# Dubai Electronic Security Center

# Dubai PKI

## Dubai Government entity issuing CA Certificate Policy

| | |
|---|---|
| **Project** | DESC CA Project |
| **Title** | Dubai Government entity issuing CA Certificate Policy |
| **Classification** | PUBLIC |
| **File Name** | Dubai PKI - Dubai Government entity issuing CA - Certificate Policy_v1.1 |
| **Created on** | 22 August 2017 |
| **Revision** | 1.1 |
| **Modified on** | 25 February 2018 |

# Document History

| Date | Revision | Author(s) | Summary |
|---|---|---|---|
| 11 September 2017 | 0.1 | | Initial version |
| 12 September 2017 | 0.2 | | Minor modifications & Incorporation of Dubai government entity Root CA option |
| 3 November 2017 | 0.3 | | Minor modifications to reflect control environment |
| 11 January 2018 | 0.4 | | Update certificate profiles and naming conventions |
| 30 January 2018 | 1.0 | | Issue final version |
| 25 April 2018 | 1.1 | | Update publication of certificate information |

# Table of contents

# 1. Introduction

This Certificate Policy (CP) defines the requirements applicable to Dubai Government Entity Subordinate Certification Authorities, referred to as "Dubai Government entity issuing CAs". Dubai Government Entities operate these subordinate CAs for issuing end-entity certificates to their subscribers.

The Dubai PKI Policy Authority (PA), which is composed of appointed members of the DESC management and DESC PKI team, is representing the policy and governing body for the Dubai PKI, including Dubai Government Entity subordinate CAs. This board is referred to in this CP document as the PA.

The PKI certification services shall be offered by Dubai Government Entities in accordance with the present CP and a dedicated Certification Practice Statement (CPS) for each Subordinate CA.

## 1.1 Overview of Dubai PKI

DESC manages a PKI referred to as the "Dubai PKI" that uses standard PKI technologies, policies and operating procedures, and application interfaces. The Dubai PKI comprises the Dubai Root CA that is the trust anchor of this PKI, which comes at the first level of the PKI hierarchy. The Dubai PKI also comprises two subordinate Certification Authorities (CAs), which come at the second level of the PKI hierarchy. Certification services provided by this PKI enable citizens, residents and government entities in Dubai to conduct secure electronic transactions; this includes securing the machine-to-machine communication, where devices can transact securely, leveraging the PKI signing and encryption capabilities.

Additionally, the Dubai Root CA also issues subordinate CAs belonging to other Dubai government entities. Such entities have their own custom needs and reasons to implement their own CAs rather than using a DESC-operated subordinate CAs.

CAs belonging to other Dubai government entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai Root CA. There are two options for issuing these CAs: Option 1 is to directly issue a Dubai Government entity issuing CA from the Dubai Root CA, which is a technically constrained subordinate CA[1] owned and operated by a Dubai Government entity. Option 2 is for entities requiring more scalable hierarchy, met by issuing them two hierarchical levels of subordinate CAs – an unconstrained Dubai Government entity Root CA that comes directly under the Dubai Root CA, and a technically constrained Dubai Government entity issuing CA(s) that comes under the Dubai Government entity Root CA.

Dubai Government Entities willing to have their own subordinate CA(s) –according to any of the above mentioned options, shall request approval from the Dubai PKI Policy Authority.

Unconstrained Dubai government entity Root CAs are operated by DESC and managed in accordance with the Dubai Root CA Certification Practice Statement.

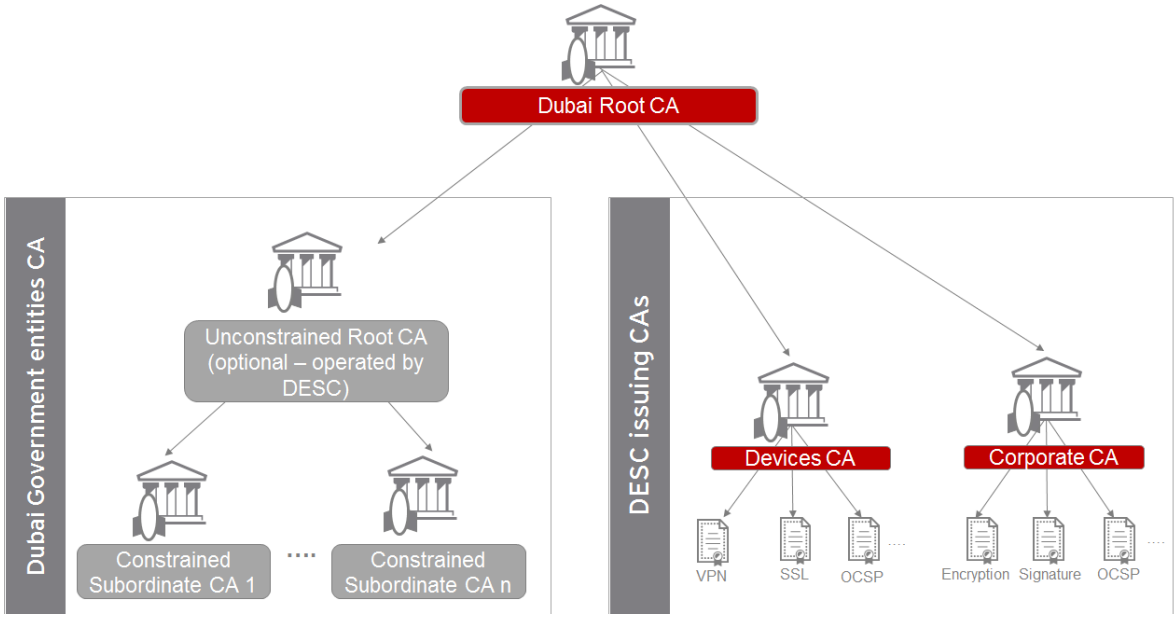
The constrained Dubai Government entity issuing CAs are managed and operated by the owning Dubai government entity, which is responsible for defining its own set of policies and practices (CPS) aligned with this Certificate Policy.

[1] *A Subordinate CA with a certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates*

The Dubai Government entity issuing CAs are established and operated by the owning Dubai Government entities once authorized by DESC. These entities are the authority that has final responsibility in providing certification services under the supervision of the Dubai PKI PA, i.e., issuing and managing end-entity certificates for entities forming its community of subscribers.

## 1.1.1 Dubai PKI Hierarchy

The below Figure depicts the Trust Model of the Dubai PKI. The Dubai Root CA is the top authority in this PKI with regard to the digital certification services offered in Dubai. The Dubai Root CA signs DESC Subordinate CAs, which come at the second level of the PKI hierarchy. In addition, the Root CA also signs subordinate CAs belonging to authorized Dubai government entities.




*Trust Model for Dubai PKI*

## 1.1.2 Certification Services

The certification services to be offered by the Dubai Government Entity issuing CAs are broken down in this document as follows:

- **Registration service:** Verifies the identity and, if applicable, any specific attributes of end-entities applying for certificates. The results of this service are passed to the certificate generation service.
- **Certificate generation service:** Creates and signs end-entity certificates based on the verification conducted by the registration service.
- **Dissemination service:** Disseminates the end-entity certificates and makes them available to relying parties. This service also makes available any public policy and practice information to subscribers and relying parties.
- **Revocation management service:** Processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the certificate validity status service.
- **Certificate validity status service:** Provides certificate validity status information to relying parties. This shall be based upon certificate suspension/revocation lists. The status information shall always reflect the current status of the certificates issued by Dubai Government Entity issuing CAs.

