Certificate Policy (CP)

Version 1.1

2021/03/04

Prepared by:

Information Technology Industry Development Agency

ITIDA

Contents

List of Figures`

1 Introduction

1.1 Overview

Pursuant to the Egyptian E-Signature Law and its Executive Regulation, ITIDA operates the Egyptian Root-CA, which issues certificates for certification service provider issuing digital certificates for electronic signatures and electronic seal. The Egyptian Root-CA serves as a trust anchor for all e-signatures based on 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 specifying the rules governing the issuance, management and usage of certificates in the Public Key Infrastructure (PKI) defined by the Egyptian Root-CA.

1.2 Document name and identification

1.3 PKI participants

The certification hierarchy of the Public Key Infrastructure (PKI) defined by the Egyptian Root-CA is shown in the following figure.

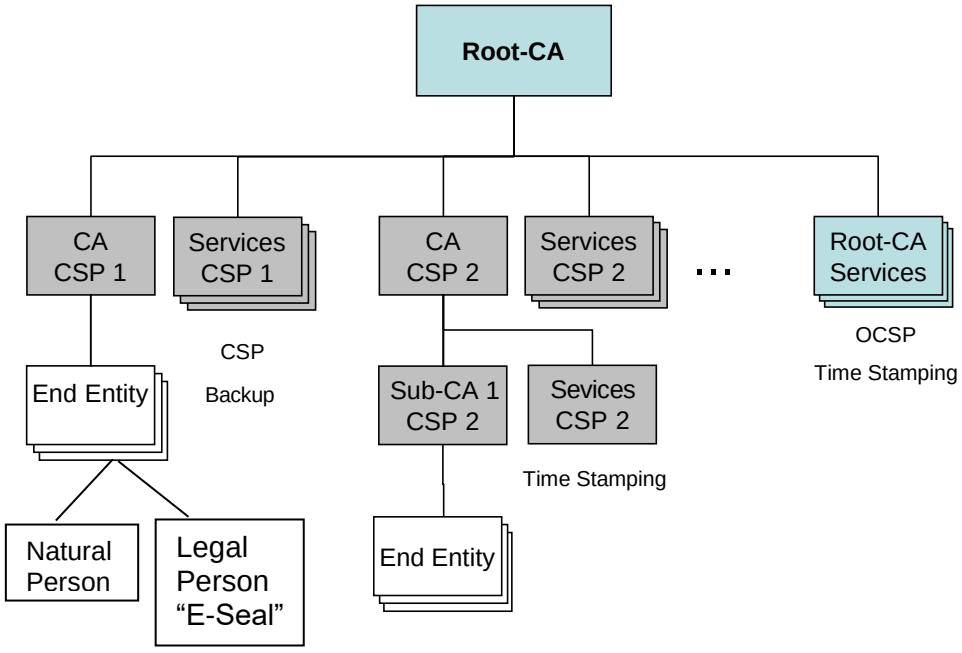

Figure 1: Certification hierarchy of the Root-CA

1.3.1 Certification authorities

In accordance with the E-Signature Law and its Executive Regulation, ITIDA operates a national root CA for Egypt. The Egyptian Root-CA constitutes the root node of the certification hierarchy and provides the trust anchors for e-signatures in Egypt.

1.3.2 Registration authorities

The Egyptian Root-CA only employs one Registration Authority (RA) which is also operated by ITIDA. Therefore, in this policy it is not distinguished between the Egyptian Root-CA and its RA.

1.3.3 Subscribers and subjects of the Egyptian Root-CA

In accordance with the E-Signature Law and its Executive Regulation, the Egyptian Root-CA issues certificates to all certification service provider (henceforth called CSP) issuing digital certificates for electronic signature and electronic Seal. In particular, the Egyptian Root-CA issues certificates to the CSPs for the following certificate services:

- Certification authorities, i.e. services issuing certificate for electronic signatures.
- CRL signers, i.e. services issuing certificate revocation list covering certificates for electronic signatures.
- OCSP responders, i.e. online status validation services based on OCSP covering certificates for electronic signatures.
- CSP backup transfer; these certificates are exclusively used for securely providing backups of data related to the issued certificates to the Root-CA.

A CSP **must** obtain certificates at least for their top level certification authorities (CAs) used to issue certificates for electronic signatures (see also section 1.3.4).

The Root-CA does not issue certificates to certification services that are not related to electronic signature/seal, i.e. for certification authorities issuing certificates for encryption or authentication, or CRL signers or OCSP services exclusively covering certificates for encryption or authentication.

In general, a CSP may provide several certificate services. In order to enable relying parties to distinguish between the individual certification services provided by the same CSP, the certificate holders specified in the certificates are not the CSP itself but the individual certification service. Therefore, the terms subscriber and subject are used in the following manner:

- The Subscribers are the CSPs.
- The Subjects are the certification services provided by the CSPs.

