ELECTRONIC SIGNATURE GUIDELINES

Version 1.1.0

February 12, 2019

Document Version Control

Date	Author	Version
12 February 2019	DPSA	Version 1.1.0

Approvals

The Electronic Signature Guidelines are approved by the Minister for Public Service and Administration.

Name	Signature	Date

Review Period

This guidelines will be reviewed annually or subsequent to any significant issue arising that has not been considered

Name	Signature	Date

Contact Information

For more information on this policy or to inquire about a variation that is not covered, email at:

Morena.Monareng@dpsa.gov.za

TABLE OF CONTENTS

Definitions/Glossary

DPSA	Department of Public Service and Administration
GCIO	Government Chief Information Office
GITOC	Government Information Technology Officer Council
SITA	State Information Technology Agency
PSA	Public Service Act
PFMA	Public Finance Management Act
POPI	The Protection of Personal Information Act
PAIA	Promotion of Access to Information Act
ICT	Information and Communications Technology
SSA	State Security Agency
MISS	Minimum Information Security Standards
ISO	International Standards Organisation
ISACA	Information Systems Audit and Control Association
NIST	The National Institute of Standards and Technology
SCISS	Standing Committee on Information Systems
ECT	Electronic Communication and Transactions Act, 2002
SAAA	South African Accreditation Authority
PKI	Public Key Infrastructure
AES	Advanced Electronic Signature
SACA	The South Africa Certification Authority
CA	Certification Authority
RA	Registration Authority
CPS	Certification Practice Statement
SAPO	South Africa Post Office

Relevant legislation

Public Service Act, 1994
Public Service Regulations, 2016
Promotion of Access to Information Act, 2000
The Protection of Personal Information Act, 2013
State Information Technology Agency Act, 1998
Intelligence Services Act, 2002
National Archives of South Africa Act, 1996
Electronic Communication and Transactions Act, 2002

1. INTRODUCTION

1.1 The development of electronic government (e-government) and electronic services (e-services) is changing the way public service departments deliver services. As a result, electronic systems and processes are becoming as important as a written signature on paper. In a paper environment, a hand signature authorises and authenticates the content of a document. A signature provides a level of trustworthiness and accountability that aids the conduct of business. Electronic signatures extend the function of handwritten signatures to electronic documents, providing a way for two parties to conduct business confidently in an electronic environment.

1.2 In an effort to support the implementation of an electronic signature solution within the public service, the DPSA developed these generic Electronic Signature Guidelines (hereafter referred to as the "Guidelines"). The Guidelines were developed in collaboration with key ICT security stakeholders in government, such as the GITOC and the SCISS.

1.3 These Guidelines are meant to be referenced by departments planning to utilise electronic signatures and their intent is to:

a) provide the framework for evaluating the appropriateness of an electronic signature technology for an intended purpose;

b) enable greater adoption of digital signature technology across government to streamline business processes, and increase information security.

1.4 The ECT Act established the legal definition for the use of electronic signatures. In terms of the ECT Act, 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*". To determine the risks and security associated with the use of electronic signatures, departments should undertake a risk-based evaluation using the National Treasury Public Sector Risk Management Framework 2010.

1.5 For the purpose of these Guidelines, reference to a ''department/s'' means a national department, a provincial department and a national or provincial government component as per the Public Service Act, 1994.

2. PURPOSE

2.1 The Guidelines are to provide guidance for departments on planning and deploying electronic signatures or digital signatures or advanced electronic solutions to modernise the department's internal efficiency and ensure delivery of the department's constitutional service delivery mandate and objectives.

3. SCOPE

3.1 The Guidelines covers considerations for using electronic signatures as an authentication mechanism of government documents.

3.2 Where relevant laws are referenced, these guidelines are not a substitute for professional guidance on legal matters.

3.3 These guidelines are primarily intended for use by:

a) GITO's of departments;
b) Information Technology Security Officers;
c) GITOC;
d) Government Chief Information Office.

To support the digitisation of services and internal processes, departments are encouraged to consider deploying electronic signature programmes.

4. Legal use of Electronic Signatures in South Africa

4.1 Electronic Signatures in South Africa

4.1.1 The use of electronic signatures in government is recognised under the ECT Act. The ECT Act provides assurance that electronic signatures will be granted the same legal authority as written signatures on paper. Therefore, if an electronic transaction meets the requirements of the electronic signature laws, neither party can repudiate a transaction based on the fact that the transaction was conducted electronically, rather than on paper. Further details on the ECT Act and electronic signatures are discussed in Appendix A.

4.1.2 Electronic signatures (Figure 1 below) come in various forms and have the capacity to meet various purposes (authentication, approval, integrity) and various uses (evidentiary, recordkeeping, etc.). In most cases, a signature required under legislation can be met using a digital alternative and will be deemed equivalent to a written signature provided it meets the criteria stipulated in the ECT Act.

