Advanced Electronic Signatures

By Grant Christianson

Up until the recent past, where the law required a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement was typically met only if the handwritten signature of the person authorised to perform those acts was used. The goal of this requirement was to safeguard authenticity and provide appropriate proof should a legal dispute arise at a later stage.

It is now possible to achieve the same end with a few simple keystrokes on a computer, thanks to innovative software development and legislative recognition of the rapidly changing manner in which business is done. The accreditation of authentication products and services in terms of s 37 of the Electronic Communications and Transactions Act 25 of 2002 (ECT Act) allows for the electronic signatures of such products and services to qualify as advanced electronic signatures, thus safeguarding the authenticity of the signature.

Accreditation is done by the South African Accreditation Authority (www.saaa.gov.za), which released accreditation regulations in 2007. These set out the criteria, standards and processes to be followed by authentication and certification providers (www.info.gov.za/view/DownloadFileAction?id=72249, accessed 21-9-2012).

Useful definitions

An e-mail can be viewed, in law, as an original written communication; a data message made up of data and compiled using a computer programme (eg Microsoft Outlook). The following definitions from the ECT Act and the Copyright Act 98 of 1978 assist in understanding this better:

- ‘E-mail’ means a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication (s 1 of the ECT Act).
- ‘Electronic communication’ means a communication by means of data messages (s 1 of the ECT Act).
- ‘Data message’ means data generated, sent, received or stored by electronic means (s 1 of the ECT Act).
- ‘Data’ means electronic representations of information in any form (s 1 of the ECT Act).
- ‘Computer programme’ means a set of instructions fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result (s 1 of the Copyright Act). Computer programmes are also referred to as ‘software’.

Further, the ECT Act provides:

- ‘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 (s 11(1)).
- A requirement in law that a document or information must be in writing is met if the document or information is in the form of a data message and is accessible in a manner usable for subsequent reference (s 12).
- Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if certain requirements are met (s 14(1)).

Signatures, electronic signatures and advanced electronic signatures

‘Signature’ is defined as: ‘A person’s name written in a distinctive way as a form of identification in authorising a … document’ (http://oxforddictionaries.com/definition/english/signature?q=signature, accessed 21-9-2012). In law, this is not the only way a document can be signed: ‘Any 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’ (*Putter v Provincial Insurance Co Ltd and Another* 1963 (3) SA 145 (W) at 148E).

An ‘electronic signature’ is data attached to, incorporated in or logically associated with other data and which is intended by the user to serve as a signature (s 1 of ECT Act). An ‘advanced electronic signature’ is an electronic signature that results from a process that has been accredited by the Accreditation Authority (ss 1 and 37 of the ECT Act).

Electronic signatures must be distinguished from advanced electronic signatures. The important factor is whether the signature is required by law. While the ECT Act recognises other forms of electronic signatures used between parties in an electronic transaction (eg a private agreement), these will not be recognised if the signature is required by law (eg signatures required in terms of the Companies Act 71 of 2008).

In this regard, the ECT Act provides:

- An electronic signature is not without legal force and effect merely on the grounds that it is in electronic form, and may be used by the parties to an electronic transaction (s 13(2) and (3) read with the definition of ‘transaction’ in s 1 of the ECT Act).
- 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 (s 13(1) of the ECT Act).

To belabour the point: While an advanced electronic signature is an electronic signature, an electronic signature is not necessarily an advanced electronic signature; the differentiator being whether or not there is accreditation by the Accreditation Authority of the authentication products and services used to create the electronic signature (s 13(2) and (3) of the ECT Act, read with the definition of 'advanced electronic signature' in s 1).

Digital certificates and public key infrastructure

Public key infrastructure (PKI) is a broad term that refers to public and private key cryptography; the hardware, software, people, processes and policies collectively implemented and used to manage risk when transacting electronically (eg online or by e-mail). PKI includes the use of digital certificates to identify the persons behind an electronic transaction (see *ISO 21188:2006, Public key infrastructure for financial services – practices and policy framework*, published by the International Organization for Standardisation (www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35707, accessed 21-9-2012), adherence thereto is required by the Accreditation Authority in a s 37 of the ECT Act accreditation exercise).

Digital certificates are typically issued by certification service providers (note: While the ECT Act refers to certification service providers, in the digital certificate/encryption services industry these entities are generally known as certificate/certification authorities or CAs).

Besides being used as a means of online access control (eg conveyancers logging on to receive bond registration instructions from banks), a digital certificate can also be used to create an electronic signature. If the digital certificate used to create such electronic signature was issued by a certification service provider that has had its authentication products and services accredited in terms of s 37 of the ECT Act, the resultant electronic signature of the individual identified in the digital certificate also qualifies as an advanced electronic signature (s 37 of the ECT Act, read with the definition of ‘advanced electronic signature’ in s 1).

