



ELECTRONIC SIGNATURE GUIDELINES

Appendices

Version 1.1.0

February 12, 2019

Table of Contents

Appendix A - ECT Act 2002 and Electronic Signatures	2
Appendix B - Overview of how digital signatures work	7
Appendix C - Risk Assessment Framework.....	8
Appendix D - Public Key Infrastructure in South Africa.....	11
Appendix E - Roles and Responsibilities – Information Security.....	19

APPENDIX A - ECT ACT 2002 AND ELECTRONIC SIGNATURES

The ECT Act defines "Electronic Signature" as:

"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;"

Based on the above definition, legally, electronic signatures may have evidence and security which would not necessarily render the electronic signature a digital or advanced electronic signature but nonetheless, provide the type of reliability and integrity sought in terms of Section 15 of the Electronic Communications and transactions Act in dealing with evidence. In assessing the weight of the evidence in legal proceedings a court is obliged to take into account all relevant factors in determining whether the signature was valid or not.

Also, the ECT Act provides:

- a) 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 (section 11(1)).
- b) 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 (section 12).
- c) *"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." (section 14(1)).*

The ECT Act does not specifically mention or refer to digital signatures, digital signatures constitute the building blocks for advanced electronic signatures cited the ECT Act.

The American Bar Association ¹ defines a digital signature as:

"A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signers public key can accurately determine:

- 1) Whether the transformation was created using the private key that corresponds to the signers public key; and
- 2) Whether the initial message has been altered since the transformation was made."

It is clear that a digital signature falls within the definition of electronic signatures in the ECT Act and a digital signature properly used within a PKI infrastructure fulfills all the functional requirements of a written signature and is superior to a written signature in several ways.

An advanced electronic signature is defined in the Act as follows:

"Advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37;"

In determining the criteria for accreditation, the accreditation regulations and the standards referred to in the Regulations have to be satisfied before accreditation can be granted. These standards are premised on the types of technologies and the policies and practices used in providing digital signatures.

Under the present law, an advanced electronic signature cannot be anything but a digital signature.

Three definitions are important in considering advanced electronic signatures. These are:

¹ Digital Signature Guidelines, The American Bar Association, 1996

"Advanced electronic signature" means an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37;”

"Authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;”

"Authentication service provider" means a person whose authentication products or services have been accredited by the Accreditation Authority under section 37 or recognised under section 40;”

In digital signatures or advanced electronic signatures, typically the requirement of a Certification Authority will be that the full names of the signatory are contained in certificates issued by that Certification Authority. Again, in this regard electronic signatures in the form of digital or advanced electronic signatures are superior to written signatures and fulfill the functional equivalent requirement upon the developing jurisprudence of electronic signatures is based.

In deciding whether to deploy electronic signatures or advanced electronic signatures, departments should consider whether the signature is required by law. The ECT Act recognises other forms of electronic signatures used between parties in an electronic transaction, these will not be recognised if the signature is required by law (e.g., signatures required in terms of the Companies Act 71 of 2008).

In addition, the ECT Act provides:

- a) “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” (section 13(2) and (3) read with the definition of ‘transaction’ in section 1 of the ECT Act).
- b) “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” (section 13(1) of the ECT Act).

Authentication and Electronic Signatures

As mentioned above, the ECT Act defines an electronic signature as “data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature”. It is therefore accepted that the function of a signature is some kind of personal mark, which may be used to identify a party and to convey or confirm an intention to be bound.

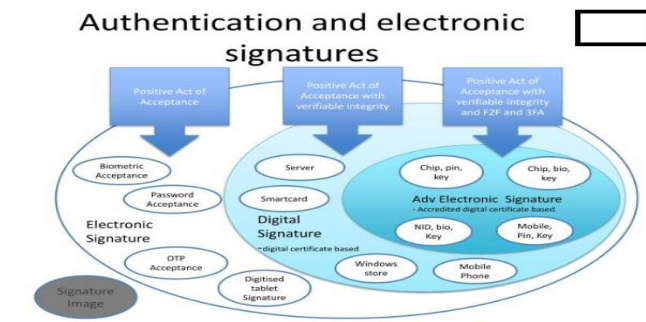


Figure 1 Authentication and Electronic Signature within the ECT Act definition (Adapted from: Lawtrust)

The diagram in figure 1 above, illustrate types of authentication and electronic signatures as per the ECT Act and their level of legal acceptance.

For Electronic Signature to be legally valid, a signature must be a positive act of acceptance, visible and clear, must identify the individual and must be verifiable.

The basic Electronic signatures that need only positive act requirements and supporting evidence are:

- a) **Electronic signatures:** Data attached to, incorporated in, or logically associated with other data, which is intended by the user to serve as a signature. Electronic signatures include digitised and digital signatures.
- b) **Digitised signature:** Digital reproduction of a handwritten signature, e.g. faxed signature, a picture of a signature or a signature capture tablet.
- c) **Biometric signature:** General description of an electronic signature made with a biometric (body measurement such as a fingerprint) as an act of authentication/acceptance.
- d) **One Time:** A one-time password token (OTP token) is a security device or software program that produces new single-use passwords or passcodes at preset time intervals. In both software and hardware versions, password tokens are programmed for a time interval upon which the old password expires and a new one is created.

The above basic electronic signatures do not use a public/private key encryption process to ensure integrity.

Both Digital Signatures and Advanced Electronic Signatures are server based and use a public/private key encryption process to ensure integrity. The public/private key encryption process assure the verifiability and integrity of evidence.

Digital signatures that need positive act requirements with the verifiable integrity of evidence are:

- a) **Windows wallet:** Window Wallet is a mobile payment and digital wallet service that lets users make payments and store loyalty cards on certain devices such as mobile phones.
- b) **Smartcard:** A smart card is a security token that has an embedded chip. Smart cards are typically the same size as a driver's license and can be made out of metal or plastic. They connect to a reader either by direct physical contact (also known as chip and dip) or through a short-range wireless connectivity standard such as Near Field Communication (NFC).

