Certificate Practice Statement (CPS)

Version 1.1

2021/03/04

Prepared by:

Information Technology Industry Development Agency

ITIDA

Contents

List of Figures

List of Tables

1 Introduction

1.1 Overview

In accordance with the Egyptian E-Signature Law and its Executive Regulation, ITIDA operates the Egyptian Root-CA, which issues certificates for certification service providers issuing certificates in Egypt. The Egyptian Root-CA serves as a trust anchor for digital certificates issued in Egypt.

In order to fulfil this function, the certification services provided by the Egyptian Root-CA must be trusted by the public. The present document aims at supporting this trust by disclosing the practises applied by the Root-CA.

1.2 Document name and identification

Egyptian RootCA Certification Practice Statement version 0.4
http://rootca.itida.gov.eg/home_files/CPS.pdf
http://rootca.gov.eg/CPS.pdf

1.3 PKI participants

The certification hierarchy and participants of the Public Key Infrastructure (PKI) defined by the Egyptian Root-CA are described in the Certificate Policy of the Root-CA.

1.4 Certificate usage and applicability

The applicability and permitted usages of the certificates issued by the Root-CA are defined by the Certificate Policy of the Root-CA.

1.5 Policy administration

This document is administered by ITIDA. This includes the following responsibilities:

- Creation and updating of the document
- Definition of version number
- Registration of Object Identifier for the document
- Publication of the document
- Determination of conformance of the Certificate Practice Statement

In case of any question regarding this document contact ITIDA or send an e-mail to mail: Info.dsss@ITIDA.gov.eg

Phone: 0235345277

1.6 Definitions and acronyms

ASN.1

Standard for data structure syntax, used for X.509 certificates and CRLs

BASE64

Method for encoding arbitrary 8 bit binary data with ASCII characters

Certificate

Also called *Digital Certificate*. In this document these terms refer to public key certificates, data structure containing the certificate holder's name and public key, as well as supplementing information (e.g. a serial number, expiration dates, admissible key usages, links to status information services) and the digital signature of the issuing certification authority.

Certificate Extension

Data fields introduced by version 3 of the X.509 certificate format, in which supplemental information can be included in a certificate. An extension must be marked as "critical", meaning that applications unable to interpret it must reject the certificate, or "not critical".

Certificate Modification

The act of applying for a new certificate replacing an existing certificate with different public key and other modified contents (beyond validity and serial number).

Certificate Policy (CP)

A public document describing the rules governing the use of a public key certificate in a particular environment

Certificate Re-key

The act of applying for a new certificate replacing an existing certificate with different public key but otherwise unchanged contents (except validity and serial number).

Certificate Renewal

The act of applying for a new certificate replacing an existing certificate with the same public key and unchanged contents (except validity and serial number).

Certification Request

A data structure in which a subscriber supplies its public key, name and other information to be included in a certificate to the certification authority

Certificate Revocation

The process by which the effectiveness of a certificate is terminated before the envisaged end of its validity

Certificate Revocation List (CRL)

A list containing revoked certificates and supplementing information

Certificate Suspension

A preliminary (i.e. reversible) revocation of a certificate

Certification Authority (CA)

Entity in a PKI which signs digital certificates

Certification Hierarchy

A tree-like structure consisting of the issuers and subjects in a PKI as nodes, and the certification relationships as edges. An entity is subordinated to another entity if it has received a certificate from the latter one.

Certification Practice Statement (CPS)

A public document describing the practices a CA employs in issuing and managing certificates

Certification Service Provider (CSP)

An entity that issues certificates or provides other certification services for electronic signatures/Seal. In the context of the present document a CSP is an entity who issues certificates in Egypt.

Certification Services

Certification services for electronic signatures are services supporting the issuance and management of certificates for electronic signature/seal. These services can comprise:

- Certificate generation services, i.e. CAs
- Registration services, i.e. RAs
- Revocation management services
- Certificate dissemination services
- Revocation status information services
- Signing device preparation services
- Timestamp services

Details are given in ETSI EN 319 411.

CMS	Cryptographic Message Syntax, standard based on PKCS#7 specified RFC 5652 and RFC 3370 and their updates RFC 5083, RFC 4853 RFC 3370 and RFC 5754 consequently for data structures containing cryptographic information, e.g. signed or encrypted data, or certificates. CMS is used to encode TSP requests and responses.
Common Criteria (CC)	Is an international standard for evaluating the security functions of IT products. It defines a framework for the oversight of evaluations, syntax for specifying the security requirements to be met and a methodology for evaluating those requirements
commonName (CN)	X.501 name attribute
country (C)	X.501 name attribute
CRL	Certificate Revocation List
CRL issuer	Entity which signs CRLs
Cross certificates	A pair of certificates mutually issued between two CAs or two key pairs of the same CA in order to establish certification paths between these CA's or key pairs, respectively.
Distinguished Encoding Rules (DER)	Method for encoding data objects, in particular objects with ASN.1 syntax
Directory Information Tree (DIT)	The hierarchical tree-like structure of a directory
Distinguished Name (Dname)	A unique, unambiguous name constructed from name attributes and corresponding values according to the standard X.501
DNS	Domain Name System
DSA	Digital Signature Algorithm, digital signature algorithm, defined in FIPS 186-4
EAL	Evaluation Assurance Level - standardised level of scrutiny in which an evaluation according to Common Criteria is conducted
ECDSA	Elliptic Curve Digital Signature Algorithm, digital signature algorithm, defined in ANSI X9.62

Electronic Signature

Electronic data logically associated with other electronic data which serves as a method for authentication.

What is on an electronically written message in the form of letters, digits, codes, signals or others and has a unique identity that identifies the signer and uniquely distinguishes him/her from others

End Entity

An entity in a PKI that does not issue certificates.

Hash Function

An algorithm that converts a message of any length into a short and unique fixed-length string of digits known as "message digest". In the context of PKI a hash function must be "collision resistant", that is it must be practically infeasible to find two messages having the same hash value. Collision resistance implies that that the hash function is one-way, i.e. that it is infeasible to determine a pre-image from a hash value

Indirect CRL

CRL which is not signed by the CA who issued the corresponding certificates, but by a dedicates CRL issuer

Issuer

The CA which has signed the certificate

ITIDA

Information Technology Industry Development Agency

ITSEC

Information Technology Security Evaluation Criteria, standard for the evaluation of security of systems and applications

Key Rollover

The process of a CA switching from one certificate or CRL signing key to another one

LDAP

Lightweight Directory Access Protocol, an internet protocol for accessing X.500 directories.

Object Identifier (OID)

Numerical identifier used to refer to a unique object. An OID can be registered at a national assignment authority which ensures its uniqueness on an international level.

OCSP

Online Certificate Status Protocol, standard specified in RFC 6960 for the interactive retrieval of certificate status information

organizationalUnitName (OU)	X.501 name attribute used in X.500 directories and X.509 certificates
organizationName (O)	X.501 name attribute used in X.500 directories and X.509 certificates
Personal Identification Number (PIN)	A sequence of digits used to verify the identity of the holder of a token (e.g. a smart card)
PIN letter	Letter in which a PIN is printed in a way that makes eavesdropping difficult and detectable
PKCS	A set of Public Key Cryptography Standards issued by RSA Data Security
PKCS#1	A standard for public key encryption and digital signatures based on RSA
PKCS#10	A standard for self-signed certificate requests
PKCS#5	A standard for password based cryptography. Among others, PKCS#5 specifies methods for key derivation from passwords, which can also be applied to compute secure hashes of passwords.
PKCS#7	A standard for the format of files which are cryptographically protected and/or contain certificates. PKCS#7 has been the basis for CMS.
Public Key Infrastructure (PKI)	A set of policies, processes, and technologies used to verify, enrol and certify users based on certificates
RA	Registration Authority
Registration	The process for receiving and processing applications for keys and certificates
Registration Authority (RA)	Entity in a PKI which performs registration and identification of subscribers and subjects

Root CA	The highest-level entity in a certification hierarchy. In the present document, the spelling "Root-CA" refers to the Egyptian root CA operated by ITIDA
RSA	Cryptosystem developed by Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman
SHA-224, SHA-256, SHA-384, SHA-512	Secure Hash Algorithm 2 with 224/256/384/512 bit output. Defined in FIPS-180-4.
Subject	Entity for who a certificate is issued
Subscriber	Entity in a PKI who applies for a certificate for itself or another entity (the subject)
Time Stamp	It is a sequence of characters or encoded information identifying when a certain event occurred, usually giving date and time of day, sometimes accurate to a small fraction of a second
Trust Anchor	It is an authoritative entity for which trust is assumed and not derived The certificates of a root CA are supposed to be used as trust anchors.
TSP	Time Stamp Protocol, protocol specified in RFC 3161 and its update RFC 5816, that allows requesting digitally signed time stamps on arbitrary data from a server over the internet.
URI	Uniform Resource Identifier, string of characters used to identify a resource on the internet. A URI is either a locator (URL) or a name (URN)
VPN	Virtual Private Network
X.500	Standard for hierarchically structured directories.
X.501	Standard defining name attributes for X.500 directory
X.509	Standard for PKI mechanisms and data structures, in particular for public key certificates (X.509v3) and CRLs (X.509v2)

E-Seal	The Electronic Seal Certificate is a certificate for legal person as a means to automated electronic administrative proceedings of the Public Administrations. Legal person can be an organization or a department identified in association with an organization. Trusted Certificate Service Providers TCSP issues the Electronic Seal Certificate, this certificate issued for advanced electronic seals. Subscribers of CSP are those organizations that contract with CSP for the issuance of Qualified Certificate for Electronic Seals in their name.

