

















































- 
- Filling out an application form and providing true and correct information.

Then after having check information provided by the Subject, the RA continues the enrollment process with the following steps:

- Generating a certificate and the key pair.
- Delivering the generated public key corresponding to the private key to the CA.
- Demonstrating possession of the private key corresponding to the public key delivered to the CA.

## **6.2 Certificate Application Processing**

---

### **6.2.1 Performing Identification and Authentication Functions**

---

The RA shall perform identification and authentication of all required information as described in Section 5.2.

### **6.2.2 Approval or Rejection of Certificate Applications**

---

The certificate application may be rejected for various reasons such as inaccurate information. The CA or RA may reject a certificate application and should justify the rejection to the applicant or any other party.

A certificate application shall not be considered accepted until the CA has accepted the application and decided to issue a certificate.

### **6.2.3 Time to Process Certificate Applications**

---

The CA or RA shall act on and process a certificate application within a time frame of five ((3)) working days from the receipt of a correctly completed application.

## **6.3 Certificate Issuance**

---

### **6.3.1 CA Actions During Certificate Issuance**

---

During the certificate issuance, the CA shall:

- Authenticate the certificate request and the RA which issued the request.
- Ensure that the public key is bound to the correct Subject and obtain proof of possession of the private key.

- 
- Approve or disapprove the certificate request.
  - Generate the certificate.
  - Provide the certificate to the Subject through the RA.
  - Publish the certificate to the repository.

### **6.3.2 Notifications to Subject by the CA of Issuance of Certificate**

---

Not applicable.

## **6.4 Certificate Acceptance**

---

### **6.4.1 Conduct Constituting Certificate Acceptance**

---

The Subject signature on a certificate acceptance form, on the Subject Agreement and Subscriber Agreement (if the Subject acts on its own behalf) shall constitute acceptance of the certificate.

The Subject signature shall be collected before the CA allows a Subject to make effective use of its private key.

### **6.4.2 Publication of the Certificate by the CA**

---

CA certificates and Subjects certificate shall be published to the repository.

### **6.4.3 Notification of Certificate Issuance by the CA to Other Entities**

---

No stipulation.

## **6.5 Key Pair and Certificate Usage**

---

### **6.5.1 Subject Private Key and Certificate Usage**

---

Subscriber and Subject responsibilities for correct use of keys and certificates shall be clearly laid out in the Subscriber and Subject Agreements.

Subjects shall not use the signature key after the associated certificate has been revoked or has expired.

Subjects shall protect their private keys from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

---

## 6.5.2 Relying Party Public Key and Certificate Usage

---

Relying Party responsibilities for correct use of public keys and certificates shall be clearly laid out in the Relying Party Agreements.

Relying Parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension if the extension is present.

---

## 6.6 Certificate Re-Key

---

Re-key a certificate means extends the certificate validity with the same name, key, and authorizations as the old one.

Certificate re-key is not allowed under this Policy.

---

## 6.7 Certificate Renewal

---

Certificate renewal is the application for the issuance of a new certificate that certifies the new key pair (public key – Private Key).

### 6.7.1 Circumstances for Certificate

Prior to the expiration of an existing Subject's certificate, it is necessary for the subject to renew the certificate to maintain continuity of certificate usage. A certificate may also be re-keyed after expiration.

---

### 6.7.2 Who May Request Certificate of a New Public Key

---

The Subject, CA or RA may request the re-key of a Subject certificate.

---

### 6.7.3 Processing Certificate Renewal Requests

---

The renewal process shall be akin to the initial certificate issuance process described in Section 6.3.

Renewal requires the generation of a new public-private key pairs and generation of the corresponding new certificates.

---

### 6.7.4 Notification of New Certificate Issuance to Subject

---

See Section 6.3.2.

---

### **6.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate**

---

See Section 6.4.1.

### **6.7.6 Publication of the Re-Keyed Certificate by the CA**

---

See Section 6.4.2.

### **6.7.7 Notification of Certificate Issuance by the CA to Other Entities**

---

See Section 6.4.3.

## **6.8 Certificate Modification**

---

Modifying (updating) a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate.

Certificate modification is not allowed under this Policy. To modify any certificate information, the process to follow shall be the same as for a new certificate request.

### **6.8.1 Circumstances for Certificate Modification**

---

Not applicable.

## 6.9 Certificate Revocation

---

### 6.9.1 Circumstances for Revocation

---

Certificates shall be revoked:

- When any of the information in the certificate changes before the certificate expires.
- When there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the Subject's private key.
- When there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the media holding the Subject's private key.
- When the Subject is no longer an employee of the organization (for certificates issued to an organization Subscriber).
- When the Subject can be shown to have violated the stipulations of the Subscriber or Subject Agreement.
- When the Subscriber can be shown to have violated the stipulations of the Subscriber Agreement.
- When there has been a loss, theft, modification, unauthorized disclosure or other compromise of the CA's private key or more generally when the CA certificate is revoked.

Whenever any of the above circumstances occur, the associated certificate is revoked and placed on the CRL.

## 6.9.2 Who Can Request Revocation

---

The revocation shall be requested by:

- The Subject holding the private key corresponding to the public key in the certificate.
- The Subscriber (or Subscriber Trusted Signatory) of the Subject certificate.
- Legal entities

## 6.9.3 Procedure for Revocation Request

---

Any format (face-to-face Revocation Form or Telephone Revocation or signed e-mail with valid certificate) that is used to request a revocation shall:

Identify the certificate to be revoked.

Explain the reason for revocation.

Allow the request to be authenticated (e.g., digitally, or manually signed).