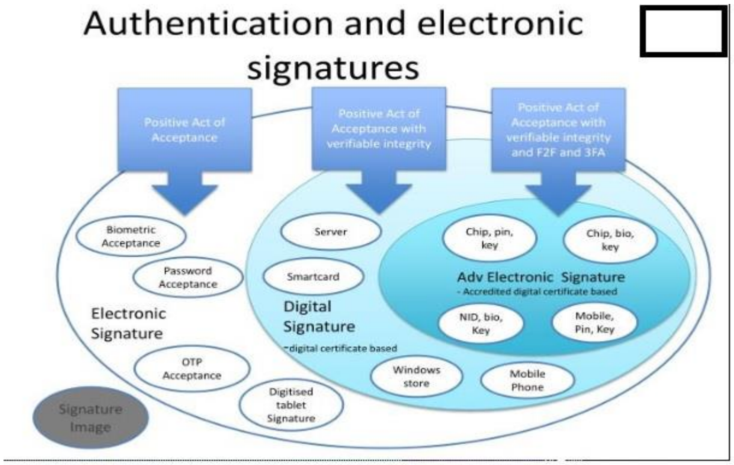

Authentication and electronic signatures
Positive Act of Acceptance
Positive Act of Acceptance with verifiable integrity
Positive Act of Acceptance with verifiable integrity and F2F and 3FA
Biometric Acceptance
Password Acceptance
Electronic Signature
OTP Acceptance
Digitised tablet Signature
Signature Image
Server
Smartcard
Digital Signature
-digital certificate based
Windows store
Mobile Phone
Chip, pin, key
Chip, bio, key
Adv Electronic Signature
- Accredited digital certificate based
NID, bio, Key
Mobile, Pin, Key

Figure 1 Electronic Signature Types as defined in the ECT Act. (Adapted from Lawtrust Ltd)

4.1.3 For many day-to-day operations, a simple electronic signature (generated through authentication or "click to accept" process) is adequate to indicate that an individual has demonstrated intent to sign or approve a transaction. Other cases will require or prefer the use of a digital signature or advanced electronic signature.

4.1.4 A digital signature is a very specific form of an electronic signature that uses cryptography to establish the authenticity and validity of the signature with much greater certainty.

4.1.5 An advanced electronic signature is a digital signature created with a digital certificate from the South African Accreditation Authority (SAAA) under section 37 of the ECT Act, following a face-to-face identification process with the user. An advanced electronic signature is deemed reliable in law and is accepted as prima facie proof of validity, i.e., is always assured to be valid and have been applied correctly, to eliminate the burden of proof. In terms of section 13 of the ECT Act, where the signature of a person is required by law and such law does not specify the type of signature required, an advanced electronic signature must be used. It must be noted that a written signature is still applicable. It is only when an electronic signature is the preferred option that one would be obliged to use an advanced electronic signature.

4.2 Electronic Signature

4.2.1 An electronic signature must be a positive act of acceptance – visible, understandable and fair and must identify the signatory and be verifiable.

4.2.2 As per section 13 of the ECT Act, where an electronic signature is required, and where parties have not agreed to the type of electronic signature to be used, the signature requirement is met if –

a) " *a method used identifies the person and indicates the person's approval of the information; and*

b) *having regard to all relevant circumstances at the time the method was used, the method was reliable and appropriate for the purpose for which the information was communicated*."

4.3 Digital Signature

4.3.1 A digital signature (although not defined in the ECT Act), is a signature that originates with a digital certificate.

4.3.2 A digital certificate is issued to a person, once that person has been verified as the person who they claimed to be.

4.3.3 A digital signature requires not only a positive act of acceptance but also has verifiable integrity as a result of a digital certificate.

4.3.4 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.

4.3.5 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.

4.4 ADVANCED ELECTRONIC SIGNATURES (AES)

4.4.1 An AES is defined in the ECT Act as "*an electronic signature which results from a process which has been accredited by the Authority*[1] *as provided for in section 37*".

4.4.2 That is, 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.

4.4.3 An AES consists of a positive act of acceptance, 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:

a. Something you are (biometrics such as fingerprint and iris scan);
b. Something you know (pin, password, passphrase or secret question);
c. Something you have (key, device).

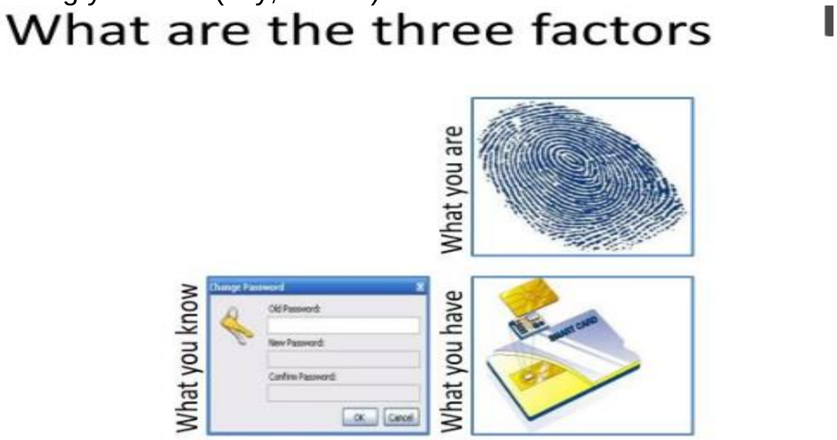


Figure 2 What are the three factors

4.4.4 The 3-factor authentication makes the AES strong, reliant and trustworthy.

4.4.5 Section 13(4) of the ECT Act states that " *where an AES has been used, such signature is regarded as being a valid electronic signature and to have been applied properly unless the contrary is proved*."

