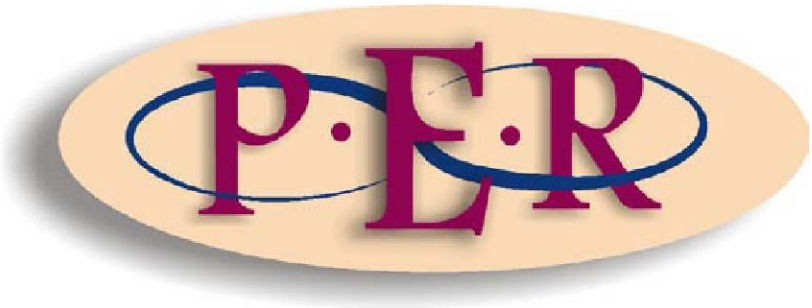
Author: S Eiselen

FIDDLING WITH THE *ECT ACT* – ELECTRONIC SIGNATURES

ISSN 1727-3781



2014 VOLUME 17 No 6

http://dx.doi.org/10.4314/pelj.v17i6.16

FIDDLING WITH THE *ECT ACT* – ELECTRONIC SIGNATURES

S Eiselen*

1 Introduction

The *Electronic Communications and Transactions Act* 25 of 2002 ("*ECT Act*") has now been in operation for more than 10 years.[1] The Act lists six objectives, amongst others, which are relevant for this discussion, namely to:

(a) facilitate ecommerce;[2]
(b) remove and prevent barriers to electronic communications in South Africa;[3]
(c) ensure that electronic transactions in the Republic conform to the highest international standards;[4]
(d) promote the development of electronic transactions services which are responsive to the needs of users and consumers;[5]
(e) ensure compliance with accepted international technical standards in the provision and development of electronic communications and transactions;[6] and
(f) promote the stability of electronic transactions in the Republic.[7]

The Act seems to be functioning very well as an enabling piece of legislation, as set out in these objectives. This is in part evidenced by the fact that there has been very little reported case law requiring an interpretation of the Act[8] other than case law

* Sieg Eiselen. BJuris LLB LLD (PU for CHE). Department of Private Law, University of South Africa. Email: eiselgts@unisa.ac.za.

1 The Act was assented to on 31 July 2002 and came into operation on 20 August 2002.

2 Section 2(1)(c) of the *Electronic Communications and Transactions Act* 25 of 2002 (the *ECT Act*): "[to] promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic".

3 Section 2(1)(d) of the *ECT Act*: "[to] remove and prevent barriers to electronic communications and transactions in the Republic".

4 Section 2(1)(h) of the *ECT Act*.

5 Section 2(1)(k) of the *ECT Act*.

6 Section 2(2)(m) of the *ECT Act*.

7 Section 2(2)(n) of the *ECT Act*.

8 See *Jafta v Ezemvelo KZN Wildlife* 2008 10 BLLR 954 (LC) dealing with offer and acceptance; *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association* 2013 ZAGPJHC 232 (19 September 2013) s 45 dealing with spamming; *Genesis Medical Scheme v Vuyani Ngalwana, The Council for Medical Schemes & Du Toit* 2013 ZAGPHC 340; *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 ZAKZDHC 44 (3 August 2012) s 23 and 26 dealing with electronic service.

dealing with the evidentiary requirements of section 15.[9] It also seems that ecommerce is flourishing in the country as it is elsewhere in the world.[10]

However, the *ECT Act* not only covers ecommerce but also aims at dealing with privacy issues, electronic government services, domain names and cybercrime. It has been recognised that not all of these provisions of the Act have been equally successful and that the Act is in need of amendment.[11] The Department of Communications issued a Bill for the amendment of the *ECT Act* late in 2012 for public comment.[12] Very few of the proposed changes that directly affect Chapter III deal with ecommerce. The only suggested amendments are to section 11(3), and these are more stylistic than anything else. Also, an addition to section 15 deals with the admissibility and evidential weight of data messages. The latter change is also more cosmetic than real.