For an electronic signature to be classified as an advanced electronic signature, it must be a Positive Act with verifiable integrity and face-to-face (F2F) certification and accredited by the SAAA. Also, three-factor authentication (3FA) is used identity-confirming credentials from three separate categories of authentication factors. Authentication factors classically fall into three categories:

- a) Knowledge factors include things a user must know in order to log in: Usernames, IDs, passwords and personal identification numbers (PINs) all fall into this category.
- b) Possession factors include anything a user must have in his possession to log in. This category includes one-time password tokens (OTP tokens), key fobs, smartphones with OTP apps, employee ID cards and SIM cards.
- c) Inherence factors include any biological traits the user has that are confirmed for login. This category includes the scope of biometrics such as retina scans, iris scans, fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry and even earlobe geometry.

Three-factor authentication is mainly used in businesses and government departments that require high degrees of security. The use of at least one element from each category is required for a system to be considered three-factor authentication.

“Where a law requires or permits a person to provide a certified copy of a document and the document exists on 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 “(section 18(3) of the ECT Act).

Advanced electronic signatures

An advanced electronic signature is deemed particularly reliable in law and is prima facie valid i.e. is always assumed to be valid and have been applied correctly so as to shift the burden of proof to the disputing party.

An advanced electronic signature is a digital signature created with a digital certificate from an accredited Authentication Services Provider after following a face-to-face identification process with the user.

The signature will:

- a) Identify the signatory
- b) Be identified as an Advanced Electronic Signature
- c) Detect any subsequent alteration or corruption of the signed data message or document legal framework for electronic signatures
- d) Make use of a 3-factor or equivalent signing mechanism so as to ensure the highest reliability of the signature.

It is an offense under section 37(3) of the act to falsely claim that you are accredited, which is punishable by a fine or a maximum of one year in prison.

South Africa Post Office (SAPO) and Lawtrust are accredited authentication service providers under the ECT Act. SAPO is the preferred service provider for the government. SAPO has a foothold in all the provinces of the country and it will facilitate rolling out e-services based on electronic signature solutions to rural areas of the country.

Signature

Notwithstanding the above definition of Advanced Electronic Signatures, an electronic signature is not without legal force and effect purely because it is electronic. The difference is that in each case of dispute, the electronic signature on the electronic transaction or document will have to be assessed in terms of the requirements for Signature, Original and Evidential Weight as stipulated in Section 13, 14 and 15 of the ECT Act.

An electronic signature has to be reasonable for the purpose for which it is to be used, must identify the signatory and be made with a positive act of acceptance from the signatory.

In other words, a certificate-based digital signature is always an electronic signature in the eyes of the law but can be an Advanced Electronic Signature if issued from an Accredited Authentication Services provider using the correct practices and technology.

Legally Binding Signatures

Legally binding electronic signatures protect against the following types of threats:

Repudiation — claims such as: "that's not my signature", "*I didn't sign this document*" or "*my digital identity was spoofed*"

Denying intent of signing — claims such as: "I didn't agree to all this, it was just a draft", "I didn't realise that I would be legally bound by this e-signature" or "I didn't understand what I was doing and the signature was created just by accident"

Questioning the integrity of the signed document — claims such as "the document was changed since I signed it" or "this is not the document I signed"

As mentioned above, ECT Act is based on the UNTAC, there are other international laws² on electronic signatures, and there is general consistency across these in terms of the fundamental requirements for electronic signatures to be considered legally binding.

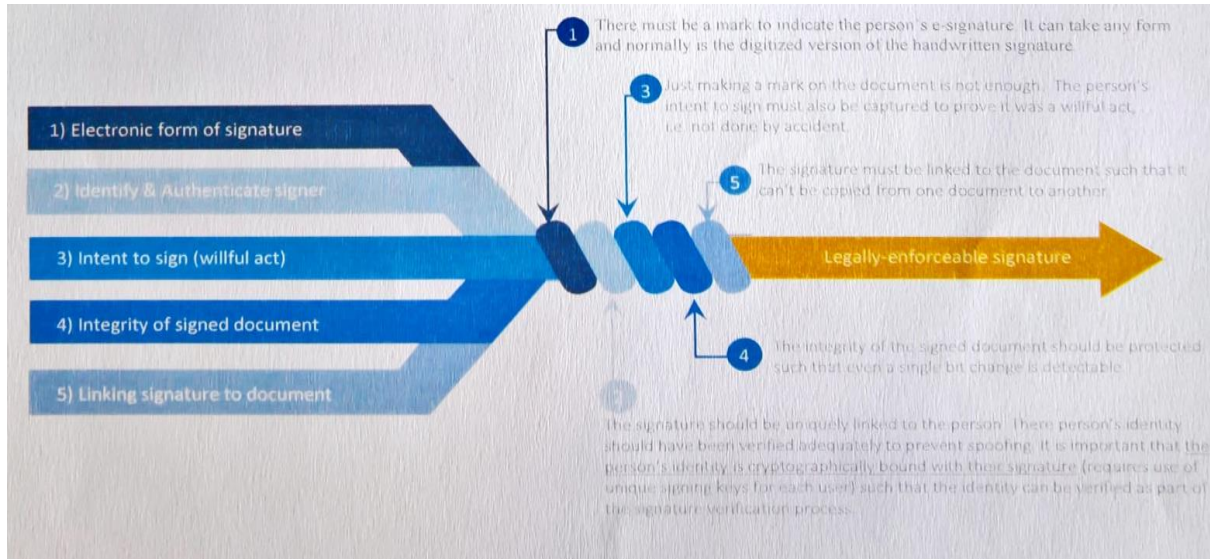


Figure 2 Legally Binding Electronic Signature requirements (Adapted from: Lawtrust)

The core requirements of these different laws are summarised as the following five elements which combined together create legally binding signatures – Figure 2 and above and a Table 1 below.