4.4.6 An AES is 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.

[1] South African Accreditation Authority

4.5 PUBLIC KEY INFRASTRUCTURE (PKI)

4.5.1 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.

4.5.2 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.

4.5.3 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.

4.6 DIGITAL SIGNATURE CERTIFICATES

4.6.1 A digital certificate (APPENDIX D) 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.

4.7 TYPES OF DIGITAL SIGNATURE CERTIFICATES

4.7.1 There are three (3) types of digital certificates and are applied depending upon the assurance level and usage requirements.

The following table provides an overview of the different types of digital certificates and the level of assurance.

Type of Certificate	Description and Assurance level
Class 2 certificate	**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
Class 3 certificate	**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.
Advanced Electronic Signatures (Class 4 Certificates)	**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.

Table 1 Types of Certificates

4.7.2 The South Africa Certification Authority (SACA) is responsible for issuing public key certificates (henceforth referred to as Certifying Authorities or CAs). 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).

4.7.3 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.

4.7.4 The guidelines should be used to assist departments in making informed decisions regarding the appropriate use of electronic signatures at each level. Departments must determine the risks and benefits of the available technologies for their specific applications. How an electronic signature works is described in Appendix B.

5. GUIDELINES FOR ELECTRONIC RECORDS

A key issue with electronic signatures is proving that the signature is from the person the signature represents and that the document has not been altered.

5.1. CHARACTERISTICS OF TRUSTWORTHY ELECTRONIC RECORDS

According to the National Archives and Record Service of South Africa Act No. 43 of 1996, the characteristics listed below are used to describe trustworthy records from a records management legal perspective.

5.1.1 Reliability

Record content can be trusted as a full and accurate representation of the transactions, or facts to which it attests and can be depended upon in the course of subsequent transactions.

5.1.2 Authenticity

A record proved to be what it claims to be or to have been created or sent by the person who claims to have created and sent it; assurance of identity.

5.1.3 Integrity

Proof that a record is complete and has not been altered.

5.1.4 Usability

A record can be located, retrieved, presented, and interpreted in connection with the transaction that created it.

5.1.5 Signature Intent

The process used to obtain the electronic signature must demonstrate that the user intended to sign the record. Establishing intent includes:

a) Identifying the purpose of signing the electronic record (could be apparent within the context of the transaction);
b) Being reasonably certain the signatory knows which electronic record is being signed; and
c) Providing notice to the signer that their electronic signature is about to be applied to, or associated with, the electronic record (such as an online notice advising the signer that continuing the process will result in an electronic signature).

5.2. ELECTRONIC RECORDS MANAGEMENT[2]

The process used to conduct electronic transactions must be documented, such as in a formal procedure, and followed consistently.

Electronic Records System Requirements

5.2.1 Consistent

The system processes information in a manner that assures the records they create are credible.

5.2.2 Complete

Contains the content, structure, and context generated by the transaction they documented.

5.2.3 Accurate

Quality control at the input level to ensure the information in the system correctly reflects what is communicated in the transaction.

5.2.4 Preserved

Continue to reflect content, structure, and context within any system by which the records are retained over time.

[2] Section 13 – Management of public records. National Archives and Records Service of South Africa Act 43 of 1996. Regulation 10 – Management and care of records. National Archives and Records Service of South Africa Act 43 of 1996 - Regulation

5.3. NON-REPUDIATION

5.3.1 A property that protects against an individual or entity from denying having performed a particular action related to the data. Non-repudiation services protect the reliability, authenticity, integrity, usability, confidentiality, and legitimate use of the electronically signed document.

Essential elements of a non-repudiation model include:

a) Evidence of the origin of the message
b) Evidence of being sent
c) Evidence of receipt
d) Timestamp, as needed, by the department of origin
e) Long-term storage of evidence
f) Designated adjudicator of prospective disputes

5.3.2 Departments shall maintain adequate documentation of the system design, implementation, use, and migration. The documentation shall include a narrative description of the system, physical and technical characteristics, and any other technical information required to access or process the electronic records.

5.4. PRESERVING ELECTRONIC RECORDS

For a record with an electronic signature to remain trustworthy over the record life cycle, it is necessary to preserve its content, context, and sometimes its structure.

5.4.1 Content

Includes the electronic signature and any associated date or other identifiers, such as organization or title. It provides evidence of a document's reliability and authenticity.

5.4.2 Context

Includes individual identifiers that are not embedded in the content of the record but are used to create and verify the validity of an electronic signature. It provides additional evidence to support the reliability and authenticity of the record.

5.4.3 Structure

Includes the physical and logical format of the record and the relationships between data elements comprising the record. If a department determines it is necessary to maintain the structure of the electronic signature, it must be able to recreate the signature or demonstrate the process used to create the signature.