The only real but important change relating to ecommerce suggested in the Bill is found in a new definition of the term "electronic signature" in section 1. The current definition provides as follows:

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

The suggested new definition for an electronic signature reads as follows:

> 'electronic signature' means a sound, symbol or process that is (i) uniquely linked to the signatory; (ii) capable of identifying the signatory; (iii) created

---

9 See *Cwele* v S 2012 4 All SA 497 (SCA); *Mohlabeng v Minister of Safety and Security* 2008 ZAGPHC 16 (28 January 2008); *Director of Public Prosecutions v Modise* 2012 1 SACR 553 (GSJ); *Firstrand Bank Ltd v Venter* 2012 ZASCA 117 (14 September 2012); *Absa Bank Ltd v Le Roux* 2014 1 SA 475 (WCC); *Buildline Projects (Pty) Ltd v JR-Stocks-Madona-Kanonibo* 2013 ZAGPPHC 341 (25 November 2013); *RMH Agencies CC t/a Midlands Mica Hardware v Pharazyn* 2010 ZAKZPHC 51 (2 September 2010); *Delta Finance, a Division of Wesbank, a Division Firstrand Bank Ltd v Opperman* 2011 ZAWCHC 554 (9 December 2011); *Trend Finance (Pty) Ltd v Commissioner for the South African Revenue Service* 2005 4 All SA 657 (C); *Private Residential Mortgages (Proprietary) Ltd v Mokone* 2013 ZAGPPHC 430 (2 December 2013).

10 See Tubbs and Ngubeni 2014 http://www.itweb.co.za/index.php?id=70515; Bronkhorst 2013 http://businesstech.co.za/news/internet/45736/the-future-of-e-commerce-in-sa/; *National Integrated ICT Policy Green Paper* (GN 44 in GG 37261 of 24 January 2014) para 3.1.2.

11 See the *National Integrated ICT Policy Green Paper* (GN 44 in GG 37261 of 24 January 2014) para 3.4.

12 *Electronic Communications and Transactions Amendment Bill*, 2012 (Gen N 888 in GG 35821 of 26 October 2012).

> using means that the signatory maintain and which are under his control; (iv) linked to the data to which it relates in such a manner that any subsequent change of the data can be detected; and (v) intended by the user to serve as a signature.

It is not clear what has caused the need for this amendment as there has been no indication from practice or the case law that the current definition, read with section 13, is problematic. This note will trace the origin of this new definition and discuss the potentially harmful implications of this rather innocuous looking amendment against the backdrop of the objectives of the *ECT Act* as set out above.

2 Current definition of electronic signature

Chapter III of the *ECT Act* is based on the *UNCITRAL Model Law on Electronic Commerce* (1996)[13] and the *UNCITRAL Model Law on Electronic Signatures* (2001).[14] UNCITRAL developed these model laws as an early response to the legal uncertainties pertaining to ecommerce around the world at that time, especially with the quick growth of the internet.[15]

UNCITRAL opted for model laws rather than a convention, recognising that the differences in domestic legal systems were probably too great for there to be any realistic chance of a convention being adopted. The advantage of a model law is that it provides a basic text and guidance to legislators around the world to base their legislation on.[16] In that way such legislation will have a harmonised undercurrent even though the different enactments are not identical. The *Model Law on Electronic Commerce* has enjoyed a great deal of success with more than 60 jurisdictions around the world using it as the point of departure for their enactments.[17]

---

13 *UNCITRAL Model Law on Electronic Commerce* (1996).

14 *UNCITRAL Model Law on Electronic Signatures* (2001). See Snail "Electronic Contracting" 48-49; Meintjes-Van der Walt "Electronic Evidence" 320-321; Eiselen "eCommerce" 165-166.

15 UNCITRAL 2005 http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2005 Convention.html paras 44-45; UNCITRAL 2012 http://www.uncitral.org/pdf/ english/texts/procurem/ml-procurement-2011/pre-guide-2012.pdf paras 1-4. Also see Estrella Faria *E-Commerce* ix-x.