Five Elements	Requirements
1. The electronic form of signature	The must be a mark to indicate the person's electronic signature. It can take any form and normally is the digitized version of the handwritten.
2. Identify & Authenticate signer	The signature should be uniquely linked to the person. The person's identity should have been verified adequately to prevent spoofing. It is important that the person's identity is cryptographically bound with their signature (requires the use of unique signing keys for each user) such that the identity can be verified as part signature verification process.
3. Intent to sign (wilful act)	Just making a mark in the document is not enough. The person's intent to sign must also be captured to prove it was a willful act, i.e. not done by accident.
4. The integrity of the signed document	The integrity of the signed document should be protected such that even a single bit change is detectable.
5. Link signature to document	The signature must be linked to the document such that it cannot be from one document to another.

² US E-SIGN Act (USA) and EU eIDAS Electronic Identity and Trust Services Regulations

Table 1 Legally Binding Electronic Signature Requirements

APPENDIX B - OVERVIEW OF HOW DIGITAL SIGNATURES WORK

The Digital Signatures require a key pair (asymmetric key pairs, mathematically related large numbers) called the Public and Private Keys. Just as physical keys are used for locking and unlocking, in cryptography, the equivalent functions are encryption and decryption. The private key is kept confidential with the owner usually on a secure media like a crypto smart card or crypto token. The public key is shared with everyone. Information encrypted by a private key can only be decrypted using the corresponding public key.

In order to digitally sign an electronic document, the sender uses his/her Private Key. In order to verify the digital signature, the recipient uses the sender's Public Key.

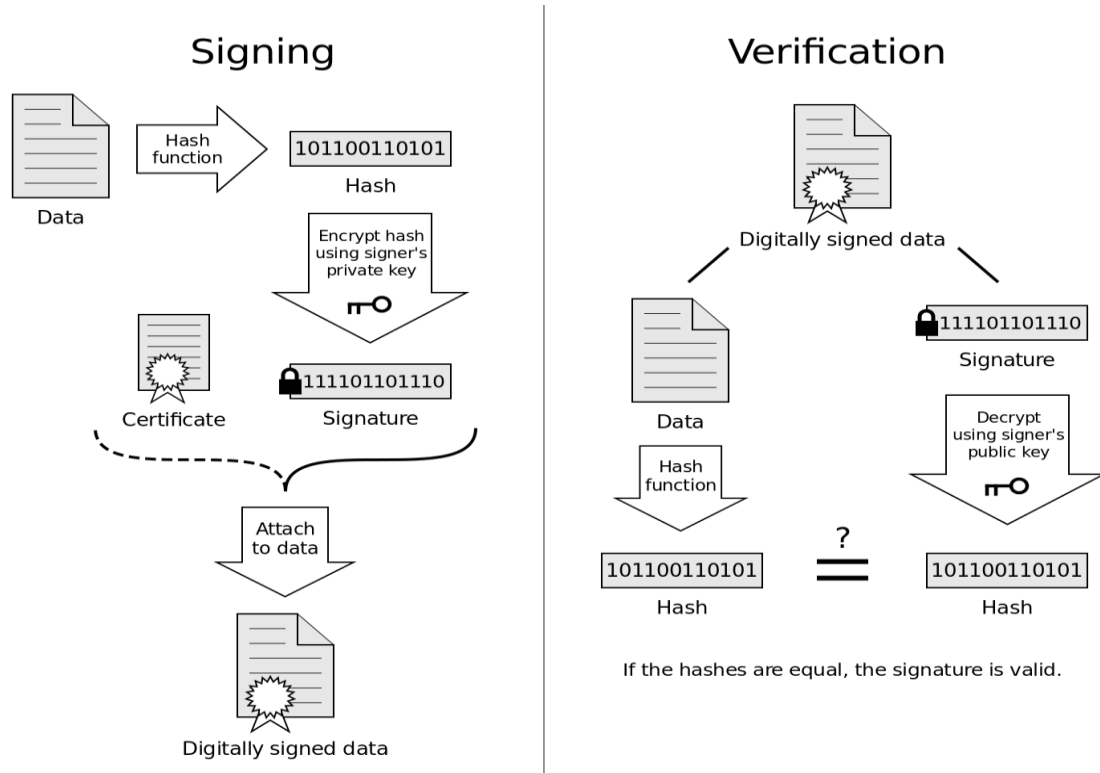


Figure 3 How digital signature is applied and verified (Source: Wikipedia)

As figure 3 above illustrates, there are typically three algorithms involved with the digital signature process:

Key generation – This algorithm provides a private key along with its corresponding public key.

Signing – This algorithm produces a signature upon receiving a private key and the message that is being signed.

Verification – This algorithm checks for the authenticity of the message by verifying it along with the signature and public key.

The process of digital signing requires that the signature generated by both the fixed message and private key can then be authenticated by its accompanying public key. Using these cryptographic algorithms, the user's signature cannot be replicated without having access to

their private key³. A secure channel is not typically required. By applying asymmetric cryptography methods, the digital signature process prevents several common attacks where the attacker attempts to gain access to the following attack methods. [1]

Advanced Electronic Signature

An advanced electronic signature is a digital signature created with a digital certificate from an accredited Authentication Service Provider under section 37 of ECT Act, following a face-to-face identification process with the user. It is deemed particularly reliable in law and is prima facie valid, i.e. is always assumed to be valid and have been applied correctly, to eliminate the burden of proof to the distributing party.

The ECT Act defines an advanced electronic signature as an electronic signature which results from a process which has been accredited by the Authority⁴ as provided for in section 37 of ECT Act”

For an electronic signature to be considered as advanced, it must meet several requirements:

- a) The signatory can be uniquely identified and linked to the signature.
- b) The signatory must have sole control of the private key that was used to create the electronic signature.
- c) The signature must be capable of identifying if its accompanying data has been tampered with after the message was signed.
- d) In the event that the accompanying data has been changed, the signature must be invalidated.