5.5. STEPS TO ENSURE ELECTRONICALLY-SIGNED RECORDS ARE TRUSTWORTHY:

5.5.1 Create and maintain documentation of the systems used to create the records that contain electronic signatures.

5.5.2 Ensure records that include electronic signatures are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.

5.5.3 Implement standard operating procedures for the creation, use, and management of records that contain electronic signatures and maintain written documentation of those procedures.

5.5.4 Create and maintain records according to the documented standard operating procedures.

5.5.5 Train department staff in the standard operating procedures.

5.5.6 Dispose of records that contain the electronic signatures and the associated records according to the established retention schedule for the department and the National Archives Act No. 43 of 1996.

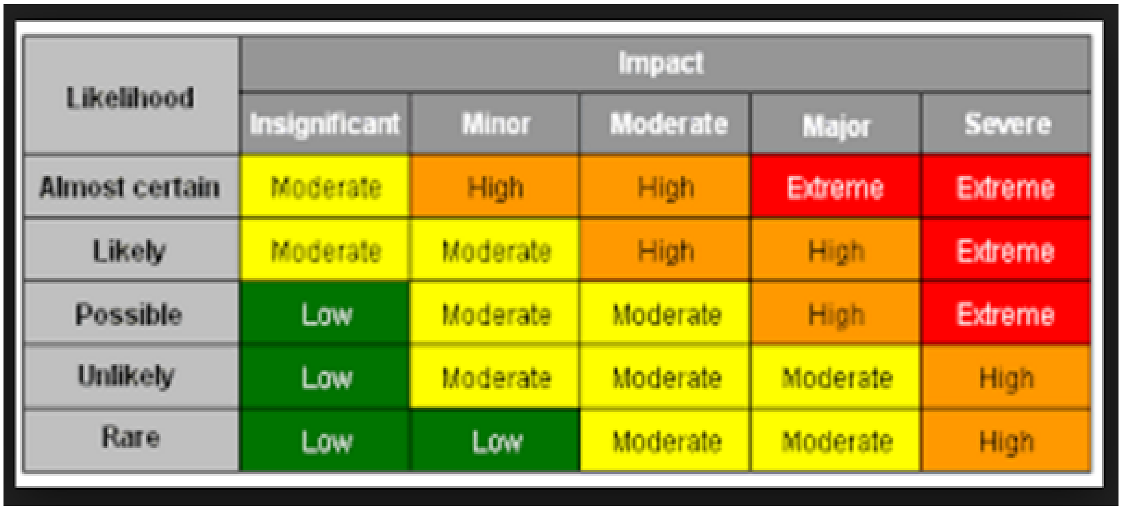
6. Risk Management of Electronic Records

6.1. The purpose of risk management is to identify transaction risk factors that could contribute to the possibility of a challenge being made to the validity or enforceability of the signature. Departments should document the process used to determine transaction risk and maintain a copy of this document in their files for future reference.

6.2. Each potential challenge to the enforceability of an electronic signature, a business analysis, and risk assessment should consider:

a) the likelihood of a successful challenge to the validity of the electronic signature; and
b) the monetary loss, or another adverse impact, that will result from such a successful challenge to the enforceability of the electronic signature.

6.3 A qualitative approach should be taken with respect to the risk analysis. Using such an approach, the risk of a challenge being successful and having a significant impact is defined in more subjective and general terms such as high, moderate, and low. In this regard, qualitative analyses depend more on the expertise, experience, and good judgment of the department managers conducting them than on quantified factors. Department risk management team should be consulted as the department's risk register may need to be updated.



Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

Figure 3 Risk Matrix

6.4 In determining whether a signing process is sufficiently reliable for a particular purpose (see also section 9.4 – The Legal Framework for using Electronic Signatures), department business assessments and risk analyses should consider, at a minimum:

a) the relationships between the parties;
b) the value of the transaction;
c) the risk of unauthorized alteration; and
d) the likely need for accessible, persuasive information regarding the transaction at some later date.

6.5 In addition, the department should consider any other risks relevant to the particular process. Once these factors are considered separately, the department should consider them together to evaluate the sensitivity of risk for a particular process, relative to the benefit that the process can bring. A Risk Assessment Framework (Appendix C) is proposed for departments. The framework is in addition to the department's internal risk assessment methodology and the National Treasury Public Sector Risk Management Framework April 2010.

6.6 There are also risks associated with digital signature certificates in that the issued certificate maybe no longer be valid (e.g., revoked, expired or suspended). Departments must verify with the Certifying Authority (CA) issuing certificates to the end-user that:

a) 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
b) 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).
c) documents signed with valid certificate prior to certificate revocation, expiration or suspension remain valid.

6.7 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.

6.8 The overall effectiveness of a given electronic signature process depends on how well the department determined the means to mitigate the risks for particular documents and records to be presented, signed, and archived. The department that carefully considers the risks associated with the types of transactions to be processed can design and implement an electronic signature process that is no riskier than, and in most cases less risky than, the same transaction using paper and a written signature. Doing so provides greater confidence that the electronic signature, when affixed within South Africa, will be admissible into evidence and enforceable.

