] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Jain, Hong and Pankanti *Biometric Identification* (2000) 43:2 Communications of the ACM 91 92.



2.1 INTRODUCTION

The information age has changed the way many transactions are completed. Everyday actions are increasingly being handled electronically, instead of face-to-face, or with pencil and paper. This increase has created a demand for a highly accurate and automatic personal identification and authentication system.[223]

A signature is associated with personal identification; that is, the association of a particular individual with an identity. Identification can be in the form of the determination of the identity of an individual from a database of persons known to the system, and/or the authentication of a claimed identity, that is verifying a user's identity utilizing, for example, a password or PIN. The goal of authentication is to protect a system against unauthorized use.

PINs and passwords suffer several drawbacks, such as being incapable of differentiating an authorized person from an impostor who fraudulently acquires a token/knowledge of that authorized person; tokens may be lost, stolen or forgotten; and PINs may be forgotten, guessed or intercepted by an impostor. Since these methods are not based on the inherent attributes of an individual, they are incapable of satisfying the security requirements of an electronically inter-connected information society. Additional and

[223] Campbell, Alyea and Dunn *Government Applications and Operations* <http://www.biometrics.org/REPORTS/CTSTG96> (2000-04-13).

convenient security mechanisms are thus needed as our society becomes increasingly computer-dependant.[224]

Biometric identification[225] potentially satisfies this requirement. It is a form of electronic signature, which entails a quality linked or attributed to the person of the user, such as fingerprints and retinal structures, within the electronic environment, which is known as *biometrics*.[226] Biometric identification, which is also referred to as the *proof by property* approach is the most advantageous means of identification and authentication, since it cannot be stolen by or transferred to other people.[227]

Biometric identification has shown promise as being able to provide powerful tools for dealing with problems where positive identification is required.[228]

---

[224] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Jain, Hong and Pankanti *Biometric Identification* (2000) 43:2 Communications of the ACM 91 92.

[225] Hopkins *An Introduction to "Biometrics" and Large Scale Civilian Identification* (1999) 13:3 International Review of Law (Computers and Technology) 337*ff*. Ashbourn *The Biometric White Paper* <http://www.biometric.freeserve.co.uk/whitepaper.htm> (2000-07-24) - the ancient Egyptians employed biometric identification in a number of everyday business situations, such as agricultural transactions and legal proceedings. This primitive application of biometrics involved unique physical human characteristics to identify individuals, such as scars, measured physical criteria, or a combination of features (complexion, eye colour and height). In the 19th Century, researchers into criminology attempted to relate physical features and characteristics with criminal tendencies. The idea of measuring individual physical characteristics and the parallel development of fingerprinting became the universal norm among law enforcement agencies for identity verification, and, in 1870, Bertillon from France invented a system (the Bertillon system) based on fingerprint analysis for identifying criminals. Later Galton, trying to improve the Bertillon system, proposed various biometric indices for facial profiles - Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[226] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 63; Malan *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153 165.

[227] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[228] See Jain, Hong and Pankanti *Biometrics: Promising Frontiers for Emerging Identification Market* <http:///www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

Thus, biometric identification is a form of electronic signature which may be used to identify an individual, and/or verify the signature of that individual, by means of measuring human characteristics of an individual within an electronic medium.

The strict definition of biometrics is "the science that involves the statistical analysis of biological characteristics", that is, "the application of computational methods to biological features", specifically in respect to the study of unique biological characteristics of humans.[229]

A more pragmatic definition of biometric identification is that "which refers to identifying an individual based on her physiological or behavioural characteristics" (biometric identifiers).[230]

Biometrics has become synonymous with the identification and verification of peoples' identities using their unique characteristics.[231]

Physiological-based techniques measure the physiological attributes of an individual, and include facial analysis, fingerprinting, hand geometry, retinal and iris analysis, and DNA profiling. Behavioural-based techniques measure aspects of an individual's behaviour, and include signature, keystroke, voice, smell and sweat pore analysis.[232] Polemi notes that systems based on physiological techniques are more accurate in relation to behavioural techniques, but the devices employed are larger and more expensive.

---

[229] Hopkins *An Introduction to "Biometrics" and Large Scale Civilian Identification* (1999) 13:3 International Review of Law (Computers and Technology) 337*ff*.

[230] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[231] Hopkins *An Introduction to "Biometrics" and Large Scale Civilian Identification* (1999) 13:3 International Review of Law (Computers and Technology) 337*ff*.

[232] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

However, behavioural-based systems, although cheaper to implement, need further enhancements in identifying, verifying and adopting individual variability.[233]

No single biometric approach meets all needs and, ideally, biometric identifiers should meet the following requirements:

i. universality - where each person possesses the requisite characteristic;
ii. uniqueness - where no two persons share the same characteristic, that is, there is a distinguishable trait;
iii. permanence - where the characteristics neither change nor can they be altered;
iv. collectability - where the characteristic is readily presentable to a sensor and is easily quantifiable.[234]

2.2 THE BIOMETRIC SYSTEM

A *biometric system* is employed to measure biometric criteria so as to facilitate identification. It is a "pattern recognition system that establishes the authenticity of a specific physiological or behavioural characteristic possessed by a user",[235] and consists of three elements, namely: a physical reader (that scans the body part used for identification); the software (that translates the image into data); and a database (where the identification data is stored for comparisons, that is, verification).[236]

---

[233] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[234] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18); Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

[235] Pankanti, Bolle and Jain *Biometrics: The Future of Identification* 2000 (February) Computer 46 46.

[236] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 82.

A biometric system can be divided into two stages, these being the enrolment module and the identification module. The enrolment module enrolls individuals into the biometric system. The biometric characteristic is scanned by a biometric sensor to acquire a digital representation of the characteristic. This digital representation is further processed by a feature extractor, so as to generate a compact and expressive representation called a template. The template may either be stored in the central database of the biometric system, or be recorded on a magnetic stripe or a smart card, that is then issued to the individual. The identification module is responsible for identifying individuals. During this stage, the biometric reader captures the characteristic of the individual to be identified and converts it to a digital format as a template. The resulting template is fed to the feature matcher, which compares it against the stored template to assess whether the two templates correspond.[237]

Biometric recognition systems can operate in one of two modes, namely the identification mode, where the system establishes an individual's identity without that individual having to claim an identity, by means of searching the entire template database for a match;[238] or in verification/authentication mode, that authenticates a person's identity by comparing the captured biometric characteristic with the template stored on the system. An individual desiring to be identified submits a claim to a particular identity existing on the system (for example, via a login name, smart or magnetic stripe card), and the system either confirms or refutes the submitted claim of identity.[239] Thus, through the use of a biometric system, a biometric characteristic, which may be construed as a form of

---

[237] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18); Pankanti, Bolle and Jain *Biometrics: The Future of Identification* 2000 (February) Computer 46 46.

[238] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18). The system identifies a person exclusively through biometric traits - Frischholz and Dieckmann *BioID: A Multimodal Biometric Identification System* 2000 (February) Computer 64 67.

[239] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18). A person gives his name/number which a system then verifies by means of biometric traits - Frischholz and Dieckmann *BioID: A Multimodal Biometric Identification System* 2000 (February) Computer 64 67.

electronic signature, has the capacity to identify as well as verify that individual's identity.

2.3 PERFORMANCE OF THE BIOMETRIC SYSTEM

Biometrics is believed to "hold the promise of fast, accurate, more reliable, user-friendly and less expensive authentication for a variety of applications".[240] However, these systems were regarded as objectionable, based upon factors such as cost, safety and user-psychology.[241] Recently, there has been an increasing interest in biometric systems because of "rising reliability and plummeting prices".[242] The overall performance of a biometric system is measured according to operational, technical, financial and manufacturing criteria.

Operational criteria includes ease of use, implying that the devices should be convenient to use. Non-contact biometric technologies, which require very little co-operation, are regarded as user-friendly.[243] The devices should have public acceptance, since people need to be educated that biometrics could be one of the most effective means of protecting individual privacy.[244] A device is deemed publicly acceptable if it is not discriminatory, that is, human factors such as gender and age should not influence the performance of a biometric device.[245] Further operational criteria are that such systems must be regarded as unique and exclusive. Thus, the outcome of the authentication

---

[240] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

[241] Poullet & Vandenberghe (Eds) Telebanking, Teleshopping and the Law (1988) 62- 63.

[242] Millman *The one and only you* <http://www.archive.infoworld.com/cgibin/displayStory.pl?/features/980629biometrics.htm> (2000-07-18).

[243] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[244] This issue will be discussed in paragraph 5 below.

[245] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

process should be unique, and not be able to change each time the user is verified by the biometric device. No other form of identification should be necessary.[246]

Technical criteria require that the space of the biometric database should be sufficient to store the templates on;[247] the time required to make an identification decision should be minimal.[248] Such a system must also be flexible enough in adjusting threshold settings, depending on the security level required,[249] and the biometric system should be accurate.

Financial prerequisites involve the costs of equipment, installation, training and updating.[250] It will become possible to make biometrics accessible to new personal identification applications, given the increasing availability of inexpensive processing power as well as the increased use of sensors. In addition, the chosen biometric system should be supported by a number of manufacturers, so as to foster improvements and encourage widespread deployment, thereby rendering it easily accessible for mass implementation.[251]

---

[246] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[247] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[248] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[249] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[250] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[251] Pankanti, Bolle and Jain *Biometrics: The Future of Identification* 2000 (February) Computer 46 46.

2.4 BIOMETRIC TECHNOLOGIES

2.4.1 PHYSIOLOGICAL BIOMETRIC TECHNIQUES

2.4.1.1 FINGERPRINT IDENTIFICATION

A *fingerprint* is the pattern of furrows and ridges on a fingertip's surface. Humans have used fingerprints for personal identification for centuries.[252]

Fingerprints are one of the most understood and studied applications of biometrics, and the validity thereof has been well-established.[253]

Fingerprint identification provides two distinct purposes:

i. fingerprints can be used to determine that an individual is unique;

ii. fingerprints can accurately verify that an individual is who they claim to be.[254]

Fingerprint identification systems generally consists of a hardware scanner and recognition software.[255]

---

[252] Fingerprints were first used in ancient China when wax seals embossed by the sender's fingerprint served as proof of the person sending a letter. In the 17th Century it was recognized that an individual's fingerprints were unique and could be classified into patterns. Toward the end of the 19th Century, law enforcement agencies began collecting fingerprints of criminals. This collection of fingerprints became routine during the 20th Century - Hopkins *An Introduction to "Biometrics" and Large Scale Civilian Identification* (1999) 13:3 International Review of Law (Computers and Technology) 337*ff*. Currently, with the advent of computers, it has become possible to automate fingerprint identification. The first commercial application of biometrics was in 1968 where a Wall Street brokerage used fingerprints to open the vault where the stock certificates were held. The application cost $20 000 in 1968, but now would cost about $300 –
O'Sullivan *Biometrics comes to life* <http://www.banking.com/aba/cover_0197.htm> (2000-08-17).

[253] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[254] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

[255] Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

During enrolment (which lasts approximately thirty seconds) the system generates a small template of the unique features of the fingerprint[256] that can be stored on a magnetic stripe or smart card, or on a server controlling access to private information. When the user wishes to gain access, he/she places the same finger on a low-cost direct fingerprint reader that compares this fingerprint with that stored on the template.[257]

The major commercial applications of fingerprint technology include controlling access to databases (through the Internet, Intranet or Extranet) and to payment environments, as well as controlling physical access to a facility.[258]

Fingerprints possess sufficient information to allow large-scale identification, and are thus regarded as highly accurate, since they rely on immutable physical attributes; as well as reliable technology.[259] Consequently, they are expected to lead biometric applications in the future.[260]

---

[256] A fingerprint is made up of a unique series of ridges that have end points and splits.

[257] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

[258] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24). This technology has extended beyond mere access to a physical facility to that as futuristic as gaining access to a revolutionary, intelligent firearm. The firearm can be switched "on" and "off" with the use of a smart card containing the authorised user's fingerprints. The weapon contains a fingerprint scanner and so will only fire if being held by the authorised person. The gun can be programmed to recognise more than one authorised person. The South African Consortium has developed this prototype - Campbell *Smart gun prototype to be ready byMarch*<http://www.engineeringnews.co.za/engnews...65bc2?OpenDocument&Highlight=0,biometric> (2000-04-07). Others are a fingerprint reader in a cellular phone which could render the device useless to thieves; biometrics-enabled cars which could unlock for authorised people only; fingerprints as an alternative to a password logon on a personal computer; and fingerprints encoded on credit cards which could verify a shopper's identity - Bloomberg News *Chips aim to make passwords obsolete* <http://www.news.cnet.com/news/0-1006-200-1510976.html> (2000-07-19).

[259] Several techniques have been used in an attempt to crack fingerprint readers but to no avail. See Anon *Breaking In* <http://www.zdnet.co.za/pcmag/features/biometrics/break.html> (2000-02-08) for various techniques used.

[260] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17);
Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

Fingerprint verification possesses criminal and Orwellian connotations, and therefore lacks acceptability by the user in many environments.[261] It is submitted that, to avoid the association with crime, fingerprints be stored in a card, and not within a central database, thereby not reproducing it for law enforcement applications.[262]

Further problems experienced with fingerprint-based biometric technologies are that automatic fingerprint identification generally requires costly computational resources;[263] parties with fingers that are either injured, swollen or missing may have problems being verified by the system; in environments where gloves are worn, fingerprint identification is not appropriate; and age, gender, occupation, race and environmental factors may influence the validity of a fingerprint system.[264]

Within the banking environment, fingerprint identification may be utilized to curb card fraud. Research conducted by Britain's Plastic Fraud Prevention Forum showed that consumers preferred fingerprints over PINs and the traditional signature as an identification technology, as it was "very secure, fast, reliable and easy to use".[265] It may further be utilized in conjunction with card systems, such as smart cards, to perform identity verification.[266] Smart cards endowed with this technology can be used for

---

[261] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Pankanti, Bolle and Jain *Biometrics: The Future of Identification* 2000 (February) Computer 46 48-49.

[262] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[263] Pankanti, Bolle and Jain *Biometrics: The Future of Identification* 2000 (February) Computer 46 48-49.

[264] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[265] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[266] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

electronic cash transactions, ATM transactions and other operations where the identification of the cardholder is critical.[267]

MasterCard has determined that the fingerprint solution provides the

> "highest degree of reliability, [combined] with a remote enrolment capability, ease of use at point of sale and a higher level of consumer acceptance based on a survey that MasterCard did with over 900 consumers, than any other biometric technology available today.... and .... believes that [it] is the most viable and realistic approach for the payment card industry. It poses the fewest problems for issuers, merchants and cardholders, and is far easier to use and more cost effective."[268]

Another method employed by banks is to require a visual fingerprint to be submitted on the face of cheques cashed by non-customers. It is an inkless process that takes advantage of a chemical reaction that produces a print on the cheque. However, it must be noted that this is not a biometric technology, but merely a deterrent, as no comparison against a template is made, and no part of the process is automated.[269]

In conclusion, fingerprinting has proved to be more popular, acceptable, implement-able and cost-effective than comparable biometric products.[270] It is thus further evident that, in addition to identifying an individual, this biometric technology may also verify or authenticate this individual, thereby binding him/her to any transaction concluded.

---

[267] Craig *Smart Card Chip Reads Fingerprints* <http://www.techweb.com/news/story/TWB19980217S0013> (2000-04-09).
At the Smart Card 2000 Trade Show held in London, a smart card called e-purse that verifies its owner through fingerprint verification or iris recognition was demonstrated. Because these types of biometrics can be used in conjunction which PINs and passwords and cannot be duplicated by imposters, the companies present opined that this type of smart card supplied the highest level of security for home banking and electronic commerce.

[268] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

[269] Anon *Inkless Fingerprinting vs Biometric Finger Scanning* <http://www.biometricgroup.com/a_biometrics_42/inkless_fingerprinting.htm> (2000-07-31)

[270] Moyer *Going Digital – With Fingerprint ID* (1997) 162:43 American Banker 16*ff*.

2.4.1.2 FACIAL ANALYSIS

Facial characteristics such as the size and shape of the nose, eyes, chin, eyebrows, and mouth are unique to each individual.[271] Facial images are the most common biometric characteristic used by humans for making personal identification. Typically, approaches to facial recognition are based upon one of the following: shape and location of facial attributes, as well as the spatial relationship; or overall analysis of the facial image, and the decomposition thereof into a number of canonical features.[272]

The system used for this type of identification employs a camera that captures the facial image, whereafter the software extracts pattern information and compares it with the user's template.[273]

There are several problems associated with this identification method. The user must look directly into the camera with a certain amount of light for the system to effectively analyse and identify the person, thereby imposing restrictions on the user. Also, the system is unable to analyse users with imposed physical characteristics such as a beard, varying hairstyles, or certain facial expressions. Further, the system may not be capable of coping with angles or facial expressions that are slightly different from those used during the encoding process. During aging, changes occur in the human facial skeleton, and, therefore, templates need regular updating.[274]

---

[271] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[272] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[273] Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

[274] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

Although the performance of facial recognition systems is reasonably adequate, it is questionable whether the face itself, with its lack of contextual information, is sufficiently effective to allow for personal identification with any degree of confidence.[275]

Facial recognition, as a natural biometric technique, may thus identify and verify an individual.

2.4.1.3 FACIAL THERMOGRAM

A unique facial signature is produced by the underlying facial vascular system when heat passes through facial tissue and is emitted from the skin. These facial signatures can be captured by means of infrared cameras to produce an image known as a *facial thermogram*. There are a number of advantages to this identification method, namely that they are unique to each individual and are not influenced by disguises.[276] Infrared cameras are capable of capturing the facial thermogram in low or changing ambient light, or even in no light at all, which severely reduces the restrictions on the acquisition of facial thermograms. Also, it is a non-intrusive biometric technique; capable of verifying identity without contact, full camera view, and co-operation.

Although facial thermograms are individual specific, it is unproven whether they are sufficiently discriminative. Another disadvantage of the method is that facial thermograms depend largely on factors that are subject to change such as the user's emotions and body temperature.[277]

---

[275] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[276] Not even plastic surgery can alter the formation of the face thermogram, because it does not re-route the flow of blood through the veins.

[277] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

Facial thermograms can be used for both identification and identity verification. However, alone they do not seem consistent enough, and must thus be utilised in conjunction with other biometric techniques.

2.4.1.4 HAND GEOMETRY

The human hand has distinctive physical characteristics, which include external contours, internal lines, hand geometry, finger length and size, palm-prints and fingerprints, and the pattern of blood vessels in the back of the hand.[278]

This particular biometric identification system works by the user aligning their hand according to guide-marks on hand reader hardware. The reader captures a three-dimensional image of the fingers and knuckles and stores the data as a template.[279]

When an individual desires access, the hand image is compared with the previously enrolled sample. The user enters their identification number on a keypad and places their hand on a platter. The hand's image is captured by a camera, whereafter it is analyzed by the software. Areas of application are mainly in physical access control.[280]

Hand geometry-based systems have been installed internationally on a large scale. The technique is simple, easy to use and cost-effective. Identification accuracy is not affected by operational environmental factors such as dry weather; or individual anomalies such

---

[278] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17);
Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[279] Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

[280] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

as dry skin. Generally, there is a high user acceptance rate.[281] Other advantages are that this system needs little data storage space and has the smallest template, as well as a short verification time.[282]

However, the technique does suffer from low discriminative capability. Also, the physical size of the system is large, thereby potentially restricting it from some applications, such as laptop computers. The biometric characteristic may be subject to variation over an individual's lifetime, particularly during childhood.[283] Factors that might influence the performance of the system include rings, swollen fingers, or no fingers. Dirt may also have an effect.[284]

Digitised images of patterns of the veins in the hand may be captured with an infrared camera, and these images provide a robust and stable pattern that can be used to make personal identification. Hand vein patterns are individual specific and are not easily changed by surgery, thereby rendering them efficient in circumventing fraud.[285]

---

[281] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18). Testing found that this system was the user's favourite compared with fingerprint, signature, voice print and retinal - Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[282] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[283] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[284] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[285] For example, Disney World uses hand geometry scanners to identify season-pass holders – Millman *The one and only you* <http://www.archive.infoworld.com/cgibin/displayStory.pl?/features/980629biometrics.htm> (2000-07-18).

Thus hand geometry identifies and verifies the identity of a user by means of the hand's distinctive characteristics. Alone it is not a perfect biometric application, and is generally employed in conjunction with a PIN or other identification number.

2.4.1.5 RETINAL PATTERN

The retina is the layer of blood vessels located at the back of the eye.[286] The pattern formed by these veins is stable and unique,[287] even between identical twins.[288]

Retinal pattern scan is one of the latest and most reliable biometric techniques. A low intensity beam of infrared light is projected into the eye and a digital image of the illuminated retina is captured.[289] The individual is required to gaze closely into an eyepiece and focus on a pre-determined spot in the visual field so that a fixed position of the retinal vasculature can be used for identification. This involves a high degree of user co-operation and involvement that may not be acceptable to the individual requiring identification.[290]

Currently retinal pattern scan is considered to be the most accurate technique,[291] and systems have been installed in several high security environments. A disadvantage is the

---

[286] Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

[287] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[288] Anon *Biometric Technology Overview* <http://www.biometricgroup.com/a_biometrics_42/biometric_technology_overview.asp> (2000-07-31).

[289] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[290] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[291] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18); Anon *Biometric Technology Overview* <http://www.biometricgroup.com/a_biometrics_42/biometric_technology_overview.asp> (2000-07-31).

high cost of retinal scanners, as well as the fact that retinal pattern scans need perfect alignment of the eye to reach the retina.[292]

The potential lack of user acceptance is largely negated by the high degree of accuracy provided by the retinal pattern in identification and verification.

2. 4. 1. 6 IRIS RECOGNITION

The iris is the annular region of the eye bordered on either side by the pupil and sclera.[293] Ophthalmologists were the first to propose that the iris may be used as an optical fingerprint for personal identification, based upon the fact that each iris is unique, and is unalterable in clinical photographs.[294]

Iris recognition is based on visible qualities of the iris; the primary visible characteristic being the trabecular meshwork (a tissue which gives the appearance of dividing the iris in a radial fashion). Other familiar visible characteristics are rings, furrows, freckles and the corona. Iris recognition technology converts these visible characteristics into a template that is stored for future identity verification.[295]

The following properties of the iris make it particularly suitable as an automatic identifier: it is protected from the external environment; it is impossible to surgically modify the iris without damaging vision; the test is natural because the iris has a physiological response to light; and, finally, the image of the iris can be registered at a

---

[292] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[293] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[294] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[295] Anon *Biometric Technology Overview* <http://www.biometricgroup.com/a_biometrics_42/biometric_technology_overview.asp> (2000-07-31).

distance from the subject without physical contact, and with relative ease.[296] In each case of reliability, security and acceptability, iris identification outperformed the traditional methods (such as the PIN and traditional signature).[297]

Potential applications of iris scanning include the prevention of cyber-crime, vehicle security, fast-tracking passport control and gaining access to telephones, computers and cars.[298] It also is predicted that iris scans may become a standard security feature for ATMs.[299]

2.4.1.7 DNA[300] PATTERN PROFILING[301]

DNA is the genetic material that contains the information necessary to produce a particular living organism. DNA profiling examines the genetic material of the genome (the total genetic makeup of a particular organism) for characteristics unique to that specific DNA, which is then compared with other DNA samples.[302] Samples of DNA

---

[296] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17). Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgiuser/web/tech/document?ID=436> (2000-07-18). In the past, iris-based identification systems required considerable user participation and were costly. However, considerable efforts are underway to improve this. A survey was done with the Nationwide Building Society of England. The results of the 1 000 participants showed the following: 91% prefer iris recognition to a PIN or traditional signature; 94% would recommend iris identification to friends and family; and 94% were at ease using the system.

[297] Negin Chmielewski Salganicoff Camus von Seelen Venetianer and Zhang *An Iris Biometric System for Public and Personal use* 2000 (February) Computer 70 70-74.

[298] Gordon-Cumming *BT is looking cybercrime in the eye* (1999) 5:7 Hi-Tech Security Systems 58 58.

[299] O'Sullivan *Biometrics comes to life* <http://www.banking.com/aba/cover_0197.htm> (2000-08-17).

[300] Deoxyribonucleic acid consists of a code of four bases, namely adenine, cytosine, guanine and thymine, and is organized within a series of sub-units called genes, which regulate specific aspects of the structure and function of the living organism.

[301] Also referred to as *DNA fingerprinting* as the DNA hereditary structures are as unique to a specific person as their fingerprints are.

[302] Kirby and Downing *The Principles and Problems of DNA- Profiling for Legal Purposes in South Africa* (1999) Obiter 307 308.

obtained from hair, skin, blood, tissue, saliva and semen have been used to fix identity,[303] as well as to ascertain paternity.[304] Thus, by identifying particular distinctive patterns in the genetic material in question, DNA profiling can determine with a high degree of accuracy whether a particular individual could have been the source of a specimen.

