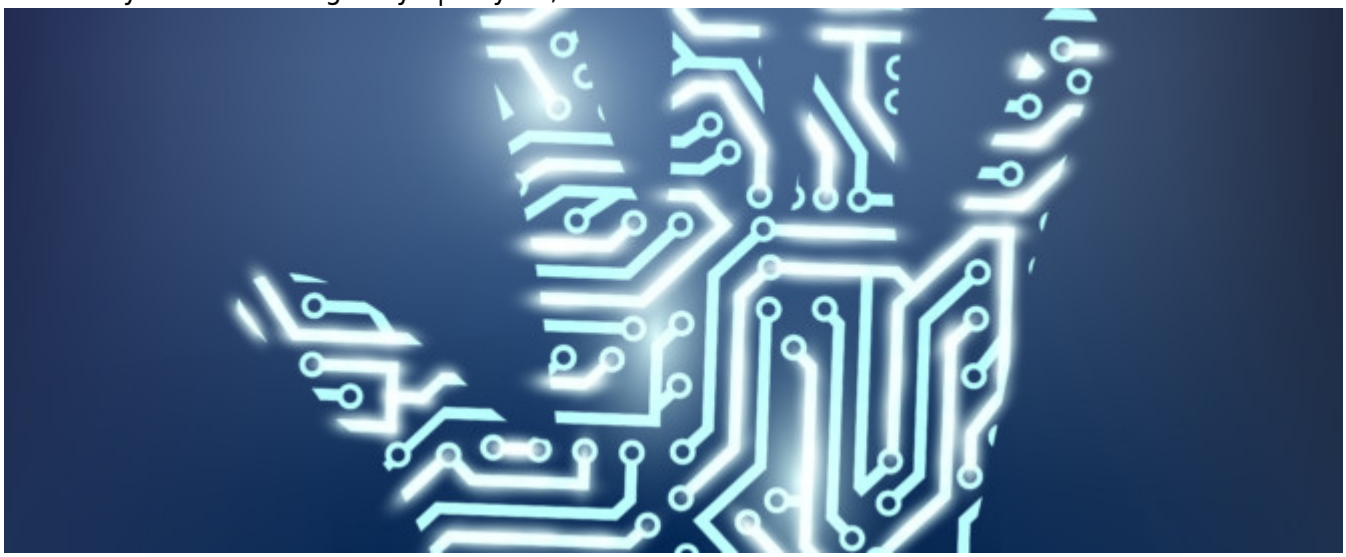
COVID-19 UPDATE: VERIFYING ELECTRONIC SIGNATURES AND NOTARISATION

Category: Commercial Law,Privacy Law, Infosec, and POPIA,Technology Law
written by Nonhlanhla Ngwenya | May 15, 2020



Within the past month, we have gone from mainly needing to authenticate and verify documents through a physical (wet-ink) signature to an era where the need to authenticate and verify documents online is inevitable. We have effectively moved from paper-based certification and verification to electronic authentication This effectively, all in a bid to safeguard against the COVID – 19 pandemic, by following specified precautions and trying to efficiently work remotely whilst maintaining social distancing practice. Stay at home, work from home, and by all means legally sign, authenticate and verify documents via electronic means. To this end, we've provided a review of the relevant legislation on how to properly use an electronic signature ("**e-signature**"), how to certify documents electronically, or how to certify a printout of electronically generated documents.

The validity of e-signatures and the legal requirements around certification are found primarily in the Justice of the Peace and Commissioner of Oaths Act, 16 of 1963 and the Electronic Communications and Transactions Act, 25 of 2002 ("**the ECT Act**").

Affixing an E-Signature

ECT Act provides that an e-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*. This definition provides that the form of an e-signature may have a legal and evidential effect on document. Importantly, the intent to sign the document electronically must exist for it to be considered legal e-signature. According to ECT Act e-signature definition the person signing must have intended to sign the document. When there are doubts around the use of e-signatures, the court will mainly focus on the intention of the parties, rather than on the form of their acts.[1]

Section 18 of the ECT Act provides for the following:

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

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form ,that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature''

In terms of ECT Act, where a document has to be signed electronically in terms of any law, an 'advanced electronic signature' is required. The use of an advanced e-signature means a signature which results from a process which has been accredited by the Authority as provided for in section 37.[2] The South African Accreditation Authority ("**SAAA**") is the primary Authority that can accredit advance signatures in accordance to section 37.[3] Section 37 provides that SAAA may accredit authentication products and services in support of advanced e-signatures , and sets out what occurs when a person falsely states, either explicitly or implicitly, that its products or services are accredited by SAAA.

There are various methods of affixing an e-signature such as; including signatures in emails, PDFs and faxes, a name typed in electronic format at the bottom of an email; using an e-pen or biometric to sign, digitised picture or image of a manual signature and/or perhaps a digital signature[4]. A digital signature which is provided by processes offered by various commercial firms, such as Nitro DocuSign and Adobe Sign would also constitute a valid e-signature[5] There are also various other software products available which secure e-signatures as long as they are affixed to or associated to a relevant document.

It must be emphasised however that there are some circumstances where the law prohibits the use of e- signatures. These circumstances include documents relating to change of legal status (such as marriage, adoption, succession), transfer of real estate rights and interests; executing wills or codicils, bills of exchange such as cheques, and long-term agreements for immovable property.

Electronic Certification and Notarisation

When certifying a copy of an original document which must be certified as "a true copy of the original "one must follow the traditional approach.[6] Additionally, one must make note of section 18 read with section 14 of the ECT Act which provides considerations of when an electronically generated document can be certified to be a true original. Section 14 of the ECT Act provides as follows:

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 the 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 ECT Act is clear that along with above requirements it requires that a Commissioner of Oaths to satisfy themselves fully with the authenticity of the original electronic document.

Although e-signature laws or certifying an electronic copy of an original document have been in effect for a number of years, they may not have been commonly used by your business. If you are only starting to sign online and are confused with what is required to validate or certify a document, contact us for good, clear, precise advice.

[1] Examine Section 13 of ECT Act for expanded understanding on electronic signature.

[2] The Regulations governing accreditation were published in Government Gazette No. 8701, No. 29995, Vol. 504).

[3] http://www.saaa.gov.za/(Last accessed 28th April 2020)

[4]. For additional examples examine Sylvia Papadopoulos, Sizwe Snail, *Cyberlaw @ SA III.* Van Schaik, 2012 p321

[5] A digital signature which is a uses cryptography to establish the authenticity and validity of the signature with much greater certainty . The data is encrypted and may prove where document came from.

[6] The traditional approach is that copy of an electronically generated document can be certified to be a true original of the electronically generated document by a ta commissioner of oaths, when certifying a copy of an original document which must be certified as a true copy of the original must be compared with the original document and the Commissioner of Oaths must be sure that the two documents are, in fact, the same Mere knowledge of the existence of the original document will not suffice – the Commissioner must personally inspect/view the original document and comparesame to the copy. If the Commissioner of Oaths is sure that the copy is in fact a true copy of the original document and no unauthorised amendments have been made, the Commissioner of Oaths must write down or stamp that he/she certifies that the document is a true copy of the original.