16 Eiselen *Globalization* 119-120.

17 See UNCITRAL 2014 http://www.uncitral.org/uncitral/en/uncitral_texts.html for a list of the countries which have used the Model Law.

The 1996 Model Law does not contain a definition for an electronic signature. The Model Law instead contains only a provision dealing with situations where the law requires a signature. Article 7 provides as follows:

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

UNCITRAL recognised that a handwritten signature in the paper world has a number of functions such as identifying a person, providing certainty as to the personal involvement of that person in the act of signing, and associating the person with the contents of the document.[18] In many legal systems certain processes such as stamping, printing and even letterheads are accorded recognition as signatures depending on the level of certainty required.[19] Accordingly the minimum requirements for an electronic signature must meet the requirements of identification, authentication and security.[20] Any requirements for electronic signatures should also not require a higher level of security or difficulty than their physical counterparts to comply with the principles of media neutrality and functional equivalence underlying the Model Law.[21] Article 7 meets all of these requirements.

In 2001 UNCITRAL published the *UNCITRAL Model Law on Electronic Signatures* as an addition to the 1996 *Model Law on Electronic Commerce*.[22] The need for this

18 *UNCITRAL Model Law on Electronic Commerce* (1996) paras 53-54; *UNCITRAL Model Law on Electronic Signatures* (2001) para 29. Also see Wang *Law of Electronic Commercial Transactions* 83-85.

19 *UNCITRAL Model Law on Electronic Commerce* (1996) paras 53-54.

20 *UNCITRAL Model Law on Electronic Commerce* (1996) paras 53-54.

21 *UNCITRAL Model Law on Electronic Commerce* (1996) para 15; *UNCITRAL Model Law on Electronic Signatures* (2001) paras 66-67. Also see Van der Merwe et al *Information and Communications Technology Law* 146.

22 *UNCITRAL Model Law on Electronic Signatures* (2001) para 4.

further Model Law to augment Article 7 is explained as follows in the Guide to Enactment:[23]

> In a modest but significant addition to the UNCITRAL Model Law on Electronic Commerce, the new Model Law offers practical standards against which the technical reliability of electronic signatures may be measured. In addition, the Model Law provides a linkage between such technical reliability and the legal effectiveness that may be expected from a given electronic signature. The Model Law adds substantially to the UNCITRAL Model Law on Electronic Commerce by adopting an approach under which the legal effectiveness of a given electronic signature technique may be predetermined (or assessed prior to being actually used). The Model Law is thus intended to foster the understanding of electronic signatures and the confidence that certain electronic signature techniques can be relied upon in legally significant transactions.

The provisions in the *Model Law on Electronic Signatures* are somewhat differently structured to those of Article 7 of the *Model Law on Electronic Commerce*, but the basic requirements and principles are retained.[24] Although only suggested in the 1996 Model Law, the 2001 Model Law makes it clear that the sufficiency of an electronic signature is first and foremost determined by the parties themselves unless there is a peremptory law requiring a signature.[25] Article 7(1) of the 2001 Model Law determines that any person or authority may determine which type of electronic signatures will satisfy the requirements contained in Article 6. Article 6 provides that where the law requires a signature, that requirement will be met if an electronic signature is used that is as reliable as is appropriate for the purpose for which the data message was generated or communicated in the light of the circumstances, including any agreement.

These requirements are essentially the same as those required in Article 7 of the 1996 Model Law. Unlike the 1996 Model Law, the 2001 Model Law contains a definition of an "electronic signature". Article 6 of the 1996 Model Law must therefore be read taking into account the following definition in Article 2:

> (a) 'Electronic signature' means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in

23 UNCITRAL 2012 http://www.uncitral.org/pdf/english/texts/procurem/ml-procurement-2011/pre-guide-2012.pdf para 4.

24 *UNCITRAL Model Law on Electronic Signatures* (2001) paras 67, 107, 111.

25 *UNCITRAL Model Law on Electronic Signatures* (2001) para 112.