7. ELECTRONIC SIGNATURE GOVERNANCE

7.1. The governance of electronic signature in a department falls within the Information Security Governance model as proposed in the Information and Communication Technology (ICT) Security Guidelines, Version 1, 09 February 2016. A governance model for ICT security management is shown in Figure 4 below.

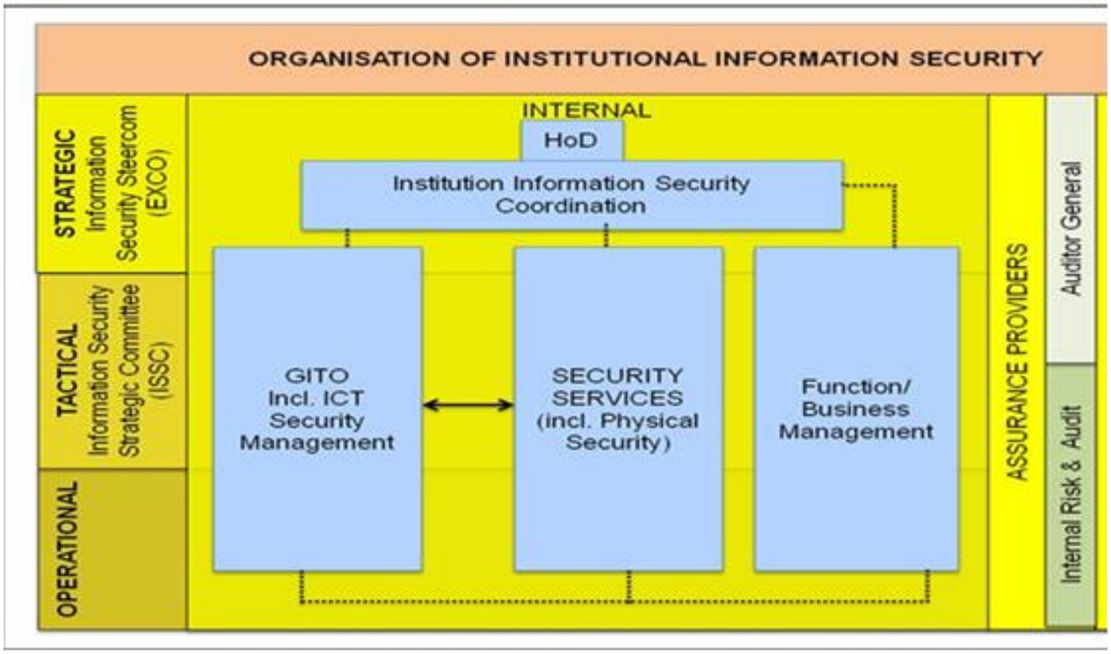

ORGANISATION OF INSTITUTIONAL INFORMATION SECURITY
STRATEGIC Information Security Steercom (EXCO)
TACTICAL Information Security Strategic Committee (ISSC)
OPERATIONAL
INTERNAL
HoD
Institution Information Security Coordination
GITO Incl. ICT Security Management
SECURITY SERVICES (incl. Physical Security)
Function/ Business Management
ASSURANCE PROVIDERS
Auditor General
Internal Risk & Audit

Figure 4 A Governance model for ICT security management

7.2 The roles and responsibility are explained in Appendix E. Where possible the proposed information security structures, roles, and responsibilities should be absorbed within the existing structures, roles, and responsibilities of the department

7.3. The ultimate responsibility for the deployment of an electronic signature solution within a department is vested in the Executive.

8. PLANNING OVERVIEW FOR AN ELECTRONIC SIGNATURE PROGRAMME

8.1. BUSINESS ANALYSIS & REQUIREMENTS

As departments gather information on the appropriate use of electronic signatures, they should include a number of subject-matter experts from within their departments. The following subject-matter experts listed below should be considered.

Stakeholder	Information Required
GITO/CIO	Information technology staff should be identified and consulted both for knowledge and guidance on the selection of a particular technology, and also for a thorough understanding of the existing technology architecture of the organization.
Department IT Security	The group should include someone with IT security knowledge and expertise to ensure adequate safeguards are included
Business/Branches	The primary decision a department will make is whether it makes business sense to adopt the use of electronic signatures or records for a particular transaction. Accordingly, knowledgeable members of the business lines impacted by any policy must be included. These members should have an understanding of existing processes and anticipated benefits of using electronic signatures or records
CFO/Finance	To help with the National Treasury requirements and PFMA prescripts
Internal Legal	The question of whether or not a signature or record is required, and whether a proposed electronic signature solution is likely to withstand a challenge should be answered. As this will be accomplished through legal research, appropriate expertise is required
SCM/Procurement	Internal procurement staff should be included so that they are well informed of the department business needs and the impacts. Also, concerns discussed during the decision-making process can be well considered when determining the method of procurement and the resultant contract terms and conditions to ensure that they support the goals of the department.
Records Management	Personnel with knowledge of department record retention and documentation requirements should be included to ensure compliance with these guidelines and other relevant records rules
Internal Audit, Risk and Compliance	Internal Audit should be consulted in order to confirm that the processes are within the prescripts of the Auditor-General requirements. Risk & Compliance to ensure compliance with the department's risk management requirements.
The State Information Technology Agency (SITA).	SITA is the government ICT implementation agency. Besides managing government networks, ICT products are procured through SITA.
Accounting Officer	Approve the use of electronic signatures

Table 2 Stakeholders Information Requirements

8.2. GATHERING REQUIREMENTS

Some areas a department might review include:

8.2.1 Existing legislation and regulations.

This area focuses on laws regarding the department's collection and/ or distribution of signatures and records. For any particular document or transaction, the first step should be to determine what the law requires the department to do. For example, is a signature even necessary for a particular transaction? Furthermore, the use of electronic signatures may be prohibited by law. Accordingly, the department should determine whether there is any law that precludes or requires the use of electronic signatures.