2 Publication and repository responsibilities

2.1 Repositories

ITIDA publishes information about the Root-CA on its web service and web site:

http://www.rootca.gov.eg

http://www.rootca.itida.gov.eg

Furthermore, ITIDA provides an X.500 directory for certificates and certificate revocation lists (CRLs).

ldap://ldap.rootca.gov.eg/cn=Egypt_RootCA_G1,ou=RootCA,o=ITIDA,c=EG?CertificateRevocationList;binary?base

The Egyptian Root CA repositories is accessible via http at:

http://rootca.gov.eg

Root CA Certificate:

http://rootca.gov.eg/EgyptRootCAG1.cer

http://rootca.itida.gov.eg/home_files/**EgyptRootCAG1.cer**

CRL:

http://www.rootca.gov.eg/CRL-G1.crl

http://rootca.itida.gov.eg/CRL-G1.crl

CP:

http://www.rootca.gov.eg/CP.pdf

http://rootca.itida.gov.eg/home_files/CP.pdf

CPS:

http://www.rootca.gov.eg/CPS.pdf

http://rootca.itida.gov.eg/home_files/CPS.pdf

Details of the X.500 directory are given in section □.

2.2 Publication of certification information

This CPS, the related Egyptian Root-CA Certificate Policy (CP), the self-signed certificates of the Root-CA certification authorities and further information related to the Root-CA are published at ITIDAs web site.

http://www.rootca.gov.eg

http://rootca.itida.gov.eg/

The self-signed certificates of the Root-CA certification authorities are published in the X.500 directory and on ITIDA's web site. In addition, the fingerprints of the self-signed certificates are published in the national gazette and on the web site of the Root-CA.

The certificates and CRLs issued by the Egyptian Root-CA), including the self-signed certificates of the Root-CA certification authorities are published in the X.500 directory of the Root-CA.

Status information of the certificates issued by the Root-CA is published in CRLs (see sections 0, 4.9.8 and 4.10.1.1) and through OCSP (see sections 4.9.9 and 4.10.1.2).

2.3 Time or frequency of publication

The latest versions of the Egyptian Root-CA's Certification Practice Statement (CPS) and Certificate Policy (CP) are published promptly on ITIDA's web site. Also all earlier versions are kept available on this web site.

Certificates and their status information (via CRL or OCSP) are published immediately after acceptance of the certificate (see section 4.4.1) and are maintained in the directories until 30 years after the certificate's expiry.

The CRL issuance frequency is regulated in point of this CPS.

2.4 Access controls to directory

The information published is accessible to everyone anonymously and without any fees.

Access controls are used to restrict the ability to write or to modify published information to authorized personnel only.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

All certificates issued by the Egyptian Root-CA contain X.501 **Distinguished Names** (DN) in the issuer and subject fields. These DN always contain the following X.501 name attributes:

- Country (C)
- Organization (O)
- Common Name (CN)

Optionally, in certificates issued to CSPs the subject DN can contain the following additional X.501 name attributes:

- Organizational unit (OU)
- Serial Number
- Domain Component
- Street Address
- Locality Name
- State or Province Name

In addition, certificates issued to CSPs can optionally contain a **Subject Alternative Name**, specifying one or several of the following name attributes:

- E-mail address
- Internet Domain Address (DNS name)
- X.500 Name
- Uniform Resource Identifier, i. e. a URL or URN
- IP address

3.1.2 Need for names to be meaningful

ITIDA verifies during the registration process, that the subject name requested by the CSP is meaningful and unambiguous. In particular, ITIDA verifies that the identity of the CSP and the name and type of service for which the certificate has been issued can be uniquely determined from the name given in the certificate.

3.1.3 Anonymity or pseudonymity of subscribers

The names in the certificate must explicitly specify the CSP. Thus, anonymity or pseudonymity is not supported.

3.1.4 Uniqueness of names

See section 3.1.2.

3.1.5 Recognition, authentication, and role of trademarks

Subscribing CSPs must ensure that they possess all necessary rights to use the names requested. ITIDA does not take any responsibility for damages or claims from their subscribers or their parties resulting from unauthorised use of trademarks.

3.2 Initial verification of identity and authorisation

3.2.1 Method to prove possession of the private key

The Egyptian Root-CA offers the following method to the CSPs:

- A CSP can apply for a certificate from the Root-CA by providing a self-signed PKCS#10 Certificate Signing Request (CSR). Only public key algorithms, signature algorithms and Profile (Section 7.2) supported by the Root-CA can be accepted. The Root-CA will only issue certificates for CSRs with valid digital signatures. However, the digital signature of the PKCS#10 request is only verified by the Root-CA. The following algorithms are supported:
    - RSA according to PKCS#1 version 1.5, with SHA-224, SHA-256, SHA-384 or SHA-512.

The Root-CA will not issue any certificate if the the digital signature of the PKCS#10 request cannot be verified.

3.2.2 Verification of identity and authorisation of organisations

In the context of the supervision of certification services, ITIDA verifies the identity of the CSP on the basis of official legal documents. Furthermore, ITIDA verifies that the CSP meets the requirements defined in section 4.1.1.

3.2.3 Verification of identity and authorisation of individuals

The persons applying for certificates (the applicants) are verified on the basis of their national ID cards in their physical presence at the premises of the Root-CA.. The verification of the ID card is based on a comparison of the photograph and the hand-written signature, and is conducted by at least two operators of the Root-CA.

The authorization of the applicants to request a certificate on behalf of the CSP must be proved by a formal authorization letter issued and signed by CSP officials. This letter is verified by at least two operators of the Root-CA. In case of any doubts, the operators will call the CSP to verify the authorization of the applicants.

3.2.4 Non-verified subscriber information

Subject names specified in the certificate as Alternative Subject Name are not verified by the Root-CA.

3.3 Verification of identity and authorisation for subsequent certification requests

The requirements and processes for identification and verification of authorization for subsequent certification requests are the same as for initial registration.

3.4 Verification of identity and authorisation for revocation requests

During CA Certificate registration, the applicants have to provide a secret phrase that had been written down and sealed in a tamper evident bag together with the names and 24-hr contact numbers for the CEO, Security Officer and Key Manager (or nominated senior managers).

During emergency revocation (such as key compromise), revocation requests via the ITIDA hotline are authenticated by the ROOT-CA team by verifying the secret phrase. Furthermore, the ROOT-CA team will attempt to call the CSP CEO, Security Officer or Key Manager for verification, confirmation by any two persons mentioned is required before proceeding with the revocation. The verification call will be recorded as evidence.

The CSP is responsible to keep the contact names and numbers up-to-date.

Non-emergency CA certificate revocation requests should always be done in-person at ROOT-CA office by at least two out of the three authorised persons for that CSP.

CA certificate revocation can also be requested and authorised by the Minister of Communications and Information Technology via an official ministerial declaration.

4 Certificate life-cycle operational practices

4.1 Certificate application

4.1.1 Who can apply for certificates

See Certificate Policy of the Egyptian Root-CA.

4.1.2 Registration process

In order to apply for one or several CA certificates, the CSP must make an appointment with the Root-CA for registration. The registration takes place inside the secure premises of the Root-CA. At least two representatives of the CSP must appear, the names of which must previously have been communicated to ITIDA by letter or fax.

The representatives are identified and their authority to apply for certificates on behalf of the CSP is verified as described in section 3.2.3.

For each certificate requested, the representatives must fill and sign a certificate application form in which they specify

- the type and data of the certificate,
- if the certificate shall be published in the X.500 directory of the Root-CA,
- general contact data of the CSP, and
- the individuals authorised to request revocation (minimum 3) with specimen signatures and 24-hr contact numbers.

An operator enters relevant registration data into the Root-CA system. The representatives then provide a secret phrase that had been written down with permanent ink and sealed in a tamper evident bag., the representatives provide a PKCS#10 Certificate Signing Request (CSR) containing the public key and some of the certificate content (see section 7.2). This CSR is imported (see section 3.2.1) and its signature is verified by the Root-CA system.

4.2 Certificate application processing

After all data has been entered by the operator, an Approver who has witnessed the registration process, reviews the application information before approving the application within the ROOT-CA system.

4.3 Certificate issuance

After the application approval;

- The PKCS#10 CSR file is submitted to the ROOT-CA system to issue the certificate. The Certificate is handed over to the CSP’s authorised representative.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

After the certificate is generated, it is inspected by the CSP’s authorised representatives and is considered accepted if there are no objections received within 24 hours.

4.4.2 Publication of the certificate by the CA

After the certificate has been accepted, the certificate is retrievable from the X.500 directory of the Root-CA via LDAP, if the CSP has specified that the certificate shall be published; otherwise, it is not retrievable.

4.5 Key Pair and Certificate Usage

Rules for the usage of the private keys are defined in the Certificate Policy of the Root-CA.

4.6 Certificate Renewal

The Egyptian Root-CA does not support the renewal of certificates, i.e. the issuance of a new certificate without changing the public key.

4.7 Certificate Re-key

The requirements and processes for certificate re-key is identical to the initial certificate application.