# 1.2 Document name and Identification

This document is named 'Dubai PKI - Certificate Policy for Dubai Government entity issuing CA' and is referenced as such in related documents.

The Object Identifier (OID) of this document is 2.16.784.1.2.2.100.1.1.2.2.

# 1.3 PKI Participants

The participants within the context of Dubai Government Entity issuing CAs shall be as follows:

- Dubai Government entity Issuing CA
- Registration Authority (RA)
- Subscribers
- Relying Parties

These participants and their roles are described in the following sections.

## 1.3.1 Dubai Government Entity Issuing CA

The Dubai Government entity issuing CAs are owned and operated by the corresponding authorized Dubai Government entities. Each entity is required to maintain a Certification Practice Statement, implementing this Certificate Policy, in which it defines the practices and/or other requirements applicable to its certification activities. This CPS is subject to approval by the Dubai PKI PA.

Approval activities consist of evaluation of the policies and procedures defined by the certification authority, including but not limited to:

- The certification authority hierarchy and certificate types
- Processes and controls in place to maintain logical, physical and environmental security
- Cryptographic modules used to generate, store and manage crypto keys

The certification activities of Dubai Government Entity issuing CAs shall conform to the rules and requirements as stated in this policy document, compliance audit requirements and requirements of the applicable agreements.

DESC requires the application of technical constraints on the Dubai Government entities issuing CAs to restrict the issuance of digital certificates, through a combination of Path Lengths, Extended Key Use and Name Constraints or alternative constraints.

The Dubai Government Entity is responsible for informing DESC in at least the following cases:

- Significant changes to its certification authority environment
- Incidents, termination or compromise related to the certification activities

The key responsibilities of the Dubai Government Entity with regard to operation of issuing CAs are as follows:

- Management of certificates, including but not limited to all aspects related to application, issuance and revocation
- Identification and authentication of subscriber information according to the applicable certificate profile requirements

- Publication of public certificates to a public repository
- Maintaining and providing certificates status information through publicly available Certificate Revocation List (CRL) and OCSP mechanisms

These CAs supports the following pre-defined certificate types for issuance:

- Device certificates non-SSL certificates for general identification, authentication or session data encryption of generic devices owned or operated by Dubai Government Entities
- End-user certificates: certificates for encryption, authentication and digital signatures for individuals

### 1.3.2 Registration Authority

The Dubai Government Entity shall set up an RA organization for its issuing CA. The RA shall comprise the individuals and systems involved in validating the identity of individuals requesting certificates, as well as in issuing and managing these certificates.

### 1.3.3 Subscribers

Subscribers of the Dubai Government Entity issuing CA must be listed within the Certification Practice Statement for the given CA.

For any certificate, the subscriber shall sign a subscriber agreement, agreeing on the terms and conditions as set forth by the Dubai Government Entity.

### 1.3.4 Relying Parties

A Relying Party is any entity within Dubai that processes a digital certificate issued by the Dubai Government Entity issuing CAs.

### 1.3.5 Other Participants

There are no other participants within the context of the Dubai Government Entity issuing CAs.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Use

Use of certificates issued from the Dubai Government Entity issuing CAs is restricted by using certificate extensions on key usage and extended key usage, which will be configured according to the certificate type. The CPS of each respective issuing CA shall specify the restrictions that apply to each type of certificate. The agreement between DESC and the Dubai Government entity will specify the types of end-entity certificates allowed to be issued by the Dubai Government entity.

### 1.4.2 Prohibited Certificate Use

Certificate use is restricted by using certificate extensions on key usage and extended key usage. Any usage of the certificate inconsistent with these extensions or with the contents of this CP and applicable CPS is unauthorized.

# 1.5 Policy Administration

## 1.5.1 Organization Administering the Document

DESC, through the Dubai PKI PA, bears the responsibility for the drafting, publishing, OID registration, maintenance, and interpretation of this CP and other policies and practices within the realm of the Dubai PKI.

This PA is composed of appointed members of the DESC management and DESC PKI team. This PA shall be the highest-level management body with final authority and responsibility for:

a. Specifying and approving the Dubai PKI infrastructure

b. Approving Dubai government entity applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy

c. Specifying, maintaining and approving the Dubai PKI practices and policies, in particular, the Certification Practice Statements (CPS) and the related Certificate Policies (CP) when applicable

d. Defining the review process for such practices and policies, including responsibilities for maintaining the Dubai PKI CP/CPSs and related policies

e. Defining the review process that ensures that the Dubai PKI properly implements the above practices

f. Defining the review process that ensures the Dubai PKI CP and CPSs support the related policies

g. Publication of CP and CPSs and its revisions

h. Specifying installation, key ceremonies, operation and life cycle management (including deprecation) procedures of the Dubai PKI

i. Evaluating the proper working of the Dubai PKI environment

j. Allocating members to the key ceremonies as witness, as well as trusted operatives and key custodians

k. Evaluating of changes to the Dubai PKI environment (management, operational, hardware, software and security)

l. Evaluating case-by-case issues where key DESC staff/personnel did not respect the security and/or operational procedures, including ethics

m. Deciding on critical issues in case of incidents, disasters and other severe problems with regard to the Dubai PKI

## 1.5.2 Contact Details

The Dubai PKI Policy Authority can be contacted at the following address:

***Dubai PKI Policy Authority***

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97142512538

E-mail pa@desc.gov.ae

DESC accepts comments regarding this CPS only when they are addressed to the PA.

### 1.5.3 Person Determining CPS Suitability for the Policy

The Dubai PKI PA determines the suitability of any CPS for this CP.

### 1.5.4 CP Approval Procedures

A dedicated process involves the PA reviewing the initial version of this CP and any subsequent updates. Amendments shall either be in the form of a document containing an amended form of the CP or an update notice. The PA formally approves the new version of the CP.

# 1.6 Definitions, Acronyms and References

## 1.6.1 Terminology and definitions

The following sections contain the definitions of terms and acronyms. The source of a definition is cited when available.

**Activation data —** Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected, for example, a PIN, a password or pass-phrase, or a manually held key share.

**CA —** Certification Authority

**CA certificate —** A certificate for one CA's public key issued by another CA

**CCTV —** Closed Circuit TV

**Certificate Policy (CP) —** A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

**Certification Practice Statement (CPS) —** A statement of the practices that a certification authority employs in issuing, certificates

**CRL —** Certificate Revocation List

**DRP —** Disaster Recovery Plan

**DN —** Distinguished Name

**FIPS —** Federal Information Processing Standards

**HSM —** Hardware Security Module — a device designed to provide cryptographic functions especially the safekeeping of private keys

**HTTP —** Hyper Text Transfer Protocol

**HVAC —** Heating, Ventilation and Air Conditioning

**IEC —** International Electro-technical Commission

**IETF —** Internet Engineering Task Force

**IPSEC —** Internet Protocol Security

**ISO —** International Standards Organization

**Issuer —** The name of the CA that signs the certificate

**ITU —** International Telecommunications Union

**KGC —** Key Generation Ceremony, the complex procedure for the generation of a CA's private key

**LDAP —** Lightweight Directory Access Protocol — a common standard for accessing directories

**DESC —** Dubai Electronic Security Centre

**OID —** Object Identifier — A value (distinguishable from all other such values) which is associated with an object. (ITU-T X680) Referenced in many RFCs and used in the ASN.1 encoding of certificates