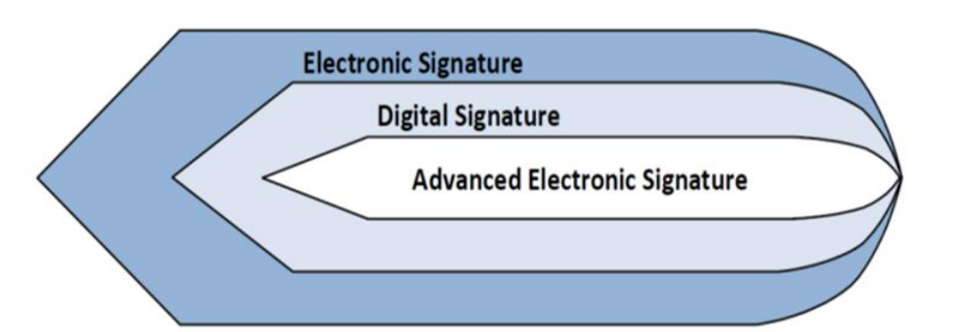


Figure 4 Electronic Signature Definition (Adapted from: The Law Society of South Africa)

As Figure 4 above illustrates, an electronic signature incorporates both digital signature and advanced electronic signature but maybe neither of those.

The definition of “electronic signature” is all-encompassing and includes digital signatures (not defined or mentioned in the ECT Act) and advanced electronic signatures.

Appendix C - Risk Assessment Framework⁵

There are six distinct risks for the electronic signature process, each of which can be examined relative to those same risks in dealing with paper and written signatures.

These six risks are discussed in detail below:

³ Turner, Dawn. "What is a digital signature - what it does, how it work". Cryptomathic.

⁴ South Africa Accreditation Authority

⁵ Enhancing the Admissibility and Enforceability of Electronically Signed Documents, Bloomberg Finance L.P 2009

- a) **Authentication Risk** — This is the risk that the signer signing a record, accepting delivery of a record, or providing a record is an imposter using a false identity; the records would then be unenforceable by the user against the person the user thought it was dealing with via electronic means.
- b) **Repudiation Risk** — This is the risk that the signer claims that the electronic records that were signed were altered after they were signed, such that the person against whom enforcement is sought attempts to repudiate the actual terms and conditions in the signed electronic record.
- c) **Admissibility Risk** — This is the risk that the other party to a transaction successfully challenges the admissibility of the necessary records, such as the signed contract or acknowledgment of receipt of certain disclosures, on the grounds of reliability.
- d) **Compliance Risk** — This is the risk that the records signed or presented do not comply with other substantive laws, such as laws mandating certain content in documents to be presented or signed, or the records do not comply with the basic requirements of ECT Act for delivery of such records.
- e) **Adoption Risk** — This is the risk that in managing the risks above, an electronic signature process is so burdensome that the intended users are not satisfied with the process or find ways to avoid certain steps in the process, thereby undermining the process.
- f) **Relative Risk** — In examining the risks above, users should evaluate the risk with a proposed electronic signature process relative to the corresponding risk in the process using paper and a written signature, in the belief that an electronic signature process may not be risk free, but should not, on the whole, be any riskier than the paper and written signature process, if feasible.

By examining the risks from the above perspective, it is easier to assess the particular risk and then determine the optimal means to mitigate the risk.

Risk Assessment and Risk Mitigation

Different categories of transactions present different risk profiles. For this reason, when designing an electronic signature process, one should assess the risks from various perspectives and design into the process the appropriate measures to mitigate the risk, in light of the risk tolerance of the department implementing the process for the particular documents to be signed.

RISK	IMPACT (high, moderate, or low)	MITIGATION
Authentication Risk Refers to the risk that a signer is in fact not the person he or she claims to be'		Possible strategies <ul style="list-style-type: none"> • The method and results used to authenticate each signer should be included in the archived signing session, or audit trail, which should then be securely archived and be capable of being retrieved securely • Deploy electronic signatures within the PKI infrastructure. Digital signature and advanced electronic signature use encryption. • Advanced electronic signature deployment requires face to face authentication.
Repudiation Risk Refers to the risk of a signer acknowledging he or she signed a document, but claiming that the electronic signature is attached to or logically associated with a document containing terms and conditions		<ul style="list-style-type: none"> • The PKI digital signature technology can render a record unalterable and eliminate the chance that the record will be later revealed to have been altered. • The PKI digital signature technology allows one to state with confidence that because the hash values for the original record (which may contain terms and conditions associated with an electronic signature)