4.8 Certificate modification

The requirements and processes for certificate modification is identical to the initial certificate application.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate is revoked in the following cases:

- The private key is compromised or there is probable cause that it is compromised.
- The private key of the Root-CA by which the certificate has been signed has been compromised or there is probable cause that it is compromised.
- The cryptographic algorithm with which the key pair is used fails to comply with the Certificate Policy of the Root-CA or the Certificate Policy of the subscriber.
- The cryptographic hardware used to generate, store or process the private key fail to comply with the Certificate Policy of the Root-CA or the Certificate Policy of the subscriber.
- The data specified in the certificate turns out to be incorrect or has changed, in particular, the subject name or the key usage.
- The subscriber ceases operation and the certificate is not needed anymore.
- The subscriber does not use the certificate and key pair in compliance with the Certificate Policy of the Root-CA or its own Certificate Policy.
- The subscriber has lost his license to issue certificates and ITIDA decides to revoke its certificates.

Furthermore, a certificate will be revoked upon any authorised revocation request. The revocation request may specify a revocation reason. If a revocation reason is specified, it must be meaningful and must reflect the true circumstances. If the operators of the Root-CA can match the revocation reason to the reason codes listed in section 7.3, it provides this reason code in its certificate status services (CRL and OCSP). If no reason has been specified or if the reason specified can not be matched to the reason codes listed in section 7.3, no reason code will be given by the certificate status services.

4.9.2 Who can request revocation

Revocation can be requested by anybody by fulfilling the requirements of section 3.4.

4.9.3 Procedure for revocation request

Emergency revocations can be requested using the revocation hotline at any time (24/7). The requirements of section 3.4 shall be fulfilled before any revocation can happen.

Non-emergency revocations should be requested face-to-face while fulfilling the requirements of section 3.4.

After fulfilling the requirements of section 3.4, the Root-CA operator will initiate the revocation via the Root-CA system. The Root-CA approver approves the revocation via the Root-CA system.

Subsequently a CRL will be generated and published.

4.9.4 Revocation request grace period

The revocation grace period depends on the circumstances of the revocation:

- If the private key is compromised or there is probable cause that it is compromised, the subscriber must immediately request revocation of the corresponding certificate.
- If the private key of the Root-CA has been compromised or there is probable cause that it is compromised, all certificates signed by this private key will be immediately revoked.
- In all other cases, ITIDA will define a grace period for revocation, depending on the specific circumstances.

4.9.5 Revocation request processing time

Emergency revocation requests to the hotline are processed immediately.

Non-emergency revocation requests are processed within one (1) working day.

The Root-CA CRL will be updated immediately after revocation.

4.9.6 Revocation checking requirements for relying parties

Whenever the relying party validates a certificate, the relying party is responsible for checking the revocation status of a certificate via (in order of priority):

a. OCSP
b. Most recent CRL (if OCSP is not available)

4.9.7 CRL issuance frequency

The Root-CA signs CRLs every month or immediately after each revocation. The validity of the CRL is set to three (3) months.

4.9.8 Maximum latency for CRLs

Root-CA CRL are published in the X.500 directory within 10 minutes of issuance.

4.9.9 Online status checking availability

The OCSP service of the Root-CA allows anybody to verify the revocation status of certificates issued by the Root-CA.

CSPs are required to provided OCSP for certificates issued under them.

4.9.10 Online status checking requirements

The requirements for checking certificates status online are defined in the Certificate Policy of the Root-CA.

4.9.11 Other forms of revocation advertisements available

Revocations of self-signed CA certificates of the Root-CA are advertised in the federal gazette, the Root-CA web and ITIDA web site page (see section 2.1) (we need to add a url for revoked self-signed CA certificates)

4.9.12 Certificate suspension

For policy reasons certificate suspension is not supported by the Root-CA, i. e. revocation of a certificate is irreversible.

4.10 Certificate status services

4.10.1 Operational characteristics

The Root-CA disseminates status information by certificate revocation lists (CRLs) and through the online status checking service provided by an OCSP responder.

The Root-CA only provides status information for the certificates it has issued. In particular, the CRL and OCSP service of the Root-CA do not cover certificates issued by the certification authorities of the CSPs.

4.10.1.1 Operational characteristics of the CRLs

The Root-CA issues a direct CRL. The Root-CA does not issue incremental CRLs (delta-CRLs). The CRL is published in the X.500 directory of the Root-CA and can be retrieved using LDAP via

http://www.rootca.itida.gov.eg/CRL-G1.crl
http://www.rootca.gov.eg/CRL-G1.crl
ldap://ldap.rootca.gov.eg/cn=Egypt_RootCA_G1,ou=RootCA,o=ITIDA,c=EG?CertificateRevocationList;binary?base

The CRL complies with X.509 and RFC 5280 and its updates and uses the profile defined in section 7.3.

The CRL contains revocation status information for certificates.

The status of the following certificates is not covered by the CRL:

- Self-signed CA certificates of the Root-CA,
- OCSP responder certificates,
- Certificates of internal services of the Root-CA.
- Certificates issued by CSPs

4.10.1.2 Operational characteristics of the OCSP service

The OCSP service uses HSM keys to sign its responses. Requests can be sent by anyone over the internet and do not need to be signed. The service is available at

http://www.rootca.gov.eg/ocsp-G1

The OCSP responder complies with RFC 6960, and uses the profile defined in section 7.4.

The OCSP service provides revocation status for certificates.

The status of the following certificates is not covered by the OCSP service.

- Self-signed certificates,[1]
- OCSP responder certificates,
- Certificates of internal services of the Root-CA.
- Certificates issued by the CSPs.

4.10.2 Service availability

The CRL and the OCSP service are designed to be available at any time (24/7). ITIDA has taken considerable efforts to ensure a very high availability of these services.

[1] The OCSP responder will respond to a query for this certificate. However, the certificate can not be revoked and hence, always the status *good* will be given.

4.10.3 Optional features

The OCSP service has the following optional features:

- The service offers a “white list information“by indicating the status unknown if a certificate has not been issued by the Root-CA. This feature allows telling authentic certificates from forged ones after a compromise of the CA key. The address and operational features of the OCSP service are given in section 4.10.1.
- The service allows cryptographically binding the response to the request by including an extension Nonce with a random value in the request. If present, this value is repeated in a corresponding extension in the response.
- The retention period for which the OCSP service provides status information (see section 4.10.1) is indicated in the response extension ArchiveCutoff.

4.11 End of subscription

By virtue of the Egyptian E-Signature Law and its Executive Regulation, all entities operating certification services in Egypt, must obtain certificates from the Egyptian Root-CA. Hence, the subscription of a CSP to the Root-CA services only ends when the CSP ceases to operate its certification services in Egypt.

4.12 Key escrow and recovery

The Root-CA does not provide any key escrow services.

5 Facility, management, and operational controls

5.1 Physical security controls

5.1.1 Site location and construction

The Egyptian Root-CA is operated in two physically separated sites:

- In the main site, the productive infrastructure of the Root-CA is hosted and operated.
- In the Backup facility site a backup infrastructure is hosted for disaster recovery purposes.

In main site, the facilities of the Root-CA is protected by multiple tiers of physical security, constructional strength of walls and doors, absence of windows, sentries, video surveillance, burglar alarm systems, electromagnetic shielding of rooms and cables, and security cabinets and safes.

Backup facility is hosted by MCIT and they are responsible for applying similar security controls of main site by signed agreement.

5.1.2 Physical access

In main site, physical access to the facilities of the Root-CA is controlled by two-factor authentication including biometrics. Access privileges are restricted to the minimum necessary for operation. Access to the most sensitive areas is only possible for two authorised persons together.

Backup facility is hosted by MCIT and they are responsible for applying similar security controls to main site by signed agreement..

5.1.3 Power and air conditioning

Both sites are equipped with an uninterruptible power supply (UPS) and controls against overvoltage.

In both sites, the room climate is controlled by air conditions and continuously monitored.

5.1.4 Water exposures

Both sites are built in locations that are not susceptible to floods. Furthermore, the rooms hosting the systems of the Root-CA are protected from water exposure by the following controls:

- The rooms are not adjacent to water conduits.
- The fire extinguishing systems do not use water.
- The rooms have raised floors.
- The rooms are equipped with water leakage detection sensors which are continuously monitored.

5.1.5 Fire prevention and protection

In both sites, all rooms are equipped with continuously monitored fire detection sensors and automatic fire extinguishing systems. Furthermore, rooms and doors are fire proof.

5.1.6 Media storage

Media are stored within the premises of the Root-CA and MCIT in locations that are protected against unauthorised access, water, fire and electromagnetic fields.

5.1.7 Waste disposal

Any waste potentially containing security sensitive information, e. g. documentation, storage media, smart cards or system components, is disposed in a way that effectively prevents information disclosure.

5.1.8 Off-site backup

Copies of all complete backups are kept in the backup facility.

5.2 Procedural controls

5.2.1 Trusted roles

The administration, operation and management of the Egyptian Root-CA is exclusively performed by a set of trusted roles. For each role, the pre-requisites, responsibility, authority and tasks are clearly defined in the Access control policy of the Root-CA. Furthermore, role exclusion rules are defined to ensure segregation of duties and mutual supervision.

The assignment of persons to the defined roles is a formal process and is documented in journals.