The major application of DNA profiling occurs when the identity of an individual is disputed or unknown, for example, at a crime scene where the perpetrator either leaves at the scene, or removes from the scene, bodily samples bearing DNA. In civil matters, the principle use of DNA profiling is seen in the confirmation of disputed paternity for children born out of wedlock. Consequently, DNA profiling has found application under South African law in the fields of criminal law, the law of persons and the law of succession for purposes of establishing identity. However, the courts have failed to establish a clear policy on the issue of whether a parent or guardian of a child can be compelled to avail themselves to such testing,[305] and there are too few judgments on the topic of DNA evidence.[306]

However, DNA profiling and the establishment and maintenance of the DNA databanks necessary to utilize DNA as a general means of identification engender certain concerns. These include:

i. the expenses involved; and
ii. the time required to test; and
iii. the affront to civil liberties (as conferred by the Constitution of the Republic of South Africa Act);[307] and

[303] Davel *et al* Law of Persons (1998) 94.

[304] *M v R* 1989 1 SA 416 (O) 426.

[305] *Van der Harst v Viljoen* 1977 1 SA 795 (C); *Seetal v Pravitha* 1983 3 SA 827 (D); *Nell v Nell* 1990 3 SA 889; *S v L* 1992 3 SA 713 (E); *O v O* 1992 4 SA 137 (C). *Contra* see *M v R* 1989 1 SA 416-429 (O).

[306] Kirby and Downing *The Principles and Problems of DNA- Profiling for Legal Purposes in South Africa* (1999) Obiter 307 314.

[307] Act 108 of 1996.

iv. the authority in terms of which it would be permissible to acquire and retain genetic specimens, the ownership of these genetic specimens, and the uses to which they could be subjected.

It is the impact on civil liberties, specifically the risk of invasion of privacy[308] and the right to bodily integrity,[309] which pose the greatest risk, as a result of the chance of medical and personal traits being disclosed to nefarious third parties, such as medical research organisations, employers and insurance companies.[310]

Consequently, DNA profiling is a means to most accurately identify and verify an individual based upon unique inherent genetic attributes. The problem, however, is the issue of user acceptance, as a result of the criminal law connotations associated therewith, as well as the potential misuse of the information stored in possible DNA databases. Also, parties are generally required to consent.

2.4.1.8 SWEAT PORE ANALYSIS

Each finger has a unique distribution of sweat pores. It is on this basis that s[illegible] pore analysis operates. A finger is positioned on a sensor, software records the pores as stars, and then stores their position relative to the area of the finger.[311]

Sweat pore analysis is a further method by means of which to establish and verify identity. However, it is still in the experimental stage, and thus the issue of accuracy has yet to be confirmed.

---

[308] s 14 (a) of Act 108 of 1996.

[309] s 12 (2)(c) of Act 108 of 1996.

[310] Mooki *DNA Typing as a Forensic Tool: Applications and Implications for Civil Liberties* (1997) 13:4 South African Journal on Human Rights 565 573.

[311] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

2.4.1.9 EAR RECOGNITION

The shape and size of an individual's ear is yet another unique physical trait, and therefore presents itself as another method of verifying and ascertaining identity with a large degree of accuracy.[312] Yet, it too is still in the experimental stage.

2.4.1.10 ODOUR DETECTION

Certain chemicals manufactured by the human body possess a distinctive smell for each individual, and thus odour detection is currently being considered as an identification method to be employed in conjunction with DNA profiling.[313]

2.4.2 BEHAVIOURAL BIOMETRIC TECHNIQUES

2.4.2.1 VOICE RECOGNITION/SPEECH ANALYSIS

Various characteristics of sound, phonetics and vocals because of unique physical attributes, such as mouth and nasal cavities, and the vocal tract can identify an individual. Although an individual's speech is distinctive, it may not contain enough information to offer speech-based identification.[314]

Speech-based verification can either be text-dependent or text-independent. The former authenticates an individual's identity based on utterance of a fixed and predetermined

---

[312] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[313] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

[314] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

phrase; whilst the latter verifies the speaker's identity independent of the phrase. This is more difficult than text-dependent verification, but it offers improved protection against fraud.[315]

Such systems operate by analysing the voice characteristics of a sample obtained when a person speaks over a telephone or into a microphone attached to the system. A set of biometric features associated with the voice is extracted and encoded into a data set or template. The system then compares it to the voice characteristics of a pre-recorded sample.[316]

There are several problems associated with this biometric technique. The enrolment procedure is generally more involved than other biometric techniques and, consequently, voice verification is regarded as unfriendly.[317] Factors such as illness, fatigue and stress affect the operation of such systems. Also, an individual's voice varies over time, which makes verification difficult, and updating of templates become necessary, which in turn has negative cost implications. People affected by alcohol, dental anesthetics or oral obstructions may also face difficulty in being verified.[318]

Voice recognition/speech analysis may thus identify an individual. However, it is mostly used to verify an individual through several mediums, ranging from computerised telephone transactions to smart cards.

---

[315] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[316] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[317] Ashbourn *The Biometric White Paper* <http://www.biometric.freeserve.co.uk/whitepaper.htm> (2000-07-24).

[318] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17). Veritel, a well-known voice biometric system has an error rate of between 1 and 2%. However, attempts by parties to breach the security of the system by mimicking the voice of the enrolled user were successful at low sensitivity levels.

2.4.2.2 KEYSTROKE DYNAMICS

The keystroke dynamic technique is based upon an individual's typing characteristics, and measures typing dynamics such as keystroke duration, time delay between each keystroke and typing error frequency.[319]

Two kinds of systems have been developed which are alternately based upon static and dynamic verification techniques. The static approach analyses the way in which a password or username is typed, using a neural network for pattern recognition,[320] whereas the dynamic approach verifies the person continually with any arbitrary text input.[321]

The static approach is deemed to be the preferred approach. If a new user wants access to the computer system, or if an existing user's password expires, they will have to type a user identification and a new password. The user must then re-enter the user identification and password for verification purposes. Based on the typing pattern entered, the typing biometrics methodology will compute a typing index for the user. The user identification (together with an associated typing index) is saved by the system along with the user's identification-password pair. On subsequent attempts to gain access, the user will enter the user identification followed by the password. The system will compute a typing index, which will then be compared to the typing index previously saved.[322] Should both the password and typing index match those saved, the user will be allowed access to the system. If the password does not match, the user will be rejected or

---

[319] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

[320] This is also known as keystroke dynamics where the system works in conjunction with the log-in information.

[321] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17)

[322] De Ru *Reinforcing Password Authentication with Typing Biometrics* (1996) 17 South African Computer Journal 26 27.

requested to re-enter the information by only the password mechanism, without utilising the biometric component. If the password is accepted, the biometrics component is used as supporting recommendation that verifies that the individual obtaining access is who he/she claims to be.[323]

The advantages inherent in this technique are that: the user's typing biometrics cannot be lost, stolen, lent or acquired; spying and trial-and-error password attacks have largely been rendered ineffective; and, throughout the duration of a session, the typing biometrics mechanism can keep on monitoring the keystroke of the user to ensure that the user is still the same user currently accessing the system. Nevertheless, the performance of this method is affected by various circumstances of users, such as hand injury or fatigue of the user. These systems are also costly, since neurological methods and dedicated terminals must be used.[324]

It is submitted that this identification and verification method should not be used independently, but rather as a supplement to a more secure authentication mechanism.

2.4.2.3 HAND-WRITTEN SIGNATURE VERIFICATION

Hand-written signatures have traditionally formed the basic method of authenticating documented transactions. However, it is difficult for banks and retailers to determine whether two signatures have actually been written by the same person. A technique for signature recognition, called hand-written signature verification, has been developed.[325]

This biometric method is based upon the fact that each person has a unique style of handwriting. However, no two signatures of a person are identical, as variations from a

[323] De Ru *Reinforcing Password Authentication with Typing Biometrics* (1996) 17 South African Computer Journal 26 33.

[324] De Ru *Reinforcing Password Authentication with Typing Biometrics* (1996) 17 South African Computer Journal 26 33.

[325] Frazer Plastic and Electronic Money (1985) 56-57.

typical signature may depend on the physical and emotional state of the signatory. Despite the variations, successful systems for signature-based authentication have been designed.[326]

There are two approaches to signature verification:

i. Static signature verification uses only the geometric features of a signature.
ii. Dynamic signature verification uses both the geometric features and the dynamic (online) features such as acceleration, velocity, rhythms and the successive touches on the writing surface.[327]

The above systems fall into two categories: a pen-based system which uses a special pen to capture the information, wherein the pen is the measuring device which captures the information; and a tablet-based system which uses special surfaces to collect the data, wherein the tablet contains the measuring device.[328]

Generally, the system divides the signature into independent events and examines each piece separately. A number of signatures are required for the enrolment process. It measures both the distinguishing features of the signature and the distinguishing features of the process of signing. These features include pen pressure, speed and the points at which the pen is lifted from the paper.[329]

---

[326] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[327] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[328] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[329] Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

At the point of verification, the user is required to sign, and the behavioural patterns are then captured through a specially designed pen and/or tablet, and compared with a template of process patterns.[330]

The signature is thus inextricably bound to the document and no aspect of the electronic document can be changed. An inherent advantage of this biometric method is that the traditional signature has been established as an acceptable form of personal identification, and can therefore be incorporated into business processes requiring signatures, such as credit card transactions. This familiarity makes the system highly acceptable for users.[331] This method has proved to be reasonably accurate, and therefore lends itself to applications wherein the signature is an accepted identifier.[332] Another advantage is that it is impossible for an impostor to obtain the dynamics information from a written signature.[333]

Disadvantages associated with this method are the inability of such a system to be used by people with Parkinson's disease or a similarly debilitating affliction, the high cost of acquisition and the processing hardware required, as well as difficulty with the individual's signatures changing radically.[334] The efficiency of this method is lessened with high illiteracy rates.[335]

---

[330] Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08).

[331] Jain Hong and Pankanti *Biometrics: Promising frontiers for emerging identification market* <http://www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[332] Ashbourn *The Biometric White Paper* <http://www.biometric.freeserve.co.uk/whitepaper.htm> (2000-07-24).

[333] Frazer Plastic and Electronic Money (1985) 57 submits that it is inconceivable that a forger could copy not only the appearance of the signature, but also the movements and pauses that it comprises of.

[334] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

[335] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17).

A well-known and widely used example of this type of electronic signature is the PenOp signature.[336] The signatory signs in his/her own handwriting using a stylus upon a digitizing pad. When the signature is inscribed and confirmed, it is sampled by the software, which measures size, shape and the relative positioning of the curves. The software produces statistics based on these features, the "act-of-signing" statistics. Once the signature has been approved the document to which the signature is affixed is hashed[337] and a digital signature[338] is produced.

The PenOp system goes further than this by creating a biometric token. The biometric token is created at the moment the signature has been captured. The system uses the "act-of-signing" statistics in addition to other information such as the claimed identity of the signatory (for example, a name or identity number), the identity of the machine and the image of the signature to compute a second hash value. The above-mentioned information together with second hash value, also known as the checksum, are encrypted to generate a biometric token.

A final hash of the checksum is calculated and incorporated into the biometric token. The entire biometric token is then encrypted and stored. In this way the biometric token not only links the signature and the document, but also the person and the signature.

Thus, the PenOp software enables the traditional hand-written signature to be directly transposed into an electronic environment, without the need to place additional technical or legal burdens upon the signing individual. Consequently, this handwritten signature verification technique (a form of an electronic signature), is capable of being accepted as a signature based upon the following attributes, namely: the affixing of the electronic signature is capable of evidencing the signatory's intention to be bound; and this electronic signature may be so attached to the relevant document that the separation of

[336] All information collected from http://www.penop.com (2001-03-17).

[337] The hash value (also referred to as a checksum) refers to the string of data that represents the contents of the electronic document.

[338] See Section B: Chapter 3 for a detailed discussion.

the two becomes impossible; it further has the capacity to be signatory specific; and it is able to provide a degree of security which is, at least, of the same level as that of a traditional signature. Hence, there appears no reason why such an electronic signature should be denied the status of a *signature* in law.

2.5 APPLICATIONS OF BIOMETRICS

The initial extensive application of biometrics was in the fields of law enforcement and prison security. However, contemporary biometric technologies have increasingly found application in civilian commercial undertakings and in the public service, where various areas[339] have been identified as being amenable to replacement or enhancement by one or other biometric application.[340]

In the field of physical access control to restricted areas,[341] hand geometry and fingerprinting are currently the biometric applications of choice.[342] However, token-based technologies hold the larger market share in this field. It is however predicted that the

---

[339] The area of immigration applications (these include passport control, bond control and visa control) indicates fingerprinting as the most common form of verifying identity among the states of North America, Africa, Asia, the Middle East, Eastern Europe and the Pacific. Yet, within Europe, fingerprint analysis is almost exclusively used in law enforcement - Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17). The social welfare payment systems of several American states have experienced large savings by the utilization of biometrics as an effective deterrent against multiple claims and other forgeries - Ashbourn *The Biometric White Paper* <http://www.biometric.freeserve.co.uk/whitepaper.htm> (2000-07-24).

[340] Jain Hong and Pankanti *Biometric Identification* (2000) 43:2 Communications of the ACM 91 94.

[341] For example, securing authorised access to casinos and hospitals, as well as recording the clock-in and clock-out times of employees.

[342] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Campbell, Alyea and Dunn *Government Applications and Operations* <http://www.biometrics.org/REPORTS/CTSTG96> (2000-04-13).

advantages of biometrics will soon result in biometric applications replacing token-based applications.[343]

Voice and/or fingerprint analysis are presently the prevailing biometric technologies regulating access to computers, databases, communication networks, cellular telephones and secured sensitive information.[344] It is anticipated that an increasing number of "information systems and computer networks will be secured with biometrics with the rapid expansion of Internet and Intranet".[345]

In the areas of banking and finance, biometrics has also found wide acceptance, largely as a result of the rapid progress of electronic commerce and electronic banking, as well as the concomitant fraudulent activities[346] involved in the general processing of electronic transactions.[347]

---

[343] Jain Hong and Pankanti *Biometric Identification* (2000) 43:2 Communications of the ACM 91 94.

[344] Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17); Campbell, Alyea and Dunn *Government Applications and Operations* <http://www.biometrics.org/REPORTS/CTSTG96> (2000-04-13).

[345] Jain Hong and Pankanti *Biometric Identification* (2000) 43:2 Communications of the ACM 91 94.

[346] 2% of the United Kingdom's GDP is attributed to cybercrime, and 40% of the world's internal websites have been hacked - Anon *Face of the New Security Technology* (1999) 5:7 Hi - Tech Security Systems 58 58.

[347] This application is not restricted to electronic transactions, but may be applied to, for example, securing the bank's safety boxes and verifying the identity of bank employees - Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17). Several large biometric security projects are being developed by Mastercard, American Express and others, including credit card and smart card security - Jain Hong and Pankanti *Biometric Identification* (2000) 43:2 Communications of the ACM 91 94.

2.6 BIOMETRICS AND FUNDAMENTAL RIGHTS

The development and application of new technologies from the South African perspective, particularly biometric technologies, must be considered in light of the provisions of the South African Bill of Rights,[348] as well as other pertinent laws, so as to gauge the extent to which fundamental human rights are impacted upon.

The primary concern of individuals regarding biometric technologies is the potential for information privacy violation, more specifically, the fear that hackers, insurance companies, revenue services and/or medical research facilities will adapt biometric technologies to utilize biometric data to trace and locate or correlate the data of an individual for their own ends. Presently, however, only two biometric technologies are capable of picking an individual from a group of a thousand or more, these being retinal scanning and fingerprinting. With retinal scanning, a large degree of co-operation on the part of the retinal subject is required for the retinal scanning system to operate successfully, and the differing methodologies of fingerprinting systems negates these systems from communicating with one another, thus temporarily nullifying the idea of a "Big Brother" surveillance conspiracy.[349]

One approach to overcome the apparent threat which biometrics may pose to an individual's privacy, is to focus on the education of the population-at-large in respect of the technology involved, and to keep the same fully informed in respect of developments. Such education would perforce be on a continuous basis, with emphasis on the advantages, and include comprehensive notification of when, how and where people are being identified and verified, and for what purpose. Thus, broadly, private sector biometric policies must state how and why biometric data will be used. These policies must further preserve the rights of the individual to control their data. While in the public sector, biometric applications must be based on transparent legal standards which define

[348] Chapter 2 of the Constitution of the Republic of South Africa Act 108 of 1996.

[349] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

and limit the circumstances wherein biometric data may be acquired, accessed, stored and used.[350]

Legislators and the courts must determine, firstly, whether the specific biometric application indeed violates a fundamental right; secondly, whether a fall-back option is available; thirdly, whether the biometric data is subject to laws regarding the protection of personal data specifically; fourthly, whether a certain degree of care has been exercised when biometric data is obtained without prior knowledge or consent from the subject; and lastly, whether the impact upon a certain fundamental right is in proportion to the degree of security required.[351]

In addition, when considering biometrics in relation to laws regulating security measures and proof, legislators and the courts should keep in mind that the demand for security may reach a level at which biometrics becomes a legal necessity; also, specific legislation would then be required in respect of the management and protection of databases containing biometrical information; and further, that biometrics should not be awarded evidentiary value of a compelling nature.[352] Additionally, a pro-privacy provision should not be construed as an anti-biometric one, and public acceptance of biometric technologies will be greatly enhanced by appropriate legislation in respect thereof, particularly legislation which takes cognizance of the reluctance of individuals to forgo privacy for enhanced convenience, and, by necessary implication, the security of the captured data.[353]

---

[350] Network World Fusion *Message Queue* <http://www.nwfusion.com/archive/2000/97677_06-05-2000.html> (2000-07-18).

[351] Van Kralingen, Prins and Grijpink *Using your body as a key; legal aspects of biometrics* <http://www.biometrics.org> (2000-04-17). In the South African context, s 36 of Act 108 of 1996 (the limitation clause) would be the ultimate yardstick in this case.

[352] Van Kralingen, Prins and Grijpink *Using your body as a key; legal aspects of biometrics* <http://www.biometrics.org> (2000-04-17).

[353] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

The South African legislature recently considered the Electronic Communications and Transaction Bill,[354] which attempts to regulate issues pertaining to electronic commerce and related technologies. The Bill seeks to protect the consumer and privacy, as well as critical data. It provides for the creation of a voluntary regime for protection of personal information, which is deemed to include any information capable of identifying an individual. Only those data collectors who subscribe to a set of universally accepted data protection principles would be allowed access to this data. [355] The South African Law Commission is presently involved in the drafting of specific data protection legislation. Also, the Bill seeks to protect critical data, that is information which, if compromised, may endanger national security or the economic or social status quo.[356]

2.7 CONCLUSION

There exists a need for a solution to the problem of reliable personal identification, which becomes increasingly dire as geographically mobile individuals seek to affirm their identity as strangers in remote locations, and as the occurrence of fraud and cyber-crime grows.[357]

Biometrics offers the preferred secure solution to the problems posed by information society's electronic environment, as it is composed of unique physiological and/or behavioural traits of an individual which may be measured, stored and compared to establish and/or verify identity.

The decline in price and size of biometric sensors, as well as in the negative perception of biometrics as an encroachment on individual privacy, coupled with the realisation that

---

[354] The Electronic Communications and Transaction Bill of 2002.

[355] Chapter VIII of the Electronic Communications and Transaction Bill of 2002.

[356] Chapter IX of the Electronic Communications and Transaction Bill of 2002.

[357] Pankanti, Bolle and Jain *Biometrics: The Future of Identification* 2000 (February) Computer 46 49.

biometrics is an effective mechanism with which to combat fraud and in fact protect privacy, will result in this technology's application in practically all transactions requiring the authentication of personal identities.[358]

The storage of the template[359] is critical to the total effectiveness of the relevant technique. These templates may be stored within the biometric device itself, in the chip or magnetic strip of a plastic card, or in a central database, which database may be managed by a trusted third party, thereby providing enhanced security. Ultimately, the degree of acceptance and reliability of a security system hinges upon two factors, namely the methods used to protect the system, and the system's ability to identify abuses. However, the basic flaw of these biometric technologies is the lack of standards and independent testing.[360]

Performance and cost considerations of the biometric techniques are more favourable than those of manual security procedures, as these biometric technologies render traditional security technologies and methods redundant, since these are incapable of effectively combating fraud and protecting computer systems and networks to the extent which a biometric system can.[361]

Advantages offered by biometric systems are manifold, and include the procurement of true positive identification, the enhancement of customer service by the acceleration of transaction time, no teller or operating interpretation is required, the burden of

---

[358] Jain, Hong and Pankanti *Biometrics: Promising Frontiers for Emerging Identification Market* <http:///www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18).

[359] Which records the biometric measurement.

[360] Polemi *Review and Evaluation of Biometric Techniques for Identification and Authentication – Final Report* (summary) <http://www.cordis.lu/infosec/src/stud5fr.htm> (2000-08-17).

[361] Polemi *Review and Evaluation of Biometric Techniques for Identification and Authentication – Final Report* (summary) <http://www.cordis.lu/infosec/src/stud5fr.htm> (2000-08-17).

examination and decision is removed from the employee, and as a deterrent to fraud, both internal and external.[362]

As technology evolves, so biometric devices will improve, becoming more accurate and reliable. The combined use of biometrics and smart cards is alleged to be on an increased growth path in the future. It is predicted that standards will become available which will allow multiple reader technologies from several manufacturers to be implemented simultaneously within the same system.[363]

The need exists for fast and accurate authentication, and biometric systems can provide therefor. The biometrics industry has traditionally focused on government and law enforcement issues. However, a specific contemporary area of application is in the realm of Internet banking and e-commerce, problem areas where biometric technologies provide a natural and logical solution to fears about stolen credit card numbers and authentication validity, factors that continue to retard the growth of e-commerce.[364]

Transactions have largely become paperless, in consequence of the developments in the various fields of electronic technology, and the use of the traditional signature alone to identify and verify the signatory is no longer practicable, as no *corpus mechanicum* is present upon which the signature can be written and fixed. Consequently, biometric identification methods have been adopted to supplement/replace the traditional signature, provided that these electronic signatures identify and bind the signatory.

---

[362] Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24).

[363] Anon *Biometric Technology Overview* <http://www.biometricgroup.com/a_biometrics_42/biometric_technology_overview.asp> (2000-07-31).

[364] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 83.

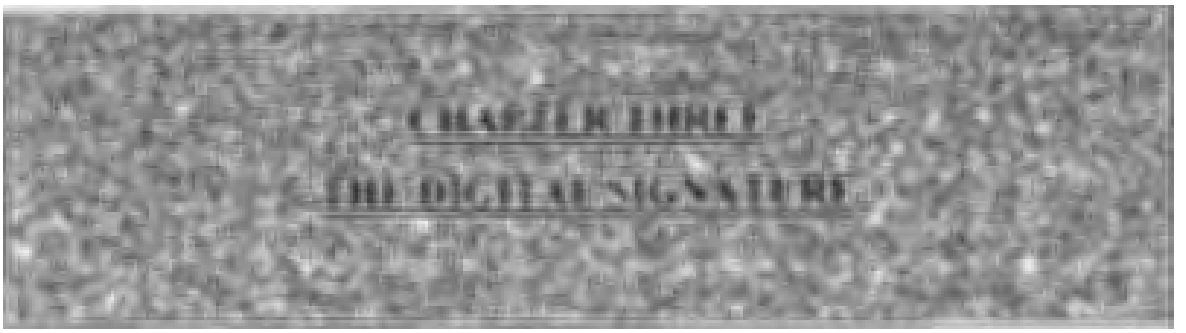
The Ministry of Communications, with the Electronic Communications and Transaction Bill,[365] failed to mandate the requirement in respect of a signature's form. Yet, the Bill[366] states "an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form". Thus, the prevailing legislative attitude seems to encourage reliance upon the function that a specific signature performs. Section 13(3) stipulates that parties to an electronic transaction which require an electronic signature (but no agreement exists *inter partes* regarding the type of electronic signature to be used) must employ an electronic signature which will identify the signatories, indicate their approval[367] of the information communicated and, considering the circumstances prevailing when the method was applied, be "as reliable as was appropriate for the purposes for which the information was communicated".[368]

[365] Bill of 2002.

[366] s 13(2).

[367] s 13(2)(a).

[368] s 13(2)(b).



3.1 INTRODUCTION

The advent of the Internet in recent years has caused a paradigm shift in the commercial, retail and banking environs. Computers and their related technology were introduced into these fields as a means by which to stem the ever-increasing flow of paper generated by such large-scale undertakings, and were initially to be found performing back-room operations. However, advances in technology allowed for the automation of these back-room processes, and computers were utilised more visibly, culminating in the present position of a practically automated undertaking, which requires minimal human interface.