**OSCP —** Online Certificate Status Protocol

**PA —** Policy Authority

**PKCS # 1 —** Public Key Cryptography Standards (PKCS) #1

**PKCS # 7 —** Cryptographic Message Syntax

**PKCS #10 —** Certification Request Syntax Specification

**PKCS #12 —** Personal Information Exchange Syntax published by RSA Security

**PKE —** Public Key Encryption

**PKI —** Public Key Infrastructure

**PKIX-CMP —** Internet X.509 Public Key Infrastructure — Certificate Management Protocol

**Policy qualifier —** Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate

**RA —** Registration Authority

**Re-key —** Ceasing use of a key pair and then generating a new key pair to replace it

**Relying party —** A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate

**Renewal —** Issuance of a new certificate to the subscriber without changing the subscriber's public key or any other information in the certificate

**Repository —** A trustworthy system for storing and retrieving certificates or other information relevant to certificates

**RSA —** The acronym for the inventors of the RSA algorithm — Ron Rivest, Adi Shamir and Leonard Adleman

**Secret Shares —** A set of devices, smart cards, PINs etc. used with MofN control

**SHA —** Secure Hash Algorithm

**S/MIME —** Secure Multipurpose Internet Mail Extensions

**SSL/TLS —** Secure Sockets Layer/Transport Layer Security

**Sponsor —** An individual or organization, authorized to vouch for another individual in their employment, or an electronic device in their control

**subjectAltName —** A certificate attribute field that often contains the subject's email address

**Subject —**The entity named in a certificate

**Subscriber —** A subject who is issued a certificate

**Trusted Role —** Those individuals who perform a security role that is critical to the operation or integrity of a PKI

**UPS —** Uninterruptible Power Supply

**URI —** Universal Resource Identifier, a URL, FTP address, email address, etc.

**X.501 —** A common standard for directory entry naming (ITU)

**X.509 —** A public key certificate specification originally developed as part of the X.500 directory specification, often used in public key systems. It is now governed by IETF standards

### 1.6.2 Acronyms

Please refer to section 1.6.1.

### 1.6.3 References

The present CP endorses the following standards:

- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- AICPA/CPA Canada Trust Service Principles and Criteria for Certification Authorities
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
- CA/B Forum Network and Certificate System Security Requirements

# 2. Publication and Repository Responsibility

## 2.1 Repositories

DESC retains an online repository of documents where it makes certain disclosures about the practices, procedures and content of certain of its policies, including the present CP. It reserves its right to make available and publish information on its policies by any means it sees fit.

DESC publishes a copy of this CP at this location. This CP is updated at the least, annually. DESC reserves its rights to publish certificate status information on third-party repositories.

The Dubai Government Entity shall publish and maintain the applicable CPS and certificate information about all digital certificates they issue through its Subordinate CA, in (an) online publicly accessible Certificate Dissemination Webpage as defined in the applicable CPS.

## 2.2 Publication of Certificate Information

The Dubai Government Entity shall publish a copy of the issuing CA certificates and retain an online repository where it makes certain disclosures about the practices, procedures and content of certain of its policies.

The Dubai Government Entity shall publish digital certificate status information in frequent intervals as indicated in this CP. The provision of the issued electronic certificate validity status information is a 24/7 available service.

The Dubai Government Entity shall operate the certificate status repository for its Subordinate CAs.

## 2.3 Time or Frequency of Publication Repositories

Due to their sensitivity, the Dubai Government Entity shall refrain from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the functioning of registration authorities, internal security polices, etc. Such documents and documented practices shall, however, conditionally available to designated authorized parties in the context of audit(s) that Dubai Government Entity owes duty to with regard to its CA activities.

### 2.3.1 Certificates

Dubai Government Entity issuing CA and OCSP certificates shall be published to the public repository once they are issued.

### 2.3.2 CRLs

The Dubai Government Entity shall publish CRLs at regular intervals and add a pointer (URL) to the relevant CRL to subscribers' certificates as part of the CDP extension whenever this extension is present.

The Dubai Government Entity shall maintain the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL for a minimum of seven years after the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the repository are uploaded within 24 hours.

The following rules shall apply for the CRL issued by the Dubai Government Entity issuing CAs:

- At the minimum, CRLs shall be refreshed every 24 hours, even if no changes have occurred since the last issuance.
- CRLs lifetime shall be set to 26 hours (24 hours update period + 2 hours pre-update period).

## 2.4 Access Controls on Repositories

Public read-only access to the CPS, certificates and CRLs published to the repository shall be available.

Access controls shall be implemented on the repository to prevent any unauthorized addition or modification of any published data.

# 3. Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

The certificates issued by the Dubai Government Entity issuing CA shall contain X.500 Distinguished Names (DNs) in English. The table below summarizes the DN formats allowed for certificates issued by the Dubai Government Entity issuing CA.

| Certification Authority | Distinguished name |
|---|---|
| **Dubai Government Entity issuing CA**<br><br>CA DN: cn=<Dubai Government Entity certification authority name>, l=<Dubai Government locality name>, s=Dubai, o=<Dubai Government entity meaningful unique name>, ou=<Dubai Government Entity organizational unit>, c=AE | • ***Device certificates (non-SSL):*** *The DN format is:*<br><br>*cn = <System unique common name> or<device external IP address>, ou = <optional organizational unit within the Dubai Government Entity>, o = <Dubai Government entity meaningful unique name>, l = <Dubai Government entity locality name>, s = Dubai , c = AE*<br><br>• ***End user certificates:*** *The DN format is:*<br><br>*cn=<individual unique name>, ou = <optional organizational unit within the Dubai government entity>, o = <Dubai government entity meaningful unique name>, l = <Dubai Government entity locality name>, s = Dubai, c = AE*<br><br>• ***OCSP Responder***<br><br>*cn = < Dubai Government Entity certification authority OCSP responder name>, ou= <optional organizational unit within the Dubai Government Entity>, o = <Dubai Government entity meaningful unique name>, l = <Dubai Government entity locality name>, s = Dubai, c = AE* |

### 3.1.2 Meaningful Names

All end-entity certificates issued by the Dubai Government Entity issuing CA shall be meaningful and uniquely identify the subject.

### 3.1.3 Anonymity and Pseudonymity of Subscribers

This policy does not permit anonymous subscribers.

### 3.1.4 Rules for Interpreting Various Name Forms

No stipulation — this section is intentionally left blank.

### 3.1.5 Uniqueness of Names

The Dubai Government Entity shall enforce the controls necessary to guarantee that subject Distinguished Name (DN) are unique. The table below summarizes the minimum controls enforced.

| Distinguished Name |
| --- |
| For certificates issued to end users, the Dubai Government Entity shall enforce a convention for a meaningful representation uniquely identifying the individual. |
| Certificates issued to devices shall uniquely identify the device. Options could be to use the registered public DNS name or public IP address. |

### 3.1.6 Recognition, authentication and role of Trademarks

No stipulation — this section is intentionally left blank.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

The Dubai Government Entity RA shall enforce submission of a Proof-of-Possession of the private key as part of certificate requests. A possible implementation would be to rely on certificate requests containing a Proof-of-Possession (e.g., PKCS#10, PKIX-CMP).

### 3.2.2 Authentication of individual identity

The Dubai Government Entity RA shall validate the identity of the certificate applicant, the association between the applicant and the organization and, if applicable, the association between the applicant and the subject.

### 3.2.3 Authentication of Domain name

No stipulation — this section is intentionally left blank.

### 3.2.4 Non-verified subscriber information

All subscriber information contained within certificate issued by the Dubai Government Entity issuing CA shall be verified by the Dubai Government Entity RA.

### 3.2.5 Validation of Authority

No stipulation — this section is intentionally left blank.

### 3.2.6 Criteria for Interoperation

No stipulation — this section is intentionally left blank.

# 3.3 Identification and Authentication for Re-keying requests

## 3.3.1 Identification and Authentication for Routine Re-Keying

Identification and authentication steps for Routine Re-Key shall be the same as applied during initial certification.