> relation to the data message and to indicate the signatory's approval of the information contained in the data message …

Read together the two provisions are almost identical to Article 7 of the 1996 Model Law. The definition adds the requirements that the data affixed or logically associated with the data message to be signed may be used to identify the signatory, connects the signatory to the data message, and indicates the signatory's approval of the information contained in the data message.[26]

It is important to note that there are no requirements that the signature should be uniquely linked to the signatory or that it must be created by means that the signatory maintain and which are under their control or that it must be capable of ensuring that any subsequent change to the data can be detected as required in the new South African definition quoted above. The requirements in the two Model Laws set out minimum standards rather than maximum standards. The standards required are determined by any peremptory law, the agreement between the parties and the relevant circumstances.[27] These additional criteria are found in Article 6(3), which creates only a presumption. They are not requirements for validity. The Article reads as follows:

> 3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
> (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
> (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
> (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
> (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

The Guide to Enactment makes it clear that subparagraphs 6(3)(a)-(d) are intended to express objective criteria of the technical reliability of electronic signatures, but it is formulated as a presumption. Subparagraph (a) focuses on the objective

---

26 This is identical to the requirements of Article 7(1)(a) of the *UNCITRAL Model Law on Electronic Commerce* (1996).

27 UNCITRAL 2012 http://www.uncitral.org/pdf/english/texts/procurem/ml-procurement-2011/pre-guide-2012.pdf para 120.

characteristics of the signature creation data, which must be "linked to the signatory and to no other person"; subparagraph (b) deals with the circumstances in which the signature creation data are used; subparagraphs (c) and (d) deal with the issues of integrity of the electronic signature and the integrity of the information being signed electronically.[28] It is significant to note that these requirements are not set as general requirements for validity, but are set only as a guideline where electronic signatures that meet these requirements are deemed reliable. This deeming provision therefore does not violate any of the basic principles underlying the original 1996 Model Law, but adds another layer to it in an attempt to provide greater legal certainty where it is needed. The principle of party autonomy is adhered to in that parties may still choose to use less certain electronic signatures which may nevertheless be valid in law provided they meet the minimum requirements set out in Article 6(1). The general requirements for validity are contained in Article 6(1) and are quite flexible, being based on the principle of party autonomy. Articles 6(1) and 6(3) are in harmony, because the requirements of Article 6(3) merely have bearing on the deemed evidential value of electronic signatures that meet those requirements.

Both of these instruments were available and were relied on when the *ECT Act* was drafted. It is immediately obvious that although the current definition of an electronic signature in the Act is not identical to the requirements contained in Article 7 of the 1996 Model Law or the definition contained in Article 2(a) of the 2001 Model Law, it does contain elements of both, namely the requirement that the data which is intended to serve as a signature must be attached to, incorporated in or logically associated with the data message to which it relates. The South African definition then simply requires that that data must be intended by the user to serve as a signature. The further requirements contained in the two Model Laws - that a method must be used which may identify the signatory, connect the signatory to the data message and indicate the signatory's approval of the information contained in

[28] UNCITRAL 2012 http://www.uncitral.org/pdf/english/texts/procurem/ml-procurement-2011/pre-guide-2012.pdf paras 121-125.

the data message - has been taken up in section 13(3)(a) of the *ECT Act*, which provides:

> (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; …

The requirement in the current definition that the data must be intended to serve as the user's signature is a uniquely South African requirement not found in any of the UNCITRAL instruments or in the legislation considered at the time of drafting the *ECT Act*. Other countries have tended to follow the UNCITRAL approach and definition.

UNCITRAL has had a third bite at this particular cherry. When it drafted the 2005 Convention[29] it chose not to define the term "electronic signature" in the Convention. Instead UNCITRAL chose to stick with the minimum requirements as set out in Article 7 of the Model Law.[30] The only novelty in Article 9 of the Convention is the provision that determines that in regard to reliability a party may prove that the electronic signature in fact fulfilled the functions or requirements set out in Article 9(3)(a).