The Internet has developed from its initial limited application[369] as a military and scientific tool to the present information and business-orientated medium, implementing electronic methods of doing business. Lourens[370] describes the Internet as "a world-wide virtual network of networks which connects thousands of computers and millions of users". Similarly, the Bill[371] defines the Internet as "an interconnected system of networks that connects computers around the world via TCP/IP[372] and includes future versions thereof".

---

[369] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 66 notes that the initial role of the Internet as we know it began in the 1960's as a United States Defence Department project to provide a decentralised, fail-safe connection for military researchers and computer defence networks that could function even in the event of war.

[370] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 66.

[371] Section 1 of the Electronic Communications and Transaction Bill of 2002.

[372] In terms of s 1 of the Electronic Communications and Transaction Bill of 2002, TCP/IP "means the Transmission Control Protocol Internet Protocol used by an information system to connect to the Internet".

The Internet, an open network, facilitates global interactive communication between parties who may not have an existing relationship. It has further increased the various methods of doing business and providing a platform from which businesses may reach customers and clients throughout the world.[373]

Electronic transactions are not new, as commercial concerns have been able to transact electronically within closed environments by means of Electronic Data Interchange (EDI), a process defined by Hill and Ferguson[374] as:

> "the movement of business data electronically between or within firms (including their agents or intermediaries) in a structured, computer-processable data format that permits data to be transferred without re-keying from a computer-supported business application in one location to a computer-supported business application in another location."

EDI is distinct from the Internet, in that EDI messages are generally formatted in a highly structured manner, involving predefined fields and contents, whereas the Internet involves *free-form* (or unstructured) communication. EDI requires minimal human intervention, whereas the Internet requires much human intervention[375] in the interpretation of information. The EDI assumes a continuing relationship between trade partners, whereas the Internet forgoes such an assumption, and focuses on casual relationships.

EDI trading partners are generally substantial commercial concerns, involved in a *business-to-business* commerce relationship, whereas the Internet is generally based upon a *business-to-consumer* relationship.[376]

---

[373] Lawack-Davids *Teaching Banking Law in the Technological Age* (1999) 2 Obiter 340 340-341. The World Wide Web (WWW) is the best known category of communication over the Internet.

[374] Hill and Ferguson *Electronic Data Interchange: A Definition and Perspective* <http://www.edigroup.com/journal/sample/html> as cited in Lourens *Electronic Commerce- the Law and is Consequences* 1998 (May) De Rebus 64 66.

[375] In respect of transacting via the Internet, the conscious acts of the sender and receiver are necessary.

[376] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 66.

Today, electronic commerce (e-commerce), in the narrow sense, amounts to the paperless exchange of business information, whereas in the broad sense, it includes commercial forms, such as EDI, electronic funds transfer (EFT), Internet trade and various commercial technologies.[377]

Timmers[378] defines e-commerce as:

> "(A)ny form of business transaction in which the parties interact electronically rather than by physical exchanges or by direct physical contact."

Consequently, e-commerce has developed from the closed network of business-to-business transactions between known parties to include a complex web of different activities in which any number of parties may partake, the vast majority of whom will never meet one another.

In future, the growth and development of the world's economies will become increasingly reliant upon e-commerce. As a result hereof, e-commerce is *de facto* becoming a new discipline of law,[379] and, consequently, the prior domination of paper-based transactions is being replaced by a move towards a paperless society.

Paper serves various functions in a paper-based transaction: it is a carrier of information and instructions, since the document lists the terms and conditions of a contract;

---

[377] Including bar coding, electronic imaging, facsimile, electronic mail (e-mail) and satellite communications.

[378] Timmers *Electronic Commerce – an Introduction* <http://www.cordis.lu/esprit/src/ecomint.htm> as cited in Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 65.

[379] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 27.

it provides a means of authentication; it performs an evidential function in that it enables a party to rely on the physical nature of the document as evidence; it may also perform a symbolic function by physically symbolising rights contained in the document; and it also serves various[380] formal legal functions.[381]

The distinctive characteristic of paper-based transactions is that it is embodied in a permanent form which must be transferred physically or delivered between the parties and cannot be easily altered without any trace of such alteration. The disadvantage, however, is that the movement of paper is time-consuming and troublesome.[382]

The advent of e-commerce has increasingly replaced standard paper-based transactions with electronic messages (thereby moving toward a paperless society) that are expressed in computer language and exist in a non-permanent form.[383] E-commerce, in contrast to paper-based transactions, "reduces costs...increases the speed of business transactions...increases reliability...is more accessible to international, global trade...[but] parties trading electronically do so in a world of legal uncertainty".[384]

Although the use of paper is being reduced, a signature is still required, albeit electronic or digital. Whatever the manner of affixing a 'signature' to a document, it must still achieve the core function of *binding the signatory to the contents of the document*, whether it is stored physically on paper, or electronically.[385]

---

[380] For example, the Alienation of Land Act 68 of 1981 requires alienations of land to be in writing and signed by the parties or by their agents, acting on their written authority; contracts of suretyship must be in writing and signed by the surety; executory donations must be in writing and signed by the donor or his/her agent acting on written authority.

[381] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 67.

[382] Meiring *The South African Payment System* (1996) 8 SA Merc LJ 164 165.

[383] Meiring *The South African Payment System* (1996) 8 SA Merc LJ 164 165.

[384] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 67.

[385] See Mallesons Stephen Jaques Solicitors *The PenOp Signature: An Australian Legal Perspective* <http://www.biometrics.org> (1999-09-12).

Because of the explosion in e-commerce, there is a demand from industry and users for a new type of signature to replace the traditional signature.[386] There is a need for the development of a mechanism whereby businesses may transmit electronic messages that carry legally binding signatures, which enable institutions to conduct transactions and enter binding contracts entirely by electronic means.

Cryptography, specifically public-key cryptography, provides for this and is regarded as the safest form of cryptography presently available.[387]

3.2 CRYPTOGRAPHY

Cryptology[388] is the multifaceted science and art of code making and code-breaking. It consists of separate yet connected fields: cryptography, the maintenance of secure communications; and cryptanalysis, the undermining of secure communications.[389]

Cryptography is the discipline of scrambling information to keep the message secret,[390] and it employs a secret key (or *cipher*), known only to the sender and authorized receiver, to respectively encode and decode the message.

The first known use of cryptography was the *Skytale* of the Spartans, 2500 years ago. The Spartans employed a wooden stick of a specific size, around which a strip of papyrus was firmly bound. The papyrus around the stick was inscribed with a message, then encoded by unwrapping the papyrus and sending it to the authorized receiver. To decode the

---

[386] See Section A: Chapter One: paragraph 1.3 for a discussion of the functions and uses which a traditional signature fulfills.

[387] Lawack-Davids *Teaching Banking Law in the Technological Age* (1999) 2 Obiter 340 352.

[388] Derived from the Greek *krypto logos*, literally the 'hidden word', or 'secret language'.

[389] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff.*

[390] Schwartau Information Warfare: Chaos on the Electronic Superhighway (1994) 148.

message, the papyrus had to be re-wrapped around a wooden stick of the same dimensions as the first. Ever since the Spartans, cryptography has experienced extensive attention during periods of war, specifically World Wars One and Two, and more recently during the Cold War. Today, cryptography is largely a field of government interest, specifically the monitoring of foreign communications and, under generally strict constitutional and judicial guidelines, the gathering of information in criminal investigations.[391]

Cryptography, in the present context, has three possible applications, namely communications, storage and digital signatures.

Communications that are vulnerable to interception in transit (such as communications over the Internet) require short-term protection. This may be achieved by means of encrypting the information prior to dispatching it, and decrypting it upon receipt. The sender's and authorised (or intended) receiver's systems must be capable of securely exchanging and co-ordinating the use of keys or *ciphers*, so as not to allow an unauthorised third party access to either the sender's or receiver's key. The storage of encrypted information requires secure storage, backup, retrieval keys and secure cryptographic mechanisms. This increases the security of the stored information, since to access the encrypted message, a specific key plus the cryptographic mechanism is required. This poses a problem, as the timeframe for securing the information must correspond with the technology of the relevant key and mechanism used to secure it. Cryptography also finds application in guaranteeing the authenticity and integrity of persons, documents and transactions by means of a digital signature. Cryptography enables the whole digitally signed message to be authenticated by means of including a checksum (or hash total) of the entire message in the digital signature prior to encryption.[392]

---

[391] Freeman *When Technology and Privacy Collide* (1995) 11:4 Information Strategy: The Executive's Journal 41*ff*.

[392] Parker Fighting Computer Crime: A New Framework for Protecting Information (1998) 374 –375.

Cryptography may exist in one of two forms: symmetric (secret-key cryptography) or asymmetric (public-key cryptography).

Symmetric key cryptography employs the same key to both encrypt and decrypt a message, which key must be known to both sender and receiver so as to ensure privacy. This key is sent in a separate transmission, rendering it susceptible to interception by unintended receivers.[393] This may be illustrated by A and B communicating using symmetric key cryptography: A and B both know and use the same secret key (A to encrypt the message, and B to decrypt the message) and, because only A and B have access to the secret key, they are confident in sending the encrypted message over an insecure network, such as the Internet. The interception of the encrypted message by H is of no consequence, since it is unintelligible to H, unless of course H has the secret key, or the technology to break the encrypted code.[394] Symmetric key cryptography has fundamental drawbacks, rendering it untenable as a means of transmitting sensitive information over insecure networks. Oei[395] notes that, for symmetric key cryptography to be of practical value, both sender and receiver must "generate, share and store the key in secret and in advance ... this is not realistic for electronic commerce...".[396] Oei opines that parties to an e-commerce transaction are not in a position to agree on and share a key prior to the transaction/communication, since e-commerce predominantly occurs between parties who do not have a pre-existing relationship. The utility of real time e-commercial exchanges is also undermined in the delay caused by requiring the transfer of keys prior to transacting. Further, communications over networks such as the Internet are inherently

---

[393] Anon *Protect Yourself: Secure Transactions* <http://www.learnthenet.com/english/html/07secur.htm> (2000-05-24); Hutchison and Saul *Fundamental Cryptographic Techniques for Electronic Commerce* 1999 (March) 16 Elektron 49 49.

[394] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[395] Oei *Primer on Cryptography* as cited in Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[396] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff* submits that Oei's arguments are equally applicable to non-commercial transactions.

insecure, and, consequently, agreeing on and transmitting the key within an insecure environment is dangerous, necessitating the initial use of an external, secure medium, the use of which will negate the various benefits afforded by on-line communication. Lastly, each proposed sender/receiver will be required to possess a separate key for each sender/receiver they wanted to communicate with. This poses expensive and unmanageable logistical and administrative procedures, open to potential abuse.[397]

Price[398] believes that these difficulties are "coextensive in that they all (*sic*) relate to the fundamental key management problem" of A and B agreeing on a "private key without revealing the private key" to H.

In 1976, Diffie and Hellman solved this key management problem with **asymmetric or public key encryption**, which increased "security and convenience since private keys never need to be transmitted or revealed to anyone".[399] Thus, the

> "receiver of data holds a secret key with which he can decipher but a different key is used by the sender to encipher and this can be made public without in any way compromising the system. This...asymmetric system [provides] secure communication only in one direction. To set up secure communication also in the other direction a second pair of keys is needed."[400]

Asymmetric (or public key) cryptography consequently involves two separate yet related keys (termed the 'key pair'), to encrypt and decrypt information. The public key is used to encrypt the message (and is available to the world at large), while the corresponding private key (which must be kept secret) is used to decrypt it.[401]

---

[397] Oei *Primer on Cryptography* as cited in Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[398] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[399] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[400] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[401] Hutchison and Saul *Fundamental Cryptographic Techniques for Electronic Commerce* 1999 (March) 16 Elektron 49 49.

Diffie and Hellman's public key encryption theory was applied in 1978 by Rivest, Shamir and Adleman (RSA) with the RSA system.[402] This system of asymmetric cryptography is based on the premise that two large prime numbers are easily multiplied, but to factorise their product is extremely difficult. As a result, the encryption key (the factorised product) may be published, and the primes (required to decrypt) which cannot be derived from the factorised product, are kept secret.[403]

Zimmermann published a computer program in 1991 based upon the RSA system, called 'Pretty Good Privacy' (or PGP).[404] PGP is fast, simple, and requires no prior knowledge of encryption. A key is created by a five-step process:

i. The key-generation process is initiated by a typed command.
ii. A pass phrase is entered that serves to protect the secret key while idle.
iii. The desired key size is selected.
iv. A user's identity (ID) is specified and associated with the key.
v. Text is typed at random, generating the key.

A pass phrase is used as it is longer than a password, and therefore more secure. This pass phrase enables access to the secret key, stored on the computer's hard drive. PGP measures the intervals between the user's keystrokes, and from these generates a large string of random numbers. The key is then generated from these numbers. PGP has *de facto* become the Internet's standard for public-key encryption.[405]

---

[402] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[403] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[404] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[405] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

In light of the aforegoing, it is evident that both approaches to contemporary cryptography have their own benefits and disadvantages. Symmetric cryptography encrypts data better and faster than asymmetric cryptography, whereas public key cryptography performs where symmetric cryptography cannot, for example, in the area of key management. Consequently, contemporary cryptography generally exists in a hybrid form of the two possible applications.[406]

Public key cryptography decreases the risk of private information being intercepted, in that it ensures the authenticity and integrity of on-line communications, thereby allowing parties to positively identify each other through digital signatures. Public key cryptography thus facilitates the implementation and application of digital signatures, on the basis that, for the creation of a digital signature, the process of encrypting and decrypting data for the purpose of confidentiality is merely reversed.[407]

The Electronic Communications and Transaction Bill of 2002 has acknowledged the application of cryptography within the South African electronic commerce environment, and defines a *cryptography product* as

> "any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring that such data can be accessed only by relevant persons; the authenticity and integrity of the data, or the source of the data can be correctly ascertained."[408]

Cryptography, therefore, facilitates the implementation and application of the digital signature, which ensures the authenticity and integrity of on-line communications, thereby allowing parties to identify each other through digital signatures. In the following

---

[406] In situations where two parties want to exchange data using the more efficient symmetric encryption, they usually use public key encryption first to pass a secure one-time-use symmetric key to both parties – Pleas *Certificates, Keys and Security Technology* <http://www.zdnet.co.za/pcmag/0707/tcert.html> (2000-02-08); Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95*ff*; Anon *Introduction to Cryptography* <http://www.ssh.fi/tech/crypto/intro.htm> (2000-06-10).

[407] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff*.

[408] Section 1 of the Electronic Communications and Transaction Bill of 2002.

section, the digital signature in its entirety will be discussed *vis-à-vis* its definition, requirements, application areas, etc.

3.3 THE DIGITAL SIGNATURE

3.3.1 DEFINITION

A digital signature is a series of bits sequentialised by a party who intends to sign an electronic document.[409] A mathematical function produces a value dependent upon the contents of a message, which is then appended to the message and encrypted by the sender's private key. The receiver decrypts the message by using the sender's public key, to wit: the receiver applies the same mathematical function to establish a further summary of the message. If the digital signature can be decrypted, and the summaries are identical, the receiver is certain of the sender's identity, as well as the integrity of the message.[410] Smuts[411] defines a digital signature as a term "used to indicate a particular authentication technique used to establish the origin of a message in order to settle disputes of what message [if any] was sent".

Thus, a digital signature amounts to a data item that is appended to a digitally encoded message, which can be used to determine the identity of the sender of a message, as well as the fact that the message has not been tampered with subsequent to receipt by the intended receiver.[412]

---

[409] Katz and Schwartz *Electronic Documents and Digital Signaturing: Changing the Way Business Is Conducted and Contracts Are Formed* <http://www.perkinscoie.com/resource/ecomm/edocs&digsig.htm> (2000-01-18).

[410] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 80.

[411] Smuts *A Survey of Information Authentication Techniques* (1994) 11 South African Computer Journal 84 84.

[412] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 28.

In the United States of America, Utah was the first state to adopt a comprehensive Bill that addressed the legal status of digital signatures. The Utah Digital Signature Act[413] defines a digital signature as

> "a transformation of a message using an asymmetric cryptosystem[414] such that a person having the initial message and the signer's public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer's public key; and (b) the message has been altered since the transformation was made."[415]

As alluded to above, digital signatures are a technology-specific form of electronic signatures. However, the terms are occasionally used interchangeably. The American state of Oregon's Electronic Signatures Act[416] defines a digital signature as a

> "...type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) whether the transformation was created using the private key that corresponds to the signer's public key; (b) whether the initial message has been altered since the transformation was made...A 'key pair' is a private key and it's corresponding public key in an asymmetric cryptosystem, under which the public key verifies a digital signature the private key creates. An 'asymmetric cryptosystem' is an algorithm or series of algorithms which provide a secure key pair."

The Electronic Signatures in Global and National Commerce Act (E-Sign Act)[417] of the United States of America defines an *electronic signature* in broad and general terms as "an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record".[418] Dorney[419] notes that the E-Sign Act was purposely drafted to be technology

---

[413] Utah Code Ann. S46-3-101 *et seq.*

[414] Also known as *public key cryptosystem* which is a method of encrypting and decrypting information that relies on two input keys: a public key that is freely disseminated to the world and a private key that is known only to its holder.

[415] McBride Baker & Coles *Table 3: Definitions of the Term "Digital Signature" in Enacted Legislation* <http://www.mbc.com/ecommerce/legis/table03.html> (2000-04-14).

[416] Electronic Signatures Act, Oregon Revised Statutes s192.825 *et seq* (1997 OR HB 3046).

[417] Act 15 USCA § 7001.

[418] Section 106 (5) of Act 15 USCA § 7001.

[419] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

neutral, so that a variety of technologies may function as an electronic signature, such as passwords, smart cards, digital signatures and biometrics.

In a similar vein, the South African Electronic Communications and Transaction Bill seemingly strives to facilitate the legal recognition of electronic signatures,[420] and advanced electronic signatures, as a secure form of electronic signing. The Bill[421] defines an *electronic signature* in broad and general terms as "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature". [422] An *advanced electronic signature* is defined as an " electronic signature which results from a process which has been accredited by the Authority ..."[423] and includes cryptographic products such as digital signatures.

The Electronic Communications and Transaction Bill appears to have been drafted purposely in broad terms so as to be technology neutral, seemingly as the legislators were unable to predict future standards, and yet were unwilling to be prescriptive, apparently leaving it to commerce to determine these future standards.

Thus, by omitting to specifically define a digital signature, both the E-Sign Act and the Bill have, particularly in light of the apparent reluctance to be prescriptive, adopted a position of technological neutrality, thereby facilitating numerous existing and future methods and versions of signing digitally.

---

[420] Section 13 of the Electronic Communications and Transaction Bill of 2002.

[421] Section 1 of the Electronic Communications and Transaction Bill of 2002.

[422] Section 1 of the Electronic Communications and Transaction Bill of 2002.

[423] Section 1 of the Electronic Communications and Transaction Bill of 2002. The Authority, in terms of s 1, refers to "for purposes of – (*a*) Chapter VI, means the Director- General acting as the Accreditation Authority as provided for in that Chapter; (*b*) Chapter X, means the .za domain name space Authority established by that Chapter..."

In essence, a digital signature is unique for every document, and it electronically seals the document to which it is appended,[424] so that not even the party who drew up the document can amend it without such an amendment being detected. Consequently, the receiver can rely on the origin, authenticity and integrity of the document.[425]

3.3.2 REQUIREMENTS FOR THE DIGITAL SIGNATURE

By the application of cryptography, a digital signature can be established which meets the following requirements:[426]

i. the totality of the message/data is signed for;
ii. secret information therein remains known to the sender only;
iii. public information therein is made available to the authorised receiver.

Thus, a digital signature will (by necessary implication) be different for each individual message so signed, as it exists as a function for each individual message to which it is appended in its entirety. Also, a party may be in possession of various digital signatures, each to be used in different circumstances,[427] depending on the degree of security required.[428]

---

[424] Wilde *Legally Binding E-Documents Move Closer to Reality* (2000) 776 Information Week 120 *ff.*

[425] Price *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95 *ff.*

[426] Von Solms *Digital Signatures for Secure Data* 1989 (January) 85 South African Journal of Science 22 22.

[427] For example, on-line contracting and banking require more protection than basic contact information.

[428] Macavinta *Signature Struggle* (1999) 5:7 Intelligence 26 27.

3.3.3 THE APPLICATION OF THE DIGITAL SIGNATURE

After a digital signature has been created for a specific message by the sender's cryptography software,[429] it is appended to this message and becomes a part of the message upon encryption. It is then transmitted to the authorised receiver, who decrypts the message by applying the sender's public key to the message, rendering the message readable, and open to scrutiny in respect of possible interception by unauthorised third parties.

A practical example of this is where A sends an **arbitrary** message to B. A applies a hash algorithm to the message so as to create a fingerprint of the message. A then encrypts the hash value with his private key (which may be protected by a password on the computer or, preferably, stored on a smart card) and transmits the encrypted hash value (A's digital signature) to B. B applies the same hash algorithm to fingerprint the message he received from A, and then decrypts the hash value he got from A using A's public key. Should the two hash values correspond, B can be satisfied that the message is authentic, and that A's digital signature is genuine.

If the entire message is of a **sensitive** nature (for example, if it contains a credit card number), A could use the same process to encrypt the entire message.[430] Thus, with his private key, A may place his digital signature on the entire electronic document and attached data by means of applying a hash algorithm to the entire message, or just to the attached data, as the circumstances require. The hash algorithm compresses the data into a few lines termed a 'message digest', from which it is impossible to return to the original data. A's private key then encrypts the message and/or data, thereby creating A's digital signature. This digital signature is then appended to the document, rendering all the hashed data signed. A then e-mails the document to B, who decrypts A's digital signature by applying A's public key to it, and converting the signature back to the message digest.

[429] Such as Zimmermann's PGP, referred to above.

[430] Prosise *Digital Signatures: How They Work* <http://www.zdnet.com/pcmag/issues/1507/pcmag0090.htm> (2000-04-17).

If the message digest produced by B corresponds with that of A, B is sure that it was A who signed the document (as only A has the associated private key), and that the data signed by A has not been tampered with by a third party.[431]

The use of a digital signature therefore generally encompasses two procedures,[432] namely:

i. **Digital signature creation**. The digital signature is created from the hash result, which itself is created from, and unique to, both the signed message and the private key. The hash result's level of security is relative to the negligible possibility that the same digital signature may be created by the combination of any other message and private key.
ii. **Digital signature verification**. The procedure of authenticating the digital signature by referring to the original message and the given public key, thus ascertaining whether the digital signature was created for the same message, using the private key which corresponds with the referenced public key.

The creation and verification of a digital signature therefore achieves the essential effects desired of a signature for various legal purposes,[433] these being:

i. **Signer authentication**. The digital signature attributes the message to the digital signer if a public and private key pair is associated with this digital signer. The digital signature is only susceptible to forgery if the private key is compromised.
ii. **Message authentication**. The signed message is identified by the digital signature more certainly and precisely than a traditional signature.

---

[431] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 27.

[432] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

[433] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

iii. **Affirmative act**. The use of the signer's private key in the creation of a digital signature may be equated with the 'ceremonial' function of informing the receiver that the signer intends consummating a transaction with legal consequences.

iv. **Efficiency**. The processes involved in the creation and verification of a digital signature establish a high degree of assurance that the digital signature is genuine. In contrast to the tedious and labour intensive methods of checking specimen signature cards, digital signatures provide this high degree of assurance without requiring excessive additional resources for their processing.

3.4 CERTIFICATION AUTHORITIES

A digital signature must be connected to a specific party to be of any real value. This connection is achieved by way of accredited certification authorities, which issue and manage digital certificates pertaining to a specific party's digital signature.[434]

A certification authority associates a key pair with a specific party by issuing a certificate in the form of an electronic record. This electronic record lists the party's public key as the 'subject' of the certificate and confirms that the party (the *subscriber*) identified on the certificate is the holder of the corresponding private key. The main function of the certificate is thus to bind the key pair with the subscriber.[435]

Digital certificates are issued by certification authorities.[436] These certificates may exist as signature certificates or key exchange certificates. A signature certificate includes

[434] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 52. Various legislatures have recognized and made provision for digital signatures in their statutes, for example the USA's Government Paperwork Elimination Act requires state agencies to post more forms online, to be signed with digital signatures. In Ontario, Canada, all 11 million residents were issued with digital certificates. Singapore's government oversees and licenses all certification authorities that issue digital signatures.