## 3.3.2 Identification and Authentication for Re-Key after revocation

Identification and authentication steps for Re-Key after revocation shall be the same as applied during initial certification.

# 3.4 Identification and Authentication for Revocation Requests

The Dubai Government Entity RA shall enforce identification and authentication for revocation requests. The RA shall validate the revocation request and the identity of the revocation request applicant.

# 4. Certificate Life Cycle Management

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

Certificate application shall be limited to applicants associated to the Dubai Government Entity. Further details shall be specified in the applicable CPS.

### 4.1.2 Enrolment Process and Responsibilities

For anyk requested certificate, the certificate applicant shall sign a dedicated subscriber agreement. Further details on the enrollment process shall be specified in the applicable CPS.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

Refer to section 3.2 of this CP.

| **Acceptance/rejection of certificate applications** |
|---|
| The RA of the Dubai Government Entity shall validate the identity of the applicant and confirm if he is authorized to receive PKI credentials from the Dubai Government Entity. If all verifications by RA are successful, the RA accepts the certificate application. The RA enrolls the individual to the PKI, and issues related PKI credentials and certificates. |
| For any issued Devices Certificate, the Dubai Government Entity RA shall validate the identity of the certificate applicant who needs to proof ownership of the device. The Dubai Government Entity RA shall then enroll the infrastructure device and issue related digital certificate. |

### 4.2.2 Approval or Rejection of Certificate Applications

The Dubai Government entity RA shall validate the identity of the certificate applicant. The RA then accepts the certificate application, enroll the end-entity and issue related digital certificate.

For further details, please refer to the applicable CPS.

### 4.2.3 Time to Process Certificate Applications

No stipulation — this section is intentionally left blank.

# 4.3 Certificate Issuance

The Dubai Government Entity shall process a certificate issuance request as follows:

- Verify that the certificate request originated from a valid RA
- Issue the required digital certificates that contain the information provided in the certificate request
- If applicable, publish the issued certificates on the Dubai Government Entity public repository

For further details, please refer to the applicable CPS.

## 4.3.1 CA Actions during Certificate Issuance

Refer to the applicable CPS.

## 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Refer to the applicable CPS.

# 4.4 Certificate Acceptance

## 4.4.1 Conduct Constituting Certificate Acceptance

It shall be possible for the applicant to verify that the issued certificates contain the required data. For further details, please refer to the applicable CPS.

## 4.4.2 Publication of the Certificate by the CA

The CA may publish the issued certificates on the dissemination page as described in section 2.2.

## 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation — this section is intentionally left blank.

# 4.5 Key Pair and Certificate Usage

## 4.5.1 Subscriber Private Key and Certificate Usage

In using a subscriber's private keys and corresponding certificates, a subscriber shall adhere to the following obligations:

- Use certificates only for their intended usage as per this CP and the related CPS
- Discontinue using a private key following expiration or revocation of the corresponding certificate
- Notify the CA or RA in the event of private key compromise.

## 4.5.2 Relying on Party Public Key and Certificate Usage

When using a subscriber's public key and corresponding certificate, a relying party shall adhere to the following obligations:

- Ensure that the key is appropriate for the intended use as set forth in this CP and that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage and certificate policies extension fields
- Check the status of the certificate against the appropriate and current CRLs.

# 4.6 Certificate Renewal

Certificate Renewal is the act of issuing a new certificate when all the identifying information and the public key from the old certificate are duplicated in the new certificate, but there is a different (longer) validity period.

Certificate Renewal shall not be supported. Only certificate re-key is supported.

# 4.7 Certificate Re-key

Certificate Re-key involves re-issuing a certificate for an existing subscriber such that identifying information from the old certificate is duplicated in the new certificate, with a different public key and validity period.

Re-key is an operation supported by the provisions of this CP. The re-key process (including identity validation, issuance) shall be similar to the initial certification.

## 4.7.1 Circumstance for Certificate Re-key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation. The re-key operation shall invalidate any existing active certificates of the same type.

## 4.7.2 Who May Request Certification of a New Public Key

As per initial certificate issuance

## 4.7.3 Processing Certificate Re-keying Requests

As per initial certificate issuance

## 4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance

## 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As per initial certificate issuance

## 4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certificate issuance

## 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate issuance

# 4.8 Certificate Modification

This CP does not provide provisions for certificate modification outside the context of certificate re-key, which results in the generation of a new certificate with the same identification information. Refer to section 4.7 of this CP for further details.

## 4.8.1 Circumstance for Certificate Modification

Not applicable beyond the normal certificate re-key operation

## 4.8.2 Who May Request Certificate Modification

Not applicable beyond the normal certificate re-key operation

## 4.8.3 Processing Certificate Modification Requests

Not applicable beyond the normal certificate re-key operation

## 4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable beyond the normal certificate re-key operation

## 4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable beyond the normal certificate re-key operation

## 4.8.6 Publication of the Modified Certificate by the CA

Not applicable beyond the normal certificate re-key operation

## 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable beyond the normal certificate re-key operation

# 4.9 Certificate Revocation and Suspension

## 4.9.1 Circumstances for Revocation

| **Circumstances for revocation** |
|---|
| The RA of the Dubai Government Entity shall revoke digital certificates corresponding to his organization when required by the organization internal processes or under the following circumstances:<br>o The subscriber discovers or has reason to believe that there has been a compromise of the corresponding private keys.<br>o The subscriber no longer requires the keys and certificates.<br>o The information in the certificates is no longer accurate and requires to be changed. |

This CP does not provide provisions for revoking an OCSP certificate apart from the compromise of the OCSP key pair which shall be considered by The Dubai Government Entity as per its disaster recovery and business continuity procedures. The following sub-sections focus only on the revocation provisions that apply for end-user and device certificates issued by The Dubai Government Entity issuing CA.

### 4.9.2 Who Can Request Revocation

Refer to section 4.9.1.

Only authorized revocation requests shall be accepted.

For further details, please refer to the applicable CPS.

### 4.9.3 Procedure for Revocation Request

Refer to the applicable CPS.

### 4.9.4 Revocation Request Grace Period

There shall be no revocation grace period. Revocation requests shall be processed as per schedule or immediately by the RA.

### 4.9.5 Revocation Request Response Time

Certification revocation requests and problem reports shall be processed within 24 hours.

### 4.9.6 Revocation Checking Requirement for Relying Parties

Revocation information is offered to relying parties through CRLs published on a publicly available repository or through its OCSP responder. Relying parties shall use any of these methods while processing a certificate issued by a Dubai Government entity subordinate CA.

### 4.9.7 CRL Issuance Frequency

CRLs are issued as per section 2.3 of this CP.

### 4.9.8 Maximum Latency for CRLs

No stipulation — this section is intentionally left blank.

### 4.9.9 Online Revocation/Status Checking Availability

An OCSP responder is offered compliant with RFC 6960. OCSP information is available immediately to relying party applications.

The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by a Dubai government entity issuing CA.

### 4.9.10 Online Revocation Checking Requirements

It is at the discretion of the relying party to decide whether to use CRL or rely on OCSP.

### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation — this section is intentionally left blank.

### 4.9.12 Special Requirements — Key Compromise

No stipulation — this section is intentionally left blank.

### 4.9.13 Circumstances for Suspension

Certificate suspension shall not be supported by the Dubai Government Entity issuing CA.

### 4.9.14 Who Can Request Suspension

Not applicable

### 4.9.15 Procedure for Suspension Request

Not applicable

### 4.9.16 Certificate Status Services

Refer to section 4.9.6 of this CP.