8.2.2 Existing department policy and practice.

Current departmental business processes should be reviewed to identify:

a) potential areas where electronic signatures could be effectively used, and
b) transactions and documents that are currently electronic in nature.

The department can also begin defining the requirements for those processes and determine the costs associated with each. The department may also put this information into the department policy as the policy is drafted.

8.2.3 Existing records requirements.

The department will need to determine what records retention requirements apply for electronic transactions under consideration, including any retention schedule specific to the department.

8.2.4 Technology capabilities.

The department should have an understanding of adequate and available technological solutions, including electronic records formats and electronic signature methods related to systems currently being used by the department. The department should also focus on the ease-of-use of an electronic signature or records solution, considering the needs and capabilities of both end-users and department personnel.

8.2.5 Current technological architecture.

Electronic signatures and records will also need to fit within the broader departmental Information Technology (IT) environment. In order to make an informed decision about compatibility or interoperability, the department should have a thorough understanding of its current system and where and how new electronic signatures and records can fit within it.

8.3. Making Electronic Signature Decision

After the department's stakeholders have identified potential candidates for electronically signed transactions, a determination can be made whether, and in what circumstances, the department will use or accept electronic signatures. For those transactions identified, the department must adopt a policy consistent with the guidelines set forth in this document.

8.3.1 Document the Business Analysis and Risk Assessment (see section 5), documenting the business purpose behind the decisions.

8.3.2 Determine which technologies can or cannot fit within the department's current technological architecture. If the current architecture is a barrier to adopting a desirable technology, consider what can or should be changed within the existing architecture to allow for such use.

8.3.3 Begin development of instructions and training materials for end-users and department personnel, particularly if the policy will represent a substantial change in current processes or procedures.

8.4. Write a Policy

Draft the departmental policy reflecting the decisions made in section 8.3. These Guidelines do not specify which electronic signature methods or processes must or should be used. Rather, those decisions are left to departments based on the business assessment and risk analyses they conduct. Departments should consider the following when drafting their policy:

The policy should clearly identify any department specific standards, limitations and processes, including:

8.4.1 Specific technology choices the department has made
8.4.2 Specific transactions the department intends to be completed electronically
8.4.3 Specific groups of constituents that can or cannot use such signatures or records (e.g., the department allows electronic signatures for only certain contracts, or allows electronic filings only for renewal transactions but not an initial application)
8.4.4 Standard processes and methodologies the department intends to follow or use, such as providing users with a document for printing or download as part of the signing process
8.4.5 End-user instructions and other training materials
8.4.6 Update Information Security Policy and Guidelines
8.4.7 Update Electronic Records Management Guidelines (see section 8.5 below)
8.4.8 Incorporate Electronic Signature Governance into the departments' ICT governance

8.5. Managing Electronic Records

8.5.1 Departments on deploying electronic signatures will need to develop a policy on how to manage electronic records.

8.5.2 The policy should be in line with the requirements of the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) on managing Public records. Public records are those created or received in the course of official business and which are kept as evidence of a governmental body's functions, activities, and transactions.

8.5.3 The Electronic Record management methodology adopted must be within the department's internal record management policy, information security policy, and the prescripts of the ECT Act 2002.

9. STEPS FOR AN ELECTRONIC SIGNATURES PROGRAMME

Departments should follow these steps to assist them in the implementation and use of electronic signatures.

9.1. IDENTIFY RELEVANT REGULATIONS, POLICIES, AND PROCEDURES

Identify department regulations, policies, and procedures affected by the ECT Act 2002 to ensure the use of electronic signatures is within the prescribed law. The following may be relevant:

a) Department's Information Security Policy
b) Minimum Information Security Standards (MISS)
c) ECT Act 2002
d) The National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended)
e) Department's Record Management Policy
f) Department's Risk Management Policy
g) PFMA No 1 of 1999
h) National Cyber Security Policy Framework
i) POPI Act

9.2. IDENTIFY STAKEHOLDERS/SUBJECT EXPERTS

Identify the stakeholders/subject experts that will be impacted by the electronic signatures programme – see section 8.1.

9.3. EVALUATE CURRENT BUSINESS PROCESS

Evaluate current business processes to determine if a signature is required on a document. Public Service Operations Management Framework: Business Process Management could be used to analyse business processes.