5.2.2 Number of persons required per tasks

Tasks that are particularly security sensitive are only performed by cooperation of several persons. These tasks include, but are not limited to:

- Verification of the identity and authorisation of applicants
- Verification of registration data
- Generation of certificates
- Preparation and handing over issued CSP certificate.
- Access to the central PKI systems
- Usage of the private keys of the PKI systems

The multiple control of conduction is enforced by the segregation of duties and role exclusions defined in the role model (see section 5.2.1).

5.2.3 Identification and authentication for each role

The authentication of trusted roles is performed by physical access control and system level access control. The authentication is based on an identification of the person accessing the room or system and the access rights configured in accordance with the person’s role.

5.3 Personnel controls

5.3.1 Qualifications and experience requirements

Persons assigned to trusted roles must have the necessary qualification and experience to reliably and correctly perform the tasks required by their responsibility. The qualification is verified prior to assignment to a role.

5.3.2 Background check procedures

Only employees of ITIDA that have been undergone a candidate screening are assigned to trusted roles.

5.3.3 Training requirements

Persons assigned to trusted roles receive comprehensive training. The training comprises, but is not limited to:

- Security controls deployed in the Root-CA
- IT-infrastructure and deployed standard systems and software
- PKI theory and standards
- PKI software deployed by the Root-CA
- Operational rules and procedures
- Information security management system implemented for the Root-CA

5.3.4 Retraining frequency and requirements

The persons assigned to trusted roles are required to continuously refresh their knowledge gained in the training using a training environment. Furthermore, trainings are repeated whenever deemed necessary.

5.3.5 Job rotation frequency and requirements

There are no requirements for job rotation.

5.3.6 Sanctions for unauthorised actions

A formal disciplinary process is defined in the Access control policy of the Root-CA, ensuring that unauthorised actions are appropriately sanctioned. In severe cases, the role assignments and corresponding privileges can be withdrawn.

5.3.7 Independent contractor requirements

Persons not employed by ITIDA that need to enter the premises of the Root-CA are treated as visitors and are continuously supervised by trusted roles.

Externals that need access to confidential information of the Root-CA must sign a non-disclosure agreement.

5.3.8 Documentation supplied to personal

Personal assigned to trusted roles is provided with all documentation needed to securely execute their tasks. The documentation comprises, but is not limited to:

- Egyptian Electronic Signature Law and its Executive Regulation
- Certificate Policy and Certification Practice Statement of the Root-CA
- Internal policies of the Root-CA
- Documentation of the operation procedures
- Manuals and relevant technical specifications of the systems deployed
- Relevant technical standards and best practice guidelines

5.4 Audit logging procedures

5.4.1 Types of events recorded

The Root-CA manually or electronically records the following system events

- Certificate life cycle events
  - Registration (including registration data)
  - Confirmation of registration data
  - Certificate generation
  - Activation and publication
  - Revocation requests
  - Revocations
- Usage of certification services
  - Issuance of CRLs
  - Requests and responses of the OCSP service
  - Requests and responses of the timestamp service
- Security related system events
  - Successful and unsuccessful authentication attempts to the physical access system
  - Successful and unsuccessful log-in attempts to operating systems and PKI applications
  - Any changes to the database
  - Administrative actions on systems
  - Outages of systems or services
  - Data backup and recovery
  - Activities of the network security systems
  - Alarm of physical security systems
  - Security attacks and unauthorized access

The log entries include the following information

- Type of event
- Date and time of event
- Identity of system or persons generating record
- Identity of system or persons causing event
- Object accessed (if applicable)

5.4.2 Frequency of processing log

The recorded audit data is examined on a regular basis and in case of incidents. Furthermore, system logs are automatically evaluated by a central monitoring system (see section 5.4.6) and in cases of severe incidents alarms are triggered.

5.4.3 Retention period for audit log

All audit records except low level (i.e. very detailed) system logs are subject to archiving. All system logs are maintained for at least 2 weeks.

5.4.4 Protection of audit log

Audit records are kept on internal systems of the Root-CA and can only be accessed by trusted roles and except for the CA records, which require two employees together to be accessed.

5.4.5 Audit log backup procedures

System logs are backed up on a daily basis.

5.4.6 Audit collection system

System logs are automatically collected on a central monitoring system.

5.4.7 Notification to event-causing subject

No notification is given to the event-causing subject.

5.4.8 Vulnerability assessment

Vulnerability assessments are conducted as part of regular audits in the context of the ISO 27001 certification.

5.5 Records archival

5.5.1 Types of records archived

The records archived include, but are not limited to:

- All audit records (see section 5.4.1)
- Issued certificates and CRLs
- Responses of the OCSP service
- Time stamps issued by the public time stamp service
- Certificate application forms and documents used to verify the identity and authorisation of the applicants
- Written certificate revocation requests
- Records of certificate revocation requests to the hotline
- Records supporting the information security management system (ISMS)
    - Assignment and withdrawal of roles and privileges
    - Visitor access to Root-CA facilities
    - Changes and maintenance of system hardware or software
    - Detection and processing of security incidents
    - Emergency drills
    - Audits
    - Risk assessment and treatment
    - Changes of assets, procedures or responsibilities
    - Changes of documentation
- Documentation of the Root-CA implementation

5.5.2 Retention period for archive

Archive data is maintained for at least 30 years.

5.5.3 Protection of archive

All archive data is digitally signed(it is not required by web trust).

In case that backup has its integrity check it will be enough

The archive is protected by the physical security controls described in section 5.1.

Access to the archive is only possible by trusted roles and by two employees together.

5.5.4 Archive backup procedures

A complete backup of the archive is maintained at the D/R site. Copies of archive media are transferred to the backup archive at least on a weekly basis.

Not stipulated

5.5.5 Requirement for time-stamping of records

All electronic archive data is complemented with a timestamp from the public time stamp service of the Root-CA (see section 6.8.2).

5.5.6 Archive collection system

Archive data is collected on an internal system.

5.5.7 Procedures to obtain and verify archive information

A formal process exists for retrieving and verifying information from the archive. Integrity verification is performed using the digital signatures attached to the archive data.

5.6 Key changeover

At about the halfway point of the Root-CA key validity or in the event the existing Root-CA needs to be replaced, a new Root-CA key pair and certificate (Gn+1) will be generated and distributed to subscribers and relying parties. Both existing (Gn) and new Root-CA (Gn+1) certificates will be active concurrently. The existing Root-CA certificate will continue to be used to issue CRLs however any new CSR signing will be performed by the new Root-CA certificate.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The Egyptian Root-CA has defined and documented formal incident handling procedures, aiming at identifying the source and reason of the incident, minimising its impact, and timely re-establishing security and availability of the Root-CA services. The incident handling procedures include appropriate escalation, incident investigation, minimisation of impact, planning and execution of corrective and preventive actions, and reporting.

5.7.2 Corruption of computing resources, software, or data

Corruption computing resources, software, or data is considered as incident and is treated by the incident handling procedures.

5.7.3 Root-CA private key compromise procedures

The Egyptian Root-CA has implemented comprehensive and effective controls to minimise the risk of a private key compromise. In the unlikely event, that there is reasonable cause that a private key of the Root-CA has been compromised, an emergency response team is set up that plans, initiates and supervises all necessary actions. These include

- Unless the compromised key is a CA key of the Root-CA, the corresponding certificate is immediately revoked, and a new certificate is issued.
- If the compromised key is a CA key of the Root-CA, the following actions are taken:
    - All certificates signed by the compromised key are immediately revoked.
    - All subscribing CSPs are notified.
    - A new Root-CA key is generated (see section 5.6).
    - A revocation notice for the old CA key and the fingerprint of the new CA key are advertised on the web site of the Root-CA and in the national gazette.
    - New certificates are issued with the new active CA key.
- An investigation is conducted, analysing the circumstances of the key compromise, potential security breaches and threats. The results of the investigation are documented in a report.
- Based on the outcome of the investigation, appropriate countermeasures are selected, planned and implemented to minimise the risks identified.
- In case of security violations by the personnel of the Root-CA, appropriate sanctions are imposed (see section 5.3.6).

5.7.4 Business continuity capabilities after a disaster

All systems implementing critical services are implemented redundantly. However, if the infrastructure at the main site fails as a result of a disaster, the following services can be quickly restored at the backup facility:

- Certificate issuance
- Certificate revocation
- CRL issuance
- Certificate and CRL publication through web service.
- Public Timestamp service

For this purpose, a backup facility is implemented at MCIT site. In order to allow for quick takeover of the services, the backup of the Root-CA system and HSM are stored at the backup facility and updated frequently.

Furthermore, the Root-CA has developed a disaster recovery plan defining the steps necessary to take over the critical services at the backup facility within 24 hours and to switch back smoothly after restoration of the main site. This plan is tested on a regular basis.

5.8 CA termination

In accordance with the E-Signature Law and its Executive Regulation, the Root-CA will overtake certain services of a CSP that ceases its operation. In particular, the Root-CA will provide the following services:

- Revocation service: Upon authorised requests, the Root-CA will revoke the certificates of the CSP. The revocation can be requested by the means specified in section 4.9. The CSP is obliged to inform its subscribers and all other affected parties about the takeover of the revocation service and how it can be used.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pairs of the Root-CA are generated inside Hardware Security Modules (HSM), which holds and processes the private key, using the random number generator of the HSM. At no time does the private key or any parts of it exposed. The key generation is performed inside the secure premises of the Root-CA.