### 4.9.17 Operational Characteristics

CRLs shall be published by the Dubai Government Entity issuing CA on a public repository which is available to relying parties through HTTP protocol queries.

The OCSP responders shall expose an HTTP interface accessible to relying parties.

### 4.9.18 Service Availability

The repository, including the latest CRL, should be available 24X7 for at least 99% of the time.

### 4.9.19 Optional Features

No stipulation — this section is intentionally left blank.

## 4.10 End of Subscription

No stipulation — this section is intentionally left blank.

## 4.11 Key Escrow and Recovery

### 4.11.1 Key Escrow and Recovery Policy and Practices

Key escrow shall not be supported by the Dubai Government Entity issuing CA.

### 4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation — this section is intentionally left blank.

# 5. Facility, Management and operational Controls

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

All critical components of the PKI solution shall be housed within a highly secure enclave within a Dubai Government Entity facility. Physical access controls shall be in place to protect the infrastructure, management systems and related operational activities of the PKI solution.

### 5.1.2 Physical Access

Physical security controls shall include security guard-controlled building access, man traps, biometric IRIS access and Closed Circuit TV (CCTV) monitoring. These physicals controls must protect the hardware and software from unauthorized access and shall be monitored on a 24x7x365 basis.

### 5.1.3 Power and Air Conditioning

The secure enclave shall be furnished with a UPS, and heating ventilating and air conditioning (HVAC) sufficient to maintain the computer equipment within the manufacturers' recommended range of operating temperatures and humidity.

### 5.1.4 Water Exposures

The PKI solution shall be installed in such a way that it is not in danger of exposure to water.

### 5.1.5 Fire Prevention and Protection

The enclave shall be protected from fire and heat by smoke detection equipment that is monitored on a 24x7x365 basis. Fire suppression equipment shall be installed within the enclave.

### 5.1.6 Media Storage

Electronic optical and other media shall be stored so that they are protected from accidental damage (water, fire, electromagnetic radiation). Media that contains audit archives and backup information shall be stored in a secure fire-proof safe while it is stored within the enclave.

### 5.1.7 Waste Disposal

All obsolete paper, magnetic media, optical media, etc., created within the enclave shall be shredded before discarding. Reusable magnetic and optical media may be reused indefinitely within the enclave, but must be properly wiped and/or destroyed depending on the confidentiality of the data stored on the medium.

### 5.1.8 Offsite Backup

System backups must provide sufficient recovery information to allow the recovery from system failure(s). Backups shall be made on a daily basis and copies shall be transferred to a secure offsite location on a periodic basis.

Backup media shall be stored in a location separate from the Dubai Government Entity main site. Facilities used for offsite backup and archives shall have the same level of security as the Dubai Government Entity's main site.

## 5.2 Procedural Controls

The Dubai Government Entity shall follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

The Dubai Government Entity shall obtain a signed statement from each member of the staff concerned on not having conflicting interests with the CA activities, maintaining confidentiality and protecting personal data.

### 5.2.1 Trusted Roles

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives).

The Dubai Government Entity shall conduct an initial investigation of all members of staff who are candidates, to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

### 5.2.2 Number of Persons Required Per Task

The Dubai Government Entity shall maintain and enforce rigorous control procedures to ensure the segregation of duties, based on job responsibility, in order to prevent single trusted personnel to perform sensitive operations.

The most sensitive tasks, such as access to and management of CA cryptographic hardware security module (HSM) shall require the involvement of two or more persons.

### 5.2.3 Identification and Authentication for Each Role

Before exercising the responsibilities of a trusted role:

- The Dubai Government Entity shall confirm the identity of the employee by carrying out background checks.
- The Dubai Government Entity shall issue an access card to administrators who need to access equipment located in the secure enclave.
- The Dubai Government Entity shall provide the necessary credentials that allow administrators to conduct their functions.

### 5.2.4 Roles Requiring Separation of Duties

The Dubai Government Entity shall ensure separation among the following discreet work groups:

- Personnel managing operations on certificates
- Administrative personnel who operate the supporting platform
- Security personnel who enforce security measures.

## 5.3 Personnel Controls

The Dubai Government Entity shall ensure implementation of security controls with regard to the duties and performance of the members of its staff with regards to the CA activities. These security controls shall be documented in an internal confidential policy and include the areas below.

### 5.3.1 Qualifications Experience and Clearance Requirements

The Dubai Government Entity shall ensure that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such background checks include:

- Criminal convictions for serious crimes
- Misrepresentations by the candidate
- Appropriateness of references
- Any clearances as deemed appropriate

### 5.3.2 Background Check Procedures

The Dubai Government Entity shall make the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

### 5.3.3 Training Requirements

The Dubai Government Entity shall make available relevant technical training for their personnel to perform their functions.

For personnel performing information verification duties (i.e., RA officers), public key infrastructure topics, authentication and vetting policies and procedures, applicable CP and CPS material and common threats to the information verification process are included.

The required skills and knowledge for validation specialists shall be tested through an examination on the information verification requirements outlined in the Baseline Requirements.

### 5.3.4 Retraining Frequency and Requirements

Periodic training shall be carried out to maintain skills and knowledge levels, and to update the training topics and related procedures.

### 5.3.5 Job Rotation Frequency and Sequence

The Dubai Government Entity shall establish a job rotation schedule for its team staff, consistent with the need to provide continuity of the PKI service and avoid dependency on key staff members.

### 5.3.6 Sanctions for Unauthorized Actions

The Dubai Government Entity shall sanction personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the Dubai Government Entity personnel, as it might be appropriate under the circumstances, and as per the prevailing HR policy and country law.

### 5.3.7 Independent Contractor Requirements

Independent Dubai Government Entity issuing CA component services subcontractors and their personnel are subject to the same background checks as Dubai Government Entity employees. The background checks include:

- Criminal convictions for serious crimes
- Misrepresentations by the candidate
- Appropriateness of references
- Any clearances as deemed appropriate
- Privacy protection
- Confidentiality conditions

### 5.3.8 Documentation Supplied to Personnel

The Dubai Government Entity shall make available documentation to personnel, during initial training and retraining.

## 5.4 Audit Logging Procedures

Details on the audit logging procedures shall be defined in the applicable CPSs. The following provisions are made in this CP.

### 5.4.1 Types of Event Recorded

Following events occurring on the Dubai Government Entity issuing CA shall be recorded:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival and destruction
  - Cryptographic device life cycle management events
- CA and Subscriber Certificate life cycle management events, including:
  - Certificate requests, re-key requests, and revocation
  - All verification activities stipulated in these requirements and the CA's Certification Practice Statement
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls
  - Acceptance and rejection of certificate requests
  - Issuance of Certificates
  - Generation of Certificate Revocation Lists and OCSP entries

- Security events, including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activities
  - Entries to and exits from the CA facility

In addition, the Dubai Government Entity shall maintain internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers
- Outages and major problems
- Physical access of personnel and other persons to sensitive parts of the Dubai Government Entity issuing CA site
- Backup and restore
- Report of disaster recovery tests
- Audit inspections
- Upgrades and changes to systems, software and infrastructure
- Security intrusions and attempts at intrusion
- Other documents that are required for audits include:
  - Infrastructure plans and descriptions
  - Physical site plans and descriptions
  - Configuration of hardware and software
  - Personnel access control lists

### 5.4.2 Frequency of Processing Log

The Dubai Government Entity shall ensure that the designated personnel reviews log files at regular intervals in order to validate log integrity and ensure timely identification of anomalous events. Designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity.