<p>different than those in the signed document.</p>		<p>match those in a later copy of that record, it is infeasible the later record could have been altered.</p> <ul style="list-style-type: none"> The digital certificate provided with the digital signature process should be stored to ensure that verification can be performed again at a later time. The audit trail for each transaction should include each document presented and signed during a given transaction where each such document has been signed
<p>Admissibility Risk Admissibility Risk is the risk that a court refuses to admit into evidence copies of electronic documents generated, presented, signed, secured, archived, and retrieved by the electronic signature process. All of the rules of evidence and evidentiary foundations that apply to paper documents and written signatures also apply to documents signed electronically, stored electronically and retrieved electronically</p>		<ul style="list-style-type: none"> Where an electronic signature is required by law to deploy Advanced Electronic Signatures (ECT Act).
<p>Compliance Risk The electronic signature process should assure that:</p> <ul style="list-style-type: none"> each document presented or signed by a signer complies with the legal requirements for the content, presentation, sequence, and information to be obtained for each such document; each document required to be presented and signed is in fact presented and signed as required by law governing the particular transaction; and The significance of each step in the signature process (whether on an acknowledgment of receipt, unilateral consent, application for goods or services, or contract) is abundantly clear to each signer 		<ul style="list-style-type: none"> The audit trail should record each step required to meet the regulatory requirements, such as the sequence and timing of presenting certain forms and the actual contents of records presented. By using an electronic signature process with an audit trail containing reliable, admissible evidence that each step was taken using the required content, a user may reduce the compliance risk considerably lower than the risk in transactions using paper and written signatures.
<p>Adoption Risk The Adoption Risk refers to the risk that the electronic signature process, in an attempt to reduce the authentication, repudiation, compliance, and admissibility risks are overly burdensome, such that the intended signers do not use the process or find alternatives that undermine the overall effectiveness of the proposed electronic signature process.</p>		<ul style="list-style-type: none"> This risk can and should be, managed by conducting a series of pilot tests before introducing the electronic signature process to potential signers for the user. By conducting such tests, the user can obtain feedback from the signers and make the appropriate adjustments to reduce this risk when the process is fully launched.
<p>Relative Risk The risks of a given electronic signature process should be considered relative to the risks associated with a paper and written signature. This allows the user to better assess the risks inherent in the particular electronic process.</p>		<ul style="list-style-type: none"> The electronic signature process can be configured to prevent a record from being signed if there are any blanks or otherwise incomplete responses in the record. The process is also able to prevent any document relating to a transaction from being submitted to the user or by the user unless all the required steps, including execution or acknowledgment of receipt of all consumer disclosures, are provided and acknowledged, and then once signed, securing documents through the digital signature process to prevent

		<p>those documents from being altered without detection.</p> <ul style="list-style-type: none"> This can significantly reduce the compliance risk below that for paper and written signatures.
--	--	---

Table 1 Risk, Impact, and Mitigation Matrix

APPENDIX D - PUBLIC KEY INFRASTRUCTURE IN SOUTH AFRICA

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, and confidential email. It is required for activities where simple passwords are an inadequate authentication method and the more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred⁶.

The office of the South African Accreditation Authority (SAAA) is established in terms of Chapter VI, Part 1 of the Electronic Communications and Transactions Act 25 of 2002. The Authority is responsible for the accreditation of authentication and certification products and services used in support of electronic signatures and monitoring of the activities of authentication and certification service providers whose products or services have been accredited by the South African Accreditation Authority within the Republic of South Africa.

The Director-General of the Department of Telecommunications & Postal Services is appointed as the South African Accreditation Authority and may appoint Deputy South African Accreditation Authorities and officers from employees of the Department after consultation with the Minister.

The current PKI organisation in South Africa consists of the Accreditation Authority (SAAA) as the apex of the body as the South African Root Certification Authority (SACA) as shown in the diagram below.



Figure 5 PKI Trust Hierarchy in South Africa

The primary duty of the South African Accreditation Authority is to accredit authentication products and service used in support of electronic signatures. In terms of sections 36 to 40 of the Act, other duties (which stem from the primary duty) (36)(1) are to:

- “monitor the conduct, systems, and operations of accredited authentication service providers in order to ensure compliance with the Act and Accreditation Regulations;”
- “temporarily suspend or revoke the accreditation of an authentication product or service subject to the provisions of the Act and Regulations; “
- “maintain a publicly accessible database in respect of accredited authentication products and service and other prescribed information;”

⁶ ‘What Is PKI (Public Key Infrastructure)? - Definition from WhatIs.com’, SearchSecurity, accessed 23 December 2016, <http://searchsecurity.techtarget.com/definition/PKI>.

- d) *“appoint independent auditing firms to conduct periodic audits of authentication service providers to ensure compliance with section 38, and other obligations of authentication service providers in terms of the Act. “*
- e) *“suspend or revoke accreditation If it is satisfied that the authentication service provider has failed or ceases to meet any of the requirements, conditions or restrictions subject to which the accreditation was granted under section 38, or for which recognition was given in terms of section 40; “*
- f) the setting, reviewing and amending standards for authentication service providers in respect of inter alia security, technology, and procedures;
- g) issue policies governing the operations and procedures for the accreditation of the products and services of authentication service providers; and
- h) provide advice and assistance to authentication service providers, users as well as other Government forums, committees and working groups set up to implement e-commerce and e-government in South Africa.

The South Africa Root Certification Authority (SACA) is responsible for issuing public key certificates (henceforth referred to as Certifying Authorities or CA). The CAs, in turn, are responsible for:

- a) issuing Digital Signature Certificates to the end user;
- b) 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
- c) in order to maintain security, indicates in a published certificate revocation list those digital certificates that are no longer valid (e.g. revoked, expired or suspended).

A Registration Authority (RA) acts as the verifier for the CA before a Digital Signature Certificate is issued to a requestor. The Registration Authorities process user requests, confirm their identities and induct them into the database.

SAAA Implementation of PKI as per ECT Act

Figure 12 below illustrates the PKI structure as implemented in South Africa for secured internet applications that ensure authentic and private transactions that cannot be repudiated at a later time. Thus, the SAAA via the South Africa Root Certification Authority certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by an accredited CA.