Following approval of the revocation request by the RA, the RA issue a revocation request to the CA which shall authenticate and approve the request then automatically and immediately perform the revocation.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. A record of the revocation request shall be maintained for audit purposes.

## 6.9.4 Revocation Request Grace Period

---

Revocation requests shall be processed and executed without delay upon receipt during the opening hours of the customer service center – Sunday to Thursday from 8:00 AM to 4:30 PM except on Egypt National Public Holydays.

The subscribers/subjects can perform their revocation requests through Egypt Trust's CALL CENTER (19877) which is available twenty-four (24) hours per day seven (7) days per week.

---

### **6.9.5 Time within Which CA Must Process the Revocation Request**

---

The CA shall process all revocation requests within one ((1)) hour of receipt during the opening time of the revocation service.

### **6.9.6 Revocation Checking Requirements for Relying Parties**

---

Relying Parties shall check the status of certificates on which they wish to rely. They shall check all certificates in the certificate validation path against the current CRL. If it is temporarily infeasible to obtain revocation information, then the Relying Party shall either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

### **6.9.7 CRL Issuance Frequency**

---

The CA shall ensure that it issues and posted to a repository an up to date (CRL at least twice (2) per day each one is valid for 24 hours, even if there are no changes or updates to be made).

Whenever a certificate is revoked, a new CRL shall be issued immediately.

### **6.9.8 Maximum Latency for CRLs**

---

The CRL shall be posted upon generation, (but within no more than forty-five ((45)) minutes after generation).

### **6.9.9 On-Line Revocation/Status Checking Availability**

---

The CA does not currently support on-line revocation/status checking.

### **6.9.10 On-Line Revocation Checking Requirements**

---

Not applicable.

### **6.9.11 Other Forms of Revocation Advertisements Available**

---

No stipulation.

### **6.9.12 Special Requirements Related to Key Compromise**

---

In the event of the compromised or suspected compromise, of the CA signing key, the CA shall notify all Subjects to whom it has issued certificates, and potentially Relying Parties.

## **6.10 Certificate Status Services**

---

### **6.10.1 Operational Characteristics**

---

The status of certificates is available through the CRL stored in the repository. It may also be available through a Web site at an URL specified in the CPS.

### **6.10.2 Service Availability**

---

The repository shall be available twenty-four (24) hours per day, seven (7) days per week subject to the maximum period of unavailability as specified in the CPS.

### **6.10.3 Optional features**

---

No stipulation.

### **6.10.4 End of Subscription**

---

The reasons for end of subscription shall include:

- Certificate expiration without renewal.
- Certificate revocation without replacing the certificate.
- The Subscriber contract termination- must be mentioned in the contract
- The CA service termination.

## **6.11 Key Escrow and Recovery**

---

The CA shall not hold in escrow Subject private keys.

### **6.11.1 Key Escrow and Recovery Policy and Practices**

---

Not applicable.

### **6.11.2 Session Key Encapsulation and Recovery Policy and Practices**

---

Not applicable.

---

## **7 Facility, Management and Operational Controls**

---

### **7.1 Physical Controls**

---

Physical security controls shall be implemented that protect the CA and RA hardware and software from unauthorized use.

#### **7.1.1 Site Location and Construction**

---

The PKI system operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

#### **7.1.2 Physical Access**

---

Physical access shall be auditable and restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones.

Dual Access concept must be adopted in entering or leaving any area related to the Online/Offline CA Rooms

Physical access shall be granted to the personnel in charge of the PKI or authorized persons.

#### **7.1.3 Power and Air Conditioning**

---

The power and air conditioning facilities shall be sufficient to support the operation of the PKI system.

#### **7.1.4 Water Exposures**

---

The PKI system shall be protected from water exposures.

#### **7.1.5 Fire Prevention and Protection**

---

The PKI system shall be protected with a fire suppression system.

#### **7.1.6 Media Storage**

---

Media shall be stored securely. Media used by the PKI system shall be protected from environmental threats such as temperature, humidity, and magnetism.

#### **7.1.7 Waste Disposal**

---

All media used for the storage of information such as keys, activation data or PKI system files shall be sanitized or destroyed before released for disposal.

---

### 7.1.8 Off-Site Backup

---

If approved Facilities used for off-site back-up shall have the same level of security as the primary PKI system site.

## 7.2 Procedural Controls

---

### 7.2.1 Trusted Roles

---

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

Trusted roles shall include, but shall not be limited to:

- Egypt Trust Certificate Policy Committee members oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
- Server Officer: this person is in charge of all tasks relating to the administration of the operating system.
- Network Officer: this person is in charge of all tasks relating to the administration of the network.
- Compliance Officer: this person is in charge of the security audit log and other archive data, the verification of network and server-side security installation. He manages physical access to the PKI system.
- PKI Operator: this person oversees the management of the CA (CA Operator) or RA (RA Operator) functions such as cryptographic functions.
- RA Operator: this person ensures the identification and authentication of prospective Subscribers and Subjects. RA Operator functions may be performed by one or several individual.

Other trusted roles and their duties may be specified in the CPS

## 7.2.2 Number of Persons Required per Task

---

Whenever possible a separate individual shall be identified for each trusted role.

All tasks relating to the CA and RA private key or certificate, such as key generation or key recovery, shall require the presence of the Egypt Trust Certificate Policy Committee.

Sensitive CA tasks shall require dual operator control.

The number or persons required per task shall be specified in the CPS.

## 7.2.3 Identification and Authentication for Each Role

---

All PKI personnel shall have their identity and authorization verified before they are:

- Included in the access list for the PKI site.
- Included in the access list for physical access to the PKI system security zone required.
- Given credentials for the performance of their trusted role.
- Given an account on the PKI system.