The current South African definition is therefore based to some extent on the requirements of Article 7 of the 1996 Model Law or the definition contained in the 2001 Model Law. The requirement that the electronic signature must have been intended by the user to be a signature is a uniquely South African requirement. It is

---

29 *UNCITRAL Convention on the Use of Electronic Communications in International Contracts* (2005) paras 44-45.

30 Article 9 of the Convention reads as follows:

> 3. Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
> (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and
> (b) The method used is either:
> (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
> (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

nothing new, however, as this intention is also required of traditional physical signatures. This requirement therefore also complies with the principle of media neutrality.[31]

3 Genesis and consequences of the new definition

The new South African definition contained in the proposed amendment to section 1 of the *ECT Act* states the following requirements for an electronic signature. It must be:

(i) uniquely linked to the signatory;
(ii) capable of identifying the signatory;
(iii) created using means that the signatory maintain and which are under his control;
(iv) linked to the data to which it relates in such a manner that any subsequent change of the data can be detected; and
(v) intended by the user to serve as a signature.

Save for the last requirement, which is contained in the current definition of the *ECT Act*, requirements (i) to (iv) seem to have their origin in the presumption contained in the definition of an advanced electronic signature of the EC Directive of 1999[32] and Article 6(3) of the *UNCITRAL Model Law on Electronic Signatures* of 2001. Under the EC Directive these requirements are not set for ordinary electronic signatures but only for advanced electronic signatures as defined in Article 1 of the Directive. Article 5(1) of the Directive determines that advanced electronic signatures must be recognised as valid signatures whereas ordinary electronic signatures may not be denied legal effect or admissibility. Article 5(1) of the Directive therefore requires the creation of a presumption of validity and admissibility for advanced electronic signatures not afforded to ordinary electronic signatures.[33] This is similar to the presumption created in Article 6(3) of the 2001 UNCITRAL Model Law. Unlike the

31 See *UNCITRAL Model Law on Electronic Signatures* (2001) para 67 for a discussion of this principle.

32 EC Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. However, that system is based on voluntary accreditation and not mandatory accreditation for advanced electronic signatures. For the position in Australia and New Zealand, see Davidson *Electronic Commerce* 40; Krelzheim and Sneddon "Digital Signatures" 63-73.

33 Wang *Law of Electronic Commercial Transactions* 97-98.

presumptions created in these instruments, the new South African definition makes these requirements peremptory for all electronic signatures.

The *ECT Act* currently uses a two-pronged approach to electronic signatures, namely a simple electronic signature identical to the provisions of the 1996 Model Law and an advanced electronic signature where "a law" requires an electronic signature.[34] The advanced electronic signature requires the involvement of a trusted third party issuing an electronic signature which is then cloaked with certain evidential advantages not provided to simple electronic signatures.[35] Section 13(4) provides that where an advanced electronic signature has been used, such a signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.[36] It therefore creates an evidential presumption which does not exist in relation to ordinary electronic signatures.

Advanced electronic signatures had been a dead letter in the Act until recently, as the Department of Communications in its capacity as the Accreditation Authority in terms of section 34 of the *ECT Act* had not accredited a single service provider until 2011. That changed with the accreditation of LAW Trusted Third Party Services (Pty) Ltd ("LAWtrust") in 2011[37] and the South African Post Office in 2013[38]. In practice the use of advanced electronic signatures is bound to be limited due to the fact that the process of obtaining such a signature is cumbersome (face-to-face identification) and expensive. A general requirement for advanced electronic signatures would therefore seriously hamper electronic commerce.

To date there has been no case law dealing with electronic signatures in the commercial domain. There are either very few problems with electronic signatures or ecommerce suppliers have found acceptable ways to deal with electronic signatures.

---

34 This is similar to the approach followed in the EC Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. See the definitions of "electronic signature" and "advanced electronic signature".

35 See s 13 (4) of the *ECT Act*.

36 This is similar to the position under the EC Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.

37 See eLawtrust 2014 http://www.lawtrust.co.za/aesign.

38 See SAPO 2014 https://www.trustcentre.co.za//index.php.

In any event it would seem that the necessity for any significant change to the existing legal regime contained in section 13 of the *ECT Act* is absent.