CSPs are responsible in generating their own key pair and the use of secure devices such as HSMs is mandatory.

6.1.2 Private key delivery to subscriber

The Root-CA does not generate Private keys on behalf of its subscribers.

6.1.3 Public key delivery to the Root-CA

Public keys are delivered as part of the PKCS#10 certification request (see sections 3.2.1 and 4.1.2).

6.1.4 Root-CA public key delivery to relying parties

The public keys of the Root-CA certification authority are published as described in section 2.2.

Furthermore, the self-signed certificates of the Root-CA certification authority are delivered to the subscribing CSPs.

6.1.5 Key sizes

The keys used or issued by the Root-CA services are 4096 bit RSA keys.

Key sizes of subscribing CSPs that generate their own key pairs must comply with the Certificate Policy of the Root-CA.

6.1.6 Public key parameters generation and quality checking

Generation of the public key parameters used by subscribing CSPs that generate their own key pairs is under the responsibility of the respective CSP. The eligibility of these public key parameters is checked by ITIDA in the context of the supervision of the CSPs. In case of applications for CSP backup transfer certificates, the Root-CA verifies that the keys are 4096 bit keys for RSA according to PKCS#1 version 1.5.

6.1.7 Key usage purposes

The private keys of the Root-CA are only used for creating digital signatures in accordance with the key usages and extended key usages specified in the certificate:

- The private keys of the certification authority of the Root-CA are only used to sign certificates and issue CRL.
- The private keys of the OCSP service of the Root-CA are only used to sign OCSP responses.
- The private keys of the time stamp service of the Root-CA are only used to sign time stamp tokens in TSP responses.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Private key multi-person control

The private keys used by the Root-CA are generated, kept and used under two-person control. In particular, activation of the Hardware Security Module (HSM) is protected by “m of n” control via physical security “tokens” that are PIN protected.

Prior to Key generation, the HSM is enrolled with 3 security “tokens” of which any 2 is required whenever the HSM needs to be activated. These security “tokens” are handed over to authorised and trusted custodians. The activation PIN for each security “token” is set by the respective custodian to ensure that the security “token” cannot be used even if it is stolen.

6.2.2 Private key escrow

No escrow is performed for the private keys used or issued by the Root-CA. The Hardware Security Module, in which the private keys are generated, stored and processed, prevent reading out the private key by technical means.

6.2.3 Private key backup

Backup is performed for the Root-CA private keys based on Hardware Security Module using secure backup mechanism.

6.2.4 Private key archival

Private keys used by the Root-CA are not archived. The private key is erased/destroyed after expiry.

6.2.5 Private key transfer into or from a cryptographic module

The key pairs of the Root-CA are generated on board a Hardware Security Module (HSM). the private keys or any parts of it are never exposed outside of the HSM nor is there a need to transfer in a private key generated externally.

6.2.6 Private key storage on cryptographic module

The Hardware Security Module (HSM) used protects the private keys at rest and has features to prevent from unauthorised access by the following means:

- The private keys can not be read out via electronic or mechanical tampering.
- Physical tampering countermeasures ensure that private keys are destroyed or at the very least the physical tampering attempt is made evident.
- Multi-person with two-factor authentication is required to activate the HSM.

6.2.7 Method for activating and deactivating private keys

The private keys used or issued by the Root-CA are protected by “m of n” security “tokens”. Usage of the private key is only possible after two (2) out of three (3) security “tokens” have been presented to the HSM. This authentication activates the private key until the power supply of the HSM is interrupted (e.g. the HSM is powered down) or a “deactivate” command is given to the HSM.

6.2.8 Method for destroying private keys

After retirement of the private key the HSM is issued a command to destroy the private key. Multi-person control also applies during the decommissioning of keys.

6.2.9 Cryptographic module rating

The Hardware Security Modules used by the Root-CA have been certified according to Common Criteria EAL5+ using the Protection Profile CWA 14169 or FIPS 140-2 Level 3 (and above).

6.3 Other aspects of key pair management

6.3.1 Public key archival

All certificates issued by the Root-CA are archived (see section 5.5).

6.3.2 Certificate operational periods and key pair usage periods

The root CA keys will be replaced halfway through their validity of 20 years. Although the retired keys will not be used anymore, their certificates are not revoked. The retired keys are securely destroyed (see section 6.2.8) once their corresponding certificate is no longer valid.

OCSP signer certificates are valid for 6 months but are replaced within 5 months of their validity.

TSA signer certificates are valid for 135 months but are replaced within 120 months of their validity.

Operational periods of subscriber certificates and corresponding keys are defined by the subscriber but must comply with the Certificate Policy of the Root-CA.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation procedure of the Hardware Security Module is in accordance to the specifications and recommendations of the manufacturer. Multi-person controls are applied throughout the process.

CSPs are advised to use similar or equivalent level of security.

6.4.2 Activation data protection

Activation data for the Hardware Security module is protected as described by the manufacturer’s certified security/protection profile. Any PIN or Password used are generated by the respective credential owners and is printed on sealed letters which is kept by the PIN owner as a backup.

Furthermore, the PINs or Passwords are of sufficient complexity and length in compliance with security best practises..

6.5 Computer security controls

6.5.1 Specific computer security technical controls

The Egyptian Root-CA implements comprehensive controls to protect their systems from unauthorised access and other threats. These controls include, but are not limited to:

- Access to systems is restricted to authorised personnel being assigned to trusted roles.
- Administrative access requires two persons. All administrative actions are logged in records.
- Usage of systems is restricted to the functions necessary to securely provide the PKI services.
- Systems are configured in a restrictive and functionally minimised way.
- Remote administrative access to RootCA main site systems is prevented.
- Only personalised accounts are used to ensure traceability o user activities.
- System time is synchronised within the network.
- Systems are monitored for failures and potential attacks.
- All media are checked for viruses on a separated system before they are connected to the Root-CA systems.
- Security patches are applied timely.
- A formal change and release management process is defined ensuring that modifications to systems are properly tested before being implemented. Tests are not performed on productive systems.
- The authenticity of software and hardware is checked.
- Details on the IT-infrastructure and source code of the PKI applications are kept strictly confidential.

The effectiveness of the computer security controls is analysed in the risk assessment conducted by the Root-CA in the context of the ISO 27001 certification, and their implementation is subject to the corresponding audits (see section 6.6.2).

6.5.2 Computer security rating

The systems implementing the OCSP and time stamp services have been evaluated according ITSEC level E2 with strength of mechanisms *high*.

6.6 Life cycle security controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

The Root-CA maintains an information security management system (ISMS) according to ISO 27001. The ISMS covers all services provided by the Root-CA and ensures that information security for these services is established, operated, monitored, reviewed and improved according to the security objectives of the Root-CA. This includes, but is not limited to:

- Management commitment to information security.
- Identification of assets and their owner.
- Conduction of a risk assessment after significant changes of assets, threats or controls.
- Selection and implementation of appropriate security controls.
- Comprehensive documentation of procedures and controls.
- Regular review of information security, in particular conduction of internal audits.
- Improvement of the processes, controls and procedures based on the results of the review.

  The Root-CA is ISO 27001 certified and complies with ISO 27001 ISMS, regular internal and external audits are performed to ensure compliance with standard.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

The Egyptian Root-CA implements comprehensive controls to protect their networks from unauthorised access and other threats. These controls include, but are not limited to:

- The network is not linked to any other networks and only contains the systems implementing or directly supporting the PKI services.

- The network implements multiple tiers of security.
- The CA system is not connected to any other systems or networks.
- Traffic in the network, as well as traffic to and from the internet is restricted to the protocols and connections required to provide the PKI services.
- Network services on systems are disabled if not needed for the operation of the Root-CA.
- Systems in the core network segments are not accessible from the internet.
- Traffic in the network is monitored for failures and potential attacks.
- Communication from and to CSPs is encrypted and mutually authenticated.

The effectiveness of the network security controls is analysed in the risk assessment conducted by the Root-CA in the context of the ISO 27001 certification, and their implementation is subject to the corresponding audits (see section 6.6.2).

6.8 Timestamping

6.8.1 Internal Timestamping

All log data contains a timestamp.

All archived data is additionally timestamped using the public timestamp service of the Root-CA (see next section).

6.8.2 Public Timestamp Service

In support of the Egyptian E-signature Law and its Executive Regulation, the Root-CA provides a public timestamp service which allows anybody to request and obtain timestamps on arbitrary data. The timestamp consists of the data provided in the request ("to be timestamped") which is a hash value of one or several[2] documents, an accurate time information and a digital signature of the TSP server over the former two data structures.

The timestamp service uses a trustworthy time source. The time information provided by the time stamp service is accurate **up to one second**. Due to their trustworthiness and accuracy, the timestamp provides evidence that the stamped data has been presented to the timestamp server (and hence has already existed) at the specified time.

The timestamp service is based on the timestamp protocol (TSP) according to RFC 3161 and its update 5816 which is transported over HTTP. The TSP profile of the timestamp service is specified in section 7.5.2. The timestamp service can be accessed at

[2] In order to generate a single hash value for several documents, "hash trees" can be applied.

http://rootca.gov.eg/tsp

If a TSP request is syntactically and semantically correct and complies with the profile defined in section 7.5.1 it is processed by the TSP responder. The TSP responder determines the actual time, forms a corresponding TSP response containing the hash value included in the request and the time information, and digitally signs it with its private signing keys.