Log files and audit trails shall be periodically archived for inspection by authorized the Dubai Government Entity personnel and designated auditors. The log files shall be properly protected by an access control mechanism, so that no others can have access. Log files and audit trails shall be backed up.

All log entries include the following elements:

- Date and time of entry
- Identity of the person making the journal entry
- Description of the entry

### 5.4.3 Retention Period for Audit Log

The audit log files shall be retained online for three months, after which they may be archived.

### 5.4.4 Protection of Audit Log

Audit logs shall be protected by a combination of physical and procedural security controls. The CA shall generate a message authentication code for each audit log file it keeps.

### 5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the Dubai Government Entity issuing CA audit log:

- Backup media shall be stored locally in the Dubai Government Entity's main site in a secure location.
- A second copy of the audit log data and files shall be stored outside Dubai Government Entity's main site, in a site that provides similar physical and environmental security as the main site.

### 5.4.6 Audit Collection System (internal vs. external)

No stipulation — this section is intentionally left blank.

### 5.4.7 Notification to Event-causing Subject

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

### 5.4.8 Vulnerability Assessments

Dubai Government Entity issuing CA systems shall be subject to an annual assessment in line with DESC system assurance policy and this CP.

## 5.5 Records Archival

The Dubai Government Entity shall keep records of the following items:

- All certificates for a period of a minimum of seven years after the expiration of that certificate
- Audit trails on the issuance of certificates for a period of a minimum of seven years after issuance of a certificate
- Audit trail of the revocation of a certificate for a period of a minimum of seven years after revocation of a certificate
- CRLs for a minimum of seven years after publishing

The CA shall retain the very last back up of the archive for seven years following the issuance of the last certificate.

The Dubai Government Entity shall archive audit logging data on a regular basis and keep archived data in a retrievable format.

The Dubai Government Entity shall ensure the integrity of the physical storage media and implement proper backups to prevent data loss.

Archives shall be accessible to authorized personnel of the Dubai Government Entity.

### 5.5.1 Types of Records Archived

The Dubai Government Entity shall retain in a trustworthy manner records of digital certificates, audit data, systems information and documentation. The Dubai Government Entity shall ensure that at least the following records are archived:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival and destruction
  - Cryptographic device life cycle management events
- CA and Subscriber Certificate life cycle management events, including:
  - Certificate requests, re-key requests, and revocation
  - All verification activities stipulated in these requirements and the CA's Certification Practice Statement
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls
  - Acceptance and rejection of certificate requests
  - Issuance of Certificates
  - Generation of Certificate Revocation Lists and OCSP entries
- Security events, including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed
  - Security profile changes
  - System crashes, hardware failures, and other anomalies
  - Firewall and router activities
  - Entries to and exits from the CA facility

### 5.5.2 Retention Period for Archive

The Dubai Government Entity shall retain in a trustworthy manner, records of digital certificates for a term as indicated under article 5.5 in this CP.

### 5.5.3 Protection of Archive

Records are archived in such a way that they cannot be deleted or destroyed. Controls are in place to ensure that only authorized personnel is able to manage the archive without modifying integrity, authenticity and confidentiality of the contained records.

### 5.5.4 Archive Backup Procedures

A full backup of records as stipulated in the previous sections shall be taken at each key ceremony.

### 5.5.5 Requirements for timestamping of Records

All recorded events shall include the date and time of when the event took place, based on the time of the operating system. Procedures shall be in place to ensure that all systems rely on and are synchronized with a trusted time source.

### 5.5.6 Archive Collection System (internal or external)

Only authorized and authenticated staff shall be allowed to handle archived material.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Only Dubai Government Entity staff members with a clear hierarchical control and a definite job description may obtain and verify archived information. The Dubai Government Entity shall retain records in electronic or paper-based format.

## 5.6 Key Changeover

Dubai Government Entity issuing CA private keys shall be maintained until such time as all relying certificates have expired.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

In a separate internal document, the Dubai Government Entity shall specify applicable incident, compromise reporting and handling procedures. The Dubai Government Entity shall specify the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

### 5.7.2 Computing Resources, Software and/or Data Corruption

The Dubai Government Entity and all other PKI Participants (other than Subscribers and Relying Parties) shall establish the necessary measures to ensure full recovery of the CA services in case of a disaster, and corrupted servers, software or data.

The Dubai Government Entity shall establish:

- Disaster recovery resources in a location sufficiently distant from the regular Dubai Government Entity issuing CA operation facility
- Fast communications between the two sites to ensure data integrity

Disaster recovery infrastructure and procedures shall be fully tested at least once a year.

### 5.7.3 Entity Private Key Compromise Procedures

For Subscribers key compromise, see section 4.9 of the present CP.

In the event of a key compromise of a Dubai Government Entity issuing CA, the following actions shall be taken by the Dubai Government Entity:

- The Dubai PKI Policy Authority shall be notified as soon as there is an indication of suspected compromise. The Dubai government entity shall work together with DESC on deciding whether to continue CA activities or cease operations.
- All active certificates issued by the CA shall be revoked.
- Organizations holding end-entity certificates shall be notified.
- A CA compromise notice shall be published toward relevant relying parties.

### 5.7.4 Business Continuity Capabilities after a Disaster

The Dubai Government Entity shall establish the necessary measures to full and automatic recovery of the online services, such as CRL availability in case of a disaster, and corrupted servers, software or data.

The Dubai Government Entity shall establish the necessary measures to ensure full recovery of the offline services service in case of a disaster, and corrupted servers, software or data.

A Business Continuity Plan shall be implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document. The business continuity plan shall include the following:

1. Conditions for activating the plan
2. Emergency procedures
3. Fallback procedures
4. Resumption procedures
5. Maintenance schedule for the plan
6. Awareness and education requirements
7. The responsibilities of the individuals
8. Recovery time objective (RTO)
9. Regular testing of contingency plans
10. The plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken
14. The distance of recovery facilities to the main site
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site

## 5.8 CA or RA Termination

If the Dubai Government Entity determines that termination of its PKI and CA services are deemed necessary, it shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

Notification procedures shall exist for informing affected entities and transferring archived CA records to an appropriate custodian. The Dubai Government Entity shall arrange for the retention of archived data specified in section 5.5 of this CP, taking into account the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate.

# 6. Technical Security Controls

## 6.1 Key Pair Generation and Installation

The requirements for generating and installing the Dubai Government Entity issuing CA are stated in the following sections.

### 6.1.1 Key Pair Generation

#### 6.1.1.1 CA Key Pair Generation

CA key pairs shall be generated within the memory of an HSM certified to the level required by this CA operation (at minimum FIPS 140-2 Level 3).

#### 6.1.1.2 Subscriber Key Pair Generation

Sufficient security shall be maintained during the subscriber key generation process and delivery of these keys and corresponding certificate to the subscriber. Cryptographic algorithms shall be approved by FIPS and specified in FIPS 186-4.Private Key Delivery to Subscriber

The generated key pair shall be encrypted with a passcode provided by the subscriber and keys shall be delivered using a secure communication channel. Public Key Delivery to Certificate Issuer

Public keys shall be delivered to subscribers through the use of delivery processes (e.g. PKCS#10 through e-mail or media exchange) and key management protocols (e.g., XKMS, PKIX CMP, SCEP …).

### 6.1.2 CA Public Key Delivery to Relying Parties

The Dubai Government Entity issuing CA should make its certificates available to subscribers and relying parties by publishing them in a public repository.

### 6.1.3 Key Sizes

The Dubai Government Entity issuing CA key pair shall be at least 4096 bit RSA.

Subscriber keys shall be at least 2048 bit RSA, recommended 4096 bit RSA or at least 256 bit ECDSA, recommended 384 bit ECDSA.