[435] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

[436] The South African Certification Authority (SACA) is contracted to, among others, the South African Reserve Bank, Absa, Old Mutual and Eskom for the issuing of digital certificates. SACA is a South African provider of digital authentication products and services for secure Internet access and e-commerce.

certain base information, a public key and a digital signature. The digital signature is verified by the public key, whereupon the digital signature verifies the validity of the digital certificate, and confirms that it has not been tampered with. A key exchange certificate is employed to encrypt information, for example, a key exchange certificate is used by parties to encrypt information sent to a certification authority.[437]

The certification authority serves to create digital signatures, to determine policy requirements regarding the qualification criteria for a digital certificate, to maintain security, and to publish a list of those digital certificates that have been revoked, suspended, or have expired.[438] A certification authority thus issues digital certificates and vouches for the validity and accuracy of the information contained in the certificate, thereby staking its reputation on the fact that steps have been taken to verify the information in the digital certificate.[439] Each individual subscriber to such a service thus has various obligations or duties, as per the American Bar Association:[440]

i. All material representations made by the subscriber to a certification authority, including all information known to the subscriber and represented in the certificate, must be accurate to the best of the subscriber's knowledge and belief,

---

[437] Pleas *Certificates, Keys and Security Technology* <http://www.zdnet.co.za/pcmag/0707/tcert.html> (2000-02-08).

[438] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 28. For example, if a subscriber misrepresents his/her identity to the certification authority, the certificate will prove unreliable. If the subscriber loses control of the private key (known as "compromise" of the private key), the certificate then proves to be unreliable and the certification authority, with/without the subscriber's request, may suspend (temporary invalidate) or revoke (permanently invalidate) the certificate.

[439] Pleas *Certificates, Keys and Security Technology* <http://www.zdnet.co.za/pcmag/0707/tcert.html> (2000-02-08). Macavinta *Signature Struggle* (1999) 5:7 Intelligence 26 27 notes that the legal liability of certification authorities as offline entities has been addressed by various nations, such as the Italian law's onus on the certification authority to confirm a customer's identity, and the position in Japan where a receiver loses liability protection if he/she fails to verify the authenticity of a key with a certification authority, and a certification authority is rendered liable should they leak a password or misidentify a customer. *Verisign*, a leading provider of digital certificates and signatures, offers warranties to customers for economic loss sustained as a result of theft, corruption or misuse of a digital signature and/or certificate.

[440] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

regardless of whether such representations are confirmed by the certification authority.

ii. A subscriber who provides an otherwise unpublished certificate to a relying party must disclose that fact to the certification authority.

iii. If the foreseeable effect would be to induce or allow reliance upon a certificate that is invalid because the subscriber has not accepted it, the subscriber must not knowingly create digital signatures using a private key corresponding to any public key listed in such certificate.

This approach necessitates the subscriber to "correct affirmative misrepresentations, ambiguities, vagueness resulting in error, and omissions that are misleading to a certification authority issuing a certificate to the subscriber".[441] The subscriber is further duty-bound to notify the certification authority should any information in the certificate be incorrect. The subscriber owes these duties to both the certification authority and to any person relying on the digital signature in question. Such a subscriber may also not contractually exclude his duty to reflect material facts, although, by agreement with the certification authority, certain details of this duty may be varied and remedies provided for non-compliance with the above duties. Also, the acceptance of a certificate by the subscriber from the certification authority renders the subscriber liable to the certification authority for any misrepresentations, on the assumption that the issuing certification authority confirmed the accuracy of the representations by the subscriber in the certificate.[442]

---

[441] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

[442] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14). Macavinta *Signature Struggle* (1999) 5:7 Intelligence 26 27 suggests that an obligation of due care should be imposed on the subscriber which relates to the protection of his/her private key.

To facilitate the identification of a public key and its specific subscriber, the digital certificate may be published in a repository.[443] Retrieval from such a repository may be done automatically by having the verification program enquire directly from the repository to procure the desired certificates.[444]

Assuming that A and B have complied with their certification authorities requirements for positive identification, and have already received their digital certificates and have these certificates stored on their hard drives, then whenever A emails B, a copy of A's certificate is automatically appended to the email, allowing B to check A's certificate and thereby ensuring that A's public key actually belongs to A. B may, in addition, consult his/her chosen certification authority's revocation list to determine if A's digital certificate has perhaps been revoked or suspended. Consequently, interference by a third party should be easily ascertainable on the premise that the certification authority positively identified A before providing him with a digital certificate. No laborious efforts are required on the part of either A or B, since their software executes all the required commands, thus B merely clicks his mouse, and A's identity is either confirmed or refuted immediately.[445]

Consequently, a digital certificate issued by a certification authority is a form of identification that can be used to authenticate the identities of participants in e-commerce, authorise certain transactions over an open network, provide proof of messages sent over the Internet, and to verify the integrity of information transmitted over the Internet.[446]

---

[443] Repositories amount to on-line databases of certificates and other information available for retrieval and use in verifying digital signatures.

[444] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

[445] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 28.

[446] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 52.

The Electronic Communications and Transaction Bill[447] empowers an accreditation authority to establish authentication service providers. An authentication service provider is defined as a party whose authentication products or services have been either accredited or recognized by this accreditation authority. The Bill further defines authentication products or services as " products or services designed to identify the holder of an electronic signature to other persons". [448]

Thus, accreditation implies the recognition of an authentication product or service by the accreditation authority,[449] which authority exists in the person of the Director-General of the Department of Communications,[450] who has a discretion to monitor the functioning and systems of the authentication service provider, so as to ensure that the provider meets the requirements and discharges the obligations stipulated in the Bill, specifically those contained in section 39.[451]

The Director-General further has the discretion to "temporarily suspend or revoke the accreditation of an authentication product or service ...".[452] The Bill compels the Director-General to keep a database to which the public has access, which database will contain authentication products or services either accredited or recogn... those accreditations or recognitions which have been suspended or revoked; and any other prescribed information.[453] The Director-General may suspend or revoke an accreditation should such Director-General be of the opinion that the authentication service provider

[447] Electronic Communications and Transaction Bill of 2002.

[448] Section 1 of Chapter 1 of the Electronic Communications and Transaction Bill of 2002.

[449] Section 34 of the Electronic Communications and Transaction Bill of 2002.

[450] Section 35(1) of the Electronic Communications and Transaction Bill of 2002.

[451] Section 37(1)(a) of the Electronic Communications and Transaction Bill of 2002.

[452] Section 37(1)(b) of the Electronic Communications and Transaction Bill of 2002.

[453] Section 37(2)(a)-(c) of the Electronic Communications and Transaction Bill of 2002.

has failed or ceases to meet any of the requirements, conditions or restrictions subject to which either accreditation was granted, or recognition given.[454]

The Bill permits the Director-General to "accredit authentication products and services in support of advanced electronic signatures",[455] and the applicant for such accreditation is compelled to apply to the Director-General in the prescribed manner, supply the prescribed information, and pay the prescribed non-refundable fee.[456] The Minister of Communications may, by way of notice in the Government Gazette, and subject to such other conditions as the Minister may determine, recognise the accreditation given to any authentication service provider, or its authentication products or services, in any foreign jurisdiction.[457]

A criterion stipulated for accreditation is that the Director-General is not permitted to endow accreditation status to authentication products or services unless he/she:

> "is satisfied that an electronic signature to which such authentication products or services relate is (a) 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."[458]

The Bill thus endeavors to create an accreditation authority within the Department of Communications, facilitative of voluntary accreditation of electronic signature technologies in accordance with minimum standards. Once accredited, such advanced electronic signatures will enable reliance upon their authenticity.

---

[454] Section 40 of the Electronic Communications and Transaction Bill of 2002.

[455] Section 38(1) of the Electronic Communications and Transaction Bill of 2002.

[456] Section 38(2) of the Electronic Communications and Transaction Bill of 2002.

[457] Section 41(1) of the Electronic Communications and Transaction Bill of 2002.

[458] Section 39(a)-(d) of the Electronic Communications and Transaction Bill of 2002.

3.5 APPLICATIONS OF THE DIGITAL SIGNATURE

It is apparent that the Internet has advanced from its initial existence as a mere communicative medium to an all-embracing commercial medium. Various ancillary aspects of this new commercial medium have yet to be brought up to speed, specifically security concerns. Rather than attempting to secure and regulate the Internet itself, digital signatures secure transactions transmitted over the Internet. This allows e-commerce to benefit from both the openness of the Internet and the protection of a closed network.[459]

Digital signatures provide Internet users with a means to prove their identity when they send correspondence (e-mail), make payment over the Internet (such as buying a product) or conclude a contract.

3.5.1 SECURING E-MAIL

A digital signature appended to an e-mail message gives the receiver confirmation of the sender's identity, and, in addition, verifies that the message has not been tampered with since being dispatched by the sender. Such a signature and its valid digital certificate negates the sender repudiating or refuting that it was indeed him/her who sent the message, thus endowing legal or contractual implications and consequences to the transmission of such a message and signature.

The process for signing e-mail messages is, firstly, to create a hash value for the contents of the message. This hash value is then signed by the sender with his/her private key. Next, the digital signature and digital certificate (which includes the sender's public key) are appended to the message. Upon receipt, the receiver uses the sender's public key to verify the certificate and to calculate the hash value for the message content. The receiver

[459] Katz and Schwartz *Electronic Documents and Digital Signaturing: Changing the Way Business Is Conducted and Contracts Are Formed* <http://www.perkinscoie.com/resource/ecomm/edocs&digsig.htm> (2000-01-18).

then compares this hash value with the attached hash value. Should these values be equal, the integrity of the message is certain.[460]

Digital certificates allow messages to be encrypted with the receiver's public key. This effectively obscures the transmitted message, and only by the receiver applying his private key is the message rendered decrypted and hence readable.[461]

Thus it is apparent that a digital signature, which involves the use of public-key cryptography, is a form of an electronic signature which identifies the sender/signatory and verifies the said identity.

3.5.2 ON-LINE PAYMENTS

3.5.2.1 INTRODUCTION

Payments over the Internet generally require the use of credit cards and smart cards. This occasions certain serious concerns in respect of the transmission of sensitive financial information over an open network as there remains a lack of trust by the purchasing public in the security and reliability of the various systems. This position necessitated the creation of a more secure, anonymous and reliable method of effecting such payments.[462]

---

[460] Pleas *Certificates, Keys and Security Technology* <http://www.zdnet.co.za/pcmag/0707/tcert.html> (2000-02-08).

[461] Pleas *Certificates, Keys and Security Technology* <http://www.zdnet.co.za/pcmag/0707/tcert.html> (2000-02-08).

[462] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 53.

A security standard referred to as SET[463] (Secure Electronic Transaction) encrypts the card number on the vendor's servers, which only banks and credit card companies can view.[464] The role of SET[465] is to ensure that confidential data (such as signature information) is not visibly transmitted over the Internet, but rather encrypted using public key cryptography.[466]

SET essentially consists of four facets, these being, firstly, a certification application (which creates digital certificates as well as cryptographic keys); secondly, a secure payment gateway from a merchant's site to the financial institution authorised to effect payment; thirdly, a so-called *e-wallet*[467] which contains the buyers information (including credit card details); and fourthly, a point of sale device which connects the merchant's site to the buyer's *e-wallet* and manages the exchange of digital certificates prior to initiating payment.[468]

3.5.2.2 PAYMENT BY CREDIT CARD OVER THE INTERNET

Credit cards are internationally accepted as a means of payment. They are presently more frequently used[469] to effect on-line payment than any other payment system. Effecting payment over the Internet by means of a credit card is achieved by the cardholder instructing the issuer of that card to pay the retailer/service provider on behalf of the cardholder. This occurs as per the conditions of use of that specific card, that is that the issuer is entitled to debit the cardholder's account with the sum that the issuer is validly

---

[463] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 84 notes that SET was developed in 1996 by Visa and MasterCard to provide confidentiality of information, payment integrity and identity authentication.

[464] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 73.

[465] SET is supported by Netscape Navigator and Microsoft Explorer.

[466] Anon *Security in Internet* <http://www.signlist.com/> (1999-09-15).

[467] For added security, users may have a password for their *e-wallets*.

[468] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 84.

[469] In relation to the other accepted means of payment over the Internet, namely debit and charge cards, which utilise the same methods and procedures as outlined above in respect of credit cards.

instructed to pay.[470] This instruction by the cardholder to the issuer occurs by the cardholder providing his card number details to the retailer/service provider, on the understanding that the retailer/service provider is entitled to transmit this provided information plus details of the payment to the issuer.[471] The advantage of this payment mechanism is that internationally recognised credit card issuers[472] are involved, facilitating the purchase of goods and the procurement of services from practically anywhere.

The disadvantages of this system are threefold: firstly, a limited number of participants in such a system is brought about by the restrictions on access to credit cards and the fact that relatively few people have access to the Internet; secondly, transaction costs occasioned by the possibility that the issuer may incur costs as a result of the card holder not paying the resultant debit balance; and thirdly, the opportunity for a third party to intercept the transmitted credit card number creates serious security concerns.[473]

These security concerns have largely been dealt with by the implementation of SET,[474] as mentioned above. The SET protocol exists as a closed trading system, regulated by contract between cardholders, card issuers and acceptors. SET introduced the use of dual digital signatures,[475] created over two related messages. The resultant signature links the two messages and may be used to validate either message. This occurs without requiring a copy of the other message, since only a message digest of the absent message is needed,

---

[470] Lawack *Electronic Innovations in the Payment Card Industry* (1998) 10 SA Merc LJ 233 233-234.

[471] Lawack *Electronic Innovations in the Payment Card Industry* (1998) 10 SA Merc LJ 233 233-234.

[472] Such as Visa and MasterCard.

[473] Lawack *Electronic Innovations in the Payment Card Industry* (1998) 10 SA Merc LJ 233 233-234.

[474] Anon *Security in Internet* <http://www.signlist.com/> (1999-09-15) notes that numerous institutions such as Microsoft, IBM, Netscape, Visa, MasterCard, American Express and various banks have agreed on and implemented SET.

[475] An extension of the application of the dual signature is the compound signature, created over multiple messages. The resulting signature may be used to validate any of the messages within the group, as well as linking the messages to one another. See further Hutchison and Saul *Fundamental Cryptographic Techniques for Electronic Commerce* 1999 (March) 16 Elektron 49 49.

thereby maintaining secure communications and/or transactions. Thus, A can send one message to B and another message to C and still maintain a link between the two messages through the signature. Consequently, B and C can agree that the signed messages that they received from A have a common source and purpose.[476]

In practice, the retailer/service provider receives a token from the purchaser. This token is then presented to the bank in return for the actual credit card number. Upon presentation, the bank either confirms or refutes the validity of the token, based upon the dual signature described above. If confirmed, an authorization number is then sent to the merchant. The merchant is assured that the card is good and the transaction is then completed. The consumer receives a digital receipt for the transaction.[477] SET thus provides the means with which to conduct secure card-based business over the open network of the Internet, while simultaneously reducing fraud. However, to be truly effective, it requires an international "standard cross-platform integration".[478]

In essence, SET protects purchasers by existing as a mechanism for the direct transmission of their credit card numbers to the credit card issuer for verification and billing without being visible to the seller.[479]

Therefore public key cryptography can be used to ensure the privacy of a customer's card and PIN numbers, and provides for non-repudiability. However, as a result of central processing, a complete record will be maintained by the card issuer of the individual's spending patterns, which may be considered an unacceptable invasion of privacy, as

---

[476] Hutchison and Saul *Fundamental Cryptographic Techniques for Electronic Commerce* 1999 (March) 16 Elektron 49 49.

[477] Lawack-Davids *Teaching Banking Law in the Technological Age* (1999) 2 Obiter 340 350

[478] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 84.

[479] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 53.

people would prefer a payment mechanism where their spending would be entirely anonymous and untraceable on the Internet.[480]

3.5.2.3 PAYMENT BY ELECTRONIC CASH OVER THE INTERNET

An alternative to payment over the Internet by means of a card payment[481] is the use of *true electronic money* or e-cash, pioneered in 1997 by Visa (in collaboration with the Bank of America), with *Visa Cash* chip cards,[482] initially aimed at relatively small purchases. These Visa Cash chip cards are typically plastic cards containing a memory chip which stores a specific amount of money, ascertainable by inserting the chip card into a Visa merchant's card reader. In cyberspace, the Visa merchant's card reader is replaced by Visa Secure Electronic Commerce, which utilizes the SET mechanisms (outlined above), in conjunction with the software of choice in place on the buyer's computer.[483]

To affect a purchase over the Internet using a chip card, the buyer selects the item/s to purchase, and a sample invoice is displayed on the buyer's monitor, prompting payment. The buyer then opens his/her *e-wallet* and removes his/her Visa card. The SET mechanisms pre-existing on the buyer's computer, exchanges information and digital signatures with the seller or merchant, verifying the exchanged information through the use of digital signatures. The buyer is confirmed as an accredited participant in e-commerce by Visa (or his/her specific financial institution), while the seller is certified to be registered with a bank and able to securely deal with the buyer's transaction. Public key cryptography then encrypts the buyer's payment details, which are transmitted to the

---

[480] Smith *et al* Internet Law and Regulation (1996) 110.

[481] Smart cards can also be used. A digital signature can be stored on the smart card, thus preventing it from being hacked as the signature itself is not stored on the computer. However, as with cheques being forged, so too do cards stand the risk of been stolen and misused. Smart cards that can be swiped through the decoding scanner, have tremendous flexibility as well as encryption capabilities.

[482] See Visa on the Web <http://www.visa.com> (2000-11-01).

[483] Lawack-Davids *Teaching Banking Law in the Technological Age* (1999) 2 Obiter 340 351.

seller. The seller then forwards this encrypted payment information to the payment authorisation system, such as Visa or MasterCard. Should the transaction be authorised, the seller then transmits confirmation to the buyer of the success of his/her transaction, and the purchased item/s are dispatched for delivery.[484]

Digicash BV, a Dutch corporation, established another method of making payments electronically, termed *E-cash*,[485] which parallels Visa's SET system. E-cash requires the purchase from a bank of tokens to a specific value in a specific currency. These tokens or E-cash are stored on the buyer's computer. To affect a transaction, the buyer deposits the required value of tokens into an on-line E-cash account, thereby verifying their validity.

Each individual token is subjected to a high-level encryption, and payment may be made and authenticated without disclosing the identity of the buyer or seller. Consequently, a third party cannot deposit the token and receive the monetary value thereof. The seller, however, redeems these tokens by depositing them with participating banks in his/her own country. E-cash thus enables trade without leaving a paper trail, as no identification details are transmitted over the Internet.

In South Africa, however, the use of E-cash could give rise to a number of legal issues, including whether E-cash could be recognized as legal tender in terms of the South African Reserve Bank Act 90 of 1989. Bagraim submits that it would not fall into the current definition and therefore would have to be dealt with by legislation.[486]

---

[484] Lawack-Davids *Teaching Banking Law in the Technological Age* (1999) 2 Obiter 340 352.

[485] Several banks such as Mark Twain Bank (USA), EUnet (Finland), Deutsche Bank (Germany) and Norske Bank (Norway) will exchange E-cash for hard currency.

[486] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 53. In South Africa, Standard Bank's Blue Bean is a form of E-cash.

3.5.2.4 INTERNATIONAL FUND TRANSFERS

The *wire transfer* method of making payments internationally was facilitated by the establishment of SWIFT,[487] a non-profit, co-operative organisation,[488] formed in 1973 by several European, Canadian and American financial institutions to affect electronic fund transfers amongst banks and other financial institutions on an international scale.[489]

SWIFT essentially transmits financial data, from the basis of a computerised global telecommunications network. It is a message switching network which "operates a global data processing system for transmitting financial messages over dedicated lines among its members and other connected users", and thereby "provide(s) a secure message service in which the messages are encoded in a standard format and encrypted for security reasons".[490]

SWIFT users are connected to a national centre in their specific location. The user transmits a message in one of the standard SWIFT formats to the national centre, where it is converted and encrypted and then sent to a main centre for processing, whereupon it is sent to the national centre in the recipient financial institution's country, and then to the recipient financial institution.[491]

SWIFT maintains a high level of security in that messages are authenticated by being automatically acknowledged upon receipt by a SWIFT terminal. Further, a recipient is prevented from acting on a message until acknowledgement has been confirmed. In addition, SWIFT keeps a log of all messages for a period of four months from the date the message was dispatched, and the message itself is encrypted using the Data

---

[487] Society for Worldwide Interbank Financial Telecommunications.

[488] Located in Brussels, and initiated in terms of Belgian law.

[489] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 115-118.

[490] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 115-118.

[491] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 115-118.

Encryption Standard, thereby rendering the decoding of messages practically impossible.[492]

3.5.2.5 CONCLUSION

In the prevailing commercial environment, business concerns which persist in utilising paper-based procedures risk losing control, as well as their competitive edge. In South Africa, the majority of commercial concerns have embraced the advantages offered by encryption and other forms of security, so as to eliminate, or at least reduce, the serious threat posed by modern technology to secure on-line transactions.

Contemporary steps taken by South African banks to increase the security of online transactions include 128 bit encryption technology, which scrambles the transaction, rendering an intercepted transaction unintelligible; log-in name and password use, which may include PINs; time-outs, whereby the link between bank and customer is discontinued if not used for a predetermined period of time; and ceiling limitations are placed upon certain transactions, as specified by the user.[493]

It is thus apparent that, in the field of electronic payments, the digital signature serves to identify a signatory, associate that signatory with the contents of the transaction and, simultaneously, provides for a high level of security.

---

[492] Lawack Electronic Payment Systems in the South African Law LLM Dissertation (1997) 115-118.

[493] Buys *Internet Banking: The Risks and Benefits* 2000 (June) De Rebus 30 31. In addition to these security steps, institutions such as Nedbank employ *firewalls* which impose a barrier between a sensitive internal network and the Internet – information obtained from Ms D. Moodaley at Port Elizabeth Nedbank (Rink Street branch).

3.5.3 INTERNET CONTRACTS

3.5.3.1 INTRODUCTION

The Internet may be employed as a medium for conducting pre-contractual negotiations, as well as for concluding binding contracts.[494] In order to enable commercial participants to place the requisite reliance upon the resultant electronic documents, common rules to authenticate and confirm the integrity of documents and their signatories are essential.[495] Yet, to date, no Internet law exists to cater specifically for e-commerce transactions.[496]

As the law in respect of documents is generally linked to the physical nature of paper itself, so the movement away from paper-based commerce toward electronic commerce is aimed at the substitution of paper without giving up the functions paper serves. This is the point at which various legal questions arise, as the *lacunae* engendered by electronic commerce flow specifically from the symbolic and evidentiary roles of paper. These *lacunae* include proving the authenticity of information, authenticating the status of digital signatures, the point at which offer and acceptance becomes effective, compliance with existing laws requiring certain information to be *written* and *signed*, privacy concerns, the admissibility of computer data as evidence and contract formation.[497]

Thus, the need exists for a viable and practical body of rules and regulations which facilitate the legal enforceability of agreements and transactions entered into

---

[494] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 139.

[495] Katz and Schwartz *Electronic Documents and Digital Signaturing: Changing the Way Business Is Conducted and Contracts Are Formed* <http://www.perkinscoie.com/resource/ecomm/edocs&digsig.htm> (2000-01-18).

[496] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 139.

[497] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 67.

electronically, since the advent of e-commerce has introduced concepts *contra* prevailing legal assumptions and placed "the current body of law under some stress".[498]

At this stage, the basic common law and statutory rules of the law of contract are applicable to electronic contracts, and, consequently the validity and enforceability of Internet contracts under our current law is uncertain.[499] However the Bill[500] endeavors to eliminate much of this uncertainty.

3.5.3.2 LEGAL REQUIREMENTS FOR INTERNET CONTRACTS

A contract has been defined as an *agreement* that is, or is intended to be, legally enforceable.[501] The basic requirements of a contract comprise contractual capacity (such capacity may be absent or limited), possibility of performance (should the objective of the contract be impossible, the contract is rendered void), lawfulness (an illegal contract is void) and formalities, which will be addressed hereunder.[502]

Generally, the validity of a contract is not dependant on compliance with any formalities since, where no formalities are required in respect of writing by statute or by parties themselves, an agreement arises when two or more parties consent to be contractually bound to each other,[503] be this agreement written, verbal or partly written and partly verbal.[504]

---

[498] Katz and Schwartz *Electronic Documents and Digital Signaturing: Changing the Way Business Is Conducted and Contracts Are Formed* <http://www.perkinscoie.com/resource/ecomm/edocs&digsig.htm> (2000-01-18).

[499] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 139; Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 50.

[500] The Electronic Communications and Transaction Bill of 2002.

[501] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 139.

[502] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 139.

[503] *Reid Bros (South Africa) Ltd v Fischer Bearings Co Ltd* 1943 AD 232 241.