7 Description of PKI data structures

7.1 Certificate profiles

All certificates issued by the Root-CA have the following general structure and contents, which are compliant with X.509v3 an RFC 5280 and its updates RFC 8398, RFC 6818, RFC 8399

Attribute	Content	Remark
Version	V3	
serialNumber	Certificate Serial Number	Unique positive integer (≤ 20 octets)
signature	1.2.840.113549.1.1.11 (sha512WithRSAEncryption)	The Root-CA signs its certificates, using RSA PKCS#1v1.5 with 4096 bit keys and SHA512.
Issuer	Name of issuing CA, equals subject name in corresponding root certificate	Only ASCII characters should be used to avoid problems with applications[3]
Validity	(notbefore, notAfter)	
notbefore	Start of validity	Start of validity = date of issuance End of validity = start of validity + validity period
notAfter	End of validity	
Subject	Name of certificate subject	Only ASCII characters should be used to avoid problems with applications
subjectPublicKeyInfo	(publicKey, algorithm)	
publicKey	Public key of subject	Coding according to RFC 3279 and its updates RFC4055, RFC4491, RFC5480, RFC5758 In case of RSA, no parameters are specified
algorithm	OID and parameters of public key algorithm or subject key	
Extensions	Various extensions an their criticality	Depends on certificate type
signatureAlgorithm	(see above)	Identical to attribute “signature”
signatureValue	Signature of issuer	

Table 1: General structure and contents of certificates issued by the Root-CA

[3] In particular, non ASCII characters in attribute “organization” can yield to ambiguous coding rules (due to concurring standards) in an LDAP-URL of the CRL distribution point.

The details of the certificate profiles, in particular, the names, validity, subject public key algorithm and extensions are defined in the subsequent sections.

The certificates are structured in ASN.1 syntax according to X.509 and binary encoded by the Distinguished Encoding Rules (DER).

7.1.1 Root Certificates

The certificate profiles used for the self-signed root certificates and the key rollover certificates (cross certificates between consecutive Root-CA keys) are defined by the general structure and contents specified in Table 1 and the following provisions:

- Both, subject and issuer name is CN=<CA>,OU=Root-CA,O=ITIDA, C=EG.
- The validity period is set as follows:
  - The validity of self-signed certificates is set to 20 years.
  - The validity of key rollover certificates is set to end with the validity of the firth of the corresponding self-signed certificates, i.e. the key rollover certificate expires with the older one of the two self-signed certificates.
- The subject public key algorithm is set to 1.2.840.113549.1.1.1 (rsaEncryption).
- The extensions are specified below.

Extension	Critical	Contents	Remarks
AuthorityKeyIdentifier	n	System generated	Identical to SubjectKeyIdentifier for self-signed certificates
SubjectKeyIdentifier	n	system generated	Identical to AuthorityKeyIdentifier for self-signed certificates
KeyUsage	y	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	
CertificatePolicies	n	OID of certificate policy OID of CPS with qualifier id-pt-cps (1.3.6.1.4.1.33399.1.2)	Refers to CP and CPS of Root-CA

Extension	Critical	Contents	Remarks
BasicConstraints	y	(cA, pathLenConstraint)	No usage of pathLenConstraint
cA		TRUE	

Table 2: Certificate profile for self-signed root certificates and key rollover certificates

7.1.2 Certificates for services of the Root-CA

7.1.2.1 Root-CA OCSP Responder Certificates

The certificate profile used for the certificates of the online status validation service of the Root-CA is defined by the general structure and contents specified in Table 1 and the following provisions:

- The subject name is cn=<OCSP Responder>, o=Root-CA, c=EG
- The validity period is set to 6 months.
- The subject public key algorithm is set to 1.2.840.113549.1.1.1 (rsaEncryption).
- The extensions are specified below.

Extension	Critical	Contents	Remarks
AuthorityKeyIdentifier	n	System generated	
SubjectKeyIdentifier	n	System generated	
KeyUsage	y	digitalSignature nonRepudiation	
BasicConstraints	y	(cA, pathLenConstraint)	
cA		FALSE	Useful to avoid misconceptions (footnote **Error! Bookmark not defined.**).
CertificatePolicies	n	OID of certificate policy OID of CPS with qualifier id-pt-cps (1.3.6.1.5.5.7.2.1)	Refers to CP and CPS of Root-CA
ExtendedKeyUsage	y	Id-kp-OCSPSigning	

		(1.3.6.1.5.5.7.3.9)	
OCSPNocheck	n	NULL (no value)	Indicates that that a client can trust the OCSP responder certificate for its lifetime, i.e. the client need no CRL information

Table 3: Certificate profile for the Root-CA OCSP responder certificates

7.1.2.2 Root-CA Time Stamp Server Certificates

The certificate profile used for the certificates of the time stamp server of the Root-CA is defined by the general structure and contents specified in Table 1 and the following provisions:

- The subject name is cn=<Time Stamp Server>, ou=Root-CA,o=ITIDA, c=EG
- The validity period is set to 5 years.
- The subject public key algorithm is set to 1.2.840.113549.1.1.1 (rsaEncryption).
- The extensions are specified below.

Extension	Critical	Contents	Remarks
AuthorityKeyIdentifier	n	System generated	
SubjectKeyIdentifier	n	System generated	
KeyUsage	y	digitalSignature nonrepudiation	
BasicConstraints	y	(cA, pathLenConstraint)	
cA		FALSE	Useful to avoid misconceptions (footnote **Error! Bookmark not defined.**).
CertificatePolicies	n	OID of certificate policy OID of CPS with qualifier id-pt-cps (1.3.6.1.5.5.7.2.1)	
ExtendedKeyUsage	y	Id-kp-timeStamping (1.3.6.1.5.5.7.3.8)	

Extension	Critical	Contents	Remarks
authorityInfoAccess	n	(accessMethod, accessLocation)	
accessMethod		id-ad-ocsp (1.3.6.1.5.5.7.48.1)	
accessLocation		URL of OCSP responder	
cRLDistributionPoints	n	(cRLIssuer, fullName)	
cRLIssuer		Subject name of the CRL signing certificates	Must match Issuer name of CRL
fullName		ldap URL incl. DName of directory node containing CRL	

Table 4: Certificate profile for the Root-CA time stamp service certificates

7.1.3 Certificates Issued to CSPs

The Root-CA will only issue certificates to CSPs after all necessary requirements and procedures have been fulfilled.

7.1.3.1 Certificates for Certificate Authorities

The certificate profile used for the certificates issued to certification authorities of CSPs is defined by the general structure and contents specified in Table 1 and the following provisions:

- The subject name can be chosen by the subscribing CSP using the following distinguishedName attributes:

Attribute	Optional / mandatory	Maximal length (characters)
commonName (cn)	M	64
serialNumber	O	64
organizationName (o)	M	64
organizationalUnitName (ou)	O	64
domainComponent (dc)	O	acc. RFC 2247 and

Attribute	Optional / mandatory	Maximal length (characters)
		its updates RFC4519, RFC4524
streetAddress	O	128
postalCode	O	40
localityName	O	128
stateOrProvinceName	O	128
countryName	M	2 (“EG”)

Table 5: Allowed name attributes for certificates issued to CSPs

Since the CSP certificates are issued to an organization and not to natural persons, attributes referring to individual data (givenName, surname, title, gender, initials) or pseudonyms are not allowed. If the CSP wishes to include further information (e.g. an e-mail address or URL) it can use the extension subjectAltName (see below).

In principle, the name attributes may contain non-ASCII characters which are encoded as UTF-8 unicode in the certificate. However, for interoperability reasons the use on non-ASCII characters in the subject name is discouraged. At least the attribute organizationName should only contain ASCII characters to avoid ambiguities in the encoding of the URLs specified in CRLDistributionPoint extensions.

- The validity period is set to 3 years.
- The subjectAltName extension can contain one or several of the following names:
  - E-mail address (rfc822Name)
  - Internet domain name (dnsName)
  - Alternative DistinguishedName (directoryName). This name may contain non-ASCII characters which are encoded as UTF-8 unicode in the certificate
  - URLs (uniformResourceIdentifier)
  - IP address (iPAddress)
- Further constraints on extensions are specified below.

Extension	Crit.	Contents	Remarks
AuthorityKeyIdentifier	n	System generated	
SubjectKeyIdentifier	n	System generated	
KeyUsage	y	keyCertSign crlSign	
BasicConstraints	y	(cA, pathLenConstraint)	
cA		TRUE	
pathLenConstraint		(value = 1)[4]	
CertificatePolicies	n	OID of certificate policy OID of CPS with qualifier id-pt-cps (1.3.6.1.5.5.7.2.1)	Refers to CP and CPS of Root-CA
SubjectAltName	n	(provided by CSP)	See explanation above
authorityInfoAccess	n	(accessMethod, accessLocation)	
accessMethod		OCSP (1.3.6.1.5.5.7.48.1)	
accessLocation		URL of OCSP responder of Root-CA	
cRLDistributionPoints	n	(cRLIssuer, fullName)	
cRLIssuer		Subject name of the Root-CA CRL signing certificates	
fullName		ldap URL incl. DName of directory node containing CRL	Refers to Root-CA ldap directory

Table 6: Certificate profile for CA certificates issued to CSPs

More specific constraints and requirements for the contents of the CSP certificates can be defined by the Certificate Policy.