The reasons for supporting the use of digital certificates originate from a commercial perspective. The issues that arise when transacting online usually have to do with how to create enforceable electronic contracts for the sale of goods and services, or how to ensure that an electronic transaction will at least be as legally enforceable and binding as a traditional paper-based transaction. Usernames and passwords have been common means of seeking to achieve this. However, there are instances when requiring the use of a username and a password is simply too risky as these can be compromised by numerous means, for example by wiretapping (covert monitoring of electronic communications), phishing (masquerading as a trustworthy entity to obtain sensitive information), keystroke logging (covert tracking of keys pressed on a computer keyboard), social engineering (obtaining confidential data by manipulating and/or deceiving people), dumpster diving (sifting through commercial data records), side-channel attacks (exploiting data security weaknesses) and other software vulnerabilities.

Digital certificates, in a well-implemented PKI, go a long way towards managing risk when communicating or transacting online, such as those presented by false identity, fraud, unauthorised access, snooping/observation, message alteration and transaction repudiation. A properly issued digital certificate is strong evidence in support of proving the function of a signature in an electronic transaction, namely the conveyance of an attestation by the person signing of his approval and authority for what is contained in the document, and that it emanates from him (*Jurgens and Others v Volkskas Bank Ltd* 1993 (1) SA 214 (A) at 220E – F).

A certification service provider plays an important role in a PKI in that it –

- issues digital certificates;
- sets policy (as stated in its certification practice statement (CPS), a statement issued by a certification service provider to specify the practices that it employs in generating and issuing digital certificates) on what identification a person must produce in order to obtain a digital certificate; and
- in order to maintain security, indicates in a published certificate revocation list those digital certificates that are no longer valid (eg revoked, expired or suspended).

A digital certificate is an electronic form of identification, much like an identity document, passport or driver's licence. Technically, it is –

- a strong method of authentication, which is likened to a 'cryptographic handshake' as opposed to a shared secret like a username and a password;
- immune to phishing scams, keystroke loggers and the like;
- the method of choice in web services development, as seen in computer programming languages like SAML and XML; and
- a roadmap for further use; that is, signing to preserve integrity of data messages, transactions, e-mail, Adobe PDF, Microsoft Word and Excel documents; based on the widely accepted X.509v3 format (an international telecommunications standard), which means system and programme interoperability is almost guaranteed.

Digital certificates and the Companies Act

Section 6(12)(*a*) of the Companies Act provides: ‘If a provision of this Act requires a document to be signed or initialled –
(*a*) by or on behalf of a person, that signing or initialling may be effected in any manner provided for in the ECT Act …’.

Consider this in line with s 13(1) of the ECT Act. Also note that s 14 of the ECT Act provides for originals to be in electronic form if certain integrity requirements are met. The cryptography behind an advanced electronic signature makes it mathematically infeasible to tamper with the document without showing evidence of tampering, for example by sending a warning.

Section 51(1)(*b*) read with s 51(2) of the Act provides that a certificate evidencing any certificated securities of a company may be signed by electronic means by two persons authorised by the company’s board (ie, electronic share certificates). Also consider s 12(5): Signing reservation of name notice; s13(1): Signing a memorandum of incorporation; s 30(3)(*c*): Signing annual financial statements; s 58(2)(*a*): Signing a proxy appointment; s 61(3): Signed demand for a shareholder meeting (eg electronically signed e-mail using an issued digital certificate); s 73(8): Signed minutes of a board meeting; s 77(3)(*a*) and (*d*): Director liability as a consequence of signing anything on behalf of a company; and s 101(5): Signed offers.

Digital certificates and the magistrates’ courts rules

The updated magistrates’ courts rules provide in r 1 for ‘signature’ to include an advanced electronic signature as defined in the ECT Act, and provides that this also applies to ‘sign’, ‘signing’ and ‘signed.’

Other legislation

Other legislation also requires signatures and, in such instances, it is worth considering the applicability of the ECT Act and the use of advanced electronic signatures.

However, there are instances when, in law, the use of an advanced electronic signature is not permitted. The ECT Act envisages this and only allows the use of advanced electronic signatures when the law does not specify the type of signature required (s 13(1) of the ECT Act). For example, s 2 of the Wills Act 7 of 1953 provides that no executed will is valid unless signed at the end thereof by the testator. ‘Sign’ is defined in s 1 of the Wills Act to include the making of initials and, only in the case of the testator, the making of a mark, and ‘signature’ has a corresponding meaning. (For information on other exclusions, see S Snail ‘Electronic contracting in South Africa e-contracts’ in S Papadopoulos & S Snail (eds) *Cyberlaw @ SA III*: *The law of the internet in South Africa* (Pretoria: Van Schaik 2012) at 51 – *Editor.*)

Electronic notarisation, acknowledgment and certification under the ECT Act

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 (s 18(1) of the ECT Act). This is relevant for admitted attorneys, who are *ex officio* commissioners of oaths.

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 (s 18(3) of the ECT Act).