## 7.2.4 Roles Requiring Separation of Duties

---

Roles requiring separation of duties shall be specified in the CPS.

## 7.3 Personnel Controls

### 7.3.1 Qualifications, Experience and Clearance Requirements

---

The CA shall ensure that all personnel performing duties with respect to the operation of the PKI system shall:

- Be appointing in writing (trusted roles shall be clearly defined in job files).
- Be long term employees.
- Be bound by contract or statute to the terms and conditions of the position they are to fill.
- Have received comprehensive training with respect to the duties they are to perform.
- Be bound by statute or contract not to disclose sensitive PKI system security-relevant information or Subscriber or Subject information.

---

### **7.3.2 Background Check Procedures**

---

All background checks shall be performed in accordance with Egypt Trust internal procedures and HR Charter.

### **7.3.3 Training Requirements**

---

The CA shall ensure that the personnel performing duties with respect to the operation of a component of the PKI system shall receive comprehensive training in:

- General security.
- Processes and procedures relevant to their trusted role.

As mentioned in Egypt Trust- Training plan

### **7.3.4 Retraining Frequency and Requirements**

---

The requirements of training described in Section 7.3.3 shall be kept current to accommodate changes in the PKI system. Refresher training must be conducted as required.

### **7.3.5 Job Rotation Frequency and Sequence**

---

No stipulation.

### **7.3.6 Sanctions for Unauthorized Actions**

---

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a component of the PKI system, the CA may suspend his or her access to the PKI system and take disciplinary actions.

### **7.3.7 Independent Contractor Requirements**

---

Not applicable.

### **7.3.8 Documentation Supplied to Personnel**

---

The CA must make available to its PKI system personnel the following documentation:

- This Policy and the full CPS.
- Other documentation needed to the personnel to perform their duties.

---

## 7.4 Audit Logging Procedures

---

### 7.4.1 Types of Events Recorded

---

The CA should record in audit log files all events relating to the security of the CA system.

At a minimum, the following type of events shall be recorded:

- All events relating to the security of the systems.
- System start-up and shutdown.
- Application start-up and shutdown.
- Attempts to create, remove, set passwords, or change the system privileges of the users (operators, security, officers ...).
- Generation of keys for PKI components
- Creation and revocation of certificates.
- Changes to PKI component details.
- Attempts to initialize, remove, Subjects.
- Write operations on the CRL.

All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event.

The CA shall also collect and consolidate, either electronically or manually, security information not PKI-system generated, such as:

- Physical access logs.
- System configuration changes and maintenance.
- Personnel changes.
- Records of the destruction of media containing key material, activation data or personal Subscriber or Subject information.

---

### **7.4.2 Frequency of Processing Log**

---

Audit logs shall be reviewed at least once (1) per week and all significant events shall be explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Manual logs shall be recorded the day the event has occurred.

### **7.4.3 Retention Period of Audit Log**

---

Audit logs shall be retained onsite for at least on (1) month after processing thereafter archived in accordance with Section 7.5.2.

### **7.4.4 Protection of Audit Log**

---

The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion.

Manual audit information must be protected from unauthorized viewing, modification, and destruction.

### **7.4.5 Audit Log Backup Procedures**

---

Audit logs and audit summaries must be backed up or copied if on paper form at least once (1) per week.

Audit log backup shall be protected with the same level of protection of audit log as described in Section 7.4.4.

### **7.4.6 Audit Collection system (Internal or External)**

---

Security audit processes shall be invoked at system startup and cease only at system shutdown.

### **7.4.7 Notification to Event-Causing Subject**

---

Where an event is logged by the audit collection system no notice need be given to the individual, organization, device, or application which caused the event.

### **7.4.8 Vulnerability Assessments**

---

The PKI system and operating personnel shall be watchful for attempts to violate the integrity of the PKI system, including the equipment, physical location, and personnel. The security audit data shall be reviewed for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. The continuity of the security audit data shall be checked. A document shall summary the results of the period review of the audit logs.

---

## 7.5 Records Archival

### 7.5.1 Types of Records Archived

---

At a minimum, the following types of record shall be archived:

- PKI system equipment configuration files.
- The CP and CPS.
- Any contractual Agreements to which the CA is bound (Subscriber, Subject, Relying Parties Agreements).
- Audit logs.
- All certificates and CRL as issued or published.
- Subject and Subscriber identification and authentication information.
- Certificate lifecycle information (certificate, revocation, and re-key application information)

### 7.5.2 Retention Period for Archive

---

Archive records shall be kept for a period of 15 years of retention for legal documents.

### 7.5.3 Protection of Archive

---

An entity maintaining an archive of records shall protect the archive so that only the entity's authorized persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time set forth in this Policy.

### 7.5.4 Archive Backup Procedures

---

Archives shall be backed up and stored at the main site, and the integrity of backups shall be verifiable.

### 7.5.5 Requirements for Timestamping of Records

---

Certificates, CRLs, and other revocation database entries shall contain time and date information.

### 7.5.6 Archive Collection System (Internal or External)

---

Archive collection system shall be specified.

---

### **7.5.7 Procedure to Obtain and Verify Archive Information**

---

Only authorized trusted personnel can obtain access to the archive. The integrity of the information shall be verified when it is restored.

### **7.6 Key Changeover**

---

The CA shall not issue certificates that extend beyond the expiration date of its own certificate and public key and CA's certificate validity period shall cover Subject certificate validity period past the last use of its private key.

The CA certificate may be renewed if ITIDA Root CA reconfirms the identity of the CA. Following such reconfirmation, ITIDA Root CA shall either approve or reject the renewal application.