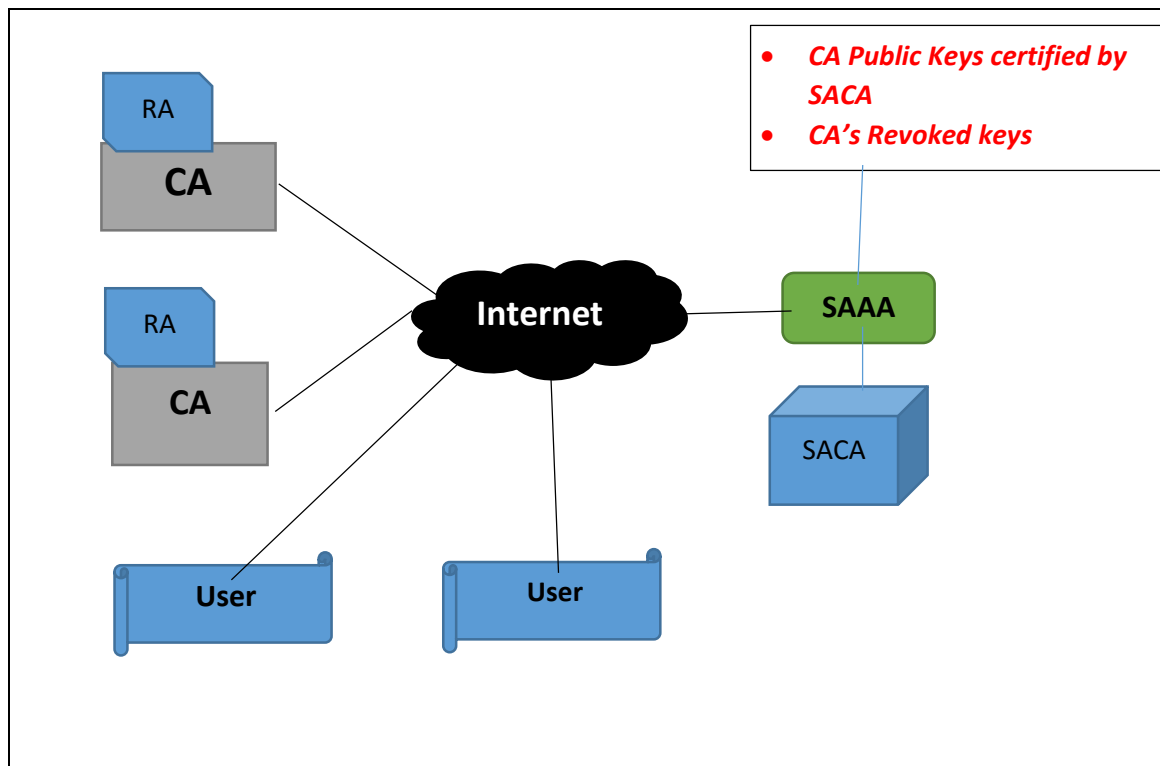


Figure 6 Overview of SAAA Implementation of PKI as per the ECT Act

Digital Signature Certificates

Certificates serve as the identity of an individual and can be presented electronically to prove your identity or your right to access information or services on the Internet.

A digital certificate is an electronic file securely linking an individual to encryption keys and identification data. This certificate belongs to a server or person and resides on a mobile token or within the certificate store of an application like an internet browser – encrypting and signing communications and transactions, protecting them from being intercepted by any unauthorised third party.

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509.

An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA). The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. The CA makes its own public key readily available through print publicity or perhaps on the Internet.

Digital Signature Certificates are endorsed by a trusted authority empowered by law to issue them, known as the Certifying Authority or CA. The CA is responsible for vetting all applications for Digital Signature Certificates, and once satisfied, generates a Digital Certificate by digitally signing the Public key of the individual along with other information using its own Private key.

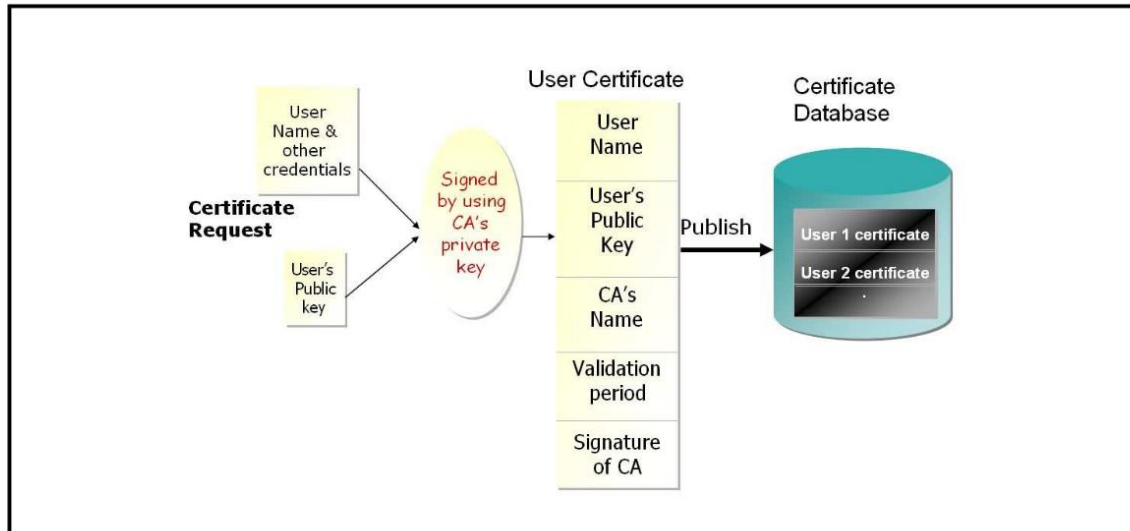


Figure 7 Overview of Digital Signatures Certificate (Courtesy: Ministry of communications and information technology- the government of India)

Classes of Digital Signatures Certificates

Depending upon the requirement of assurance level and usage of Digital Signature Certificate the following are the classes of Digital Signature Certificates⁷:

