INTRODUCTION
This opinion relates to electronic signatures in South Africa and specifically aims to address the requirements, validity and legal force of an electronic signature.

LEGISLATION & CASE LAW
The Electronic Communications and Transactions Act 25 2002 (Ect Act) and Spring Forest Trading v Wilberry will be consulted to address the matter of electronic signatures and electronic documentation.

Section 1 - Definition of Electronic Signature & Advanced Electronic Signature
An electronic signature is defined as “data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature”.
An advance electronic signature is defined as “an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37”.

Section 11 - Legal recognition of data messages
This section provides that “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”, therefore providing authorisation to draft, store and access information in electronic format.

Section 12 - Writing
Section 12 addresses the requirement present in various corporate agreements, which relates to a document and any subsequent amendments to be in writing. This section provides that the “requirement in law that a document or information must be in writing is met if the document or information is -

(a) in the form of a data message; and
(b) accessible in a manner usable for subsequent reference.”

Therefore if information is in electronic format and able to be viewed as such, the writing requirement in law has been satisfied.
Section 13 - Signature

Section 13 is the most important section for purposes of this opinion, in that it deals with electronic signatures. The section provides that:

“(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”.

Law, as referred to in this context, includes not only statutory legislation, but also common law as well as secondary legislation (Spring Forest Trading v Wilberry) explicitly stating that a document has to be signed in order to be valid. Examples of such documents are suretyship agreements and a franchise agreement.

“(2) ...an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form”.

This sub-section explains that in essence, an electronic signature will have the same force and effect as a manuscript/paper-based signature.

“(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”.

Section 13(3) seems strict at first glance, but in a recent supreme court of appeal judgment (Spring Forest Trading v Wilberry), the interpretation of this section came under fire and was expressed that the name of a person at the bottom of an email, can constitute an electronic signature. The judge in this case held that “so long as the ‘data’ in an email is intended by the user to serve as a signature and is logically connected with other data in the email the requirement for an electronic signature is satisfied” (Spring Forest Trading v Wilberry). The judge went further as to confirm that the reliability of an email and the accuracy of the information communicated between the parties, conform to the requirements set out in section 13(3)(b).

“(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”.

"
The use of an Advanced Electronic Signature (AES) is therefore *prima facie* proof that the signature is valid and binding. The burden of proof thus shifts to the person alleging and not the person who signed with an AES.

“(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”.

This section confirms that an expression of intent in electronic format will be valid and admissible. From these brief extracts, it is clear that, electronic signatures and electronic documents are permitted and legally enforceable, thus, allowing for the implementation of a digital means of transacting and signing.

**Section 37 - Accreditation of authentication products and services**

“(1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.

(3) A person falsely holding out its products or services to be accredited by the Accreditation Authority is guilty of an offence.”

**TECHNICAL & DETAILED DISCUSSION OF ELECTRONIC SIGNATURES**

**Electronic Signatures**

An electronic signature is defined as “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 as provided for by the ECT Act is not very clear in explaining exactly what constitutes an electronic signature and can be open to interpretation. This definition can be simplified - an electronic signature needs to consist of a positive act, it must be able to identify the signatory, the signature must be verifiable and it must be visible. All of these characteristics mentioned, have to be in electronic format for it to qualify as an electronic signature. For an electronic signature to be recognised, the simple intention to sign is required, in order for an image/symbol/name/signature to be recognised as a signature, therefore if the intention for a name at the end of an email, is to serve as an electronic signature, as discussed in the Spring Forest Trading v Wilberry judgment, it will be sufficient.
Digital Signatures

A digital signature (although not defined in the ECT Act), is a signature that originates with a digital certificate. A digital certificate is issued to a person, once that person has been verified as the person who they claimed to be. A digital signature requires not only a positive act but also has verifiable integrity as a result of a digital certificate. A digital certificate is a positive identification of a device/server or entity that operates very similar to how an identity document identifies a specific person. A digital certificate is managed by a Public Key Infrastructure (PKI), which is a combination of hardware, software and procedures implemented in order to manage digital certificates.

Advanced Electronic Signatures

An AES is defined in the ECT Act as “an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37”. In short, an AES is a digital certificate based signature, which utilises mechanisms to ensure security and integrity, as well as to confirm the identity of the signatory. For clarity, AES consists of a positive act, together with verifiable integrity (digital certificate based on confirmation of the identity of the applicant) with an added face-to-face verification mechanism, as well as 3-factor authentication (or similar). The 3-factor authentication is briefly:

- Something you are (biometrics such as fingerprint and iris scan);
- Something you know (pin, password, pass phrase or secret question);
- Something you have (key, device).

The ‘something similar’ referred to in legislation, would be something that offers the same type of security but does not incorporate all three authentication factors mentioned above. These added mechanisms are what make this type of signature so strong, reliant and trustworthy. As was seen in section 13(4) of the ECT Act, this signature is presumed to be valid, unless proven otherwise, therefore shifting the burden of proof away from the signatory and onto to the person who alleges.

PKI (Public Key Infrastructure)

Electronic signatures based on PKI (digital signatures and AES), use an algorithm in order to generate two keys, private and public, that are mathematically linked to each other. In order to create a digital signature, software is utilised to create a one-way hash (cryptographic process) of the electronic document that is to be signed. The private key that was generated, is used to encrypt the hash. The encrypted hash, with other information such as the hashing algorithm, constitutes the digital signature. The hash value is unique and prevents any subsequent changes to the document signed (which will alter the hash value and warn the recipient of alterations to the document). The digital certificate used to
create a digital signature on an electronic document, links a public key to an identity and can be utilised to confirm who the owner of that public key is.

An AES is therefore the most secure signature available in South Africa. Even though it does not have to be applied to all documents, the user has the option available to use it on all documents. For documents not demanding an AES and not excluded by the ECT Act, an electronic signature would suffice.

**CONCLUSION & RECOMMENDATIONS**

The effect of the ECT Act is that electronic signatures and electronic documents are permitted and legally enforceable, thus, allowing for the implementation of a digital means of transacting and signing. For an electronic signature to be recognised, the simple intention to sign is required, in order for an image/symbol/name/signature to be recognised as a signature. Not all electronic agreements require a signature, therefore do not require the use of an advanced electronic signature (AES). Only in instances where the law requires a document/agreement to be signed and such law does not specify the type of signature, is the use of an AES required.

As stated above, not all agreements need to be signed in order to give legal force and effect to. Both electronic signatures (as defined and explained above) as well as an AES have legal force and effect in South Africa. Only in instances where an AES is required by law will the use of an AES validate the document/agreement. In all other instances a normal electronic signature or digital signature is valid and binding (unless such agreement or document is excluded by the ECT Act itself).