Following an approval of a renewal request, the CA shall conduct a key generation ceremony to generate a new key pair for the CA. The CA shall issue a certificate request that shall be sent to the ITIDA Root CA. The ITIDA Root CA shall sign and issue the CA a new certificate and send it to the CA. The new CA key shall be used to issue new certificate. The old CA key shall continue to be available for CRL signing until all certificates issued under this key have expired.

New CA certificate containing the new CA public key generated during such key generation ceremony shall be made available to Relying Parties.

All Subject certificates shall have a lifetime up to three ((3) ) years,.

### **7.7 Compromise and Disaster Recovery**

---

#### **7.7.1 Incident and Compromise Handling Procedures**

---

If a hacking attempt or other form of potential compromise of a CA becomes known, it shall be investigated to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 7.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

#### **7.7.2 Computing Resources, Software and/or Data Are Corrupted**

---

The CA shall maintain backup copies of system, databases, and private keys to rebuild the PKI system capability in case of software and/or data corruption.

---

### 7.7.3 Entity Private Key Compromise Procedures

---

In case of a CA key compromise, the CA shall immediately notify:

- The Egypt Trust Top Management.
- All PKI components.
- All Subjects.
- All Relying Parties if possible.

The CA shall also:

- Request the ITIDA Root CA to revoke its certificate and publish a new CRL.
- Revoke all issued certificates and issue a new CRL.

After addressing the factors that led to revocation, the CA shall:

- Generate a new CA signing key pair through a key generation ceremony and request the ITIDA Root CA to issue a new certificate for this new public key.
- Make available the new CA certificate containing the new CA public key generated during key generation ceremony
- Issue a new CRL and ensure the new CRL is signed using the new key pair.

The CA may re-issue certificates to all Entities.

### 7.7.4 Business Continuity Capabilities After a Disaster

---

The CA shall establish a disaster recovery plan for business continuity that outline the steps to be taken in the event of a natural or other type of disaster such as the corruption or loss of computing resources, software and/or data.

The repository service shall be restored within four ((4)) hours and standard certificate issuing services shall be restored within forty-eight ((48)) hours.

---

## 7.8 CA or RA Termination

---

In the event of termination of CA services:

- The Egypt Trust Certificate Policy Committee shall notify all contracted parties in writing, according to the contractual conditions.
- The Committee shall notify the ITIDA Root CA.
- The Committee shall notify Subjects that their certificates shall be revoked.
- The CA shall revoke all valid issued certificates and issue a new CRL.
- The ITIDA Root CA shall revoke the CA certificate and issue a new CRL.
- The CA signing key pair or the cryptographic module that holds the keys shall be destroyed.
- The archives shall be retained by the Committee in the manner and for the time described in Section 7.5.

In the event of change in management of the CA's operations, the Committee shall notify all other PKI components, all contracted parties and the ITIDA Root CA.

The notification of termination of CA services shall be communicated three (3) months prior the cease of CA services.

---

## **8 Technical Security Controls**

---

### **8.1 Key Pair Generation and Installation**

---

#### **8.1.1 Key Pair Generation**

---

All CA keys shall be generated by the CA and stored in a trusted hardware cryptographic module that meets at least FIPS PUB 140-1 level 3 requirements and requires multiple secret-shareholders.

The CA private key shall be only used for signing certificates and CRL.

CA keys are generated in a key generation ceremony.

RA keys shall be generated by the CA or RA and stored in a cryptographic container.

Subject keys shall be generated by a trusted hardware cryptographic module and stored in that module that meets at least security evaluation ITSEC E4 or FIPS PUB 140-1 level 2 requirements.

#### **8.1.2 Private Key Delivery to CA component**

---

Private key shall be delivered to CA component in a face-to-face process with the CA/RA. The component shall be identified and authenticate before delivery.

#### **8.1.3 Private Key Delivery to Subject**

---

Private Key shall be delivered to Subject in a face-to-face process with the RA. The Subject shall be identified and authenticated before delivery.

#### **8.1.4 Public Key Delivery to Certificate Issuer**

---

When a public key is transferred to the issuing CA to be certified, it shall be delivered through a mechanism ensuring that the public key has not been altered during transit and that the Subject possesses the private key corresponding to the transferred public key. An acceptable mechanism for public key delivery is a PKCS#10 certificate request package or an equivalent method.

#### **8.1.5 CA Public Key Delivery to Relying Parties**

---

The CA public key shall be delivered to Relying Party using an X.509 certificate. An acceptable mechanism for public key delivery is a PKCS#7 file with or not the complete certificate path.

---

The CA public key may be delivered directly on Subject tokens or may be download from a repository (website or directory).

### **8.1.6 Key Sizes**

---

The CA shall use a 4096 bits RSA key pair.

The RA shall use a 4096 bits RSA key pair.

Subjects shall use a 2048 bits RSA key pair.

### **8.1.7 Public Key Parameters Generation and Quality Checking**

---

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto algorithm in which the parameters are to be used.

The key pairs of the CA and RA have been created using at least FIPS PUB 140-1 level 3 certified cryptographic modules.

The key pairs of the Subjects have been created using at least ITSEC E4 or FIPS PUB 140-1 level 2 cryptographic modules.

### **8.1.8 Key Usage Purposes (as per X.509 V3 Key Usage Field)**

---

The signing keys of the CA are the only keys permitted for signing certificates and CRLs and have keyCertSign and CRLSign key usage bits set.

Subject keys may be used for authentication, non-repudiation and digital signature and have Digital Signature and Non-Repudiation key usage bits set.

## **8.2 Private Key Protection and Cryptographic Module Engineering Controls**

---

### **8.2.1 Cryptographic Module Standards and Controls**

---

The cryptographic module used for CA and RA meets at least FIPS PUB 140-1 level 3 requirements.