### 6.1.4 Public Key Parameters Generation and Quality Checking

The Dubai Government Entity issuing CA shall rely on off-the-shelf implementation of key PKI functionality including public key parameters generations (in accordance with standards, such as PKCS#10).

### 6.1.5 Key Usage Purposes (as per X.509 v3 key usage field)

Certificates issued by the Dubai Government Entity issuing CA should always contain a key usage bit string in accordance with RFC 5280.

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

The Dubai Government Entity shall generate subordinate key pairs and store their private keys within a HSM that is certified according to the rating specified in 6.2.11.

### 6.2.2 Private Key Multi-Role Control

The Dubai Government Entity shall implement technical and procedural mechanisms that implement the principles of dual control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with CAs cryptographic hardware.

### 6.2.3 Private Key Escrow

Not applicable

### 6.2.4 Private Key Backup

The Dubai Government Entity issuing CA private keys shall be backed up within backup tokens that meet the same certification level as the CA HSM and as described in section 6.2.1.

The creation of key backups on backup tokens shall be conducted using the principles of dual controls and split knowledge, involving at least two PKI officers. At least one backup of the CA keys shall be taken. This backup shall be stored in a locked safe at the disaster recovery site.

### 6.2.5 Private Key Archival

Not applicable.

### 6.2.6 Private Key Transfer Into or From a HSM

The Dubai Government Entity issuing CA key pairs shall only be transferred to another hardware cryptographic token of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control.

At no time shall the CA private key be copied to disk or other media during this operation.

### 6.2.7 Private Key Storage on Cryptographic Module

No further stipulation other than those stated in 6.2.1.

### 6.2.8 Method of Activating Private Key

Private keys for the Dubai Government Entity issuing CA shall be activated by a minimum of two privileged users using the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the CA HSM.

Subscribers are responsible for activating and protecting their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

### 6.2.9 Method of Deactivating Private Key

Private keys for the Dubai Government Entity issuing CA shall be deactivated in situations such as:

- There is a power failure within the CA room.
- The CA HSM is operated outside the range of supported temperatures.
- The HSM detects a security breach and deletes all key material within its internal memory.

When private keys are deactivated, they shall be cleared from memory before the memory is de-allocated and shall be kept in encrypted form only. Any disk space where keys were stored shall be over-written before the space is released to the operating system.

### 6.2.10 Method of Destroying Private Key

At the end of their lifetime, taking into account business purpose and legal obligations, the Dubai Government Entity issuing CA private keys shall be destroyed by multi-person presence, in order to ensure that these private keys cannot ever be retrieved and used again.

### 6.2.11 Cryptographic Module Rating

The Dubai Government Entity shall use an HSM certified to FIPS 140-2 Level 3 or ISO 15408 Common Criteria (CC) EAL 4+ or above.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

Refer to section 5.5 of this CP.

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

- The maximum operational period of the CA's key pair shall be set for eight years. Periodic re-key and notice requirements must be defined to avoid disruption of CA services.
- The maximum operational period for a subscriber's key pair shall generally be five years unless otherwise specified in the applicable CPS.

# 6.4 Activation Data

## 6.4.1 Activation Data Generation and Installation

### 6.4.1.1 CA Key Generation

The Dubai Government Entity issuing CA's activation data shall correspond to PIN and passwords that are used to activate HSMs hosting CA keys. CA keys and their activation data shall be generated in accordance with the requirements of section 6.2, using security tokens for the protection of the CA's private key.

During the key generation ceremony of a Dubai Government Entity issuing CA, trusted individuals (key custodians) shall receive their activation data. These shall be managed according to section 6.2 of this CP.

### 6.4.1.2 Subscribers keys

The Dubai Government Entity shall register its subscribers prior to issuing digital certificates to the subscribers.

The enrolment of a subscriber shall result in activation data being randomly generated by the CA. This activation data shall be securely delivered to the subscriber, who will use it to apply for digital certificates.

## 6.4.2 Activation Data Protection

Activation data for subscribers shall be generated randomly. Any activation data shall be bound to one subscriber only and shall have a limited lifetime. Activation data shall be transmitted securely to the subscriber.

## 6.4.3 Other Aspects of Activation Data

No stipulation — this section is intentionally left blank.

# 6.5 Computer Security Controls

The Dubai Government Entity issuing CA shall perform all CA and RA functions using trustworthy systems that meet DESC security and audit requirements.

## 6.5.1 Specific Computer Security Technical Requirements

The Dubai Government Entity issuing CA shall be operated according to the following security controls:

- Physical access control to the CA servers shall be enforced
- Separation of duties and dual controls for CA sensitive operations
- Identification and authentication of PKI roles and their associated identities
- Archival of CAs history and audit data
- Audit of security-related events
- Automatic and regular validation of the CA systems' integrity

- Recovery mechanisms for keys and CA systems
- Hardening CA servers' operating system according to best practices and PKI vendor requirements
- Network protection, including intrusion detection systems

### 6.5.2 Computer Security Rating

No stipulation — this section is intentionally left blank.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

Applications shall be tested, developed and implemented in accordance with industry best practice development and change management standards.

Purchased hardware or software shall be shipped or delivered in a sealed or shrink-wrapped container and be installed by trained personnel.

### 6.6.2 Security Management Controls

The hardware and software used to set up the Dubai Government Entity issuing CA shall be dedicated to performing only CA-related tasks. There shall be no other applications, hardware devices, network connections or component software, which are not part of the Dubai PKI, connected to or installed on CA hardware.

The Dubai Government Entity issuing CA and RA functionality shall be scanned for malicious code on first use and periodically afterward.

Upon installation, and at least once a week, the integrity of the Dubai Government Entity issuing CA databases shall be validated.

### 6.6.3 Life Cycle Security Controls

No stipulation — this section is intentionally left blank.

## 6.7 Network Security Controls

The Dubai Government Entity shall ensure maintenance of network security, including managed firewalls and intrusion detection systems.

The network shall be segmented into several zones, based on their functional, logical and physical relationship. Network boundaries shall be applied to limit the communication between systems (within zones) and communication between zones, with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations, disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

Issuing Systems, Certificate Management Systems, and Security Support Systems shall be maintained and protected in at least a Secure Zone.

## 6.8 Time-stamping

The CA servers' internal clock shall be synchronized using Network Time Protocol.

# 7. Certificate, CRL profiles

## 7.1 Certificate Profile

The CRL profile must comply with the requirements of RFC 5280.

At least the following subject fields shall be included in the certificate profile:

- CountryName
- OrganizationUnitName
- OrganizationName
- LocalityName
- StateOrProvinceName
- CommonName

For further details, please refer to the applicable CPS.

### 7.1.1 Version Number

The Dubai Government Entity issuing CA shall issue X.509 version 3 certificates as defined in RFC 5280.

### 7.1.2 Certificate Extensions

Certificates require at least the use of the following extensions. For the complete profile, refer to the applicable CPS.

- Certificate policies (not critical)
  - Policy identifier
  - Policy qualifiers
    - Policy qualifier ID
- cRL distribution points (not critical)
- Authority information access (not critical)
  - URL of the issuing CA's OCSP responder
  - URL of the issuing CA's certificate
- Key usage (not critical)
- Extended key usage (critical)
- Authority key identifier (not critical)

The values allowed for the key usage and extended key usage field depend on the type of certificate:

| Certificate type | Key Usage | Extended Key Usage |
|---|---|---|
| Device certificate (non-SSL) | • digitalSignature<br>• nonRepudiation<br>• keyEncipherment | • clientAuth |
| End-user certificate | • digitalSignature<br>• nonRepudiation<br>• keyEncipherment | • clientAuth<br>• emailProtection |

### 7.1.3 Algorithm Object Identifiers

X.509v3 standard OIDs shall be used. Algorithm shall be RSA encryption for the subject key and SHA256 with RSA encryption for the certificate signature.