⁷ Source: SOPA Trust Centre

Class	Subscriber	Confirmation of Identity	Suitable applications
2	Unaffiliated or affiliated natural persons	Name and e-mail address search within the CA to ensure that the distinguished name is unique and unambiguous. Ensure that the Subscriber has access to given email address.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a medium level of assurance in comparison with the other Classes, such as some natural person and intra- and inter-company e-mail, on-line subscriptions, account applications, and password replacement. This Certificate is not recommended for high value transactions. E.g. over R 1 000.
3	Affiliated natural persons	Same as Class 2, plus confirmation of affiliation by the Sponsor, RA or Appointed Agent.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurance in comparison with other Classes, such as corporate database access and exchanging low sensitivity confidential information. This certificate is not recommended for transactions over R 5 000.
3	Juristic persons	Check of third-party database or other documentation showing proof of right to be linked to Juristic Person. Verification check by telephone (or comparable procedure) to confirm information in, and authorization of, the application. In the case of web server Certificates, confirmation that the applicant has the right to use the domain name to be placed in the Certificate.	Server authentication, confidentiality encryption and client authentication when communication with other servers (SSL Server Certificates) Authentication, message integrity, and confidentiality encryption when communicating with Electronic Data Interchange (EDI Certificates) Integrity of software and other content (e.g. code signing Certificate).
4	Natural and Juristic persons	Distinguished Name, Affiliation and e-mail address search to ensure that the distinguished name is unique and unambiguous, plus personal presence, plus validation of non-South African Citizens ID credentials and capture of applicant's biometric data and or a picture for validation and match with DHA in the case of South African Citizens. Juristic Persons credentials will be checked by a search at an appropriate third Party to ensure its existence. E-mail unique URL check to ensure that the Subscriber has control over the email address.	Enhancing the security of e-mail through confidentiality encryption, digital signatures for authentication, and web based access control. Applications requiring a high level of assurance and signatures as "advanced electronic signatures" under the ECT Act Number 25 of 2002. This Certificate is recommended for transactions of up to R 250 000.

Table 2 Class Type

Types of Digital Signatures Certificates

The following table provides an overview of the different types of Digital Signature Certificates.

Type of Certificate	Description and Assurance level
Class 2 certificate Class 2 Root CA certificate Class 2 CA certificate Class 2 Root CA Certificate Revocation list Class 2 Certificate Revocation list.	Medium assurance 1024 bit certificates that are for standard commercial use . These certificates are ideal for medium-level authentication, signing, and encryption of electronic communications like email

<p>Class 3 certificate</p> <p>Class 3 Root CA Certificate Class 3 CA Certificate SSL CA Certificate Class 3 Root CA Certificate Revocation list SSL Certificate Revocation list Class 3 Certificate Revocation list</p>	<p>High assurance, closed community certificates for commercial use. These certificates are only available to organisations who wish to authenticate users within their own closed user groups (staff and/or customers). They are ideal for high-level authentication, access control, signing and encryption of electronic communications, transactions and processes within a closed environment.</p>
<p>Advanced Electronic Signatures (Class 4 Certificates) Class 4 Root CA Certificate Class 4 CA Certificate Class 4 Root CA Certificate Revocation list Advanced Electronic Signatures (Class 4 Certificates) Revocation list</p>	<p>Advanced Electronic Signature. These certificates are available to users and organisations that wish to transact and communicate with clear legal status. A high level of independent identity authentication is provided through the collection of personal identity information, including fingerprints, and the verification of the information provided by the Department of Home Affairs. Advanced Electronic Signatures are strongly recommended for strong authentication, signing, and encryption of electronic communications, transactions and processes.</p>

Table 3 Type of Certificate

Procurement of Digital Signature Certificates

The office of the South African Accreditation Authority (SAAA), an agency of the Department of Telecommunications and Postal Services (DTPS), was established in terms of Chapter VI, Part 1 of the ECT Act 25 of 2002. The role of SAAA is to accredit the authentication products and services in support of electronic signatures.

To date, the SAAA has granted the Certificates of Accreditation to issue advanced electronic signatures to LawTrust Third Party (Pty) Limited and the South African Post Office⁸. The relevant provision states:

“The authentication product/service used in support of an electronic signature is hereby accredited as an advanced electronic signature.”

Criteria for Accreditation

The criteria for accreditation are provided in Section 38(1) of the ECT Act and the requirements of an advanced electronic signature are;

“The Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—

- a) is uniquely linked to the user;*
- b) is capable of identifying that user;*
- c) is created using means that can be maintained under the sole control of that user;*
and
- d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;*
- e) is based on the face-to-face identification of the user”*

Accreditation

⁸ The South Africa Post Office is legislated as the Preferred Authentication Service Provider to Government.

The Post Office Trust Centre⁹ has been accredited by the South African Accreditation Authority in terms of section 37 of the Electronic Communications and Transactions Act 25 of 2002. The Electronic Communications and Transactions (ECT) Act 25 of 2002 sets the platform for transactions with legislated status and evidentiary weight.

In this regard, the extracts from the Act below indicate the legislated status of authentication products and services.

Preferred Authentication Service Provider: The South African Post Office is legislated as the Preferred Authentication Service Provider to Government.

Accreditation: In terms of Section 37 of the ECT Act organisations may apply to have their products and services accredited as Advanced Electronic Signature.

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

For a Legislated Electronic Signature or Seal: Once accreditation has been received, Advanced Electronic Signatures may be used in cases where South African Law requires an electronic document to be signed. See Section 13(1) & 19 (3) below

13. (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”.*

19. (3) *“Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that it is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed”.*

Evidentiary Weight: When Accreditation has been received and an Advanced Electronic Signature is used the burden of proof shifts away from the party receiving the electronically signed data and onto the signatory to prove that the signature is not his or hers.

13. (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”.*

As an Electronic Notary Signature: Once accreditation has been received an Advanced Electronic Signature may be used for notarizing of electronic documents.

18. (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”.*

For creating a Certified Electronic Copy of a paper document: Once accreditation has been received an Advanced Electronic Signature may be used for certifying electronic copies of paper documents.

18. (3) *“Where a law requires or permits a person to provide a certified copy of a document and the document exists on paper or another physical form, that requirement*

⁹ Source: South Africa Post Office

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”.

As mentioned above, a public key infrastructure is a set of hardware, software, people, policies and procedures needed to create, manage, distribute, use, store and revoke digital certificates. Trust Centre digital certificates provide the legislative authentication needed to open the doors for safe electronic communicating and transacting.

A digital certificate is an electronic file securely linking an individual to encryption keys and identification data. This certificate belongs to a server or person and resides on a mobile token or within the certificate store of an application like an internet browser – encrypting and signing communications and transactions, protecting them from being intercepted by any unauthorised third party.