The cryptographic module used for Subjects meets at least ITSEC E4 or FIPS PUB 140-1 level 2 and may be a smartcard or an USB token.

All cryptographic modules shall be operated such that the private keys shall never be output in plain text.

Cryptographic modules shall check the quality of key pairs they generate.

---

### 8.2.2 Private Key (3 out of 5) Multi-Person Control

---

There shall be multiple person control for CA key generation operations. The Egypt Trust Certificate Policy Committee shall be present. Data used for key generation shall be shared by five (5) secret holders.

The CA keys may only be recovered under three (3) person control shareholders.

### 8.2.3 Private Key Escrow

---

No private keys shall be hold in escrow.

### 8.2.4 Private Key Backup

---

Private keys of the CA shall be backed up in an encrypted form that requires the use of three (3) key shares out of five (5). This backup shall be stored securely (e.g., in a safe) in accordance with Section 7.1.6 and 7.1.8.

### 8.2.5 Private Key Archival

---

See Section 8.2.4.

### 8.2.6 Private Key Transfer into or Form a Cryptographic Module

---

The CA private keys shall be transferred into a cryptographic module for the following reasons:

- Test of the disaster recovery plan.
- Change of the cryptographic module.
- Change of the CA software.

If a private key shall be transported from one cryptographic module to another, the private key shall be encrypted during transport and require the use of three (3) key shares out of five (5). Private keys shall never exist in plaintext from outside the cryptographic module boundary.

### 8.2.7 Private Key Storage on Cryptographic Module

---

The CA private keys stored in the cryptographic module shall be protected from unauthorized access and use in accordance with the FIPS PUB 140-1 level 3 requirements applicable for the module.

The Subject private keys stored in the cryptographic module shall be protected from unauthorized access and use in accordance with the ITSEC E4 or FIPS PUB 140-1 level 2 requirements applicable for the module.

---

### 8.2.8 Method of Activating Private Key

---

CA private key shall be activated in accordance with the internal processes of the cryptographic module on which keys are generated.

PIN shall be used to activate the Subject private key.

### 8.2.9 Method of Deactivating Private Key

---

CA private key shall be deactivated when the cryptographic module power is cut or when key is erased from the cryptographic module.

Subject private key shall be deactivated after a pre-set period of inactivity or when the smartcard is removed from the smartcard reader or when the token is removed from the computer.

### 8.2.10 Method of Destroying Private Key

---

On termination of use of the CA private key, all backup of the private key shall be destroyed. The private key inside the cryptographic module shall be removed.

On termination of CA services, the cryptographic module shall be re-initialized, and backup of the private key and shares shall be destroyed.

Subject private key shall be destroyed when the key is erased from the smartcard or token or when the chip of the smartcard or the token is cut in two.

### 8.2.11 Cryptographic Module Rating

---

Requirements for cryptographic modules are as stated above in Section 8.2.1.

## 8.3 Other Aspects of Key Pair Management

---

### 8.3.1 Public Key Archival

---

Public keys are archived as part of the certificate archival.

### 8.3.2 Certificate Operational Periods and Key Pair Usage Periods

---

Key usage periods for keying material shall be as follow:

- The CA key pairs are valid 5 years.
- Subject key pairs are valid up to (3) years.

---

## 8.4 Activation Data

---

### 8.4.1 Activation Data Generation and Installation

---

PIN shall be used to protect access to Subject private keys. These PIN are called activation data. Subject activation data shall use random numbers and/or characters and shall be provided to the Subject in a sealed envelope.

### 8.4.2 Activation Data Protection

---

Activation data for cryptographic modules should be memorized, not written down. If written down, it shall be stored securely (e.g., in a safe) in accordance with Section 7.1.6.

### 8.4.3 Other Aspects of Activation Data

---

PIN shall be at minimum six (6) digits and/or characters. PIN can be modified at any time.

## 8.5 Computer Security Controls

---

### 8.5.1 Specific Computer Security Technical Requirements

---

PKI system equipment shall use operating systems that require authenticated logins, provide discretionary access control and a security audit control.

No stipulation for Subject computer.

### 8.5.2 Computer Security Rating

---

No stipulation.

## 8.6 Life Cycle Technical Controls

---

### 8.6.1 System Development Controls

---

The PKI system shall use software that has been designed and developed by a formal methodology.

### 8.6.2 Security Management Controls

---

The configuration of the PKI system as well as any modifications and upgrades shall be documented and controlled. There shall be a method of detecting unauthorized modification to the PKI software or configuration.

### 8.6.3 Life Cycle Security Controls

No stipulation.

### 8.7 Network Security Controls

The CA and RA server shall be protected from attack through any open or general-purpose network with which it is connected. Such protection must be provided through the installation of a device configured to allow only the protocols and commands required for the operation of the CA and RA.