9.4. THE LEGAL FRAMEWORK FOR USE OF ELECTRONIC SIGNATURES

Consider the legal framework for deploying the electronic signature solution. When determining the type of signature that needs to be applied, departments must consider ECT Act Signature decision tree model figure 3 below:

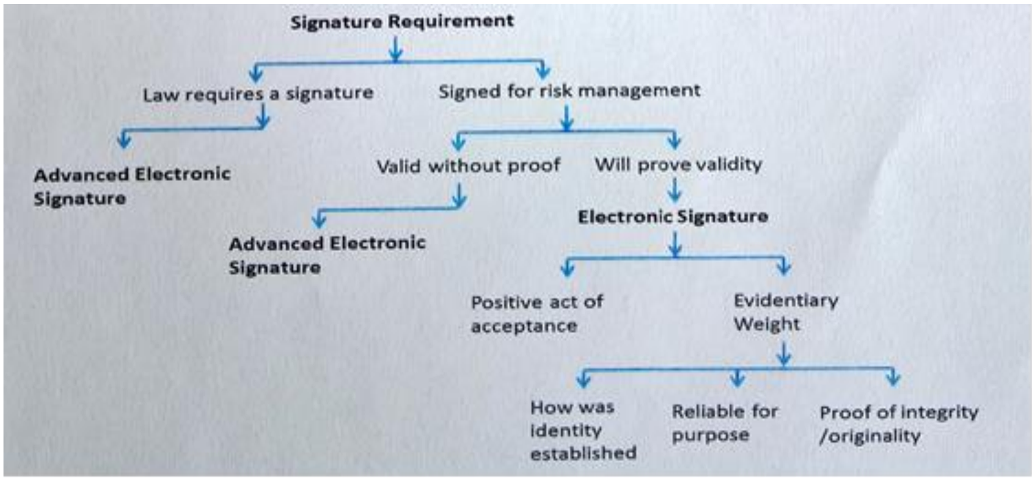

Signature Requirement
Law requires a signature
Signed for risk management
Advanced Electronic Signature
Valid without proof
Will prove validity
Electronic Signature
Advanced Electronic Signature
Positive act of acceptance
Evidentiary Weight
How was identity established
Reliable for purpose
Proof of integrity /originality

Figure 5 ECT Act Signature decision tree (Adapted from Lawtrust)

9.4.1 To understand the decision tree model (figure 5 above), departments must reference section on the type of digital certificates and assurance level – see section 4.7 and Risk Management of Electronic Records - see section 6.

9.4.2 Most of the departments are likely to deploy Class 3 digital certificates, as these certificates are suitable for close communities.

9.4.3 Where the law requires a signature, that is, valid without proof, only an Advanced Electronic signature can be used.

In summary, the following areas of the ECT Act are of specific importance to deriving benefit from electronic signatures:

9.4.3. 1 Original

An original may be electronic in form, as long as the integrity of the document is assured. This requirement is supported by digital signatures from X.509 digital certificates, which ensures that tampering of the data can be detected.

9.4.3. 2 Evidential Weight

Electronic evidence, including an electronic signature, is subject to assessment for evidential weight.

The assessment will look at:

a) The reliability of data evidence generation, transmission, and storage
b) The reliability of the integrity of the data evidence
c) The method used to identify the parties to the transaction or data evidence
d) Any other factor that is relevant

This requirement is again easily met by the practices around digital certificates and digital signatures which not only ensures the integrity of data but also creates policy and practices which ensures that the identity of an originator is established formally and in an auditable manner.

9.4.3.3 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.

The department's internal legal unit must be consulted for advice on the requirements of the ECT Act 2002.

9.5. THE DECISION TO UTILISE ELECTRONIC SIGNATURE SOLUTION

If a signature is necessary, evaluate each business process in the areas listed below to determine which type of electronic signature meets the business requirements of that document.

9.5.1 Scope of deployment

Determine if the transaction is employee-to-organization, customer-to-organization, organization-to-supplier, etc. Some relationships are inherently more trusted than others. See section 6 Types of Digital Certificates.

9.5.2 Department ICT Technical Infrastructure

An electronic signature solution deployed must complements or fits within the existing technology infrastructure.

9.5.4 Government Regulations

Government Regulations: Determine if any regulations prohibit or restrict the use of electronic signatures for the particular application.

9.6. GOVERNANCE AND SECURITY

9.6.1 The Director-General must approve the deployment of electronic signatures solution.

9.6.2 Departments must engage their internal security unit to facilitate the vetting of the service provider.

9.6.3 Departments do not have to develop separate governance structures but incorporate electronic signature governance into the department's corporate governance of ICT.

9.6.4 The information security policy should be updated to include electronic signature security. The accounting officer must approve the updated policy.

9.6.5 The level of electronic signature selected must ensure the proper level of authentication, confidentiality, integrity, security, and non-repudiation. Departments must consult their internal legal units for advice on the prescripts of the ECT Act 2002.

9.6.6 Department employees must protect and not disclose or make available their digital signature private key or password to other persons.

9.6.7 The department must revoke or send a revocation notice to the certification authority for employees no longer authorized to conduct electronic business on behalf of the department.

9.6.8 Departments must document the process used to electronically sign documents and coordinate this process with the department record management policy and guidelines.