[4] A value *n* means that at most *n* levels of sub-CA's may exist below the subject CA.

7.1.3.2 CSP Backup Transfer Certificates

The certificate profile for the CSP backup transfer certificates is defined by the general structure and contents specified in Table 1 and the following provisions:

- For the subject name the same rules apply as for the certificates for certification authorities of CSPs (see section 7.1.3.1).
- The validity period is set to 3 years.
- The subject public key algorithm must be 1.2.840.113549.1.1.1 (rsaEncryption).
- The extensions are specified below.

Extension	Critical	Contents	Remarks
AuthorityKeyIdentifier	n	System generated	
SubjectKeyIdentifier	n	System generated	
KeyUsage	y	digitalSignature	
BasicConstraints	y	(cA, pathLenConstraint)	
cA		FALSE	

Table 7: Certificate profile for CSP backup transfer certificates

7.1.4 Certificates Issued to Natural End Entity

Attribute	Description	Content
Version	2	“2” means X.509v3
Serial number	Certificate univocal identification number	7c 88 54 93 b6 c9 (sample)

Issuer	Issuer Distinguished Name	CN = Egypt Trust Corporate CA G2
		O = Egypt Trust
		C = EG

signatureAlgorithm	1.2.840.113549.1.1.11 (sha256WithRSAEncryption)	OID of algorithm for signing the certificate
Validity	(notbefore, notAfter)	
Notbefore	Start of validity	Start of validity = date of issuance End of validity = start of validity + validity period
notAfter	End of validity	

Subject	certificate Distinguished name(Only ASCII characters should be used to avoid problems with applications)	T = Engineer
		E = test@test.gov.eg
		SERIALNUMBER = EgID:28512111799094
		CN = for test
		OU = Account
		O = ITIDA
		C = EG

publicKey	Public key of subject	Coding according to RFC 3279 and its updates In case of RSA, no parameters are specified

Table 8: Certificate profile for End entity “natural person “

Extension	Crit.	Contents	Remarks
AuthorityKeyIdentifier	N	Identification of the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys	In reference to RFC 5280
SubjectKeyIdentifier	N	Subject public key identifier (derived from the subject public key using hash function)	In reference to RFC 5280
KeyUsage	Y	Digital Signature	Used when the subject public key is used for verifying digital signatures
BasicConstraints	Y	(Subject Type, pathLenConstraint)	
Subject Type		End Entity	
pathLenConstraint		None	
cRLDistributionPoints	N	URLs of published CRL	Indicates how to obtain the CRL information

Table 9: Certificate profile for End entity “natural person “

7.2 Profile of certification requests

The certificate requests provided by CSPs must comply with PKCS#10 and have the following structure and contents:

Attribute	Content	Remark
Version	0	"0" means PKCS#10 Version 1
Subject	Name of certificate subject	See section 7.1.3.1
subjectPublicKeyInfo	(publicKey, algorithm)	
publicKey	Public key of subject	See section 7.1.3.1
algorithm	OID and parameters of public key algorithm or subject key	
Attributes		Only the following Attribute is supported, others are deprecated
ExtensionRequest	subjectAltName	Optional Admissible syntax defined in section 7.1.3.1
	basicConstraints Boolean ca (true) path length constraint (an integer >=0, optional)	Optional Applicable to certificates for Certificate Authorities only (please refer to subsection 7.1.3.1 starting on page 54)
signatureAlgorithm	OID of signature algorithm used to sign the certificate.	SignatureAlgorithm must be consistent with subjectPublicKeyInfo.
signatureValue	Signature of issuer	Self-signed, i.e. signed with private key corresponding to contained public key

Table 8: Structure and contents of certificates requests

7.3 CRL Profile

For the CRLs issued by the Root-CA the following structure is used:

Attribute	Content	Remark
Version	V2	
Issuer	Name of CRL signer, equals subject name in corresponding CRL signer or CA certificate	
Effective Date	Date and time of CRL generation	
Next Update	Date and time when next regular CRL is issued	
CRL Extensions	Various CRL extensions as their criticality	
revokedCertificates	List of (userCertificate, revocationDate)	
userCertificate	Serial number of revoked certificate	
revocationDate	Date and time of revocation	
crlEntryExtensions	Various CRL entry extensions and their criticality	(See below)
signatureAlgorithm	Equals attribute “signature”	
signatureValue	Signature of CRL issuer	

Table 9: Profile of CRLs

The following CRL extensions are used.

Extension	Critical	Contents	Remarks
AuthorityKeyIdentifier	n	System generated	Matches SubjectKeyIdentifier in certificate of CRL Issuer
Authority Info Access	n	http://www.rootca.gov.eg/EgyptRootCAG1.cer	
CRLNumber	n	Sequence number of CRL	Increased by one for each CRL
IssuingDistributionPoint	n	http://www.rootca.gov.eg/CRL-G1.crl	

Table 10: CRL extensions

The following CRL entry extensions are used.

Extension	Critical	Contents	Remarks
ReasonCode	n	Code of reason for revocation according to RFC 5280 and its updates RFC 8398, RFC 6818, RFC 8399	optional, only included if provided with revocation request Codes are specified below
Certificate Issuer	y	IssuerName of certificate	Name of the issuing instance of the Root-CA

Table 11: CRL entry extensions

The following reason codes will be used:

- unspecified (0). This code is used if no reason code has been given by the requestor.
- keyCompromise(1). This code indicates that the private key corresponding to the public key in the certificate is suspected or assumed to be compromised. In accordance with X.509, this code is only used for end-entity certificates (i.e. not in CA certificates).
- cAcompromise (2). This code indicates that the private key of the Root-CA by which the certificate was signed is suspected or assumed to be compromised, rendering the certificate insecure. In accordance with X.509, this code is only used for CA certificates (i.e. for CA certificates of CSPs or key rollover certificates).
- affiliationChanged (3). This code indicates that the certificate has been revoked due to a change of the subject information (i.e. names) included. This code is used for all certificates.
- superseded (4). This code indicates that the certificate has been revoked only because it has been replaced by another certificate (e.g. for a new key pair). This code is used for all certificates.
- cessationOfOperation (5). This code indicates that the certificate has been revoked, because the subject has terminated the respective service. This code is used for all certificate types[5].

The following codes are not used in the CRL of the Root-CA:

- certificateHold (6). This code indicates that a revocation is preliminary (suspension) and the certificate could by reactivated later. For policy reasons certificate suspension is not supported by the Root-CA.
- removeFromCRL (8).[6] According to X.509 this code is only admissible in deltaCRLs.
- privilegeWithdrawn (9). No use case for this code has been identified.
- aaCompromise (10). This code is only eligible for attribute certificates.

7.4 OCSP profile

7.4.1 OCSP Requests

The request must contain the following elements:

```
POST <http://www.rootca.gov.eg/ocsp-G1>

...

Content-Type: application/ocsp-request

Content-Length: ...
```

[5] However, it is not supposed to be used for the Root-CA certificates until the Root-CA terminates the respective services.

[6] The code (7) is not defined in X.509.

<DER coded OCSPRequest object>

...

OCSP requests are transmitted in binary form, i.e. without base64 encoding.

The OCSP responder accepts requests that comply with the OCSP profile specified in RFC6960.

The following Extensions are supported:

- Nonce (RequestExtension). If present its value is included in a corresponding extension in the response to bind the response to the request.
- AcceptableResponsesis (RequestExtension). If present, it must contain the value id-pkix-ocsp-basic.
- ServiceLocator (SingleRequestExtension). This extension is not evaluated.

7.4.2 OCSP Responses

The responses are generated in compliance to RFC 6960:

7.5 Time Stamp Service

7.5.1 TSP Requests

TSP requests can be submitted to the Root-CA by anybody. The requests must be sent to the TSP/TSP gateway via the HTTP POST method. The request must contain the following elements:

POST <http://rootca.itida.gov.eg/tsp>

...

Content-Type: application/time-stamp-request

Content-Length: ...

<DER coded TimeStampReq object>

...

TSP requests are transmitted in binary form, i.e. without base64 encoding.

The requests must comply with the following profiling of RFC 3161 and its update RFC 5816:

- The hash algorithm specified in the messageImprint should be:

  - SHA256 (2.16.840.1.101.3.4.2.1)
- If the field reqPolicy is present, it must contain the value 0.4.0.2023.1.1 (baseline time-stamp policy according to ETSI EN 319 421).
- If the field Nonce is present, its value is copied to the corresponding field in the response to bind the response to the request.
- If certReq is set to TRUE, the certificates of the TSP server and its issuer are included in the response (see below).
- No extensions must be present.

7.5.2 TSP Responses

The responses use the following profiling of RFC 3161 and its update RFC 5816:

- In the field PKIStatusInfo the following values are used:
  - The subfield status can only contain the values granted and rejection.
  - The subfield statusString is not used.
  - The subfield failInfo does **not** contain the values timeNotAvailable and addInfoNotAvailable.
- The field accuracy specifies 1 second.
- The field ordering is not used.
- The field nonce is only used if it was present in the request. In this case the value from the request is included in the response.
- The field tsa contains the subject name from the certificate of the TSP server (corresponding to the key used to sign the time stamp).
- No extensions are used.
- The certificate of the TSP server (corresponding to the key used to sign the time stamp) and its issuer certificate are referenced by certificate identifiers inside a SigningCertificate attribute (according to RFC 2634 and its update RFC5035) which is part of the signerInfo field of the CMS data structure according to RFC 5652. The certificate identifiers are encoded as ESSCertID Attribute according to RFC 5035 and contain the SHA-256 hash value of the corresponding certificate.[7]
- If the field certReq in the TSP request has been set to TRUE, the certificate of the TSP server and its issuer certificate are included in the response in the certificates field of the CMS data structure SignedData.