## 9 Certificate, CRL and OCSP Profiles

### 9.1 Certificate Profile

Field	Content	Critical	
Version	“2” (for X.509 version 3)	√	
serial Number	Unique value within the CA	√	
Signature	Algorithm used to sign the certificate algorithm                      Sha256WithRSAEncryption	√	
Issuer	CA’s DN	√	
validity	Activation and expiry date for certificate notBefore                      Activation date (UTCTime) notAfter                        Expiry date (UTCTime)	√	
Subject	Subject’s DN	√	
subjectPublicKeyInfo	Subject’s public key algorithm                      RSAEncryption subjectPublicKey              Subject’s public key	√	
Extension	AuthorityKeyIdentifier	Key identifier of the issuing CA’s public key	√

	keyIdentifier	Derived from 160-bit SHA-2 of the issuing CA's public key	
SubjectKeyIdentifier	Key identifier of the subject's public key		√
	keyIdentifier	Derived from 160-bit SHA-2 of the Subject's public key	
KeyUsage	Authorized key usages		√
	digitalSignature	"1"	
	nonRepudation	"1"	
CertificatePolicies	Certificate policies OID and URL		√
	policyIdentifier	Certificate Policy OID	
	CPSuri	URL where CPS can be found	
	userNotice	Policy description including usage limits	
BasicConstraints	End-entity certificate		no
	cA	"FALSE" (End Entity)	
	pathLenConstraint	"0" (None)	
extKeyUsage	Extended authorized key usages		no
	email protection,	1.3.6.1.5.5.7.3.4,	
	client	1.3.6.1.5.5.7.3.2,	
	authentication,	1.3.6.1.5.5.7.3.3	
	code signing		
CRLDistributionPoints	URL to CRL distribution point (LDAP and/or HTTP)		no
	distributionPoint	URL to CRL	
QcStatement	Qualified certificate		no
	QcStatement	"1.3.6.1.5.5.7.11.2"	
	QcCompliance	"0.4.0.1862.1.1"	
	QcLimitValue	"0.4.0.1862.1.2" and limit value and Egyptian currency	
signatureAlgorithm	Sha256 With RSA Encryption		√
signatureValue			no

---

### 9.1.1 Version Number(s)

---

Certificates shall be X.509 Version 3 certificates, in accordance with the RFC3280 PKIX Certificate and CRL Profile.

Relying Party software shall support all the base (non-extension) X.509 fields:

<b>Version</b>	Version of X.509 certificate, version 3
<b>serial Number</b>	Unique serial number for certificate
<b>Signature</b>	CA signature to authenticate certificate
<b>Issuer</b>	DN of CA
<b>Validity</b>	Activation and expiry date for certificate
<b>Subject</b>	Subject's Distinguished Name
<b>Subject Public Key identifier</b>	Composed of 160-bit SHA-1

As well as the certificate extensions defined in Section 9.1.2.

### 9.1.2 Certificate Extensions

---

Certificate extensions used are:

<b>Authority Key Identifier</b>	Contains the key identifier of the issuing CA's public key (SHA2)
<b>Subject Key Identifier</b>	Contains the key identifier of the Subject's public key (SHA2)
<b>Key Usage</b>	Authorized key usages
<b>Certificate Policies</b>	Certificate policies OID and URL
<b>Subject Alt Name</b>	Subject's e-mail address
<b>Basic Constraints</b>	Specify the certificate is an end-entity certificate
<b>Extended Key Usage</b>	Extended authorized key usages
<b>CRL Distribution Point</b>	URL to CRL distribution point (LDAP and/or HTTP)

The Key Usage field shall be set as critical. Other fields shall be set as non-critical.

---

### 9.1.3 Algorithm Object Identifiers

---

The following OID algorithm is used:

**SHA256 With RSA Encryption**    SHA-2    1.2.84.113549.1.1.11

### 9.1.4 Name Forms

---

Every Distinguished Name (DN) shall be in the form of an X.501 printable String.

### 9.1.5 Name Constraints

---

Subject and Issuer DNs shall comply with RFC 3739 and RFC 3280 standards and be present in all certificates.

### 9.1.6 Certificate Policy Object Identifier

---

The CA shall ensure that the Policy OID is contained within the certificates it issues.

The OID for Egypt Trust General Signature Certificates policy identifier (1.3.6.1.4.1.33399.1.2)

### 9.1.7 Usage of Policy Constraints Extension

---

No stipulation.

### 9.1.8 Policy Qualifiers Syntax and Semantics

---

Certificates shall include the policy Qualifier extension with the URL of its CPS and the user Notice extension.

### 9.1.9 Processing Semantics for the Critical Certificate Policies Extension

---

Critical extensions shall be interpreted as defined in RFC 3280.



---

## 9.2.2 CRL and CRL Entry Extensions

---

All Relying Party software shall correctly process all CRL extensions identified in the RFC 3280 PKIX Certificate and CRL profile.

CRL extensions used are:

<b>AuthorityKeyIdentifier</b>	Contains the key identifier of the issuing CA's public key (SHA1)
<b>CRLNumber</b>	Contains a number incremented by the CA each time the CRL is modified
<b>reasonCode</b>	Revocation reason code

---

## 9.3 OCSP Profile

---

### 9.3.1 Version Number(s)

---

Not applicable.

### 9.3.2 OCSP Extensions

---

Not applicable.

## **10 Compliance Audit and Other Assessments**

### **10.1 Frequency and Circumstances of Assessment**

A compliance audit shall be completed prior to begin PKI service to demonstrate compliance with the process and procedural requirements of this Policy and the ITIDA requirements. Annual internal audits shall be conducted on the same basis.

The PA has the right to require an internal or external compliance audit of the PKI system at any time and shall do so immediately on discovering any breach of security or processes, or suspicion of such a breach.

### **10.2 Identify/Qualifications of Assessor**

The assessor shall demonstrate competence in the field of audit compliance PKI and cryptographic technologies.

### **10.3 Assessor's Relationship to Assessed Entity**

For external audit, the compliance assessor shall be independent and have no connections with the audited parties. Such assessor shall not have a conflict of interest that hinders their ability to perform auditing services.

### **10.4 Topics Covered by Assessment**

The purpose of a compliance audit shall be to verify that the audited party has in place, a system to assure the quality of the services that it provides, and that it complies with all of the requirements of this CP and its CPS. All aspects of the audited party's operation related to this Policy shall be subject to compliance audit inspections.