[504] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

However, there are certain exceptions to the rule that no formalities are necessary for a contract. If both parties, or one of them, or a statute requires writing and/or signature,[505] those requirements must, generally, be met for the contract to be valid.[506] The legislature, in a number of statutes, has prescribed various formalities for different categories of agreements.[507]

Before the arrival of electronic media, the law of the United States of America seldom questioned the medium upon which the *writing* was presented, and their courts accepted telexes and telegrams[508] as *writings*. Consequently, their courts regarded the existence of a *writing* confirmed if the recipient acquired a piece of paper as a result of the communication.[509] Such a *writing* was believed to more accurately memorialise an agreement than the memory of a witness and, accordingly, the value of a *signed writing* was to be found in its reliability, and was thus required for those transactions where the parties had more to gain from lying. In light of the aforegoing, it is apparent that the concerns about the reliability of electronic messages lay in the ability to delete and/or amend words and phrases post-delivery, but prior to the message being printed out in a finalised form.[510]

---

[505] Kerr The Principles of the Law of Contract (1998) 136 notes that "in most instances when the legislature requires reduction to writing there is no *vinculium iuris* until a written contract has been signed".

[506] *Goldblatt v Fremantle* 1920 AD 123 128.

[507] Examples of statutes which impose formalities on specific forms of contracts are the Alienation of Land Act 68 of 1981, the Credit Agreements Act 75 of 1980, the Property Timesharing Control Act 75 of 1983, Formalities in Respect of Leases of Land Act 18 of 1969, the Rent Control Act 80 of 1976, Participation Bonds Act 65 of 1981, Security by Means of Moveable Property Act 57 of 1993, Copyright Act 98 of 1979 and Trade Marks Act 194 of 1993.

[508] Both telexes and telegrams involve a series of electrical impulses prior to the production of a paper copy.

[509] In the case of *Howey v Whipple* 48 N.H. 487 (1869) the court stated that "when a contract is (concluded) by telegraph, rather than by a hand-written letter, it does not make any difference that in the one case common red ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office".

[510] In relation to telexes, telegrams and facsimiles, only electronic messages are not printed in a format that is identical to that initially transmitted, that is the hard copy.

The application of digital signature technology to an electronic message greatly reduces the possibility of post-delivery deletion and/or amendments, since the checksum value would not match if the message had been altered after transmission. Thus digital signatures provide electronic documents with the same immutability as traditional paper-based writings.[511]

The Electronic Communications and Transaction Bill of 2002 provides a broad recognition for data messages, by stating that information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message,[512] or it is referred to in such a data message.[513] A data message is defined as

> "data generated, sent, received or stored by electronic means and includes-
> *(a)* voice, where the voice is used in an automated transaction;
> *(b)* a web page; and
> *(c)* a stored record."[514]

Further, the Bill holds that information in an agreement is regarded as being incorporated into a data message if such information is referred to in such a way that a reasonable person will have noticed the reference to it, and it is in an accessible and readable form which can be stored and retrieved by the other party.[515]

The position where a law requires a document or information to be reduced to writing is regarded as complied with provided that such document or information is in the form of a data message, and accessible in a manner usable for subsequent reference.[516]

---

[511] Theofanos and Phillips *Digital Signatures: Signing and Notarizing Electronic Forms* 1994 (April) Records Management Quarterly 18.

[512] s 11 (1) of the Electronic Communications and Transaction Bill of 2002.

[513] s 11 (2) of the Electronic Communications and Transaction Bill of 2002.

[514] Section 1 of the Electronic Communication and Transaction Bill of 2002.

[515] Section 11 (3)(a)-(b) of the Electronic Communications and Transaction Bill of 2002.

[516] Section 12 of the Electronic Communications and Transaction Bill of 2002.

Where a law requires a document or information to be rendered in its original form, such document or information may be regarded as original should it comply with the requirement of section 14 of the Bill. Section 14 holds that:

> " (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if
>
> *(a)* the integrity of the information from time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
>
> *(b)* that information is capable of being displayed or produced to the person to whom it is to be presented.
>
> (2) For the purposes of subsection 1 (*a*) the integrity must be assessed-
>
> *(a)* by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
>
> *(b)* in the light of the purpose for which the information was generated; and
>
> *(c)* having regard to all other relevant circumstances."

The Bill also confers due evidential weight to data messages, subject to certain consideration set out in section 15 (2) and (3) of the Bill, and such a data message will not be inadmissible in legal proceedings merely on the grounds of it being a data message, per section 15(1)(a).

Further, provision is made for the legal recognition of electronic signatures,[517] and advanced electronic signatures, as a secure form of electronic signing.

Where a signature is required by law, the requirement will only be met if an advanced electronic signature is used, and it is expressly stated that an electronic signature is not without legal effect merely in consequence of its electronic form.[518]

Where an electronic signature is required, and there is no agreement by the parties to the electronic transaction in respect of the type of electronic signature to be used, then any method will be acceptable, on condition that it identifies the person, indicates approval, and is a reliable method for the purposes for which the information is communicated.[519]

---

[517] Section 13 of the Electronic Communications and Transaction Bill of 2002.

[518] Section 13 (2) of the Electronic Communications and Transaction Bill of 2002.

[519] Section 13 of the Electronic Communications and Transaction Bill of 2002.

Therefore, from the South African perspective, the specific requirements regarding the terms *signature, original* and *writing* per the Bill lend support to the opinion that our law will emphasise the substance of a signature over the form thereof. Additionally, a digital signature supplied by an accredited authority includes all the common law *inducia* required to perform the same function and possess the same recognition and evidential weight as traditional manuscript signatures.[520]

The main impetus of the Bill is to provide that electronic signatures, specifically advanced electronic signatures (digital signatures being a form), comply with the legal requirements that a contract be in *writing* and *signed.*

3.5.3.3 THE CONCLUSION OF INTERNET CONTRACTS (*CYBERCONTRACTS*)

A contract under South African law is generally deemed concluded once an offer made by one party is accepted by another party, and, as no South African Internet law yet exists, the basic rules of the law of contract continue to be applicable to contracts concluded electronically.[521]

3.5.3.3.1 THE OFFER

In terms of the South African common law of contract, a contract is concluded once one party accepts an offer made by another party, and informs the other party that the offer has been accepted. For a valid offer to be complete, it must include definite terms of performance, and it must be made with the intention of it being accepted by the other party.[522]

---

[520] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 26.

[521] The vast majority of online contracts entail simple retail purchases, and for the present time, it seems improbable that major commercial deals will be concluded purely online, since, as a result of the prevailing legal uncertainty, these should be supplemented with a final written and signed contract.

[522] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 140; Kerr The Principles of the Law of Contract (1998) 61.

The question of a valid offer is of relevance when assessing where and when an electronic contract has come into being, since it must be determined if the seller's website, web page or e-mail (the medium soliciting the transaction) amounts to an *offer* in terms of South African contract law.[523]

By responding to the retailer's intention to sell, an offer is made by the potential buyer to the retailer, who may then either accept the offer and conclude a contract of sale, or refuse the offer. Thus, on the Internet, the placing of an order by a buyer in response to an advertisement by a retailer does not amount to a contract, but merely to an offer to do business.[524]

A contract will only come into being when this order is received, accepted and processed by the retailer, and is generally manifested by the retailer sending the purchased item to the buyer. Prior to this acceptance by the retailer, no legal relationship exists between retailer and buyer. Consequently, an advertisement does not constitute an *offer*, but merely an *invitation to do business*, as per the decision in *Crawley v Rex*:[525]

> "The mere fact that a tradesman advertises the price at which he sells goods, does not appear to me to be an offer to any member of the public to enter the shop and purchase goods, nor do I think that a contract is constituted with any member of the public that comes in and tenders the price mentioned in the advertisement ... it seems to me to amount simply to an announcement of his intention to sell at the price he advertises. There is nothing so far I know which obliges a tradesman to sell to any customer who chooses to present himself in the shop ..."

It is therefore apparent from case law that a contract comes into existence when the advertiser accepts the offer to buy tendered by the purchaser.

However, declarations contained in advertisements or similar expressions of intention could result in an offer, depending on the specific wording. In this case, a valid offer will

---

[523] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18). It must be noted that in South African law, contracts come into being upon acceptance of the offer.

[524] *Bird v Summerville and Another* 1960 4 SA 395 (N) 401.

[525] 1909 TS 1106-1108.

be established with any party who accepts the offer in the predetermined manner.[526] A contemporary example hereof is the amalgamation of advertising and selling evident on a commercial website which combines *shop displays* and *shop selling*. It follows that if a reasonable person will be convinced that a statement constitutes an offer, then a court will be likely to reach the same conclusion. Bagraim warns that website owners must exercise caution by ensuring that "the advertising material on their website does not itself constitute an offer but an invitation to do business".[527]

3.5.3.3.2. THE ACCEPTANCE

For a contract to be binding, there must exist an *acceptance* of an offer, which acceptance is to be manifest in an unequivocal act, which engenders the logical inference of the offeree's acceptance.[528] An offeror may even determine the mode of acceptance, which must then be complied with by the offeree.[529]

In *R v Nel*[530] it was held that the requirement of communicating the acceptance may be impliedly waived[531] by means of requiring the offeree to signify acceptance by a specific act. Thus, the offeror may prescribe that the offer be accepted tacitly by means of the offeree performing some act, which act evidences the offeree's acceptance of the terms of

[526] *Carlill v Carbolic Smoke Ball Company* [1893] 1 QB 256 (CA).

[527] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 50. In addition, website owners should state that they will not be bound by any communications from third parties, but will inform them should the communication be accepted.

[528] *Collen v Rietfontein Engineering Works* 1948 1 SA 413 (A) 429-430; *Reid Bros (South Africa) Ltd v Fisher Bearings Co Ltd* 1943 AD 232-241; Kerr The Principles of the Law of Contract (1998) 94.

[529] *Laws v Rutherfurd* (1924) AD 261 261-264; *Driftwood Properties (Pty) Ltd v McLean* 1971 3 SA 591 (A).

[530] (1921) AD 339-352.

[531] Or expressly done away with.

the contract, and, consequently, this act amounts to the equivalent in law of the signing of a contract.[532]

In the light of an offer and an acceptance over the Internet, a contract is created as soon as the offeror becomes aware that the offeree has accepted the offer, which approach is known in South African law as the *information theory*.

Section 21(a) of the Electronic Communications and Transaction Bill[533] permits an electronic agent to perform a legally required act for the formation of an agreement, and such an agreement may be concluded between two or more electronic agents.[534] A party employing an electronic agent to contract will be bound by the terms of the contract,[535] provided that these terms are capable of being reviewed by a natural person prior to concluding the contract.[536] No contract will be concluded should a natural person, while employing the electronic agent of another, make a material error while formulating a data message, and either:

i. the electronic agent failed to give this natural person an option to correct or prevent this error, or
ii. that natural person either advises the other party of the error as soon as is possible, or
iii. takes reasonable steps to return any performance received, or fails to receive, alternately fails to use any material benefit or value received.[537]

---

[532] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[533] The Electronic Communications and Transaction Bill of 2002.

[534] Section 21 (b) of the Electronic Communications and Transaction Bill of 2002.

[535] Section 21 (c) of the Electronic Communications and Transaction Bill of 2002.

[536] Section 21 (d) of the Electronic Communications and Transaction Bill of 2002.

[537] Section 21 (e)(i)-(iv) of the Electronic Communications and Transaction Bill of 2002.

An Internet website may be so designed that an electronic agent[538] accepts an offer on behalf of the website's owner. Such a facility encumbers the website owner, in that this owner must "ensure that the terms of the offer submitted are the terms of the offer expected" and offers which have been adjusted are identified and denied submission.[539] The *mouse-click-on-icon* mechanism of acceptance is the prevailing norm employed by webvendors to bind purchasers to standard terms of contracts,[540]and this mechanism may exist in one of two forms, the *shrink-wrap agreement* or the *click-wrap agreement.*

3.5.3.3.2.1 THE SHRINK-WRAP AGREEMENT

Standard form contracts[541] negate both the signature requirement as well as the possibility of negotiation, thus the offeree merely either accepts or refuses the offer. Should it be proved that the purchaser read the document, the purchaser is bound by the terms thereof. If it cannot be proved that the purchaser has read the document, and the vendor/supplier has done that which is reasonably necessary or possible in the circumstances to make the purchaser aware of the terms contained in or referred to in the document, or the document itself suffices to make the reasonable purchaser aware of its contents, the purchaser will be bound by these terms. Various computer programmes' licence terms are *shrink-wrapped*, or contained within software packaging which may only be accepted by *unwrapping* the software. Pistorius[542] maintains that South African law recognizes the

---

[538] A computer programme that operates without direct human supervision and initiates or answers electronic messages, generally by means of generating automated responses to electronic messages which it receives. See further Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 51.

[539] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 51.

[540] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[541] These are also referred to as *contracts of adhesion*, and date back to the twelfth century. Contemporary standard form contracts are to be found in practically all economic undertakings, from insurance contracts to bills of lading, and are employed in circumstances where a vendor or supplier presents the customer with a document containing or referring to terms upon which the vendor/supplier is prepared to do business, and which does not require the customer's signature, but may provide proof that the customer is bound to its terms.

[542] Pistorius *The Rights of the User of a Computer Program and the Legality of Shrink-Wrap Licences* (1991) 3 SA Merc LJ 57; Pistorius *The Enforceability of Shrink-Wrap Agreements in South Africa* (1993) 1 SA Merc LJ 1.

enforceability of these *shrink-wrap agreements*. This position is desirable as certain business activities would become inconvenienced if each customer were required to supply their signature. Consequently, it is necessary to substitute the principle of *caveat subscriptor*,[543] while still incorporating the parole evidence rule.[544]

As a result of the construction of the separation of the *shrink-wrap* agreement and of the transaction of sale, whether the purchaser realises the terms of the *shrink-wrap* agreement before or after the sale is concluded is of no relevance.[545] But, should the retailer fail to draw the purchaser's notice to the terms contained in the *shrink-wrap* agreement, non-disclosure may render the contract voidable.[546]

3.5.3.3.2.2 THE CLICK-WRAP AGREEMENT

Developed specifically for e-commerce, *click-wrap* agreements are displayed on the web vendor's web page, setting out the terms and conditions of a contract of sale.[547] Should the user wish to purchase an item from this website, instructions direct the user to *click* certain icons, thereby indicating acceptance of the said terms of the contract. This set-up seeks to protect the proprietary rights of web vendors and to limit their liability.[548]

---

[543] By appending his signature to a document, the signatory acknowledges the terms of the document, regardless of whether he/she actually read those terms or not.

[544] Generally, no evidence other than the terms of the agreement are admissible to prove the true intention of the parties.

[545] All sales involving *shrink-wrap* agreements may be cancelled if the user refuses the terms of the *shrink-wrap* agreement.

[546] See *Gollach & Gomperts (1967) (Pty) Ltd v Universal Mills & Produce Co (Pty) Ltd and Others* 1978 1 SA 914 (A) 924B: "A man cannot be said to conceal what he is not bound to reveal, suppress what he is under no duty to express, or keep back what he is not required to put forward".

[547] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[548] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 52 notes that the content of these agreements generally include copyright and trademark notices, disclaimers regarding the accuracy or reliability of transmitted information, limitations on liability, and waivers of proprietary rights by those who submit copyrighted material.

Click-wrap agreements are distinct from *shrink-wrap* agreements in that the purchaser is made aware of the contractual terms prior to the purchase.[549] The web vendor may be required to maintain an electronic audit, which will be used to prove that the purchaser actually agreed to the terms of the contract.[550]

The Directive on Electronic Commerce, formulated for the European Union, expressly refers to electronic contracts in which the purchaser indicates acceptance by *clicking on an icon*, thereby tacitly referring to *click-wrap* agreements.[551]

Pistorius[552]opines that *click-wrap* agreements are integral to e-commerce and that, like *shrink-wrap* agreements, they are fully enforceable under South African law.[553]

3.5.3.4 THE TIME AND PLACE WHERE INTERNET CONTRACTS COME INTO EFFECT

The way in which an acceptance of an offer is communicated by the offeree to the offeror influences both the time and place of when and where the contract is deemed concluded.

As a *lacuna* exits in respect of the time and place of concluding an electronic contract, general principles of the South African law of contract must be applicable until such time as either case law or statute regulates this area of law.

---

[549] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[550] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[551] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[552] Pistorius *The Rights of the User of a Computer Program and the Legality of Shrink-Wrap Licences* (1991) 3 SA Merc LJ 57; Pistorius *The Enforceability of Shrink-Wrap Agreements in South Africa* (1993) 1 SA Merc LJ 1.

[553] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

In terms of the *expedition theory*, a contract is deemed concluded as soon as the letter containing the acceptance is posted,[554] and in terms of the *information theory*, contracts concluded over the telephone are regarded as analogous to contracts concluded in the presence of the parties, that is, a contract is deemed concluded as soon as the offeror is made aware of the acceptance.[555]

It is noted in *Entores Ltd v Miles Far East Corporation*[556] and in *S v Henckert*[557] that where parties are in instantaneous and direct communication with each other, such as by means of telephone or telex, the expedition theory will not apply, rather the information theory will be applicable. Various views are held by writers as to which theory is applicable to contracts concluded over the Internet or by means of e-mail.

South African jurists hold divergent views in respect of which theory to apply when determining the time the contract comes into effect.

Schlechtriem[558] opines that the expedition theory is applicable in respect of contracts concluded using an electronic mail box or an email address.

---

[554] Applicable in circumstances where postal communications are employed, and where no particular method of acceptance is specified. See *Cape Explosives Works Ltd v South African Oil & Fat Industries Ltd* 1 1921 CPD 244; *Kergeulen Sealing & Whaling Co Ltd v Commissioner for Inland Revenue* 1939 AD 487; *Yates v Dolton* 1938 EDL 177.

[555] *S v Henckert* 1981 3 SA 445 (A) 451A-B.

[556] [1958] 2 ALL ER 493 (CA).

[557] 1981 3 SA 445 (A).

[558] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

Kerr[559] and Van der Merwe[560] believe that contracts concluded by electronic data interchange (EDI) and other forms of instantaneous communication are subject to the information theory, that is the moment the offeror becomes aware of the acceptance.

Pistorius holds that the effect of the medium employed should be decisive, and not the type of machine used to cause the effect, and thus neither the expedition nor the information theory should slavishly be used to determine when and where a contract has been concluded over the Internet.[561]

The case of *Kergeulen Sealing & Whaling Co Ltd v Commissioner for Inland Revenue*[562] largely settled the question of the *place* where the contract comes into effect by determining the *locus contractus* as the place where the last step was taken that is required to effect the contract's completion.[563]

The Electronic Communications and Transaction Bill of 2002 concurs with Kerr and Van der Merwe, since it states that an agreement concluded between parties by means of data messages is concluded at the time when, and at the place where, the acceptance of the offer was received or came to the intention of the offeror, hence the *information theory*.[564]

---

559 Kerr The Principles of the Law of Contract (1998) 110.

560 Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 141.

561 Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

562 1939 AD 487.

563 Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18) notes undecidedly that the *locus contractus* might be the place where offeror is made aware that the offeree has accepted the contract, or where the letter containing the acceptance was posted. Where the contract was made also determines where it comes into effect.

564 Section 23 (2) of the Electronic Communications and Transaction Bill of 2002.

The Bill further provides for the time and place of communications, dispatch and receipt in terms similar to the provisions set out by the UNCITRAL (United Nations Commission for International Trade Law) Model Law. Concisely, the UNCITRAL Model Law[565] provides that, unless otherwise agreed, the time of dispatch of an electronic communication is when it enters a single information system outside the control of the sender. The time of receipt of the electronic communication is the time when it enters the information system of the recipient, if and when such information system had been designated by the recipient (when the recipient did not indicate an information system for receipt, the communication will be deemed to have been received only when the communication comes to the attention of the recipient). The place of dispatch of the communication is the place where the sender has its place of business and the place of receipt is the place where the recipient has its place of business.

The Bill states in very similar terms, in that a data message must be regarded as having been sent when it enters an information system outside the control of the originator, alternatively, should the originator and addressee be within the same information system, when it is *capable of being retrieved* by the addressee.[566] A data message is regarded as been received when the complete data message enters an information system either designated or used by the addressee.[567] Also, a data message is regarded as been sent from the originator's usual place of business and received at the addressee's usual place of business.[568]

---

[565] Article 15.

[566] Section 24 (a) of the Electronic Communications and Transaction Bill of 2002.

[567] Section 24 (b) of the Electronic Communications and Transaction Bill of 2002.

[568] Section 24 (c) of the Electronic Communications and Transaction Bill of 2002.

3.5.3.5 PROVING THE EXISTENCE AND TERMS OF INTERNET CONTRACTS

Together with the growth of electronic commerce have grown concerns over the verification of electronic documents, unauthorized transactions, information privacy and the interception and corruption of messages. The use of digital signatures has, to an extent, allayed these concerns by identifying and authenticating the source of the electronic transmission, thereby ensuring a high level of authenticity and integrity of electronic communications.[569]

There exists, however, no universal definition of a *signature*, and, in South African law, no generally accepted definition of a *signature* [570] is to be found, let alone that of a *digital signature*.

The conventional method of appending one's signature to a contract, so as to indicate one's acceptance thereof, is untenable when transacting over the Internet. Van der Merwe[571] argues that, since a *mark* in South African law means any mark created with the intention of it being regarded as a binding signature, then a party who clicks a specific icon to indicate his acceptance of an online contract's terms and conditions may be construed as *signing* the online contract by clicking the icon which indicates his acceptance.

Van der Merwe[572] notes further that, should the party who clicked the icon indicating acceptance deny that he clicked on the icon, the other party "would have an almost impossible task proving the opposite".

---

[569] Bagraim *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50 52.

[570] In South African law, a *signature* refers to any *mark* made by a party intending this *mark* to be construed as a *signature*. See further Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 141.

[571] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 141.

[572] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 141-142.

Proving that such a contract has been concluded over the Internet thus presents both a legal and a practical problem.

A witness is generally called to prove a document's authenticity. Such witnesses may include the drafter of the document, the executor thereof, or a signatory thereto, or a party who witnessed the drafting or signing of the document, as well as a handwriting expert, and a party who can identify the drafter's signature.[573]

The Computer Evidence Act[574] states that, in civil proceedings, an affidavit verifying the authenticity of a computer printout may be submitted as evidence in proof of any fact recorded in this printout, if direct oral evidence would be admissible to prove this fact or printout.[575] The Criminal Procedure Act[576] defines the term *document* as inclusive of any recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded or stored.[577] It is submitted that the provisions of the Computer Evidence Act are archaic and narrow, and the provisions of the Criminal Procedure Act suffer by reason of their qualified applicability to proof of entries in accounting records and the documentation of banks.

Consequently, in the move from the traditional paper-based approach to the prevailing electronic orientation, practically all the guarantees of authenticity and reliability have been lost, and, as Van der Merwe[578] proposes, satisfactory substitutes must be found. The introduction of accredited certification authorities may prove a satisfactory substitute as they will provide such guarantees.

---

[573] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 142.

[574] Act 57 of 1983.

[575] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 142.

[576] Act 51 of 1977.

[577] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 142.

[578] Van der Merwe *Cybercontracts* (1998) 6:4 Juta's Business Law 138 142.

The Electronic Communications and Transaction Bill of 2002 seeks to remedy this position, as it makes provision for the removal of legal barriers to electronic transacting by facilitating their admissibility in legal proceedings, and according these transactions with evidential weight.[579] Further, in respect of advanced electronic signatures, the Bill makes provision for the establishment of accreditation authorities, which will enable parties to rely upon the authenticity of these signatures.[580] However, this does not preclude any party from adducing evidence of the non-validity of an advanced electronic signature.[581]

3.5.3.6 JURISDICTION

Before the "age of the Internet", the jurisdiction of the various courts could be ascertained with a high degree of certainty.[582] However, as web vendors may now conclude contracts internationally over the Internet, it is crucial for jurisdiction to be determined, preferably by means of inserting *choice of law* clauses into their contracts, which clauses predetermine jurisdiction in the event of a dispute arising.

In terms of section 95 of the Bill,[583] the jurisdiction of South African courts is established in respect of an offence committed under the envisaged Act.

---

[579] Section 15 of the Electronic Communications and Transaction Bill of 2002. See also s 17 of this Bill which deals with the production of the document or information in court.

[580] s 38 (1) and s 39 (1) of the Electronic Communications and Transaction Bill of 2002.

[581] s 13 (5)(b) of the Electronic Communications and Transaction Bill of 2002.

[582] Van der Merwe (1998) 6:4 *Cybercontracts* Juta's Business Law 138 138.

[583] The Electronic Communications and Transaction Bill of 2002.

3.5.3.6 FUTURISTIC DISPUTE RESOLUTION

With such development in technology, an inevitable consequence will be the explosion in disputes arising from online contracts. Resolving disputes through the same medium in which transactions were concluded is a very real option.

The growth of e-commerce and its ancillary fields requires of the law of South Africa to adapt and develop to meet the inescapable consequence of cyber-disputes arising from Internet contracting.