It is submitted that the suggested change represents a major shift in the general requirements for electronic signatures, is contrary to the basic principles of party autonomy, media-neutrality and functional equivalence underlying Chapter III of the *ECT Act*, and should for that reason not be adopted. The suggested change is at odds with the provision of a simple electronic signature provided for in section 13(3) of the *ECT Act*, and would render the simple electronic signature a dead letter as it would invariably require the involvement of a third party. Instead of facilitating electronic commerce, the suggested amendment will place a new obstacle in the path of electronic commerce, if the standard is required for all electronic signatures. The suggested change is also contrary to current international best practice as evidenced in the 2005 UNCITRAL Electronic Communications Convention.

It may be useful to amend section 13 and include the presumption contained in Article 6(3) of the *UNCITRAL Model Law on Electronic Signatures* as an additional subsection providing for a media-neutral presumption where parties use a method that meets those criteria.

4 Conclusion

The proposed new definition for electronic signatures in the *Electronic Communications and Transactions Amendment Bill*, 2012[39] is ill conceived even though it is based on section 6 of the *UNCITRAL Model Law on Electronic Signatures* of 2001. Unlike the 2001 Model Law, which provides for a presumption of validity and authenticity if certain requirements are met, including those requirements in a definition fundamentally alters the requirements for all electronic signatures. It is at odds with the simple electronic signature currently contained in section 13(3) of the *ECT Act* and the principle of party autonomy.

[39] *Electronic Communications and Transactions Amendment Bill*, 2012 (Gen N 888 in GG 35821 of 26 October 2012).

It is suggested that the current definition of an electronic signature be retained and that the proposed new criteria be added as a presumption in section 13 in the same manner as in the 2001 UNCITRAL Model Law. This will provide parties with the opportunity to use technology which meets these criteria even though the signatures are not advanced electronic signatures, which will have a higher probative value where needed.

BIBLIOGRAPHY

Literature

Davidson *Electronic Commerce*

Davidson A *The Law of Electronic Commerce* (CUP Melbourne 2009)

Eiselen "eCommerce"

Eiselen S "eCommerce" in Van der Merwe D *et al Information and Communications Technology Law* (LexisNexis Durban 2008) 141-199

Eiselen "Globalization"

Eiselen S "Globalization and Harmonization of International Trade Law" in Faure M and Van der Walt A (eds) *Globalization and Private Law – The Way Forward* (Edgar Elgar Cheltenham 2010) 97-136

Estrella Faria *E-Commerce*

Estrella Faria JA "Introduction" in Campbell D (ed) *E-Commerce and the Law of Digital Signatures* (Oceana Dobbs Ferry 2005) ix-x

Krelzheim and Sneddon "Digital Signatures"

Krelzheim D and Sneddon M "Digital Signatures" in Campbell D (ed) *E-Commerce and the Law of Digital Signatures* (Oceana Dobbs Ferry 2005) 63-73

Meintjes-Van der Walt "Electronic Evidence"

Meintjes-Van der Walt L "Electronic Evidence" in Papadopoulos S and Snail S (eds) *Cyberlaw @SA III* 3rd ed (Van Schaik Pretoria 2012) 315-330

Snail "Electronic Contracting"

Snail S "Electronic Contracting in South Africa (econtracts)" in Papadopoulos S and Snail S (eds) *Cyberlaw @SA III* 3rd ed (Van Schaik Pretoria 2012) 41-59

Van der Merwe *et al Information and Communications Technology Law*
Van der Merwe DP *et al Information and Communications Technology Law* (LexisNexis Durban 2008)

Wang *Law of Electronic Commercial Transactions*
Wang FF *Law of Electronic Commercial Transactions – Contemporary Issues in the EU, US and China* (Routledge London 2010)

Case law

Absa Bank Ltd v Le Roux 2014 1 SA 475 (WCC)

Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association 2013 ZAGPJHC 232 (19 September 2013)

Mohlabeng v Minister of Safety and Security 2008 ZAGPHC 16 (28 January 2008)