### **10.5 Actions Taken as a Result of Deficiency**

When the compliance auditor finds a discrepancy between the PKI's operation and the stipulations of its CPS, the auditor shall note the discrepancy and notify the parties identified in Section 10.6 of the discrepancy. Then, the audited party or the auditor will propose a remedy.

Any decision regarding which actions shall be taken shall be based on the severity of the discrepancy.

---

## 10.6 Communications of Results

---

The compliance auditor shall report the results of a compliance audit to the Egypt Trust Certificate Committee. The Committee is responsible for reporting the results of the compliance audit to the PKI operators. The implementation of remedies shall be communicated to the Committee.

---

## **11 Other Business and Legal Matters**

---

### **11.1 Fees**

---

#### **11.1.1 Certificate Issuance or Renewal Fees**

---

The CA is entitled to charge Subscribers and/or Subjects for the issuance, management, and renewal of certificates.

Communication of fees is done through Subscriber Agreement and/or Subject Agreement.

#### **11.1.2 Certificate Access Fees**

---

Egypt Trust shall not charge any certificate access fees on Subscribers, Subjects and Relying Parties.

#### **11.1.3 Revocation or Status Information Access Fees**

---

Egypt Trust shall not charge any fees for accessing the CRL.

#### **11.1.4 Fees for Other Services**

---

Egypt Trust shall not charge any fees for access to this CPS or other related information.

#### **11.1.5 Refund Policy**

---

The CA may at its discretion provide a full or partial refund of certificate fees in the event it is unable to meet his obligation as described in the CPS.

## **11.2 Financial Responsibility**

---

### **11.2.1 Insurance Coverage**

---

No stipulation.

### **11.2.2 Other Assets**

---

Egypt Trust shall have sufficient financial resources to maintain their operations and perform their duties.

---

### 11.2.3 Insurance or Warranty Coverage for End-entities

## 11.3 Egypt Trust provides warranty for manufacturing deficits with vendors agreements. Confidentiality of Business Information

---

### 11.3.1 Scope of Confidential Information

---

All information provided by Subscribers and Subjects shall be kept confidential and private except that which are bound into the certificate.

The following information is also considered confidential:

- Private keys of PKI components and Subjects.
- Activation data of PKI components and Subjects.
- PKI components' audit logs.

No one shall have access to a private key or activation data but the owner.

### 11.3.2 Information Not Within the Scope of Confidential Information

---

Information which are not considered confidential are:

- Certificates.
- CRL.

### 11.3.3 Responsibility to Protect Confidentiality Information

---

All reasonable effort shall be made to protect confidential information from compromise or disclosure.

## 11.4 Privacy of Personal Information

---

### 11.4.1 Privacy Plan

---

All Subscribers and Subjects information is sensitive and confidential and is protected at the appropriate level. Under no circumstance is personal information to be released, unless there is a case concerning misuse.

---

#### **11.4.2 Information Treated as Private**

---

All information about Subscribers and Subjects that it is not publicly available through the content of the issued certificate or CRL is treated as private.

---

#### **11.4.3 Information Not Deemed Private**

---

All information made public in a certificate is deemed not private.

---

#### **11.4.4 Responsibility to Protect Private Information**

---

All reasonable effort shall be made to protect private information from compromise and disclosure to third parties.

---

#### **11.4.5 Notice and Consent to Use Private Information**

---

Private information shall not be used without the consent of the party to whom that information applies.

---

#### **11.4.6 Disclosure Pursuant to Judicial or Administrative Process**

---

Confidential/private information shall be disclosed in response to judicial, administrative, or other legal process.

---

#### **11.4.7 Other Information Disclosure Circumstances**

---

No stipulation.

---

### **11.5 Intellectual Property Rights**

---

Egypt Trust shall retain ownership and intellectual property rights for this CPS, and any public key certificates and private keys that it issues.

---

### **11.6 Representations and Warranties**

---

---

#### **11.6.1 CA Representations and Warranties**

---

The CA shall conform to the stipulations of this Policy, including the following obligations:

- Comply with this CPS.
- Protect the integrity and confidentiality of its private keys.
- Use its public and private keys only for the purpose for which they were issued and with the authorized mechanisms, signature of certificates and CRL.

- Comply with agreements or contracts with PKI components, Subscribers, Subjects or Relying Parties.
- Accept the compliance audit results and consequences and take actions to solve discrepancies underlying in the compliance audit report.
- Provide documentation for internal management procedures.
- Provide infrastructure and certification services, including personnel for the secure and quality operation of public certificate services.
- Provide in an online repository its certificate and the ITIDA Root CA certificate.
- Provide in an online repository this CPS, Subscriber Agreements, Subject agreements, and Relying Party Agreements.
- Publish in an online repository the issued certificates and CRL.
- Ensure that information included in a certificate has been verified, in accordance with this CPS, whenever a certificate is issued.
- Upon receipt of a certificate request or revocation request, verify the RA issuing the request is an authorized RA.
- Provide prompt notice in case of compromise of its own private keys.
- Store and manage its private keys through a hardware cryptographic module.
- Archive securely its private keys.

Subscriber and Subject Agreements may include additional representations and warranties.

### **11.6.2 RA/LRA Representations and Warranties**

RA shall conform to the stipulations of this Document, including the following obligations:

- Protect the integrity and confidentiality of its private keys.
- Use its public and private keys only for the purpose for which they were issued and with the authorized mechanisms, authentication with PKI component and certificate and revocation requests signature.

