CGF
RESEARCH INSTITUTE
(PTY) LTD
Corporate Governance Framework®

ARTICLE

FROM SIGNETS TO ELECTRONIC SIGNATURES
Johannesburg
20 March 2015

Article by Terrance M. Booysen and reviewed by Niel Maritz (MKM Attorneys: Senior Partner)

As far back as biblical times, it seems that people were also concerned with the authenticity of a person's signature. Although there were far fewer people in those ancient times who actually had the power, authority and means to validate official documents, most of those in positions of authority wore and used signet rings. Signet rings were unique to that person who was permitted to sign royal proclamations, among other official documents.

Interestingly, a signet ring usually contained a unique mirror emblem, specific to its owner, and the ring was used to press its markings into the wax or clay as a seal – or mark – of that person's approval to assure that they had personally sealed such proclamations or official documents.

Expectedly, the signet ring was seldom removed from the finger of the person who bore its authority; these people were typically from royalty, or they were politicians, wealthy citizens or religious leaders. Signet rings (or seal rings) were therefore a person's unique, official signature which allowed people to reasonably test (or compare) one signet compression to the next with little chances of tampering. Needless to say, the signet ring was highly treasured as it provided various assurances to validate the 'genuineness' of a person and or the transaction being undertaken.

As centuries have since passed - with the advent of electronic business which is entrenched worldwide by millions of people and operates across many technological platforms -- including multi-functional mobile devices used across geographical boundaries -- it has become paramount for people to be able to validate the authenticity of the person with whom they are interacting. In other words, it is essential to know *who* you are dealing with and that their signature is *actually* theirs and that their signature can be relied upon with little doubt or hesitation. Before the rise of the technological era, the law in most jurisdictions required signatures to be handwritten and either witnessed, notarised or commissioned. The reason for these requirements was to safeguard the authenticity of the signature and provide appropriate evidence should a legal dispute arise in the future. But as technology has advanced and electronic signatures have become more popular, the methods used to sign documentation have evolved and become far more sophisticated. It is now a commonly accepted practice in the workplace to ensure there is the required authenticity when signing and or receiving documentation electronically, and especially so if such documentation has any form of priority status.

"Your best-laid plans of going paperless come to a screeching halt when you need to get someone's signature on a document. That process typically involves printing the document, signing it yourself, faxing it to the other party, and waiting for them to print, sign, and fax it back - where it's printed yet a third time and filed away in a cabinet forever.

It's an antiquated regimen. It's busy work. But there is a better way.

Electronic signature schemes have become big business. In fact, the e-signing sector is on track to grow north of $5 billion by the end of the decade…"

CMO Dustin Grosse (DocuSign Inc. – Senior Vice President)

The Oxford dictionary defines the term 'electronic signature' as "symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document." If particular requirements are not specified for validity, an electronic signature could be as simple as a typed name or a digitalised image of a handwritten signature. Whilst the terms 'electronic signature' and 'digital signature' may be similar, they may not always be used interchangeably. The term 'digital signature is defined as "a digital code which is attached to an electronically transmitted document to verify its contents and the sender's identity". Digital signatures are encrypted in order to protect its authenticity, whereas an electronic signature is not necessarily encrypted. Interestingly, an *advanced* electronic signature -- unlike an electronic signature -- involves the use of a digital signature which is created with a digital certificate. The digital certificate is provided by an accredited third party Authentication Service Provider, who has completed a face-to-face identification process with its subscriber. Expectedly, an *advanced* electronic signature offers a greater degree of security than a general 'electronic signature' and it is for this reason that certain transactions will require accredited software before the electronic signature will be legally enforceable.

PROUDLY SOUTH AFRICAN

Electronic signatures may be validly used in many types of transactions and contracts and its use is subject to certain exceptions. For example, agreements for the sale of immovable property and wills may not generally be signed electronically. That said, electronic signatures are a valid and legally enforceable method of signing documentation in many countries, including South Africa. However, certain requirements must be met before an electronic signature will be deemed to be valid. Whilst the legal definitions of electronic, digital and advanced electronic signatures may vary between various legal jurisdictions, including the international conventions, it goes without saying that organisations need to be up-to-date with these variances and extremely vigilant in order to determine the validity of a person's so-called 'authority' which underpins electronic documentation.

In South Africa, electronic signatures are a legally enforceable method of signing many different types of documentation and notably, a number of South African pieces of legislation allows its use which include;

- the Electronic Communications and Transaction Act 25 of 2002,
- the National Credit Act of 2005,
- the Companies Act 71 of 2008,
- the Magistrates' Court Rules of 2010, and
- the Consumer Protection Act 68 of 2008.

In terms of the Electronic Communications and Transaction Act ('ECTA'), it is interesting to note that if the law requires a signature and the engaging parties have not agreed to the specific type of signature they require, an electronic signature has legal force and it is binding on the parties. Specifically, in terms of Section 13 (3) of the ECTA, if a digital signature is used (i.e. an advanced electronic signature) then a set of minimum requirements must be met, namely that;

- a method is used to identify the person and to indicate the person's approval of the information communicated; and
- the method of capturing the signature must be reliable.

From an international perspective, the UNECIC (United Nations Convention on the Use of Electronic Communications in International Contracts) is an international convention that regulates the use of electronic communications. Accordingly, the signatories of the UNECIC's are bound by its provisions in respect of their use of 'electronic communications' vis-à-vis the *formation* or *performance* of a contract between the parties and whose places of business are in different countries. Save for various requirements, the UNECIC validates the use of electronic signatures and holds these legally enforceable as a method of signing documentation. Interestingly, the requirements that must be met before an electronic signature is recognised in the UNECIC are similar to those stated in the Model Law on Electronic Commerce, the Model Law on Electronic Signatures and South African law regulating electronic signatures. Indeed, the International Organisation for Standardisation ('ISO') has developed and published an international standard on advanced electronic signatures, and this is found in ISO 14533. Within this standard, it aims to inter alia, assist businesses and governments worldwide to guarantee the long term authenticity of electronic signatures.

Understandably, there are pros and cons linked to electronic signatures but notably their proper application and diligent use will greatly assist the productivity and efficiencies within an organisation. But getting these instruments wrong can also be very costly and this can undoubtedly increase the risk of fraud, as devious parties find ways to copy and store other unsuspecting people's electronic signatures for improper, unauthorised use.

ENDS

Words: 1,187

For further information contact:

CGF Research Institute (Pty) Ltd
Terry Booysen (Chief Executive Officer)
Tel: 011 476 8264
Cell: 082 373 2249
E-mail: tbooysen@cgf.co.za

MKM Attorneys
Niel Maritz (Senior Partner)
Tel: (012) 362 1958
E-mail: niel@mkmattorneys.co.za