Hurter[584] notes that while formal litigation is presently used to resolve disputes, the issues of costs, efficiency and time may soon render our prevailing concept of litigation redundant. Hurter[585] quotes Schreiner and Kuner[586] who state that "while parties prepare for a rapid expansion in Internet-related commerce they continue to rely on dispute resolution procedures more suited to a country road than to the *Information Highway*".

It is thus apparent that our existing legal apparatus needs to adapt and develop from the "traditional cumbersome litigation procedures", and to recognize the need to [redacted]ing our arbitration legislation "up to speed with (our times and) the rest of the international community".[587]

---

[584] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 200.

[585] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 200.

[586] Schreiner and Kuner *Dispute Resolution in International Electronic Commerce* (1998) 14 Journal of International Arbitration 5 5.

[587] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 200.

Hurter notes further that the

> "very nature of the Internet compels the use of alternative dispute resolution ... (it) subverts traditional legal rules and concepts ... (yet it) exists in *virtual space* and nullifies the legal concept that noteworthy legal actions are ... location bound ... (the) effect is the total dissolution of geographical boundaries, national borders and communication barriers ... (it) is an instant and direct link, integrating diverse cultures, countries, individuals, groups and organizations."[588]

By resolving their disputes through the same medium by which they do business, an incentive is established for parties to agree upon a system of dispute resolution, thereby promoting party autonomy,[589] enhancing privacy and confidentiality, disposing of disputes more quickly,[590] while maintaining good relationships[591] between the parties in dispute. Perhaps most importantly of all, costs will probably be a fraction of what they would be if formal litigation were employed.[592]

Yet, despite the aforegoing advantages, online arbitration's single largest obstacle seems to be the absence of "an alternative dispute-resolution culture".[593] Further, arbitrators may not be able to deal with the "demands that online arbitration will present" and the "accountability of arbitrators to participants and to the community at large also poses a problem".[594] Also, online arbitration may not always be less expensive than its present

---

[588] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 202.

[589] The implication being that parties will be able to choose the method of determining their dispute.

[590] The Internet is accessible 24 hours a day, 7 days a week, and thus negates potential time zone problems, court delays, postponements, etc.

[591] Since the inherent adversarial nature of civil litigation will be avoided.

[592] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 203.

[593] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 205. Hurter notes that this is specifically applicable in the South African context since "the general conservatism of the legal fraternity, the lack of knowledge of alternative dispute resolution on the part of lawyers and the public, as well as a basic resistance to change may lead to the non-adoption of online arbitration for many years to come".

[594] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 205.

counterpart, and issues of security and confidentiality will need to be addressed. Finally, a formal infrastructure which creates "rules and institutions to facilitate online arbitration" needs to be established.[595]

Examples of online arbitration already in existence are the Cybertribunal of the University of Montreal, the Online Ombuds Office[596] of the University of Massachusetts, and the Virtual Magistrate[597] of the Villanova Law School and the American Arbitration Association.

The arbitration procedure in any of the above online arbitration facilities may loosely correspond with the following WIPO[598] procedure:[599]

i. the arbitration website is accessed;
ii. a request is electronically filed with the WIPO Arbitration Centre, including the statement of facts and legal arguments;
iii. the respondent transmits a response, together with a defence (and counterclaim if applicable);
iv. the parties elect an arbitrator (if the parties fail to agree, the Centre appoints one);
v. the Centre stipulates the place of arbitration;
vi. the matter is heard by the arbitrator and a decision is reached;
vii. a final award is made, from which no appeal is available.

---

[595] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 205.

[596] See the website <http://128.119.27/centre/ombuds/default/htm>.

[597] Hailed as an early attempt by the Internet community to police itself, and illustrative of the various issues which impacted upon the development and evolution of online dispute resolution - Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 205.

[598] The World Intellectual Property Organization Online Dispute Resolution Process, which focuses primarily on challenges to domain name registration.

[599] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 206-207.

In terms of the American Bar Association (ABA), if a digital signature were to be involved in a dispute, it would be "rebuttably presumed that:

(1) the information listed in a valid certificate is correct, except for unverified subscriber information,
(2) a digital signature verified by reference to the public key listed in a valid certificate is the digital signature of the subscriber listed in that certificate,
(3) the message associated with a verified digital signature has not been altered from its original form,
(4) a certificate of a certification authority, which is either published or made available to the subscriber listed in it, is issued by that certification authority, and
(5) a digital signature was created before it was time-stamped[600] by a trustworthy system."[601]

The ABA submits that the burden of proof is on the party challenging the authenticity of the digital signature and that a court should thereupon hold the digitally signed evidence to have been *prima facie* authenticated and admissible, unless evidence is introduced to the contrary. Therefore the presumption that a verified digital signature is the subscriber's is analogous to the presumption that a paper signature is genuine.

With the velocity of development and the pace of technological advancement, an inescapable consequence will be an explosion in the number of disputes arising from contracts concluded online. Online dispute resolution could therefore possibly provide the solution by way of voluntary arbitration, and decentralised rulemaking may provide for the cost-effective, expeditious and legitimate resolution of disputes. Section 73 of the Bill[602] provides for alternative dispute resolution. However, the section fails to confront matters in detail, and seemingly exclusively provides for domain name disputes, while noting that due regard must be had to existing international precedent.[603]

---

[600] This allows the verifier to determine reliably whether the digital signature was created during the operational period of the digital signature, stated in the certificate, which is a condition upon verifiability of a digital signature. Moreover it allows a determination as to whether it was created before or after the filing of a revocation or suspension of the certificate as well as provides increased assurance of non-repudiatability.

[601] American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg.html> (2000-08-14).

[602] The Electronic Communications and Transaction Bill of 2002.

[603] Section 73 (2) of the Electronic Communications and Transaction Bill of 2002.

3.5.3.8 CONCLUSION

From the above, it is clear that a contract may validly be concluded by means of an offer and acceptance through the Internet. The contractual approach is, however, limited in that it cannot overcome many of the legal obstacles which might result from mandatory provisions of statutory or case law.[604]

Christianson and Mostert[605] are of the opinion that

> "in the absence of specific requirements with regard to *signature*, *original* and/or *writing*.... the law will have regard to the substance rather than the form of a signature (and).... that digital signatures provided by respectable certification authorities contain all the *indicia* required to fulfil the same function and to enjoy the same recognition and evidential weight (or even more) than traditional signatures."

The Bill echoes the above sentiment providing for the legal recognition of online contracts and their concomitant aspects, such as the requirements of signature, original and writing, the time and place of concluding contracts, jurisdiction and so on.

However, as no South African Internet law yet exists, the basic rules of the law of contract are applicable to contracts concluded electronically. Hofman *et al* [606]submit that it would be presumptuous to assume that technological change will fundamentally alter the way we contract. It will rather adapt to accommodate cyberspace. It is foreseen that the contract law that will emerge, will not be new or revolutionary, but rather old principles that will be applied to the new environment and will over time "evolve to further reflect cyberspace's idiosyncrasies".[607]

---

[604] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 68.

[605] Christianson and Mostert *Digital Signatures* 2000 (May) De Rebus 26 26.

[606] Hofman Johnston Handa and Morgan Cyberlaw: A Guide for South Africans Doing Business Online (1999) 118.

[607] Hofman *et al* Cyberlaw: A Guide for South Africans Doing Business Online (1999) 118.

Until legislature addresses and provides uniform standards to solve these legal issues, the regulation of electronic commerce takes place on an *ad hoc* basis. Until then, parties intending to transact in cyberspace should supplement their electronic agreement with a final written document.

3.6 MISCELLANEOUS APPLICATIONS

Aside and apart from the mainstream applications of the digital signature, there are numerous miscellaneous application areas. As divergent fields and disciplines encounter digital signatures and recognise the potential impact of electronic speed and user-friendly interface in combination with leading security technologies, so the manifold uses and applications of digital signatures continues to grow.

In the United States, certain police precincts request search warrants from a judge directly via computer, thereby establishing the world's first *electronic warrant interchange*. The investigating officer selects the suspected crime from the menu provided by the computer program, the state code for that crime is then displayed on the monitor with blanks to be filled in according to the circumstances of the particular offence. Upon completion, and should sufficient evidence exist to satisfy the judge, a warrant is authorised by the judge and police officer signing signature pads.[608]

Elections are also being evaluated as a target for minimalising paperwork via the introduction of ballots that are digitally signed over the Internet, thereby drastically reducing costs and manpower both in establishing the infrastructure, and in the laborious counting process.[609]

Employee travel claims may be completed on computer, then e-mailed to the company's accounts office for filing and processing, the filing of which over the Internet would not

[608] Stanford *Getting Arrest Warrants Via Computer* <http://www.cnn.com> (1998-03-05).

[609] Hall and Thibodeau *Calif. Signs Up Digital Signature Provider* 1999 (October) 33:42 Computerworld 12*ff*.

be possible without digital signatures, thereby reducing possible fraudulent claims and delays in payment.[610]

The United States' Internal Revenue Service (IRS) has experimented with a tax return submission system whereby taxpayers may electronically submit their digitally signed tax returns to the IRS. Taxpayers send their returns to a transmitter that guarantees privacy, which transmitter in turn transmits the return to the IRS using secure telephone lines.[611]

Cybernotaries are a group of notarial attorneys in the European Union and Latin America who provide, legally and technically, digital notarial services, while ensuring the security, validity and evidential value of the data with which they deal. In America, *cybernotaries* are intended to be attorneys who are legally and technically able to provide digital notarial services that are secure, valid and of evidentiary value, and they may also be entitled to perform other international notarial services.

In South Africa, the Bill[612] seeks to make provision for notarisation, acknowledgment and certification in circumstances where a signature, statement or document is to be notarised, acknowledged, verified or made under oath, and such a requirement will be met should the advanced electronic signature (a digital signature) of the party authorised to perform the aforementioned act is either attached to, incorporated in, or logically associated with the electronic signature or data message.[613]

---

[610] Hall and Thibodeau *Calif. Signs Up Digital Signature Provider* 1999(October) 33:42 Computerworld 12*ff*.

[611] Anon *Public Key Infrastructure and Electronic Filing of Tax Returns: Security and E-commerce* <http://www.webcom.com/~pjones/digital.html> (2000-04-17).

[612] The Electronic Communications and Transaction Bill of 2002.

[613] Section 18 (1) of the Electronic Communications and Transaction Bill of 2002.

The Bill further provides that where the law "requires or permits ... a certified copy of a document and the document exists in electronic form, that requirement is met ... (by) ... a print-out certified to be a true reproduction of the document or information".[614]

Without asymmetric encryption and digital certificates, *cybernotaries* would not be feasible.[615]

The lodging of deeds electronically, specifically bond registrations and property transfers, is now an option[616] available to conveyancing attorneys in South Africa, utilising a particular virtual private network[617] in conjunction with a certification authority's electronic infrastructure.[618] These processes traditionally took up to eight weeks to finalise, but may now be achieved within a few days, procuring a substantial reduction in administrative costs and turnaround time.

3.7 DIGITAL SIGNATURES AND FUNDAMENTAL RIGHTS

When conducting online business, sensitive and/or personal information may be transmitted.

Consequently, vast amounts of private and confidential information is presently more accessible than ever before, for example personal identification and driver's license numbers, tax identification numbers, fingerprints and so forth, which is stored online in

---

[614] Section 18 (2) of the Electronic Communications and Transaction Bill of 2002.

[615] Bond and Whiteley *Untangling the Web: a Review of Certain Secure E-Commerce Legal Issues* 1998 (July) 12:2 International Review of Law 349 *ff.*

[616] See the website <www.law-sa.co.za>.

[617] L@W's Omnilink Virtual Private Network.

[618] The South African Certification Agency, see <www.saca.net>.

computer databases, on proprietary networks of credit reference services, and on the Internet.[619]

Privacy concerns have come to the fore recently as a result of a combination of factors, namely:

i. a digital economy by necessary implication amounts to a networked economy, and once private information appears in the public stream in a digital format, its circulation becomes uncontrollable;
ii. an information economy is an accelerated economy, and access to digitally rendered credit histories, for example, may be purchased or hacked with relative ease.[620]

In combination with the aforegoing is the state's need to access such information in the interests of public safety, crime control, national intelligence and regulatory requirements.[621]

However, while the individual and the population at large require the protection of the state at various levels, so too do they require that their fundamental rights are not arbitrarily discarded in the process, more specifically the fundamental right to privacy.

Thus, a balance must be established between the maintenance of law and order on the one hand, and individual fundamental rights and the free-flow of information on the other.

---

[619] Saunders & Zucker *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act* 1999 (August) 13:2 International Review of Law 183 *ff*.

[620] Hofman *et al* Cyberlaw: A Guide for South Africans Doing Business Online (1999) 43.

[621] Department of Communications Green Paper on E-Commerce: "Making it your business" (November 2000) 61.

The right to privacy in South Africa flows from section 14 of the Constitution of the Republic of South Africa Act (the Constitution),[622] as well as from the common law. The right to privacy under the common law holds that privacy constitutes an aspect of one's *dignitas*, and infringements thereof are actionable as *injuriae*.[623] In the case of *Bernstein and Others v Bester and Others NNO*[624] the reading of private documents amounted to a breach of privacy under the common law.

Section 14 of the Constitution

> "embodies both a general right to privacy as well as certain specific rights, but extends only as far as those aspects of a person's life in which a legitimate expectation of privacy can be assumed ... (A) legitimate expectation of privacy may be described as a subjective expectation of privacy, which is objectively reasonable."[625]

Section 32 of the Constitution provides everyone with the right of access to any information held either by the state[626] or by another person.[627] Section 32(2)[628] states that national legislation is to be enacted to give impetus to the rights enunciated in Section 32(1), which legislation may be so formulated so as to "alleviate the administrative and financial burden on the state". As a result, the Promotion of Access to Information Act[629] was enacted to give effect to the rights propounded in Section 32.

---

622 Act 108 of 1996.

623 Johnson *E-Spy vs The Right to Privacy* 2000 (November) De Rebus 54 54.

624 1996 2 SA 751 (CC); 1996 4 BCLR 449 (CC).

625 Johnson *E-Spy vs The Right to Privacy* 2000 (November) De Rebus 54 54.

626 Section 32 (1)(a) of Act 108 of 1996.

627 Section 32 (1)(b) of Act 108 of 1996 subject to the proviso that the information be necessary for either the exercise or protection of a right.

628 Act 108 of 1996.

629 Act 2 of 2000.

It is apparent that neither Section 14 nor Section 32 were formulated in the light of the prevailing online experience, since these sections fail to establish "a general right of access to information".[630]

At the Meeting of Experts on Cyberspace Law in 1998, it was highlighted that a need existed to recognise the "importance of the fundamental right of each individual to privacy, including the right to communicate confidentially using specific techniques such as cryptographic systems and pseudonyms".[631]

Also, as a result of the increasing demand for a move toward electronic signatures to access, for example, government on-line services, a need has arisen to recognize the rights of every individual to a digital/electronic signature and to sign anonymously, the corollary right to request the state to "maintain paper procedures for 'cyber have-nots' and, finally, the right to use several signatures in order to avoid the signature becoming a unique identification liable to be subjected to numerous processes".[632]

The right to privacy envisages a prohibition on the state decrypting data arbitrarily, but the right to freedom of expression includes both the production of a cryptographic product, as well as their application in protecting the expression and storage of data.[633]

Yet, these guarantees are not absolute, since, in terms of Section 36 of the Constitution, they may be limited, should such limitation be reasonable and justifiable, and thus

---

[630] Hofman *et al* Cyberlaw: A Guide for South Africans Doing Business Online (1999) 51.

[631] See Poullet's chapter: *Some considerations on Cyberspace Law* in de Padirac (Ed.) The International Dimensions of Cyberspace Law (2000) 151.

[632] See Poullet's chapter : *Some considerations on Cyberspace Law* in de Padirac (Ed.) The International Dimensions of Cyberspace Law (2000) 151.

[633] Department of Communications Green Paper on E-Commerce: "Making it your business" (November 2000) 61.

privacy may be invaded, data seized, or communications intercepted upon judicial authorisation.[634]

The Electronic Communications and Transaction Bill[635] states as one of its aims the protection of the consumer and of privacy, as well as the protection of critical data. The Bill provides for the creation of a voluntary regime for protection of personal information, which is deemed to include any information capable of identifying an individual. Only those data collectors who subscribe to a set of universally accepted data protection principles will be allowed access to this data. [636] The South African Law Commission is presently involved in the drafting of specific data protection legislation. Also, the Bill seeks to protect critical data, that is information which, if compromised, may endanger national security or the economic or social status quo.[637]

Thus, while society guards against incursions into fundamental rights by criminals, terrorists and other *mala fide* groups, so too must society guard against these exact incursions by those who seek to protect society from these groups.[638] As US Supreme Court Justice Louis Brandeis warned as far back as 1927:

> *"Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent ... (T)he greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."*[639]

---

[634] Department of Communications Green Paper on E-Commerce: "Making it your business" (November 2000) 61.

[635] The Electronic Communications and Transaction Bill of 2002.

[636] Chapter VIII of the Electronic Communications and Transaction Bill of 2002.

[637] Chapter IX of the Electronic Communications and Transaction Bill of 2002.

[638] Strossen *Cybercrimes v Cyberliberties* 2000 (March) 14:1 International Review of Law 11*ff*.

[639] *Olmstead v US* 27 US 438, 479 (1928) (Brandeis J dissenting), overruled by *Katz v US* 289 US 347 (1967) as cited in Strossen *Cybercrimes v Cyberliberties* 2000 (March) 14:1 International Review of Law 11*ff*.

3.8 CONCLUSION

The Internet has comprehensively and positively altered the manner in which business is conducted. Yet, this is only the tip of the iceberg, as the prevailing growth has been constrained by the remaining substantial bottleneck – the secure signing of documents and transactions in the online arena.

The growth in business conducted over the Internet has seen a commensurate surge in the call for a secure and legally binding method of electronically signing online documentation, as the potential efficiency is being hamstrung by the present need for traditional, paper-based signatures, which are not feasible when contracting parties are separated by continents and time-zones, since the use of the traditional signature alone to identify and verify the signatory is no longer practicable, as no *corpus mechanicum* is present upon which the signature can be written and fixed. In response hereto, digital signatures have been adopted to supplement and/or replace the traditional signature, provided that these electronic signatures identify and bind the signatory.

The Electronic Communications and Transaction Bill[640] has neglected to establish any requirements in respect of a signature's form, while stating that "an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form".[641] Thus, the prevailing legislative attitude seems to encourage reliance upon the function that a specific signature performs, thereby embracing digital signature technology. Section 13(3) stipulates an electronic signature will be deemed a valid signature if it employs a method to identify the signatories, indicate their approval[642] of the information communicated and, considering the circumstances prevailing when the method was

[640] The Electronic Communications and Transaction Bill of 2002

[641] Section 13 (2).

[642] Section 13 (2)(a).

applied, that the said method "was as reliable as was appropriate for the purposes for which the information was communicated".[643]

The future world economy is envisaged as a "knowledge-based society built on the foundation of a global networked information community ... without conceivable boundaries".[644] South Africa, still coming to terms with the concept of a transparent democracy, "now faces the new and equally crucial challenge of being part of the global evolutionary process".[645] Securely verifying the authenticity of online identities and privileges is pivotal if the full potential of e-commerce is to be realised.[646]

The acceptance and application of digital signature technology breaches numerous and diverse possibilities for both government and business to alter the manner in which transactions occur electronically, as the ability to transmit electronic messages embodying legally binding signatures will enable government and business to conduct transactions and contract exclusively by electronic means.[647]

Common rules to authenticate and confirm the integrity of on-line documentation and their signatories is therefore required before heavy reliance may be placed on electronic documents,[648] which has, to a large extent been canvassed by the Electronic Communications and Transaction Bill of 2002.

---

[643] Section 13 (2)(b).

[644] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 SA Merc LJ 199 199.

[645] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Dispute Arbitration* (2000) 12 SA Merc LJ 199 199.

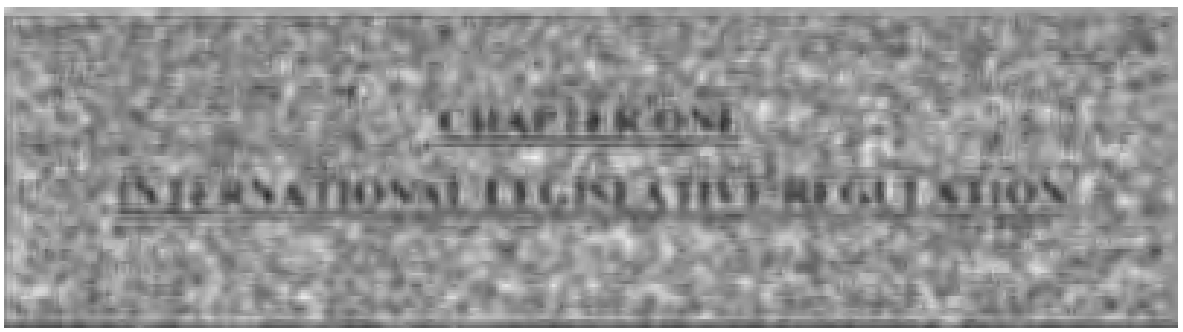
[646] Ford *Identity Authentication and 'E-Commerce'* <http://elj.warwick.ac.uk/jilt/98-3/ford.html> (2000-04-15).

[647] Ford *Identity Authentication and 'E-Commerce'* <http://elj.warwick.ac.uk/jilt/98-3/ford.html> (2000-04-15).

[648] Katz and Schwartz *Electronic Documents and Digital Signaturing: Changing the Way Business Is Conducted and Contracts Are Formed* <http://www.perkinscoie.com/resource/ecomm/edocs&digsig.htm> (2000-01-18).

SECTION I.

INTERNATIONAL LEGISLATIVE REGULATION.



1.1 INTRODUCTION

The Internet and related forms of paperless technologies have introduced novel legal issues which need to be assessed and addressed so as to ensure that electronic signatures can perform the same functions that traditional handwritten signatures do, specifically the securing of transactions and dispute-prevention. Legislatures should establish the foundation for the future development and advancement of the information society, by creating an environment within which people feel confident and secure in partaking in e-commerce.

Many countries have thus experienced the need for electronic signature legislation in an effort not only to find clarity on certain fundamental issues relating to the Internet and other new technologies, but also to promote the growth of e-commerce. A number of foreign countries have recently assimilated electronic signatures into their law, giving traditional and electronic signatures the same status. A cursory examination of current international trends concerning the status of the signature, and the South African stance in respect thereof, is necessary and dealt with hereunder.

1.2 FOREIGN APPROACHES TO ELECTRONIC SIGNATURE LEGISLATION

1.2.1 THE EUROPEAN UNION

The European Commission produced the Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures[649] in May 1998, which defined an *electronic signature* as

> "data in electronic form ... attached to or logically associated with other electronic data and which serves as a method of authentication."

and defined an *advanced electronic signature* as

> "an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."[650]

Article 5 of the Directive[651] determines the circumstances under which an electronic signature will be regarded as "valid, enforceable and legally effective". In respect of simple electronic signatures, this provision is negative, as it enjoins Member States to

> "ensure that signatures of this type are not denied validity, enforceability and effectiveness solely on the grounds that they are in an electronic form or are not certified ... (but) ... Member States are free to refuse to recognize electronic signatures for any other reason."

Article 5[652] treats certified advanced electronic signatures more positively, since such a signature will "receive the benefit of a higher level of validity if it is based on a qualified certificate which was created using a secure-signature-creation device". The certificate, to

---

649 Directive 1999/93/EC.

650 Article 2 (1) of Directive 1999/93/EC.

651 Directive 1999/93/EC.

652 Directive 1999/93/EC.

be considered *qualified*, must "link the signature verification data used to the signatory and confirm his identity, and be issued by a certification-service-provider...".[653]

The practical effect of these requirements is that, by virtue of Article 5(1),[654] an electronic signature is treated on a par with the traditional manuscript signature.[655]

1.2.2 THE UNITED KINGDOM

The UK Electronic Communications Act 2000 was created in consequence of the adoption of modified provisions of the above Directive into the Department of Trade and Industry's Building Confidence in Electronic Commerce[656] consultation document, wherein identical provisions for the basic conditions for signature validity were established, and qualifying electronic signatures received the equivalent recognition of traditional manuscript signatures.

---

[653] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[654] Directive 1999/93/EC. The Article provides that an electronic signature satisfies "the legal requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper-based data ... and is admissible as evidence in legal proceedings".

