CERTIFICATION OF DOCUMENTS ELECTRONICALLY

BY ALISON LEE

26 MAY 2015

QUERY

Is it possible for a Commissioner of Oaths to certify a printout of an electronically generated document as a copy of the original?

I’m thinking of bank statements and the like which are increasingly sent by email these days, as well as information on web portals such as tax documentation accessible via the SARS eFiling website.

Is the correct approach that the Commissioner of Oaths need only view the original document on screen first (and provide the usual certification along the lines of “certified a true copy of the original”) or should one also change the wording of the standard certification in some way?

ANSWER

Yes, it is possible for a Commissioner of Oaths to certify a printout of an electronically generated document as a copy of the original.

This is permitted under section 18 of the ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 (ECTA).

In short a reproduced document in soft copy of an electronically generated document can be certified to be a true original of the electronically generated document by a Commissioner of Oaths which is done by following the normal approach used in the past, i.e “certified a true copy of the original”, save that the document in original format is electronic. The wording – “certified a true copy of the original” will stay the same.

In turn a document in soft copy can be scanned and this electronic document can then be certified electronically as a true copy of the original soft copy, by a Commissioner of Oaths provided that he / or she uses an “advanced electronic signature” when certifying and signing the electronic document, which “advanced electronic signature” is a special type of signature which is encrypted and which one has to purchase from an accredited service provider.
Following the above

1. Normal procedure – copy of a soft copy

If a soft copy needs to be certified as a true original- then the soft copy is duplicated and presented with the original to the Commissioner of Oaths. He/she will then make sure it is a true copy and stamp the copy using his COA stamp and sign and date the document - indicating it is a true copy of the original document.

2. Copy of an electronically generated document

If the document is an electronic document - i.e. it is an email or is an electronic bank statement – then one should make a copy- i.e print a copy, and present this to the COA – he or she will then look at the electronic document on the Laptop or PC and the copy and if in agreement that they correspond – certify the copy as being an original as above- i.e stamp the copy using his COA stamp and sign and date the document - indicating it is a true copy of the original document.

3. Copy of a soft document - electronically certified

Conversely - If the document is a paper / soft document and one wants to have it certified in electronic format - then one should provide a duplicate in electronic format i.e. scan or photograph the original soft copy and present this electronic version to the COA – he or she will then look at the soft copy original and the electronic document on the Laptop or PC and if they correspond - he or she will certify and sign the electronic version indicating that the electronic version is a copy of the soft version /original – but the signature must be an “advanced electronic signature”.

4. What is an advanced electronic signature?

An ‘advanced electronic signature’ has been defined as “an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37”.

Conversely an ‘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”.

In terms of ECTA- where a document has to be signed in terms of any law, then an ‘advanced electronic signature’ has to be used.

On the other hand, where the parties have agreed that an electronic document may be signed, and there is no law which requires a signature, and the parties have not agreed on a type of signature then the document can be signed by applying an ‘electronic signature’, which can be any data incorporated in, or logically associated with other data and which is intended by the user to serve as a signature or alternatively some other method is used to identify the person and to indicate the person’s approval of the information communicated.

Accredited ‘advanced electronic signatures’ are available for purchase in South Africa. See note at the end of this opinion.

Please find below some more detail on the above as well as the references used to support the opinion.

Regards

Alison Lee
Lee’s Compliance
DETAILED SYNOPSIS

The section which applies to your query is section 18 of ECTA - reproduced below:

018 NOTARISATION, ACKNOWLEDGEMENT AND CERTIFICATION

(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.

The above should be read with section 14 of the Act which reads as follows:

014 ORIGINAL

(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 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.

Following the above

1. Normal procedure – copy of a soft copy

If a soft copy needs to be certified as a true original- then the soft copy is duplicated and presented with the original to the Commissioner of Oaths. He/she will then make sure it is a true copy and stamp the copy using his COA stamp and sign and date the document - indicating it is a true copy of the original document.

2. Copy of an electronically generated document

If the document is an electronic – i.e. it is an email or is an electronic bank statement –then one should make a copy- i.e print a copy, and present this to the COA – he or she will then look at the electronic document on the Laptop or PC and the copy and if in agreement that they correspond – certify the copy as being an original as above- i.e stamp the copy using his COA stamp and sign and date the document - indicating it is a true copy of the original document.