9.6.9 Each department that uses digital signature technology must establish a digital signature implementation and use policy that:

a) describes how the department will determine which employees will have a digital signature, the scope of the employee's authority to use the digital signature and for what purposes;

b) identifies the roles and responsibilities of issuing digital signatures, letters authorizing the issuance of certificates, procedures to protect digital signatures, and procedures for suspension or revocation of digital signature certificates;

9.6.10 Certification Authorities (CA) must provide the following information or meet the following requirements to be authorized to issue digital certificates in South Africa:

a) Certification Practice Statement (CPS) that documents the practices, procedures, and controls employed by the certification authority.

b) Statement of compliance with X.509V3 Certificate.

c) Approved (registered) service provider accredited by SAAA

9.7 Risk Assessment and Management

In order to implement a digital signature programme which uses the PKI system in the department, the following must be in place:

9.7.1 The risk assessment must have been conducted by those who are implementing the project together with the internal ICT security team of a department.

9.7.2 The report of the risk assessment should form part of the motivation to implement the program.

9.7.3 A comprehensive risk management program must be in place to militate against the identified risks which were identified in the above-mentioned assessment report.

9.7.4 Make any necessary revisions regarding the use of signatures to the affected policies e.g., incorporate Electronic Signature policy into the Information Security Policy, and procedures.

9.8 UPDATE DOCUMENT RETENTION AND ARCHIVING POLICY

9.8.1 Records created as a result of electronic transactions must be retained according to the department's retention policy, and the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended).

9.8.2 Electronically signed records must contain all the information necessary to reproduce the entire electronic record and associated signatures in a form that permits the person viewing or printing the entire electronic record to verify:

a) The contents of the electronic record
b) The method used to sign the electronic record, if applicable
c) The person(s) signing the electronic record
d) The date when the signature was executed

9.9 DEVELOP ELECTRONIC SIGNATURE SECURITY AWARENESS TRAINING

Department must develop Electronic Signature Security Awareness guidelines. Department must ensure that employees are trained on:

a) the use of the application
b) the implications of its use
c) the way in which electronically authorised documents should be handled and filed.

9.10 SEEK APPROVAL FROM ACCOUNTING OFFICER

The Executive must approve the use of electronic signature in the National Department. In the Provincial Department or government, the Premier must approve.

Documents to be furnished with the request for approval:

a) Motivation/Business Case for utilising Electronic Signatures solution
b) List of documents to be signed electronically
c) Internal legal advice

10. REFERENCES

1. Electronic Communications and Transactions Act of 2002
2. LSSA Guidelines Electronic Signatures for South African Law Firms October 2014.pdf [WWW Document], n.d. URL http://www.lssa.org.za/upload/documents/LSSA%20Guidelines_Electronic%20Signatures%20for%20South%20African%20Law%20Firms_October%202014.pdf (accessed 12.7.16).
3. National Cybersecurity Policy Framework - 39475_gon609.pdf [WWW Document], n.d. URL http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf (accessed 12.23.16).
4. National Archives of South Africa Act 43 of 1996 - Act43of1996.pdf [WWW Document], n.d. URL http://www.gov.za/sites/www.gov.za/files/Act43of1996.pdf (accessed 12.16.16).
5. New EU regulation for electronic signatures | Insights | DLA Piper Global Law Firm [WWW Document], n.d. DLA Piper. URL https://www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/ (accessed 12.16.16).
6. Electronic signature - Wikipedia [WWW Document], n.d. URL https://en.wikipedia.org/wiki/Electronic_signature (accessed 12.16.16).
7. Public key infrastructure - Wikipedia [WWW Document], n.d. URL https://en.wikipedia.org/wiki/Public_key_infrastructure (accessed 1.4.17).
8. Trust Centre - Powered by the SA Post Office [WWW Document], n.d. URL https://www.trustcentre.co.za/index.php (accessed 1.7.17).
9. Global Guide to Electronic Signature Law - adobe-global-guide-electronic-signatures.pdf [WWW Document], n.d. URL https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf (accessed 12.7.16).
10. Electronic Signatures and Trust Services - beis-16-15-electronic-signatures-guidance.pdf [WWW Document], n.d. URL https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/545098/beis-16-15-electronic-signatures-guidance.pdf (accessed 12.7.16).
11. ‘New EU Regulation for Electronic Signatures | Insights | DLA Piper Global Law Firm’. DLA Piper. Accessed 7 December 2016. https://www.dlapiper.com/en/us/insights/publications/2015/08/new-eu-regulation-for-electronic-signatures/.
12. ‘What Is PKI (Public Key Infrastructure)? - Definition from WhatIs.com’. *SearchSecurity*. Accessed 23 December 2016. http://searchsecurity.techtarget.com/definition/PKI.
13. Guidelines for Usage of Digital Signatures in e-Governance - v1.0 - Guideline-for-digital-signature.pdf [WWW Document], n.d. URL http://www.daman.nic.in/downloads/2015/Guideline-for-digital-signature.pdf (accessed 12.16.16).

11. APPENDICES

Appendices attached as a separate document.