Private Residential Mortgages (Proprietary) Ltd v Mokone 2013 ZAGPPHC 430 (2 December 2013)

RMH Agencies CC t/a Midlands Mica Hardware v Pharazyn 2010 ZAKZPHC 51 (2 September 2010)

Trend Finance (Pty) Ltd v Commissioner for the South African Revenue Service 2005 4 All SA 657 (C)

Legislation

Electronic Communications and Transactions Act 25 of 2002

International instruments

EC Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures

UNCITRAL Convention on the Use of Electronic Communications in International Contracts (2005)

UNCITRAL Model Law on Electronic Commerce (1996)

UNCITRAL Model Law on Electronic Signatures (2001)

Government publications

Electronic Communications and Transactions Amendment Bill, 2012 (Gen N 888 in GG 35821 of 26 October 2012)

National Integrated ICT Policy Green Paper (GN 44 in GG 37261 of 24 January 2014)

Internet sources

Bronkhorst 2013 http://businesstech.co.za/news/internet/45736/the-future-of-e-commerce-in-sa/

Bronkhorst Q 2013 "The Future of E-commerce in SA" http://businesstech.co.za/news/internet/45736/the-future-of-e-commerce-in-sa/ accessed 10 September 2014

eLawtrust 2014 http://www.lawtrust.co.za/aesign

eLawtrust 2014 *Advanced Electronic Signatures* http://www.lawtrust.co.za/aesign accessed 10 September 2014

SAPO 2014 https://www.trustcentre.co.za//index.php

South African Post Office 2014 *Trust Centre* https://www.trustcentre.co.za//index.php accessed 10 September 2014

Tubbs and Ngubeni 2014 http://www.itweb.co.za/index.php?id=70515

Tubbs B and Ngubeni T 2014 "Smooth Upward Trajectory for SA E-commerce" http://www.itweb.co.za/index.php?id=70515 accessed 10 September 2014

UNCITRAL 2005 http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2005Convention.html

UNCITRAL 2005 *Secretariat Explanatory Note to the Convention on the Use of Electronic Communications in International Contracts* http://www.uncitral.org/

uncitral/uncitral_texts/electronic_commerce/2005Convention.html accessed 10 September 2014

UNCITRAL 2012 http://www.uncitral.org/pdf/english/texts/procurem/ml-procurement-2011/pre-guide-2012.pdf

UNCITRAL 2012 *Guide to Enactment of the UNCITRAL Model Law on Public Procurement* http://www.uncitral.org/pdf/english/texts/procurem/ml-procurement-2011/pre-guide-2012.pdf accessed 10 September 2014

UNCITRAL 2014 http://www.uncitral.org/uncitral/en/uncitral_texts.html

UNCITRAL 2014 *UNCITRAL Texts and Status* http://www.uncitral.org/uncitral/en/uncitral_texts.html accessed 10 September 2014

LIST OF ABBREVIATIONS

ECT Act	Electronic Communications and Transactions Act
SAPO	South African Post Office
UNCITRAL	United Nations Commission for International Trade Law

FIDDLING WITH THE *ECT ACT* – ELECTRONIC SIGNATURES

S Eiselen*

SUMMARY

Amongst the changes the Department of Trade and Industry is considering is an amendment of the definition of "electronic signature". Although the amendment seems to be in line with the provisions of the UNCITRAL Model Laws on eCommerce and the 2005 UN Convention on the Use of Electronic Communications in International Contracts, the amendment sets additional and more onerous requirements for all electronic signatures. The note illustrates how this amendment undermines the key principles of functional equivalence, media neutrality and party autonomy, and how this innocuous looking amendment may have very harmful practical consequences. It is suggested that amendments to section 13 would be more appropriate to achieve the objectives of the legislature.

KEYWORDS: Electronic signatures; digital signatures; *Electronic Communications and Transactions Act*; UNCITRAL Model Law.

* Sieg Eiselen. BJuris LLB LLD (PU for CHE). Department of Private Law, University of South Africa. Email: eiselgts@unisa.ac.za.