[655] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[656] Consultation Document: Department of Trade and Industry (5 March 1999, URN 99/642) as quoted by Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

The consultation document stipulated that this will be achieved:

> "by creating, in statute, a rebuttable presumption that an electronic signature, meeting certain conditions, correctly identifies the signatory it purports to identify; and, where it purports to guarantee that the accompanying data has not been altered since signature, that it has not."[657]

However, when finally enacted, the UK Electronic Communications Act 2000 provisions relating to the validity of electronic signatures were less explicit, as Section 7(1) states that:

> "in any legal proceedings ... an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and ... the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data."[658]

Under prevailing English law, traditional manuscript signatures are not granted any particular presumptions of validity, but are construed as per their individual merits for evidential effectiveness in authenticating the signed document. Yet, the UK Electronic Communications Act of 2000[659] now ensures that both simple and certified advanced electronic signatures are treated equally with traditional signatures and "other physical-world manifestations of signatures" by the English courts.[660]

1.2.3 THE UNITED STATES OF AMERICA

Despite initial contrasting approaches among certain individual states, the minimalist approach has prevailed on a national level in the United States of America with the

---

[657] Consultation Document: Department of Trade and Industry (5 March 1999, URN 99/642) as quoted by Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[658] The UK Electronic Communications Act 2000 as quoted by Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

[659] Act of 2000.

[660] Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21).

adoption in 2000 of the Electronic Signatures in Global and National Commerce Act[661] (E-Sign Act), which endows electronic signatures with the legal validity of traditional manuscript signatures, and "explicitly forbids the denial of an electronic agreement simply because it is not in writing".[662]

The E-Sign Act is intended to "spur the growth of electronic commerce by insuring (*sic*) that electronic contracts, signatures and records will have the same legal status and effect as their ink and paper counterparts".[663]

The E-Sign Act defines an *electronic signature* as "an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record",[664] and defines an *electronic record* as "a contract or other record created, generated, sent, communicated, received or stored by electronic means".[665]

In an effort to prevent a conflict of approaches at a state level, the E-Sign Act prohibits any state legislation or regulation that limits, modifies or supercedes the E-Sign Act in a way that would discriminate for or against a specific technology.[666] *Party autonomy* principles have been incorporated into the E-Sign Act as it avoids compelling parties to agree to use or accept electronic signatures and/or records.[667]

---

[661] Act 15 USCA § 7001.

[662] Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

[663] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

[664] Section 106 (5) of Act 15 USCA § 7001.

[665] Section 106 (4) of Act 15 USCA § 7001.

[666] Section 104 of Act 15 USCA § 7001.

[667] Alston and Bird *How the New E-Sign Act Will Affect E-Commerce* <http://www.gigalaw.com/articles/alston-2000-06-p2.html> (2001-05-01).

Dorney[668] notes that the E-Sign Act is intended to be technology neutral, in terms whereof a variety of technologies may function as an electronic signature, such as passwords, smart cards, digital certificates and biometrics (including fingerprint recognition and retinal scan technology). Also noted is the recognition by the E-Sign Act of the ability to utilise electronic agents to create binding contracts, provided the actions of the electronic agent are attributable to the party to be bound.[669]

The E-Sign Act ultimately aims "to clarify the legal status of electronic signatures and records in the context of existing legal requirements in respect of writings and signatures".[670] However, an electronic signature is not immune to being declared a forgery, or that it was used without authority, or that it is invalid for any reason, such as lack of capacity, which would invalidate a traditional manuscript signature. Also, any signature or record that needs to be notarised or witnessed by a commissioner of oaths, may be so notarised or commissioned electronically, on condition that all the other legal requirements imposed by the applicable statute are complied with.[671]

The E-Sign Act contains express exclusions in respect of certain legal and commercial instruments, to the extent that they are regulated by legislation or other rules of law, such as the creation and execution of wills and testamentary trusts, matters involving family law, court orders and official court documents, and notices involving the cancellation of utility services or health or life insurance.[672]

---

[668] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

[669] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

[670] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

[671] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

[672] Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

Thus, the E-Sign Act elevates electronic signatures to the legal status enjoyed by traditional manuscript signatures for purposes of e-commerce transactions, but it fails to stipulate how to implement electronic signatures and which technology to use.[673] The E-Sign Act has been criticised for its lack of technology understanding, as well as the potential for consumer abuse.[674] Further, it neglects to compel the use of electronic signatures and the maintenance of electronic records, as well as avoids addressing the issues of interoperability among digital certificate vendors, the complexity of the technology and the cost implications connected to deploying this technology.[675] The E-Sign Act has been purposefully cast in broad terms, as the drafters were "unable to predict a future standard and unwilling to prescribe one ... the lawmakers ... (have) ... tried to be as vague as possible, leaving it to business to decide on the most effective technology".[676]

In South Africa, our laws regulate traditional paper-based transactions and do not contemplate electronic commerce. South Africa has yet to implement electronic signature legislation. If it is to do this, there is a need for international comparison, conformity and co-operation in the process of considering any electronic commerce-specific legislation for South Africa. An analysis is necessary to ascertain the viability of this type of legislation and the legal framework concomitant thereto.

---

673 Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01).

674 Koch *The Electronic Signatures in Global and National Commerce Act: Eliminating a Legal Barrier to Electronic Commerce* <http://www.vonbreisen.com/mak_digisign800.htm> (2001-05-01).

675 Rosencrance *A Closer Look at the E-Signatures Law* <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51990,00.html> (2000-11-01).

676 Neethling *E-Signatures Become Legal Tender* <http://www.mg.co.za/pc/2000/10/2010_digisign.htm> (2000-10-25).

1.3 THE POSSIBILITY OF LEGISLATIVE INTERVENTION IN SOUTH AFRICA

Internet users, business entities and the State are faced with a myriad of new and unique[677] legal issues arising from the growth of the Internet and its concomitant aspects, which issues are presently dealt with in South Africa by the application of the existing legal framework, *sans* the formal recognition of the nature of electronic communication.

A legal foundation needs to be established which enables users to fully utilise the Internet and all its applications without apprehension, and to enhance the reliability of e-commerce and other network-orientated social and economic activities. South Africa is without legislation specifically regulating contemporary Internet and Internet-related issues, specifically in respect of conferring electronic and digital signatures with the same status enjoyed by traditional signatures. Consequently, it is pertinent to analyse whether South Africa should merely extend and develop existing legislation, or create legislation that is technology-neutral. Retention of existing law during a period of rapid technological innovation could create instability and uncertainty. Conversely, when the law moves with change in business practice, it could have its most stabilising effect and facilitate economic growth.[678]

A key issue to the aforegoing involves the extent to which the state will permit the Internet to regulate itself. Self-regulation contains the inherent advantage of flexibility, thus predicting technological advances and proactively establishing legal blueprints for the same, whereas government regulation is generally retroactive; however, it is more

---

[677] Sommer *Against Cyberlaw* <http://www.law.berkeley.edu/journals/btlj/articles/15_3/sommer/sommer.html> (2001-12-01) notes contra that "if the Internet or personal computers have the promised transformative social impact, they are unlikely to generate a characteristic body of law. Unlike other social practices, technologies seldom (directly) generate law. Although social practices incorporate various technologies, they seldom break along technological fault lines. A new information technology is likely to affect many social practices and hence many bodies of law. However, it is not likely to generate a field of law all its own."

[678] Smedinghoff & Bro *The Core Legislative Concern: Electronic and Digital Signatures* <http://www.profs.lp.findlaw.com/signatures/signature_2.html> (2000-12-20).

effective in the area of maintaining fundamental standards.[679] Yet, the above *light* approach adopted by the majority of governments, coupled with the innovative and entrepreneurial nature of the Internet, has resulted in the success of the Internet in the face of the absence of restrictive regulation.[680]

On a fundamental level, public policy regarding the Internet is extremely simple: should an action be illegal offline, then it will be illegal online. In this way, the Internet and e-commerce applications are already regulated. It is the unique characteristics of the Internet and its diverse applications that necessitate the clarification of existing law and development of new law, and "the general principle should be against the special regulation of the Internet, unless this is warranted by public policy which cannot be assured without additional regulation because of the unique nature of the Internet".[681]

From a global perspective, the Internet seems to be the most regulated area of society, since a

> "patchwork of national laws and contractual restrictions potentially affect e-commerce, with most countries applying their own legal rules ... and private regulators imposing conditions on Internet transactions taking place within the borders of the states in which they are located ... reformers throughout the world are constantly promulgating new proposals for laws and conventions intended to facilitate Internet-based trade."[682]

Therefore, on a general global scale, Internet legislation and regulation have been presented in a piecemeal manner, as countries try to accommodate cyberspace within "the four corners of their (familiar) domestic jurisprudence", and "supranational and international bodies have been guilty of simply extending previous rules to the realm of

---

[679] Le Roux *E-commerce – The Legal Framework* <http://www.derebus.org.za/scripts> (2000-05-09).

[680] Armstrong *The Internet and E-Commerce* <http://www.internetpolicy.org/briefing/3_00.html> (2001-03-24).

[681] Armstrong *The Internet and E-Commerce* <http://www.internetpolicy.org/briefing/3_00.html> (2001-03-24).

[682] Murray, Vick and Wortley *Regulating E-Commerce: Formal Transactions in the Digital Age* http://www.internetpolicy.org/briefing (2001-03-24).

cyberspace".[683] This has occurred by adopting a *functional equivalent* approach to law-making, in terms of which regulators examine the role of a particular legal rule offline, identify its potential applicability online, and then extend this rule by analogy to cyberspace. Consequently, a broad *laissez faire* approach prevails, causing the supranational nature of the Internet to evince a "strange dichotomy of a medium" which is simultaneously "highly regulated yet subject to minimal policing".[684]

Another issue is the friction between the objectives of technological neutrality, and that of specific prescriptive legal consequences. Technology-specific legislation facilitates a measure of legal certainty, whereas technology neutral legislation facilitates development and adaptation, an inherent attribute of the Internet realm.[685]

In addition, national initiatives need to recognize the international nature of the Internet, thereby requiring a global approach in respect of regulatory issues, so as to enhance global legal predictability. Thus, when drafting legislation that impacts on a field relating to the Internet, legislators must have regard to international developments and the prevailing comparable legislation of other countries.[686]

A legal foundation needs to be established which allows electronic signatures to function in the same manner as the traditional handwritten signature. When constructing this legal foundation, consideration must simultaneously be given to the fact that electronic signatures are secure in terms of the identity of the user and the incorruptibility of the transmitted data, as well as to the fact that, for example, a digital signature will become defunct once a certification organ issues a flawed certificate in respect thereof, or when the recipient of such a certificate misuses it. Also, provision must be made for a wide

---

[683] Murray, Vick and Wortley *Regulating E-Commerce: Formal Transactions in the Digital Age* http://www.internetpolicy.org/briefing (2001-03-24).

[684] Murray, Vick and Wortley *Regulating E-Commerce: Formal Transactions in the Digital Age* http://www.internetpolicy.org/briefing (2001-03-24).

[685] Le Roux *E-commerce – The Legal Framework* <http://www.derebus.org.za/scripts> (2000-05-09).

[686] Le Roux *E-commerce – The Legal Framework* <http://www.derebus.org.za/scripts> (2000-05-09).

range of identity-verification methods that can be adapted to the multimedia resources available in e-commerce and other Internet-related spheres. Further, the definition of, for example, an electronic signature, must be rendered in language that appreciates the speed and flexibility of developing technologies, as well as the need for general users to easily comprehend such definitions.[687]

Kuner and Baker[688] have identified three basic approaches when a state considers how to accommodate electronic signatures. Firstly, the minimalist approach, which focuses on facilitating the use of electronic signatures generally, instead of prescribing a specific tool or methodology, thereby removing legal obstacles by ensuring that electronic signatures meet existing legal requirements for traditional signatures. Generally, legislation and case law are limited in terms of this approach to defining circumstances wherein an electronic signature will satisfy the said requirements, with the ultimate goal of creating a standard of proof. Thus, the minimalist approach seeks to verify the intention of the signatory, as opposed to "developing particularized forms and guidelines".[689]

The second approach is prescriptive, where the relevant state seeks to "establish a legal framework for the operation of PKI's [Public Key Infrastructure] – whether or not other forms of secure authentication are included or permitted – as well as a reflection of form and handwriting requirements that apply in the offline world".[690] The legislation and case law developed under this approach generally evince the following characteristics: asymmetric cryptography is adopted as the accepted means with which to create a digital signature; various operational and financial requirements are imposed upon the

---

[687] Ministries of Post and Telecommunication, International Trade and Industry, and of Justice (Japan) *Legal Provisions Relating to Electronic Signatures and Certification: Promoting Electronic Commerce and Otherwise Laying the Foundation for Network-Based Social and Economic Activities* <http://www.info.mpt.go.jp/whatsnew/english/LegalProvisions-e.html> (2001-05-01).

[688] Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

[689] Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

[690] Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

certification authorities; the duties of key holders are prescribed; and there occurs a definition of the circumstances under which reliance on an electronic signature is justified. This approach enables the state to directly influence the "setting of standards for and ... the direction of new technologies".[691]

The third approach amounts to a convergence and synthesis of the minimalist and prescriptive approaches, and is referred to as the two-tier approach. The general theme under this approach sees laws being enacted that prescribe standards, while simultaneously adopting "a broad view of what constitutes a valid electronic signature for legal purposes".[692] The two-tier approach thus achieves legal neutrality, as it grants a minimum recognition to the majority of authentication technologies, while also "creating a better- defined, more predictable legal environment by incorporating provisions for an authentication technology of choice".[693]

It is significant to note that the adoption of these approaches falls closely in line with the systems of law within which each has evolved. Traditional common law states, such as America, Canada, the United Kingdom, Australia and New Zealand, have favoured the minimalist approach, whereas civil law countries, such as Germany, Argentina and Malaysia have opted, generally, for the prescriptive approach. The two-tier approach has found increasing support from within the European Union and Singapore.[694]

At present in South Africa, there are no specific statutes regulating Internet law, or the law pertaining to online fields, such as domain names, copyright, trade issues or

---

691 Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

692 Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

693 Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

694 Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18).

electronic signatures, while, in the offline world, volumes of law and legal thought exist. Heske[695] notes that the major problem with the development of a South African law of the Internet is that there is "no adequate regulatory, self-regulatory mechanisms or representatives in place to cope with the forging of electronic commerce law".

The Department of Communications' Green Paper on E-Commerce[696] (the Paper) is the governments' tentative attempt to ultimately fashion Heske's mechanisms and representatives. The Paper notes that "our law, statutory and non-statutory, was made with either a concept of commerce which did not include electronic commerce or without even contemplating the impact of electronic ways of engaging in commercial activity".[697] It notes further that "legislation regulating traditional paper-based commercial transactions ... creates an obstacle because of the language used"[698] such as *document*, *signature* and *writing*. Also, in certain cases, compliance may be uncertain as a result of the manner in which existing legislation is drafted.

The Paper identifies a related obstacle to the aforegoing in respect of the reliance that would need to be placed on electronic messages and exchanges as proof of contracts, payment and correspondence. Thus, the acknowledgement of electronic messages as evidence by the South African courts is a prerequisite for the enforcement of rights procured by means of electronic transactions.

The Paper highlights the need for "international comparison, conformity and co-operation in the process of considering any electronic commerce-specific legislation for South

---

[695] Heske *The Cashless Society* (2000) 6:2 Intelligence 71 82.

[696] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[697] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[698] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

Africa",[699] since, should South African *cyberlaw* not conform with global standards, it will be ineffective.

In conclusion, the Paper suggests that an immediate priority is "the issues of extending the meaning of words such as *writing* and *signature* in a myriad of legislation to include electronic writing and signature as well as to change both civil and criminal evidential laws to recognize (*sic*) electronic evidence".[700] Consequently, when contemplating the removal of disparity between electronic messages and their traditional, paper-based counterparts, it is submitted that the state should consider the following: allow the courts to remove any uncertainty; amend the Interpretation Act;[701] amend specific pieces of legislation; and/or draft electronic commerce-specific legislation.

In early 2002, the Electronic Communications and Transaction Bill ("the Bill") was introduced in the South African National Assembly by the Minister of Communications, based upon the principles in, and the responses to, the above Paper. The stated objective of the Bill is to permit and encourage electronic transactions by establishing legal certainty in respect of communications and transactions conducted by electronic means. More specifically, the Bill seeks to promote the understanding, acceptance and growth in the number of electronic transactions in South Africa; to eliminate and prevent obstacles to electronic transactions; to promote technology neutrality in the application of legislation to electronic transactions; and to ensure that electronic transactions in the Republic conform to the highest international standards.[702]

---

[699] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[700] Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999) <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18).

[701] Act 33 of 1957.

[702] Section 2 of the Electronic Communications and Transaction Bill of 2002.

The Bill states that it is not to be interpreted so as to exclude the applicability to electronic transactions of any statutory or common law.[703] By providing for the legal recognition of data messages and records, it appears to negate legal barriers to electronic transacting, since such a data message will not be without legal force merely because it is in the form of a data message. If such information is referred to in such a way that a reasonable person will have noticed the reference to it, and it is in an accessible and readable form which can be stored and retrieved by the other party, then this will suffice.[704]

Subject to certain conditions, electronic data will be retained for purposes of statutory record retention, as well as be regarded as "writing"[705] a true copy of an "original"[706] record.

Further, provision is made for attaching appropriate evidentiary weight to electronic evidence,[707] as well as for the legal recognition of electronic signatures,[708] and advanced electronic signatures, as a secure form of electronic signing. The Bill defines *electronic*[709] as a digital or other intangible form; and *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".[710] An *advanced electronic signature* is defined as an "electronic signature which results from a process which has been accredited by the Authority ...".[711] Where a signature is required by law, the requirement will only be met if an advanced

[703] Section 3 of the Electronic Communications and Transaction Bill of 2002.

[704] Section 11 of the Electronic Communications and Transaction Bill of 2002.

[705] Section 12 of the Electronic Communications and Transaction Bill of 2002.

[706] Section 14 of the Electronic Communications and Transaction Bill of 2002.

[707] Section 15 of the Electronic Communications and Transaction Bill of 2002.

[708] Section 13 of the Electronic Communications and Transaction Bill of 2002.

[709] Section 1 of the Electronic Communications and Transaction Bill of 2002.

[710] Section 1 of the Electronic Communications and Transaction Bill of 2002.

[711] Section 1 of the Electronic Communications and Transaction Bill of 2002.

electronic signature is used. It is expressly stated that an electronic signature is not without legal effect merely because of its electronic form. Where an electronic signature is required, and there is no agreement by the parties to the electronic transaction in respect of the type of electronic signature to be used, then any method will be acceptable, on condition that it identifies the person, indicates approval, and is a reliable method for the purposes for which the information is communicated.[712]

The legal requirement that certain signatures, statements or documents are to be notarised, acknowledged, verified or made under oath, will be met if an advanced electronic signature of the person authorised to perform these acts is attached or associated with the electronic signature or data message. Also, where a certified copy of a document which exists in electronic form, is subsequently rendered in hardcopy, or printed out, this copy may then be certified to be the true reproduction of the electronic document.[713]

The Bill requires the registration of cryptography providers as, without them, security will be greatly reduced. These providers will have to register with the Department of Communications, where all their details will be lodged.[714] The Bill further envisages the establishment of an Accreditation Authority within the Department, allowing accreditation of electronic signature technologies in accordance with minimum standards. Once accredited, these advanced electronic signatures will allow a party to rely on their authenticity.[715] Protection of the consumer is further enhanced by the introduction of a "cooling off period" in respect of certain types of transactions, irrespective of the legal system applicable to the agreement.[716]

---

[712] Section 13 of the Electronic Communications and Transaction Bill of 2002.

[713] Section 18 of the Electronic Communications and Transaction Bill of 2002.

[714] Section 30 of the Electronic Communications and Transaction Bill of 2002.

[715] Section 34-42 of the Electronic Communications and Transaction Bill of 2002.

[716] Section 45 of Electronic Communications and Transaction Bill of 2002.

1.4 CONCLUSION

> "No single solution or analogy will remedy the regulatory challenges posed by the Internet. Rather, as in real space, a combination of approaches will be necessary to create an effective regulatory framework."[717]

Thus, in essence, the problem of legislating the Internet stems from the manner in which our law is made: based upon precedent "from years of carefully analyzed policy concerns considered by scholars, developed by judges ... (addressed by policymakers) ... then further considered by scholars, and developed by judges".[718] The thread running throughout this process is that the fundamental premises upon which our law is based have essentially remained untouched. Consequently, it is believed that the "best final result is embodied in the law which can then build upon itself to adapt to specific situations and variances in the underlying issues".[719]

Retention of existing law in a period of rapid technological innovation can create instability and uncertainty, while the limitation of legislative assistance to electronic commerce carries the inherent risk that "benign neglect may well produce stagnation or at least slow the development of business online.".[720]

However, the Internet and it's related technologies represent a departure from the above process, in that the speed and complexity at which these have continued to develop have rendered the traditional law-making process redundant, thus causing interested parties to

---

[717] Geist *The Reality of Bytes: Regulating Economic Activity in the Age of the Internet* <http://www.law.washington.edu/WLR/GEIST.HTM> as quoted by Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24).

[718] Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24).

[719] Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24).

[720] Smedinghoff & Bro *The Core Legislative Concern: Electronic and Digital Signatures* <http://www.profs.lp.findlaw.com/signatures/signature_2.html> (2000-12-20).

such matters to resolve their disputes themselves, or the dispute is dissolved altogether through technological advance.[721]

Yet, the continuous metamorphoses of electronic technology and techniques may soon result in legislation which is obsolete. Consequently, the rapid increase of electronic transactions and the plethora of involved technologies will inevitably result in legislation- and regulation-conundrums on a global scale, as the machinery of legislatures fails to keep up the pace.[722]

Hofman *et al* believe:

> "Legislation that is drafted in terms of obsolescent technology will be worse than no legislation and could wreak havoc with a developing system of cyber-commerce."[723]

Therefore, legal rules and solutions to cyberspace problems, should these indeed be put in place, may not be flexible enough "to adapt to the rapid and continuous transformations of the medium".[724] Legislative processes will need to be adapted as new business models and technologies emerge, and as case law develops.[725]

Shore believes that there is no solution. Rather, the matter must be "processed through often illogical and inefficient stages, as it presses toward a solution".[726]

---

[721] Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24).

[722] Zekos *EDI: Electronic Techniques of EDI, Legal Problems and European Union Law* <http://www.diavlos.com/zekos> (2001-03-24).

[723] Hofman *et al* Cyberlaw: A Guide for South Africans Doing Business Online (1999) 80.

[724] Anon. *Developments in the Law: The Law of Cyberspace* <http://www.harvardlawreview.org/issues/112/7_1634.htm> as quoted by Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24).

[725] Smedinghoff & Bro *The Core Legislative Concern: Electronic and Digital Signatures* <http://www.profs.lp.findlaw.com/signatures/signature_2.html> (2000-12-20).

[726] Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24).

The Electronic Communications and Transaction Bill, as with the United States of America's E-Sign Act, appears to have been drafted purposely in broad terms and to be technology neutral, seemingly as the legislators were unable to predict future standards, and yet were unwilling to be prescriptive, apparently leaving it to commerce to determine these future standards. The Bill is framed in terms eminently suitable as a facilitative cornerstone upon which the future bastion of a new chapter of South African law may make its presence felt, domestically as well as globally. However, the intimations regarding the potential level of State involvement may result in reluctance on the part of both local and international role players to actively participate in South African electronic commerce.

Further, as regards electronic signatures specifically, the Bill has endowed electronic signatures with the same force and effect as traditional signatures have offline, thus keeping in step with international trends in respect hereof. This may uplift South Africa to a position from which she may freely and with relative ease participate in international electronic commerce.

The regulation of e-commerce presently occurs on an *ad hoc* basis that is until such time as legislatures internationally co-operate to provide uniform standards, thus allowing e-commerce unhindered potential for growth.[727]

> "Venturing into this black hole of possibilities and uncertainties called cyberspace is as exciting as it is daunting. Every conceivable aspect of society as we know it, whether in a corporate, commercial, governmental or personal sphere, will be subject to fundamental change. It is of paramount importance, considering South Africa's history of isolation, that we keep abreast of new developments and trends and start playing a more progressive role in the global community; we should not merely react to the pressure of circumstances."[728]

[727] Lourens *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64 68.

[728] Hurter *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Dispute Resolution* (2000) 12 SA Merc LJ 199 199.

GENERAL CONCLUSION

In 1890, the court in the case of *In Re Knox's Estate*[1] noted:

> " What, therefore, shall constitute a sufficient signature must depend largely on the custom of the time and place, the habit of the individual, and the circumstances of each particular case."

The formal requirements for legal transactions, including the need for signatures, vary in different legal systems, as do the legal consequences of failure to cast the transaction in the required form. In South Africa, although a signature is generally not required to establish a valid and binding contract, it is invariably appended to a document to identify the signatory, to affirm the signatory's intention to append his/her signature and to indicate the adoption by the signatory of the contents of the document.

A signature may be analysed on the basis of its form, as well as on the function that it performs. After analysing the role of the signature in the various areas of application, it is evident that the traditional manuscript signature has gained a wide interpretation in respect of its form. It does, however, evince certain inadequacies, such as an inherent susceptibility to forgery, as well as time and cost implications in respect of the visual comparison of the same.