The Trust Centre provides all three existing types of personal digital certificates in meeting the information security needs of prospective clients.

Medium and high assurance certificates are provided for standard commercial use with varying degrees of security, and then there are advanced electronic signature certificates which provide the strongest authentication available for users and organisations looking to transact and communicate with clear legal status.

The Trust Centre will also offer secure socket layer (SSL) certificates which provide strong authentication of servers and Web sites.

The Trust Centre incorporates an environment housed within a secure perimeter with eight levels of encryption security.

It is at level eight that the encryption keys are stored. The control of each lies with a number of reputable and independent people and organisations, including Government, audit houses and private companies.

Through its PKI, the Trust Centre will authenticate and ensure the user is who they say they are; validate the transaction to ensure non-repudiation; protect messages from tampering; encrypt messages to protect the message from unauthorised access; and will digitally sign transactions and communications to authenticate code, data messages and documents.

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.

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

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

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.

APPENDIX E - ROLES AND RESPONSIBILITIES – INFORMATION SECURITY

Director-General

The Director-General should:

- a) Provide strategic leadership and management;
- b) Demonstrate commitment to Information Security Management, mandate policy, and assign information security roles, responsibilities and authorities;
- c) Be accountable for the provisioning and maintenance of information within the institution in accordance with the relevant prescripts;
- d) Ensure that appropriate capability and capacity are provided;
- e) Determine the delegation of authority, personal responsibility and accountability to the Executive Management with regards to the management of physical, human, information and technology security;
- f) Ensure that related policies for the institutionalisation of information security management are developed and approved, and implemented by Executive Management;
- g) Ensure that information security risks are regularly assessed and managed;
- h) Monitor overall information ICT security statuses and initiatives; and
- i) Ensure the monitoring and evaluation of the effectiveness of the Information Security Management System.

Institutional Information Security Coordinating Function

As Information Security spans different disciplines such as Business Units (information owners), Security Services (including physical security) and ICT (electronic information and infrastructure), it is desirable that this coordinating function resides in the Office of the Head of the Institution. The requirements to optimally manage information security risks can sometimes have an impact on ICT performance, which could create conflicts when critical decisions have to be made. The Director-General has the mandate to delegate this function.

Note: If the Institution has an existing Information Security Officer (“DISO”), this function should be executed by such a person/component.

The Information Security Coordination function should achieve the following:

- a) Ensure that information security is considered throughout the institution;
- b) Oversee and coordinate physical and electronic information security;
- c) Monitor the security of ICT systems and co-authorizes, monitors and controls specific security improvement projects;
- d) Establish, implement and maintain security policies, standards strategies, guidelines, and processes;
- e) Develop and implement security awareness initiatives;
- f) Identify areas of non-compliance to security prescripts;
- g) Design, implement, and provide information security compliance monitoring services to business units;

- h) Direct and monitor the operational ICT risk management; and
- i) Assess the impact of ICT risk on the institution and the efficiency of mitigation measures.

GITO

- a) Ensure the confidentiality, integrity, and availability of ICT systems within the ICT environment;
- b) Manage information security within the institution's ICT infrastructure landscape;
- c) Maintain security of data on the institution's network;
- d) Manage information security within information systems (IS) within the ambit of the ICT function;
- e) Server and Network administration;
- f) Maintain agreed to application security;
- g) Maintain security of data of IS systems and lifecycle management;
- h) Ensure that ICT security arrangements limit security breaches, threats, vulnerabilities and business impacts and if it does occur, to have in place the necessary mitigation arrangements.
- i) Closely collaborate with the head of security services, business management and internal system owners on risks that might impact on electronic information security.

Functional/Business Unit Senior Management

Within the ambit of their functional jurisdiction, the Business Owner of information is also responsible for the management of the life cycle of and the protection electronic information, such as the: classification of information; who should have access to this information; how it should be stored, maintained and disposed of.

Senior management should understand the impact of significant changes within their respective business/functional areas (for example, the creation of new projects, changes in structures, etc.) in order to determine the impact of such changes within the larger realms of information security.

Structures

Information Security Steering Committee

Due to the strategic nature of this committee should be composed of the executive management of the Institution. The committee should oversee the Information Security function and its activities. Ensure clear direction and visible management support for security initiatives. Recommend security policies to the Head of Institution. This does not have to be a separate committee than the Executive Management Committee of an institution (EXCO).

Due to the strategic direction and impact of this committee should be chaired by the Director-General.

Information Security Strategic Committee (ISSC)

A centralized Information Security Coordinating Committee should be established to ensure a clear direction for security initiatives and visible management support. This

committee should consist of a group of individuals in the institution who are responsible for Information Security (both electronic and manual), and who can assist those charged with the governance of information security and those using information systems and technology in carrying out their responsibilities to protect the integrity, availability and confidentiality of public service information assets. The management of Internal Risk should also be a member of this committee.

The chairperson of this committee should be the person to which the Institutional Information Security coordinating function is delegated to.

The objectives of this committee should be, but are not limited to:

- a) Formal involvement of functional units in information security initiatives;
- b) Provide guidance, direction, and request authorization for information security activities for the institution from the Information Security Steering Committee;
- c) Reporting; and
- d) Monitoring

Assurance Providers (AGSA, Internal Audit and other)

The role of Assurance Providers such as internal and external audit is to:

- a) Assess the risk related institutional strategy in the context of its mandate in order to identify the appropriate information system and technology strategy, and operational and control environment's requirements that support the institution in attaining its goals;
- b) To assess, either via the use of a good practice or the use of the institution's own governance and management frameworks whether sufficient means, mechanisms, and controls exist to amicably address these risks within the risk appetite of the institution; and
- c) To raise findings (where applicable) in order to support the institution in improving its governance, management, and operational practices.

Information Security should be included in the activities of the internal Risk and Audit Committees, which should assist the Head of the Institution in carrying out his/her accountabilities and responsibilities in this regard.