RA/LRA shall conform to the stipulations of this Policy, including the following obligations:

- Comply with this CPS.
- Comply with agreements or contracts with PKI components, Subscribers, Subjects or Relying Parties.
- Provide documentation for internal management procedures.
- Provide infrastructure and certification services, including personnel for the secure and quality operation of public certificate services.
- Receive, verify and relay certification requests and revocation requests.
- Protect the integrity and confidentiality of all personal and identifying information collected during registration processes.
- Verify the authenticity of identifying information provided by Subscribers and Subjects.
- Generate Subject private keys in a hardware cryptographic module such as smartcards, which should be protected by a PIN code or passphrase.
- Provide Subject activation data and public/private keys to Subject securely and confidentially.

Subscriber and Subject Agreements may include additional representations and warranties.

### **11.6.3 Subject Representations and Warranties**

---

Subjects shall conform to the stipulations of this Policy, including the following obligations:

- Comply with this CPS.
- Protect the integrity and confidentiality of its private keys and activation data.
- Use its public and private keys only for the purpose for which they were issued and with the authorized mechanisms.
- Accept the compliance audit results and consequences.
- Notify the RA in case of compromise of its own private keys.
- Ensure the accuracy of information provide to the RA in certificate or revocation requests.
- Notify the RA in case of change of information in the certificate.

Subject Agreements may include additional representations and warranties.

---

#### **11.6.4 Subscriber Representations and Warranties**

---

Subscriber shall conform to the stipulations of this Policy, including the following obligations:

- Comply with this CPS.
- Ensure the accuracy of information provide to the RA.
- Notify the RA in case of the Subject is no more an employee of the organization for certificates issued within organization Subscriber.

Subscriber Agreements may include additional representations and warranties.

---

#### **11.6.5 Relying Party Representations and Warranties**

---

Relying parties shall conform to the stipulations of this Policy, including the following obligations:

- Use the certificate for the purpose for which it was issued, as indicated in key usage certificate information.
- Check each certificate for validity, using CRL, prior to reliance.
- Establish trust in the CA which issued a certificate by verifying the certificate path.
- Use the public key extracted from the certificate only for verifying a digital signature.

Relying Party Agreements may include additional representations and warranties.

---

#### **11.7 Disclaimers of Warranties**

---

Warranty Disclaimer shall be specified in the relevant Subscriber Agreements, Subject Agreements and Relying Party Agreements.

---

#### **11.8 Limitations of Liability**

---

Unless otherwise agreed in a Subscriber Agreement, Subject Agreement, Relying Customer Agreement, or similar contract, and except as mandated by law Egypt Trust accepts no liability for consequential damages relating to a failure of the services provided under this CPS, or for matters other than the correct identification of a Subject in a digital certificate.

---

## **11.9 Term and Termination**

---

### **11.9.1 Term**

---

This CPS shall remain in effect until either a new CPS is approved by the Egypt Trust Certificate Policy Committee and published in the repository, or the PKI is terminated.

### **11.9.2 Termination**

---

This CPS shall survive any termination of the CA. The requirements of this CPS shall remain in effect through the end of the archive period.

### **11.9.3 Effect of Termination and Survival**

---

The responsibilities for protecting confidential and private information and Egypt Trust intellectual property rights shall survive the termination of this CPS.

## **11.10 Individual Notices and Communications with Participants**

---

If not specified by agreements between the parties, participants shall use adequate methods to communicate with each other in accordance with criticality and subject matter of the communication.

## **11.11 Amendments**

---

### **11.11.1 Procedure for Amendment**

---

Errors, updates, or suggested changes to this CPS shall be communicated to the contact in Section 3.5.2. Such communication shall include a description of the change, a change justification and contact information for the person requesting the change.

.

When the Committee reviews this CPS, the reviewed CPS shall be published on a web site and sent to the CA. The CA shall notify its PKI components, Subscribers and Subjects.

### **11.11.2 Notification Mechanism and Period**

---

The Egypt Trust Certificate Policy Committee reserve the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and change to contact information. The Egypt Trust Certificate Policy Committee shall designate whether amendments are material or non-material.

The Egypt Trust Certificate Policy Committee shall notify the CA of material amendments to this CPS proposed by the PA. The notification shall contain a statement of proposed changes, the comment period, and the proposed effective date of change. The Egypt Trust Certificate Policy Committee may request the CA to notify its PKI components, Subscribers and Subjects. Proposed amendments shall be published on a web site.

Written and signed comments on proposed changes shall be directed to the Committee. Decisions with respect to the proposed changes are at the sole discretion of the Committee.

The Committee shall accept, with modification, or reject the proposed change after completion of the review period. The Committee will determine the period for final change notice.

### **11.12 Dispute Resolution Provisions**

---

A dispute should be resolved by negotiation by the Committee if possible. A dispute not settled by negotiation should be resolved by Egyptian domestic courts.

### **11.13 Governing Law**

---

The laws of Egypt shall govern this CPS.

### **11.14 Compliance with Applicable Law**

---

Egypt Trust CA operates under the requirements of Egyptian Law Number 15 of 2004, Regulating Electronic Signatures and the Ministry of Communications and Information Technology Decree Number 109 for 2005, Executive Regulations of the Digital Signature Law, regulated by the Information Technology Industry Development Authority (ITIDA).

### **11.15 Miscellaneous Provisions**

---

#### **11.15.1 Entire Agreement**

---

No stipulation.

### **11.15.2 Severability**

---

If a section of this CPS is determined incorrect or invalid by a court of law or other tribunal having authority, the other sections of this CPS shall remain valid until the document is updated.

### **11.15.3 Enforcement (Attorney's Fees and Waiver of Rights)**

---

No stipulation.

### **11.15.4 Force Majeure**

---

No stipulation.

### **11.16 Other Provisions**

---

No stipulation.