Prevailing computer and communication technologies have rendered it possible and, in certain instances, imperative to adopt a method of signing fundamentally different from

[1] *Re Knox's Estate* 131 Pa 220, 6 LRA 353, 17 Am St Rep 798, 18 Atl 1021 (1890).

the traditional manuscript signature, to wit the electronic signature, which exists as PINs, passwords, biometrics and digital signatures.

PINs and passwords have been adopted as forms of an electronic signature and are able to identify the signatory. However, they suffer a number of inherent drawbacks including the incapability of differentiating an authorised person from an impostor who fraudulently acquires a token/knowledge from that person. Tokens may be easily lost or stolen, and PINs may be forgotten or intercepted by impostors.

Additional and convenient security mechanisms are however needed as society moves increasingly towards becoming more computer-dependant. Biometric identification, a form of electronic signature, satisfies this dilemma and may be used to identify the user and/or authenticate the signature of the individual, by means of measuring the human characteristics of that person, such as fingerprints and hand geometry, within an electronic medium. The use of biometrics is becoming more prevalent as the price and size of biometric sensors decline, as well as the lessening of the negative perception of it as an encroachment on individual privacy, coupled with the realisation that it is an effective mechanism with which to combat fraud and protect privacy.

As technology evolves, so biometrics will improve, becoming more accurate and reliable. The combined use of biometrics and smart cards, specifically within the realm of Internet banking and e-commerce, is on the increase, and it is predicted that standards will become available that will allow multiple technologies from several manufacturers to be implemented simultaneously within the same system. However, the basic flaw inherent in these biometric technologies at present is the lack of standards and independent testing.

With the advent of the Internet and the increased amount of e-commerce transactions being concluded, a digital signature is required whereby individuals may transmit electronic messages that carry legally binding signatures which enable institutions to conclude and enter binding contracts entirely by electronic means. Digital signatures have been adopted to supplement and/or replace the traditional signature, provided that these

electronic signatures identify and bind the signatory to the contents of the agreement. The areas of application of the digital signature seem extensive and it is envisaged that a heavier reliance will be placed on it in future. Common rules to authenticate and confirm the integrity of on-line documentation and their signatories are required if such a reliance is to take place.

Consequently, as law has not yet mandated a requirement in respect of the form of the signature, the judicial approach seems to determine the validity of the various signature methods with reference to the functions which the specific signature performs. Electronic signatures satisfy all the function requirements of a *signature* presently required by our law. Whatever mark is used to indicate a signature, be it letters, characters or codes of an electronic record, they may be deemed a signature provided they can be reliably linked to the signatory and thus identify and bind him/her to the contents of the document. It thus appears that there exists no apparent bar to the legal recognition of an electronic signature on the basis of the form and function.

Currently, South Africa is without legislation pertaining to the status of signatures as well as electronic commerce. Legal issues such as privacy concerns (guaranteed in our Constitution) and the satisfaction of laws which require certain legal information to be "written" and "signed" have all yet to be addressed. In the meantime, all issues are been dealt with by the application of the existing legal framework.

Many countries have experienced the need for electronic signature legislation in an effort to find clarity on the legal issues and at the same time, promote the growth of e-commerce. The European Union, the United Kingdom and the United States of America have passed legislation to the effect that electronic and traditional signatures are to be treated on a par with each other. The Acts are legislated in such a way so as to allow for technology neutrality, leaving the concept *signature* open to a wide interpretation.

Recently, South Africa has introduced the Electronic Communications and Transaction Bill of 2002 that appears to be drafted in purposely broad terms, thereby echoing their

international counterparts in being technology neutral in application. The legislators have in so doing endowed electronic signatures with the same force and effect as traditional signatures.

A signature, as a legal concept, bears no relationship to the popular conception of a name, on paper, in the signatory's own handwriting. A signature is not a 'thing', but a process. If that process produces sufficient evidence that a person has adopted a document as his/her own, and that document before the court is the same document to which the process was applied, then the document has been signed. It is irrelevant whether the result of the process is a visible name, symbol, or a logical alteration of information content, as long as it provides sufficient evidence of the transaction.

It seems as if the statement made in 1890 by the court in *In Re Knox's Estate*[2] should be endorsed since although the use of paper is being reduced, a signature is still needed, albeit electronic. Whatever the manner of affixing a *signature* to a document, it must achieve the core function of *identifying the signatory and binding him/her to the contents of the document* (be it stored electronically or in a physical form).

[2] *Re Knox's Estate* 131 Pa 220, 6 LRA 353, 17 Am St Rep 798, 18 Atl 1021 (1890).

BIBLIOGRAPHY

A. BOOKS AND ARTICLES

Anon *Face of the New Security Technology* (1999) 5:7 Hi - Tech Security Systems 58.

Arora A Electronic Banking and the Law (1988) London: IBC Financial Books Ltd.

Bagraim P *Transacting in Cyberspace* (1998) 6:2 Juta's Business Law 50.

Bond R and Whiteley C *Untangling the Web: a Review of Certain Secure E-Commerce Legal Issues* 1998 (July) 12:2 International Review of Law 349.

Buys R Cyberlaw@SA (2000) Pretoria: Van Schaik.

Buys R *Internet Banking: The Risks and Benefits* 2000 (June) De Rebus 30.

Christianson G and Mostert W *Digital Signatures* 2000 (May) De Rebus 26.

Cowen DV and Gering L The Law of Negotiable instruments in South Africa 1 5th ed (1985) Cape Town: Juta & Co Ltd.

Davel CJ and Jordaan RA Law of Persons (1998) Cape Town: Juta & Co Ltd.

De Beer CR *Die Effek van die Kruising van Poswissels met Besondere Verwysing na die Regsposisie van die Poskantoor* (1987) 20 De Jure 285.

De Padirac B (Ed) The International Dimensions of Cyberspace Law (2000) Hants (England): Ashgate Publishing Limited, Vermont (United States o f America): Ashgate Publishing Company.

De Ru WG Reinforcing Password Authentication with Typing Biometrics (1996) 17 South African Computer Journal 26.

De Waal MJ and Schoeman MC Law of Succession (1996) Cape Town: Juta & Co Ltd.

Frazer P Plastic and Electronic Money (1985) Cambridge: Woodhead: Faulkner.

Freeman EH *When Technology and Privacy Collide* (1995) 11:4 Information Strategy: The Executive's Journal 41.

Frischholz M and Dieckmann J *BioID: A Multimodal Biometric Identification System* 2000 (February) Computer 64.

Gering L Handbook on the Law of Negotiable Instruments (1997) Cape Town: Juta & Co Ltd.

Goode RM Electronic Banking (1985) London: The Institute of Bankers.

Gordon-Cumming I *BT is looking cybercrime in the eye* (1999) 5:7 Hi-Tech Security Systems 58.

Hall M and Thibodeau P *Calif. Signs Up Digital Signature Provider* 1999 (October) 33:42 Computerworld 12.

Harms LTC Civil Procedure in the Supreme Court (1995) Durban: Butterworths.

Heske P *The Cashless Society* (2000) 6:2 Intelligence 71.

Hofman J, Johnston D, Handa S and Morgan C Cyberlaw: A Guide for South Africans Doing Business Online (1999) Cape Town: Ampersand Press.

Hopkins R *An Introduction to "Biometrics" and Large Scale Civilian Identification* (1999) 13:3 International Review of Law (Computers and Technology) 337.

Hurter E *Dispute Resolution in Cyberspace: A Futuristic Look at the Possibility of Online Intellectual Property and E-Commerce Arbitration* (2000) 12 South African Mercantile Law Journal 199.

Hutchinson DB *Signatures, Marks and the Wills Act of 1953* 1981 Acta Juridica 101.

Hutchison A and Saul E *Fundamental Cryptographic Techniques for Electronic Commerce* 1999 (March) 16 Elektron 49.

Jain A, Hong L and Pankanti S *Biometric Identification* (2000) 43:2 Communications of the ACM 91.

Johnson J *E-Spy vs The Right to Privacy* 2000 (November) De Rebus 54.

Kerr AJ The Principles of the Law of Contract 5th Ed (1998) Durban: Butterworths.

Kirby R and Downing TG *The Principles and Problems of DNA- Profiling for Legal Purposes in South Africa* (1999) Obiter 307.

Lawack VA *Electronic Innovations in the Payment Card Industry* (1998) 10 South African Mercantile Law Journal 233.

Lawack VA Electronic Payment Systems in the South African Law (1997) unpubl LLM Dissertation UPE.

Lawack-Davids VA *Teaching Banking Law in the Technological Age* (1999) 2 Obiter 340.

Lourens J *Electronic Commerce- the Law and its Consequences* 1998 (May) De Rebus 64.

Macavinta C *Signature Struggle* (1999) 5:7 Intelligence 26.

Malan FR and Pretorius JT Malan on Bills of Exchange, Cheques and Promissory Notes in South African Law 3rd ed (1997) Durban: Butterworths.

Malan FR *Legal Implications of Electronic Storage* (1990) 2 Stellenbosch Law Review 153.

Meiring I *ATM's and EFTPOS: Some Legal Considerations* (1987) 9 Modern Business Law 115.

Meiring I *The South African Payment System* (1996) 8 South African Mercantile Law Journal 164.

Monaghan V Who Says the Signature's Genuine? (1997) 5:2 Juta's Business Law 53.

Mooki O DNA Typing as a Forensic Tool: Applications and Implications for Civil Liberties (1997) 13:4 South African Journal on Human Rights 565.

Moyer L *Going Digital – With Fingerprint ID* (1997) 162:43 American Banker 16.

Negin M, Chmielewski TA, Salganicoff M, Camus TH, von Seelen UMC, Venetianer PL and Zhang GG *An Iris Biometric System for Public and Personal use* 2000 (February) Computer 70.

Newman SP The Legal Implications of Credit Card Agreements in South Africa (1999) unpubl LLM Dissertation UPE.

Pankanti S, Bolle RM and Jain A *Biometrics: The Future of Identification* 2000 (February) Computer 46.

Parker DB Fighting Computer Crime: A New Framework for Protecting Information (1998) New York: Wiley Computer Publishing.

Pistorius T *The Enforceability of Shrink-Wrap Agreements in South Africa* (1993) 1 South African Mercantile Law Journal 1.

Pistorius T *The Rights of the User of a Computer Program and the Legality of Shrink-Wrap Licences* (1991) 3 South African Mercantile Law Journal 57.

Poullet Y *et al* Telebanking, Teleshopping and the Law (1988) London: Kluwer Law and Taxation Publishers.

Price SA *Understanding Contemporary Cryptography and its Wider Impact Upon the General Law* 1999 (August) 13:2 International Review of Law 95.

Reed C Electronic Finance Law (1991) London: Woodhead: Faulkner.

Saunders K and Zucker B *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act* 1999 (August) 13:2 International Review of Law 183.

Schreiner ME and Kuner C *Dispute Resolution in International Electronic Commerce* (1998) 14 Journal of International Arbitration 5.

Schwartau W Information Warfare: Chaos on the Electronic Superhighway (1994) New York: Thunder's Mouth Press.

Schwellnus T Die Aard en Rol van die Handtekening as Betalingsmagtiging (1991) unpubl LLM Dissertation PU for CHE.

Schwellnus T *Die effektiwiteit van die Handtekening as Identifikasiemiddel met Verwysing na Poswissels* (1992) Obiter 125.

Sharrock R Business Transactions Law (1989) Cape Town: Juta & Co Ltd.

Sharrock R Business Transactions Law 4th ed (1996) Cape Town: Juta & Co Ltd.

Sher A *Authentication and Legalization of Foreign Documents* 1998 (May) De Rebus 30.

Smith GJH *et al* Internet Law and Regulation (1996) FT Law & Tax.

Smuts WB *A Survey of Information Authentication Techniques* (1994) 11 South African Computer Journal 84.

Sonnekus JC *Videotestamente Naas Skriftelike Testamente* 1990 Tydskrif vir die Suid-Afrikaanse Reg 114.

Stassen JC *Legal nature of Travellers' cheques* (1978) 95 South African Law Journal 180.

Strossen N *Cybercrimes v Cyberliberties* 2000 (March) 14:1 International Review of Law 11.

Sykes JB (Ed) The Concise Oxford Dictionary of Current English (1984) Oxford (England): Clarendon Press, New York: Oxford University Press.

Theofanos M and Phillips J *Digital Signatures: Signing and Notarizing Electronic Forms* Records Management Quarterly (April 1994) 18.

Van der Merwe M *Cybercontracts* (1998) 6:4 Juta's Business Law 138.

Van Jaarsveld IL *About Credit Cards and Liability* (XXXXI) 2 Codicillus 92.

Visser C *Banking in the Computer Age: The Allocation of Some of the Risks Arising from the Introduction of Automated Teller Machines* (1985) 102 South African Law Journal 646.

Visser C *The Evolution of Electronic Payment Systems* (1989) 1 South African Mercantile Law Journal 189.

Von Solms SH *Digital Signatures for Secure Data* 1989 (January) 85 South African Journal of Science 22.

Wilde C *Legally Binding E-Documents Move Closer to Reality* (2000) 776 Information Week 120.

B. TABLE OF CASES

Associated Engineers Co Ltd v Goldblatt 1938 WLD 139.

Bernstein and Others v Bester and Others NNO 1996 2 SA 751 (CC).

Bernstein and Others v Bester and Others NNO 1996 4 BCLR 449 (CC).

Bird v Summerville and Another 1960 4 SA 395 (N).

Cape Explosives Works Ltd v South African Oil & Fat Industries Ltd 1 1921 CPD 244.

Carlill v Carbolic Smoke Ball Company [1893] 1 QB 256 (CA).

Chisnall and Chisnall v Sturgeon and Sturgeon 1993 2 SA 642 (W).

Colee Investments v Papageorge 1985 3 SA 305 (W).

Collen v Rietfontein Engineering Works 1948 1 SA 413 (A).

Crawley v Rex 1909 TS 1106-1108.

Dempers and others v The Master and others 1977 4 SA 44 (SWA).

Driftwood Properties (Pty) Ltd v McLean 1971 3 SA 591 (A).

Entores Ltd v Miles Far East Corporation [1958] 2 ALL ER 493 (CA).

Ex Parte Goldman and Kalmer 1965 1 SA 464 (W).

Ex Parte Singh 1981 1 SA 793 (W).

Goldblatt v Fremantle 1920 AD 123.

Gollach & Gomperts (1967) (Pty) Ltd v Universal Mills & Produce Co (Pty) Ltd and Others 1978 1 SA 914 (A).

Goodman v J Eban Ltd 1954 1 QB 550 (CA).

Harpur v Govindamall 1993 4 SA 751 (A).

Howey v Whipple 48 N.H. 487 (1869).

In re Trollip (1895) 12 SC 243.

Jhajbhai v The Master 1971 2 SA 370 (D).

Jonnes v Anglo-African Shipping Co (1936) Ltd 1972 2 SA 827 (A).

Jurgens v Volkskas 1993 1 SA 214 (AD).

Kergeulen Sealing & Whaling Co Ltd v Commissioner for Inland Revenue 1939 AD 487.

Laws v Rutherford (1924) AD 261.

M v R 1989 1 SA 416 (O).

Mellvill and Another NNO v The Master and Others 1984 3 SA 387 (C).

Morton v Copeland (1855) 16 CB 517.

Navidas v Essop 1994 4 SA 141 (AD).

Nell v Nell 1990 3 SA 889.

O v O 1992 4 SA 137 (C).

Putter v Provincial Insurance Co Ltd and Another 1963 3 SA 145 (W).

R v Nel (1921) AD 339.

Reid Bros (South Africa) Ltd v Fischer Bearings Co Ltd 1943 AD 232.

S v Henckert 1981 3 SA 445 (A).

S v Katsikaris 1980 3 SA 580 (A).

S v L 1992 3 SA 713 (E).

Seetal v Pravitha 1983 3 SA 827 (D).

Swart v Vosloo 1965 1 SA 100 (A).

Van der Harst v Viljoen 1977 1 SA 795 (C).

Van Niekerk v Smit 1952 3 SA 17 (T).

Yates v Dolton 1938 EDL 177.

C. LEGISLATION

Alienation of Land Act 68 of 1981

Bills of Exchange Act 34 of 1964

Computer Evidence Act 57 of 1983

Constitution of the Republic of South Africa Act 108 of 1996

Copyright Act 98 of 1979

Credit Agreements Act 75 of 1980

Criminal Procedure Act 51 of 1977

Electronic Communications and Transaction Bill of 2002 (pending)

Electronic Fund Transfer Act 1978 15 USC 1693

Electronic Signatures Act, Oregon Revised Statutes s192.825 (1997 OR HB 3046)

Electronic Signatures in Global and National Commerce Act 15 USCA 7001

Formalities in Respect of Leases of Land Act 18 of 1969

Interpretation Act 33 of 1957

Law of Succession Amendment Act 43 of 1992

Participation Bonds Act 65 of 1981

Post Office Act 44 of 1958

Promotion of Access to Information Act 2 of 2000

Property Timesharing Control Act 75 of 1983

Rent Control Act 80 of 1976

Security by Means of Movable Property Act 57 of 1993

Supreme Court Act 59 of 1959

Trade Marks Act 193 of 1994

UNCITRAL (United Nations Commission for International Trade Law) Model Law on Electronic Commerce and the Guide to Enactment

United Kingdom (U K) Electronic Communications Act of 2000

United States Uniform Commercial Code 1990

Utah Code Ann. S46-3-101

Wills Act 7 of 1953 (as amended)

D. INTERNET ARTICLES

American Bar Association *The Digital Signature Guidelines* <http://www.abanet.org/scitech/ec/isc/dsg-html> (2000-08-14)

Anon *Biometric Technology Overview* <http://www.biometricgroup.com/a_biometrics_42/biometric_technology_overview.asp> (2000-07-31)

Anon *Breaking In* <http://www.zdnet.co.za/pcmag/features/biometrics/break.html> (2000-02-08)

Anon *Inkless Fingerprinting vs Biometric Finger Scanning* <http://www.biometricgroup.com/a_biometrics_42/inkless_fingerprinting.htm> (2000-07-31)

Anon *Introduction to Cryptography* <http://www.ssh.fi/tech/crypto/intro.htm> (2000-06-10)

Anon *Is a Digital Signature Legal?* <http://www.salaw.co.za/library/digsigleg.htm> (2002-03-10)

Anon *Protect Yourself: Secure Transactions* <http://www.learnthenet.com/english/html/07secur.htm> (2000-05-24)

Anon *Security in Internet* <http://www.signlist.com/> (1999-09-15)

Ashbourn *The Biometric White Paper* <http://www.biometric.freeserve.co.uk/whitepaper.htm> (2000-07-24)

Bloomberg News *Chips aim to make passwords obsolete* <http://www.news.cnet.com/news/0-1006-200-1510976.html> (2000-07-19)

Campbell *Smart gun prototype to be ready by March* at <http://www.engineeringnews.co.za/engnews...65bc2?OpenDocument&Highlight=0,biometric> (2000-04-07)

Campbell, Alyea and Dunn *Government Applications and Operations* <http://www.biometrics.org/REPORTS/CTSTG96> (2000-04-13)

Committee on Banking and Financial Services *Hearing on Biometrics and the Future of Money* <http://www.house.gov/banking/52098cas.htm> (2000-07-24)

Craig *Smart Card Chip Reads Fingerprints* <http://www.techweb.com/news/story/TWB19980217S0013> (2000-04-09)

Department of Communications *Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce* <http://www.ecomm-debate.co.za/docs/report.html> (2000-05-18)

Dorney *Electronic Signatures in Global and National Commerce Act* <http://www.gcwf.com/articles/interest/interest_36.html> (2001-05-01)

Featherly *Expert: Encryption Gets Better, but Remains Imperfect* <http://www.computeruser.com/news/00/06/19/news8.html> (2000-07-08)

Ford *Identity Authentication and 'E-Commerce'* <http://elj.warwick.ac.uk/jilt/98-3/ford.html> (2000-04-15)

<http://128.119.27/centre/ombuds/default/htm>

<http://www.law-sa.co.za>

<http://www.penop.com> (2001-03-17)

<http://www.saca.net>

<http://www.visa.com> (2000-11-01)

Jain, Hong and Pankanti *Biometrics: Promising Frontiers for Emerging Identification Market* <http:///www.cse.msu.edu/cgi-user/web/tech/document?ID=436> (2000-07-18)

Katz and Schwartz *Electronic Documents and Digital Signaturing: Changing the Way Business Is Conducted and Contracts Are Formed* <http://www.perkinscoie.com/resource/ecomm/edocs&digsig.htm> (2000-01-18)

Koch *The Electronic Signatures in Global and National Commerce Act: Eliminating a Legal Barrier to Electronic Commerce* <http://www.vonbreisen.com/mak_digisign800.htm> (2001-05-01)

Kuner and Baker *An Analysis of International Electronic and Digital Signature Implementation Initiatives* <http://www.ilpf.org/digsig/analysis_IEDSII.htm> (2000-12-18)

Le Roux *E-commerce – The Legal Framework* <http://www.derebus.org.za/scripts> (2000-05-09)

Mallesons Stephen Jaques Solicitors *The PenOp Signature: An Australian Legal Perspective* <http://www.biometrics.org> (1999-09-12)

McBride Baker & Coles *Table 3: Definitions of the Term "Digital Signature" in Enacted Legislation* <http://www.mbc.com/ecommerce/legis/table03.html> (2000-04-14)

Millman *The one and only you* <http://www.archive.infoworld.com/cgi-bin/displayStory.pl?/features/980629biometrics.htm> (2000-07-18)

Ministries of Post and Telecommunication, International Trade and Industry, and of Justice (Japan) *Legal Provisions Relating to Electronic Signatures and Certification: Promoting Electronic Commerce and Otherwise Laying the Foundation for Network-Based Social and Economic Activities* <http://www.info.mpt.go.jp/whatsnew/english/LegalProvisions-e.html> (2001-05-01)

Murray, Vick and Wortley *Regulating E-Commerce: Formal Transactions in the Digital Age* <http://www.internetpolicy.org/briefing> (2001-03-24)

Neethling *E-Signatures Become Legal Tender* <http://www.mg.co.za/pc/2000/10/2010_digisign.htm> (2000-10-25)

Network World Fusion *Message Queue* <http://www.nwfusion.com/archive/2000/97677_06-05-2000.html> (2000-07-18)

O'Sullivan *Biometrics comes to life* <http://www.banking.com/aba/cover_0197.htm> (2000-08-17)

Pleas *Certificates, Keys and Security Technology* <http://www.zdnet.co.za/pcmag/0707/tcert.html> (2000-02-08)

Polemi *Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas Where They are Most Applicable (Final Report)* <http://www.cordis.lu/infosec/src/std5d.htm> (2000-08-17)

Polemi *Review and Evaluation of Biometric Techniques for Identification and Authentication - Final Report* (summary) <http://www.cordis.lu/infosec/src/stud5fr.htm> (2000-08-17)

Prosise *Digital Signatures: How They Work* <http://www.zdnet.com/pcmag/issues/1507/pcmag0090.htm> (2000-04-17)

Randall *Biometric Basics* <http://www.zdnet.co.za/pcmag/stories/reviews/0,6755,392609,00.html> (2000-02-08)

Reed *What is a Signature?* <http://elj.warwick.ac.uk/jilt/00-3/reed.html/> (2001-02-21)

Rosencrance *A Closer Look at the E-Signatures Law* <http://www.computerworld.com/cwi/story/0,1199,NAV47_STO51990,00.html> (2000-11-01)

Shore *Kubler-Ross in Cyberspace: 5 Stages of "Good Grief"* <http://raven.cc.ukans.edu/~cybermom/CLJ/shore/shore.html> (2001-03-24)

Smedinghoff & Bro *The Core Legislative Concern: Electronic and Digital Signatures* <http://www.profs.lp.findlaw.com/signatures/signature_2.html> (2000-12-20)

Sommer *Against Cyberlaw* <http://www.law.berkeley.edu/journals/btlj/articles/15_3/sommer/sommer.html> (2001-12-01)

Stanford *Getting Arrest Warrants Via Computer* <http://www.cnn.com> (1998-03-05)

Van Kralingen, Prins and Grijpink *Using your body as a key; legal aspects of biometrics* <http://www.biometrics.org> (2000-04-17)

Zekos *EDI: Electronic Techniques of EDI, Legal Problems and European Union Law* <http://www.diavlos.com/zekos> (2001-03-24)

E. REPORTS

Department of Communications Green Paper on E-Commerce: "Making it your business" (November 2000)

Department of Communications Report on Electronic Commerce Legal Issues: Discussion Paper on Electronic Commerce (July 1999)

European Commission: Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures: Directive 1999/93/EC (May 1998)

The South African Law Commission Project 50: Investigation into the Payments System in South African Law (1994)

F. REGULATIONS

RK 608 in GN 6429 of 29/04/1960 as amended

RK 609 in GN 6429 of 29/04/1960