[7] Since RFC 5035 has been published only recently, it is not referenced by RFC 3161. However, since RFC 5035 updates the referenced RFC 2643, our encoding is the most natural choice for applying SHA-2.

7.6 E-Seal Certificate Profile

Attribute	Description	Content
Version	3	
Serial number	Certificate univocal identification number	7c 88 54 93 b6 c9 (sample)

Issuer	Issuer Distinguished Name	CN = Egypt Trust Corporate CA G2
		O = Egypt Trust
		C = EG

signatureAlgorithm	1.2.840.113549.1.1.11 (sha256WithRSAEncryption)	OID of algorithm for signing the certificate
Validity	(notbefore, notAfter)	
Notbefore	Start of validity	Start of validity = date of issuance End of validity = start of validity + validity period
NotAfter	End of validity	

Subject	certificate Distinguished name(Only ASCII characters should be used to avoid problems with applications)	CN = for test
		O = test
		2.5.4.97 = VATEG-333777999
		C = EG

publicKey	Public key of subject	Coding according to RFC 3279 and its updates In case of RSA, no parameters are specified

Certificate Extensions

Extension	Crit.	Contents	Remarks
AuthorityKeyIdentifier	N	Identification of the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys	In reference to RFC 5280
SubjectKeyIdentifier	N	Subject public key identifier (derived from the subject public key using hash function)	In reference to RFC 5280
KeyUsage	Y	Digital Signature, nonRepudiation	Used when the subject public key is used for verifying digital signatures
BasicConstraints	Y	(Subject Type, pathLenConstraint)	
Subject Type		End Entity	
pathLenConstraint		None	
cRLDistributionPoints	N	URLs of published CRL	Indicates how to obtain the CRL information

7.7 LDAP schema and directory information tree

- The LDAP directory of the Root-CA complies with RFC 3494, RFC 4510, RFC 4510, RFC 4511, RFC 4512, RFC 4513, RFC 4523, and RFC 4519, and ensures that LDAP searches with specific LDAP attributes (LDAP search filter) result in correct search results.
- The DIT (directory information tree) is built upon the attributes C, O, OU and CN of the LDAP scheme. These LDAP attributes correspond to the equivalent attributes in the certificates issuer and subject DNames.
- The (C and o) node is the structural root node of the LDAP tree. It stores no PKI relevant data and only serves as ‚entry-point' into the tree. Additional prefixes are possible (e. g. DC nodes).
- for RootCA ou is defined, which can be regarded as the logical root node of the RootCA PKI tree.
- The CN node under an OU node represent the subject of Egypt_RootCA_G1. There, the Root-CA's CRL is stored in the attribute certificateRevocationList and the RootCA's certificate is stored in attribute cACertificate.
- The following table lists the attributes and their values of the individual directory nodes.

Nodes	Attributes and Values
C	Country.countryName=EG
o (ITIDA)	Organization.organizationName=ITIDA
Ou (RootCA)	OrganizationalUnit.organizationalUnitName=<cn attribute of the RootCA certificate>

cn
(Egypt_RootCA_G1)
	cACertificate=<All self-signed root certificates>
	cACertificateRevocationList=<Issued CRL By RootCA>

Table 12: Contents of the directory nodes

The directory information tree (DIT) of the X.500 directory is shown in the following figure.

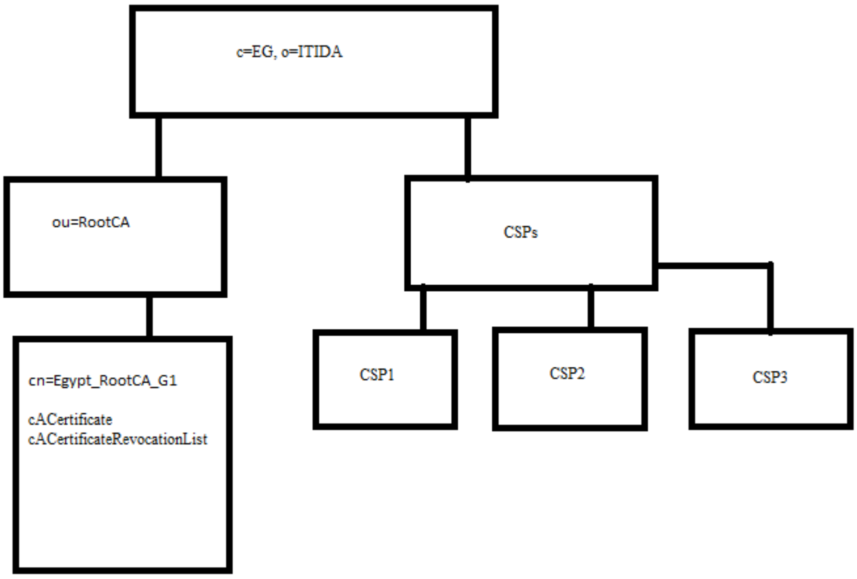

Figure 1: Directory information tree of LDAP directory

8 Compliance audit and other assessments

- Root CA succeeded in obtaining ISO 27001 certification.
- Internal compliance audit is performed on a regular basis.

8.1 Frequency or circumstances of assessment

One a year.

8.2 Identity/qualifications of assessor

The audits will be performed by an accredited ISO 27001 assessor appointed internal auditor (it could be from the licences department.

8.3 Assessor's relationship to assessed entity

The neutrality of the assessor is ensured by the standards and procedures for ISO 27001 certification from the licences department of ITIDA.

8.4 Topics covered by assessment

Subject to ISO 27001 audits is the complete information security management system. This comprises the technical infrastructure, processes, organisation and documentation of the Root-CA.

8.5 Actions taken as a result of deficiency

Any deficiencies will be removed without undue delay.

8.6 Communication of results

The success of the assessment will be announced at the Root-CA web site.

9 Reference

[1] Law No. 15 of the Year 2004, Regulating Electronic Signature (E-Signature) and Establishing the Information Technology Industry Development Agency (ITIDA). Official Journal – Issue No. 17 (Supplement-D), 2004.

[2] Executive directive of the Electronic Signature Law. Decree No. 109 of 2005, Ministry of Communications and Information Technology.

[3] Egyptian Root-CA – Certificate Policy. Version X, ITIDA, 2009.

[4] ANSI X9.62-1999, Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA). American Bankers Association, 1999.

[5] CEN Workshop Agreement (CWA) 14169, Secure Signature-Creation Devices "EAL 4+". European Committee for Standardization. 2002

[6] Common Criteria for Information Technology Security Evaluation. Version 2.0, Common Criteria Project Sponsoring Organisation, 1998.

[7] ETSI EN 319 411, Policy and security requirements for Trust Service Providers issuing certificates. European Telecommunications Standards Institute. Version 1.2.2, 2018.

[8] FIPS 180-4 , Secure Hash Standard. Federal Information Processing Standards Publication 180-4, U.S. Department of Commerce/N.I.S.T., National Information Service, August 2015.

[9] FIPS 186-4, Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-1, U.S. Department of Commerce/N.I.S.T., National Information Service, July 2013.

[10] Common ISIS-MTT Specifications for Interoperable PKI Applications – Part 1: Certificate and CRL Profiles, T7 and TeleTrust, Version 1.1, 2004.

[11] ISO/IEC 10118-3:2003, Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions. International Organization for Standardization, 2003.

[12] ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization, 2013.

[13] Information Technology Security Evaluation Criteria. Version 1.2, Office for Official RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Publications of the European Communities, November 2003.

[14] ITU-T Recommendation X.500 (2005), Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services. International Telecommunication Union, 2005

[15] ITU-T Recommendation X.501 (2005), Information technology – Open Systems Interconnection – The Directory: Models. International Telecommunication Union, 2005

[16] ITU-T Recommendation X.509 (2005), Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. International Telecommunication Union. 2005.

[17] PKCS#1: RSA Encryption Standard. RSA Laboratories. Version 2.1. 2002.

[18] PKCS#5: Password-Based Cryptography Standard. RSA Laboratories. Version 2.0, 1999.

[19] PKCS#7: Cryptographic Message Syntax Standard. RSA Laboratories. Version 1.5. 1993.

[20] PKCS#10: Certification Request Syntax Standard. RSA Laboratories. Version 1.7. 2000.

[21] RFC 6960, X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP. M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, June 2013.

[22] RFC 5652 and RFC 3370 and their updates RFC 5083, RFC 4853 RFC 3370 and RFC 5754 consequently , Cryptographic Message Syntax..

[23] RFC 3161 and its update RFC 5816, X.509 Internet Public Key Infrastructure – Time-Stamp Protocol (TSP). C. Adams, P. Cain, D. Pinkas, R. Zuccherato, 2001.

[24] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, 2003.

[25] RFC 4511, Lightweight Directory Access Protocol (LDAP): The Protocol. J. Sermersheim, ed. 2006.