1.3.4 Sub-level certification services

The CSPs are not free to insert further levels in the certification hierarchy by implementing subordinated certification authorities (sub-CAs) and other certification services for electronic signature/Seal (see section 3) which obtain certificates from their own certification authorities. The Root-CA imposes limit for the depth of the certification paths and the hierarchy. However, the following restrictions apply:

- CSPs are not permitted to issue certificates to certification services which are not provided under their own responsibility, i.e. for certification services provided by other CSPs.
- Sub-CAs in the certification hierarchy defined by the Egyptian Root-CA must only issue certificates for electronic signature/seal or certification services for electronic signatures.
- Certification services using certificates within the certification hierarchy defined by the Egyptian Root-CA must provide services related to electronic signatures. However, the services may also deal with other purposes for certificates, e.g. provide revocation status also for encryption certificates.

1.3.5 Relying parties

Relying party can be any entity involved in a transaction based on electronic signature/seal and certificates or other certification services provided in Egypt.

1.3.6 End entities

The end entities (end user) are persons, companies, authorities, organizations, organization units, systems or services that obtain certificates for electronic signature/seal from a CSP and do not use these certificates to implement a certification service. In the certification hierarchy, end entities represent the leaf nodes.

The Egyptian Root-CA does not issue certificates to end entities.

1.4 Certificate usage and applicability

1.4.1 Certificate and key usage

All certificates issued under the certification hierarchy of the Egyptian Root-CA shall only be used in accordance with the following rules:

- Certificates issued to certification services and the corresponding keys shall only be used for the provision of the service that is explicitly specified in the certificate.
- Certificates issued to end entities and the corresponding keys shall only be used for the creation and verification of electronic signatures/seal.
- Certificates and keys must only be used in accordance with the Certificate Policy of the issuing CA.
- The usage of the keys must conform to the key usage specified in the certificate.
- Technically, the keys corresponding to the certificates shall only be used for the creation and verification of digital signature/seal.
- Private keys must not be used after expiry or revocation of the corresponding certificate.
- The validation of certificates shall be based on the self-signed CA certificates of the Root-CA as trust anchors. Revocation status shall be checked for all certificates except those of the revocation status information services of the Root-CA and the self-signed CA certificates of the Root-CA. If supported by the verifying party, online status checking should be used.

1.4.2 Legal significance

The certificates issued by the Egyptian Root-CA allow legal interpretations. In accordance with the E-Signature Law and its Executive Regulation, relying parties may conclude that electronic signature/seal that are valid under the certification hierarchy of the Egyptian Root-CA

- Satisfy the legal requirements of a signature in the same manner as a hand written signature.
- It admissible as evidence in legal proceedings.

1.5 Conformance

This Certificate Policy complies with the Egyptian E-Signature Law and its Executive Regulation, as well as with ETSI EN 319 411 and RFC 3647.

The present Certificate Policy is based on the Policy NCP+ specified in ETSI EN 319 411. The additional rules and provisions specified in section 2 do not violate conformity to this policy. However, some provisions set forth in clause 7.3.1 of ETSI EN 319 411 are not applicable to the Egyptian Root-CA, because ITIDA as the supervision authority for certification services in Egypt does not have a contractual relationship to the subscribers of the Root-CA. Instead, this relationship is only based on

the relevant legal norms, in particular, on the Egyptian E-Signature Law and its Executive Regulation.

1.6 Certification Practice Statement

This Certificate Policy is complemented by the Certification Practice Statement (CPS) of the Egyptian Root-CA. The CPS describes details on the practices that the Root-CA applies in issuing and maintaining certificates and which implement the rules and provisions set forth in the present Certificate Policy. The CPS of the Root-CA is available through the web site of the Root-CA (http://www.rootca.itida.gov.eg) or upon request (contact details are given in section 1.7).

Remark: The CPS is structured in accordance with RFC 3647 whereas the present CP is based on ETSI EN 319 411. Therefore, the CPS and the present CP do not share a common document structure..

1.7 Policy administration

The authority and responsibility for the maintenance, endorsement and issuance of this Certificate Policy rests with ITIDA.

1.7.1 Update Procedure

ITIDA will inform all CSPs and the public 3 months prior to any update of the Certificate Policy. New versions become effective with their publication at the Root-CA's web site:

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

Previous version will also be maintained at the web site for historical reasons.

1.7.2 Contact data

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

2 Additional provisions to ETSI EN 319 411

While the Certificate Policy of the Egyptian Root-CA is generally compliant with ETSI EN 319 411, the following additional provisions apply.

2.1 Additional rules for the Root-CA

In addition to the requirements set forth in sections 6of ETSI EN 319 411, the Egyptian Root-CA adhere to the following:

- It's organisation and operation must comply with the provisions of the Egyptian Electronic Signature Law and its Executive Regulation.
- The usage of its certificates and corresponding keys must comply with the provisions set forth in section 6.3.5.
- Eligibility of algorithms: The cryptographic algorithms, key lengths and parameters used for electronic signatures and respective certification services must be eligible for meeting the requirements of the Egyptian Electronic Signature Law and its Executive Regulation.
- Registration:
  - The identity and authorisation of the agents registering on behalf of the subscribing CSP is verified.
  - It is verified that the subject name allows unique identification of the subscribing CSP and the certification service.
  - It is verified that the cryptographic security of the public key for which the certificate is requested and of the related algorithms and parameters is sufficient for the certificate's intended lifetime.
- Certificate Issuance: Certificate renewal is not supported by the Root-CA, i.e. the Root-CA does not issue new certificates for a public key for which a certificate had already been issued.
- CSPs well generate their key pairs using their own devices and provide the public keys to the Root-CA.
- Certificate publication by the Root-CA: The subscribing CSPs can choose, whether the Egyptian Root-CA publishes its certificates.
- Key escrow: Any kind of key escrow is prohibited.