3. Copy of a soft document - electronically certified

Conversely - If the document is a paper / soft document and one wants to have it certified in electronic format -then one should provide a duplicate in electronic format i.e. scan or photograph the original soft copy and and present this
electronic version to the COA – he or she will then look at the soft copy original and the electronic document on the Laptop or PC and if they correspond - he or she will certify and sign the electronic version indicating that the electronic version is a copy of the soft version /original – but the signature must be an “advanced electronic signature”.

4. What is an advanced electronic signature?

An ‘advanced electronic signature’ has been defined as “an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37”.

Conversely an ‘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”.

In terms of ECTA- where a document has to be signed in terms of any law, then an ‘advanced electronic signature’ has to be used.

On the other hand, where the parties have agreed that an electronic document may be signed, and there is no law which requires a signature, and the parties have not agreed on a type of signature then the document can be signed by applying an ‘electronic signature’, which can be any data incorporated in, or logically associated with other data and which is intended by the user to serve as a signature or alternatively some other method is used to identify the person and to indicate the person's approval of the information communicated.

This is as per section 13 of the Act, which is referenced below:

013 SIGNATURE

(1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

(2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.

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

(a) a method is used to identify the person and 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 electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.

(5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that-

(a) it is in the form of a data message; or
(b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred.
APPLYING ADVANCED ELECTRONIC SIGNATURES

LAWtrust

LAWtrust is a specialist IT application security integrator and developer, assisting organisations to create trust in their information and transactional systems, which will enable real business to be done securely and efficiently. LAWtrust, a member of the LAW Holdings Group, is the security partner of choice for organisations in the areas of cryptographic-based security such as digital certificates, PKI, digital signing, encryption, integrity and non-repudiation.

LAWtrust has become the first accredited Authentication Service Provider in South Africa, under the requirements of the ECT Act of 2002, for the provision of Advanced Electronic Signatures. Accredited Advanced Electronic Signatures (AeSigns) are the only signatures that are deemed by law to have been valid and applied correctly by the signatory. These high-assurance signatures are the equivalent of a handwritten signature verified to be true by a handwriting expert and thus can be relied on implicitly in all forms of transactions, approvals, contracts and certified copies.

LAWtrust is rated as a level 2 contributor BBBEE company and includes customers in both the public and private sectors such as the largest departments in central government and the ‘Big Six’ banks.
REFERENCES

"Reproduced under Government Printer’s Copyright Authority No. 11441 dated 29 April 2009”.

MY ACTS > ELECTRONIC COMMUNICATION & INFORMATION > ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002 > ACT

ACKNOWLEDGEMENTS

Government Printer

DISCLAIMER

Whilst care has been taken in the compilation of this publication, the editors and publishers do not accept responsibility for any loss or damage that may be sustained as a result of reliance by any person on the information contained herein.

In particular, readers who may be affected by any statutory provisions dealt with in this publication should refer to the relevant Government Gazette as originally published.

Supplementary information, explanation or opinion given by the authors listed; by Alison Lee; or editorial contributions are merely summaries of the respective Acts and Regulations and are merely opinions of the authors and do not necessarily reflect their views.

The completeness or accuracy of the contents is not warranted and for further and more factual advice please contact CJ LEE ATTORNEYS / Lee’s Compliance at alison.lee@mweb.co.za

COPYRIGHT

Documents on this website may not be copied or published in whole or in part without the permission of the copyright owner

© Lee’s Compliance / Alison Lee 2007-2012

COPYRIGHT AUTHORITY NUMBER 11441 ON SOUTH AFRICAN STATUTES: LEE’S COMPLIANCE PTY LIMITED

“Statutes in original format reproduced under Government Printer’s Copyright Authority No. 11441 dated 29 April 2009”.

COMPANY DETAILS

COMPLIANCE RISK CONTROLLED

Lee's Legal Compliance Services (Pty) Ltd
t/a Lee's Compliance
Reg No: 2010/007346/07  Vat No: 4210182129
Telephone +27 11 476 3217 ext 1 or 2
Cell +27 83 671 3996 ·
Fax +27 11 476 9863 ·
www.leelegal@co.za
75 King Street, Berario, Northcliff, Johannesburg, 2195
P.O. Box 731336, Fairlands, 2030
South Africa