Transacting online

As stated above, most computer systems require some form of access control. Most common is the username and password combination, which can be too risky when business risks are high. Take for example conveyancing online, namely the electronic communication of bond information (eg instruction, re-instruction, not taken up (NTU), acknowledgment, milestone status, payment advice and rating files) between the home loan divisions of banks and their panels of conveyancing attorneys. In a conveyancing transaction one cannot run the very real risk of allowing fraud to be committed as a result of unauthorised data access, data manipulation and leakage, and misuse of access by unknown persons. The companies involved need to know with a degree of certainty who is accessing their computer systems online, and need for those persons to take responsibility for that which they do online with them. It should also provide those companies with a level of confidence that only personnel authorised to communicate electronically on the company's behalf can in fact do so. Standard components of a sound security solution include authentication that makes use of encryption technologies; that is, digital certificates. (Examples of other components not dealt with here, but which are also important, include firewalls, anti-virus scanners, content security management, intrusion-prevention systems, virtual private networks and security-incident and event-manager tools).

Public and private key cryptography

Digital certificates, as already stated, make use of public and private key cryptography. This means using standard Microsoft computer programme functionality: Two data keys are generated on the digital certificate holder's computer. These keys are mathematically related to each other (sometimes referred to as asymmetric encryption). One data key is called the private key and the other the public key. It is mathematically infeasible, using the best computing power available today, to break the algorithms used to create these keys. The private key is required to be kept private and is not to be shared with anyone and is usually stored in the browser of a computer or on a cryptographic memory stick.

The digital certificate is simply a piece of data that lists the public key and identifies the individual holding the corresponding private key, and also identifies the certification services provider that issued the digital certificate in the first place; effectively vouching for the identity of the individual identified in the digital certificate based on the identity verification criteria set out in its CPS; compliance against which is audited from time to time by the Accreditation Authority.

When an electronic signature is created, it is only the public key and the digital certificate that become 'embedded' in the electronic document being signed, but these can only be 'embedded' if the corresponding private key is used. Therefore, the recipient of an electronic document (eg e-mail message or PDF document) that contains the author's public key and digital certificate should be assured that the author of the document, (ie, the only person who exercises control over the corresponding private key) is the same person identified in the digital certificate. The document is then said to contain the author's electronic signature or advanced electronic signature, as the case may be.

Problems arise if the private key becomes compromised as a stranger exercising control over the private key of another can impersonate the person identified in the corresponding digital certificate. It is therefore important to be diligent in retaining control of the private key associated to the public key listed in the digital certificate, including retaining control of any pass-phrase, pin or token used to activate the private key and to prevent disclosure to any person not authorised to create one's electronic signature.

Applying for a digital certificate

To be issued with a digital certificate that can be used to sign electronic documents with an advanced electronic signature (and which can also be used to access computer systems over the internet), a person needs to register his details with a certification services provider that has been accredited by the Accreditation Authority. This is an enrolment process that can be frustrating at times, but is ultimately worth it when the risks sought to be addressed are properly mitigated.

An applicant (also referred to as a subscriber) typically needs to –

- complete a personal digital certificate application form;
- sign a subscriber agreement; and
- present the original and one copy of his identity document

(there might be other criteria that need to be adhered to, depending on which certification services provider is selected).

In my experience, after verifying the applicant's identity and completing certain internal checks and controls, the certification services provider will issue a digital certificate. The applicant will then be notified and directed as to how to download the digital certificate and commence using it to access computer systems online.

Using a digital certificate

At present, in my experience, the Adobe Acrobat Professional computer programme appears to have the most user-friendly functionality to sign an electronic document. It is also possible to sign a Microsoft Word document. Once a document is ready for signature, it is to be converted/saved to the Adobe PDF format. The step-by-step functionality to signing the document is fairly easy to follow. This electronically signed document can then be attached to an e-mail and forwarded to the intended recipient. It can be encrypted as well if need be.

There are also online signing services, such as Signing Hub (www.signinghub.com), that do away with the need to incur the cost of obtaining an Adobe Acrobat Professional licence and which enable the uploading, sharing and signature (using digital certificates) of documents, and which also assist in managing costs of printing, faxing, couriers, postage, scanning, storage and searching.

A word of caution

Digital certificates and the functionality to use digital certificates to create electronic signatures have been around for years. It is important for the recipient of a signed electronic document to carefully scrutinise the digital certificate to confirm whether the signature created with that digital certificate qualifies as an advanced electronic signature or is merely an electronic signature.

To do this, two important things must be verified –

- that the certification services provider that issued the digital certificate is in fact accredited by the Accreditation Authority in terms of s 37 of the ECT Act (accreditation confirmation can be viewed on the Accreditation Authority's website at www.saaa.gov.za/accreditation_ProductsServices.htm or confirmed telephonically on (012) 427 8070/8000); and
- that the digital certificate makes reference to an advanced electronic signature.

Conclusion

As practitioners, it is imperative to keep pace with technological developments, especially those that facilitate business transactions in an increasingly global economy, without sacrificing the integrity of the process and the documents involved. The advent of advanced electronic signatures and digital certificates, together with other electronic security enhancements, enable both to the advantage of the client.

- See also 2005 (Dec) *DR* 24.

Grant Christianson *BA LLB (UKZN) LLM (UJ) MAP (Wits) Post Grad Dip (UJ)* is group legal adviser and company secretary at Law Holdings (Pty) Ltd in Johannesburg.