- Certificate suspension: Certificate suspension is prohibited, i.e. revocations must be irreversible.
- Records archiving: Records concerning certificates must be held for 30 years beginning from the time of its expiry or revocation.
- Must receive and maintain regular backups certificates issued by the CSPs, as ell as the corresponding status information and registration data.
- In case that a CSP ceases its operation, the Root-CA must take over the services necessary for using and validating the certificates issued by the CSP. Details are specified in the Certification Practice Statement of the Root-CA.

2.2 Additional rules for CSPs

The CSPs must adhere to the following:

- It must comply with the provisions of the Egyptian Electronic Signature Law and its Executive Regulation.
- In providing its certification services, it must comply with the provisions of section 6 of ETSI EN 319 411.
- It must integrate its certification services for electronic signatures into the certification hierarchy of the Egyptian Root-CA as defined in sections 1.3.3 and 1.3.4.
- The cryptographic algorithms, key lengths and parameters used for electronic signatures and respective certification services must be eligible for meeting the requirements of the Egyptian Electronic Signature Law and its Executive Regulation. The eligibility of algorithms and parameters is determined by ITIDA.
- The usage of its certificates and corresponding keys must comply with the provisions set forth in section 1.4.1.
- If the CSP applies for a certificate from the Root-CA without requesting the issuance of a smart card, it must provide the public key corresponding to the private key to be used for the respective certification service. In particular, the CSP must have possession of the corresponding private key, and the generation, storage and management of the key pair must conform to ETSI EN 319 411.
- When applying for a certificate at the Root-CA, CSPs must ensure that they possess all necessary rights to use the names requested. ITIDA does not take any responsibility for losses or claims to their subscribers or third parties resulting from unauthorised use of names and trademarks.
- The CSP must maintain a sufficient number of key pairs to ensure an availability of its services according to its business needs and to the Egyptian Electronic

Signature Law. ITIDA does not take any responsibility for damages or losses resulting from the loss or compromise of a CSP private key.

- The CSP is obliged to apply for a certificate **at least 4 weeks before it is needed**. In particular, the CSP must apply
  - for its initial certificates at least 4 weeks before the corresponding certification services are supposed to start, and
  - for a new certificate (certificate re-key or certificate modification) at least 4 weeks before the old certificate expires.
- If a CSP fails to meet this requirement, the Root-CA does not take any responsibility for losses resulting from a delayed issuance of the certificate.
- The validity of certificates issued by CSPs must not exceed the validity of the issuer's certificate.
- The CSP may support certificate renewals, i.e. may issue new certificates for public keys for which it had already issued a certificate. However, for this process the following rules apply:
  - The CA must ensure that the private key corresponding to the public key is still under sole control of the subject and is maintained and used in accordance with all applicable rules, in particular with the Egyptian Signature Law, the present certificate policy and the certificate policy of the issuing CA.
  - The CA must ensure that the algorithm and parameters associated with the key pair (in particular the key length) conforms to all applicable rules (see above) and is expected to provide sufficient security throughout the lifetime of the new certificate.
  - At any time, only one certificate must exist for a public key, i.e. the old certificate for that public key have been revoked before the new certificate is issued.
  - The old certificate for this public key must had been issued by the same CA.
- Any kind of key escrow of private keys used for electronic signatures is prohibited. This rule applies to the private keys corresponding to the certificates issued by the Root-CA to the CSPs as well as to the private keys corresponding to the certificates issued by the CSPs.
- Suspension of certificates issued by the CSPs is prohibited, i.e. revocations must be irreversible.
- The CSP must provide regular data backups of certificate related data to the Root-CA. The data must be provided in compliance with the specifications defined by the Root-CA.

- The CSP must notify ITIDA duly before it ceases its operation to allow a take over its services. The CSP must support ITIDA in the take over.

3 Definitions and acronyms

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 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).
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. 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 signatures. 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.
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.
Electronic Signature	Electronic data logically associated with other electronic data which serves as a method for authentication.
End Entity	An entity in a PKI that does not issue certificates.
Issuer	The CA which has signed the certificate
ITIDA	Information Technology Industry Development

	Agency
OCSP	Online Certificate Status Protocol, standard specified in RFC 2560 for the interactive retrieval of certificate status information
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
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)
Trust Anchor	The public key (or certificate) which is a priori trusted by an entity (the relying party). The certificates of a root CA are supposed to be used as trust anchors.

4 References

[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 – Certification Practice Statement, Version 1.1, ITIDA, 2021.

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

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

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

[7] 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.