### 7.1.4 Name Forms

As per the naming conventions and constraints listed in section 3.1 of this CP.

### 7.1.5 Name Constraints

As per the naming conventions and constraints listed in section 3.1 of this CP.

### 7.1.6 Certificate Policy Object Identifier

Refer to the ASN1 definitions described in the below subsections.

### 7.1.7 Usage of Policy Constraints Extension

No stipulation — this section is intentionally left blank.

### 7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation — this section is intentionally left blank.

### 7.1.9 Processing Semantics for Critical Certificate Extensions

Critical extensions, when marked, shall be interpreted by relying parties correctly.

## 7.2 CRL Profile

The version field in the certificate shall state 1, indicating X.509v2 CRL.

The CRL profile must comply with the requirements of RFC 5280.

For further details, please refer to the applicable CPS.

### 7.2.1 Version Number(s)

The version field in the certificate states 1, indicating X.509v2 CRL.

### 7.2.2 CRL and CRL Entry Extensions

The CRL extensions shall contain the CRL number (a sequential number incremented with each new CRL produced).

## 7.3 OCSP Profile

The OCSP profile must comply with the requirements of RFC 6960.

OCSP response signing certificates must the use of the following extensions:

- Key usage (not critical)
- Authority key ID (not critical)
- Extended key usage (critical)
- OCSP no check (not critical)

For further details, please refer to the applicable CPS.

# 8. Compliance Audit and Other Assessments

DESC reserves the right to organize compliance audits in order to ensure Dubai Government entities meet the requirements, standards, procedures and service levels according to this CP and other controls agreed upon between DESC and the Dubai Government entity. The Dubai PKI PA evaluates the results of such audits and will define the required measures that should be taken by the Dubai Government entity in order to rectify the situation and ensure compliance.

If the proposed measures are not timely and sufficiently implemented by the Dubai Government entity, DESC may decide to cancel the agreement and revoke the respective Dubai Government entity issuing CA(s).

# 9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of certificates issued by the CAs implementing this CP as described in this section.

## 9.1 Fees

Refer to the applicable CPS.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

This CP contains no financial limits on the use of certificates issued by the certificates managed under policy. Rather, entities, acting as relying parties, shall determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

### 9.2.2 Other Assets

Not applicable.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

## 9.3 Confidentiality of Business Information

Provisions relating to the treatment of confidential information that PKI Participants may communicate to each other, and in particular relating to the scope of what is considered as information within or not within the scope of confidential information, to the responsibility to protect confidential information, and to disclosure conditions, are ruled by private agreements with the Dubai Government Entity and DESC.

The Dubai Government Entity and DESC guarantee the confidentiality of any data not published in the certificates issued by the CAs implementing this CP, according to the applicable laws on privacy.

# 9.4 Privacy of Personal Information

The Dubai Government Entity shall observe personal data privacy rules and confidentiality rules as described in this CP. Confidential information includes:

- Any personal identifiable information of citizens, other than that contained in a certificate
- Exact reason for the revocation of a certificate
- Audit trails
- Logging information for reporting purposes, such as logs of requests by the RA
- Correspondence regarding services

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

The Dubai Government Entity does not release or is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the Dubai Government Entity owes a duty to keep information confidential with regards to its activities. It owes such a duty to the RA and promptly responds to any such requests
- A court order

Both confidential and non-confidential information can be subject to data privacy rules if the information contains personal data. For further information on the processing of personal data by Dubai Root CA, please consult The Dubai Root CA privacy policy.

Parties requesting and receiving confidential information are granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third-parties.

Also, these parties are bound to observe personal data privacy rules in accordance with the law.

The Dubai Government Entity will respect all applicable privacy, confidential information, and trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention and disclosure of non-public information.

Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- The status of a single certificate is provided per inquiry by a subscriber or relying party
- A subscriber can consult non-confidential information The Dubai Government Entity holds about it in the context of the Dubai PKI activities

Confidential information will not be disclosed by the Dubai Government Entity to subscribers or relying parties with the exception of information about:

- Themselves
- Persons in their custody

Only the RA is permitted to access confidential information.

The Dubai Government Entity properly manages the disclosure of information to the Dubai PKI personnel.

The Dubai Government Entity authenticates itself to any party requesting the disclosure of information by:

- Presenting an authentication certificate at the request of the citizen or relying party
- Signing CRLs and delta CRLs

All communications of confidential information are encrypted, including:

- The communications link between The Dubai Government Entity and the RA.
- Sessions to deliver certificates and certificate status information

Next to the information retained by the Dubai Government Entity, information pertaining to the subscribers' certificates can also be retained by the RA.

# 9.5 Intellectual Property Rights

The Dubai Government Entity and DESC own and reserve all intellectual property rights associated with its own databases, web sites, the CAs' digital certificates and any other publication whatsoever originating from the Dubai PKI including this CP.

When the Dubai Government Entity or DESC use software from suppliers, it is possible that this software remains intellectual property of the supplier. This is defined in the license agreement of contract of this supplier.

# 9.6 Representations and Warranties

DESC uses this CP to convey legal conditions of usage of certificates to subscribers and relying parties.

DESC warrants to the Subject, Subscriber, Relying parties and all Application Software Suppliers with whom DESC has entered into a contract for inclusion of its Certificate in software distributed by such Application Software Suppliers

# 9.7 Disclaimers of Warranties

Within the limitations of the laws of DESC cannot be held liable (except in case of fraud or deliberate abuse) for:

- Profit loss
- Loss of data
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant or if it is the result of negligence or with intent to deceive DESC or any person receiving or relying on the certificate
- Any liability incurred as a result of the applicant breaking any laws applicable in Dubai, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- Other damage

## 9.8 Limitations of Liability

DESC does not offer any guarantees or warranties, or enter into agreements that could be the subject of performance penalties, that could lead to legal actions on behalf of subscribers or relying parties.

## 9.9 Indemnities

Not applicable.

## 9.10 Term and Termination

This CP remains in force until notice of the opposite is communicated by DESC on its document repository (see Chapter 2 “Publication and Repository Responsibilities”).

Notified changes are appropriately marked by an indicated version. Changes are applicable [30] days after publication.

## 9.11 Individual Notices and Communications with Participants

Notices related to this CP can be addressed to DESC contact address as stated in section 1.5.

## 9.12 Amendments

Minor changes to this CP that do not materially affect the assurance level are indicated by version number that contains a decimal number, e.g., version 1.1 for a version with minor changes as opposed to, e.g., version 2.0 that addresses major issues.

Minor changes to this CP do not require a change in the CP OID or the CP pointer qualifier (URL) that might be communicated by DESC. Major changes that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the CP OID or CP pointer qualifier (URL).

## 9.13 Dispute Resolution Procedures

All disputes associated with this CP will be in all cases resolved according to the laws of Dubai

## 9.14 Governing Law

The laws of Dubai shall govern the enforceability, construction, interpretation and validity of the present CP.

## 9.15 Compliance with Applicable Law

The present CP is compliant to relevant, and applicable laws of Dubai.

# 9.16 Miscellaneous Provisions

DESC incorporates by reference the following information in all digital certificates it issues:

- Terms and conditions in this CP
- The mandatory elements of applicable standards
- Any non-mandatory, but customized elements of applicable standards
- Content of extensions and enhanced naming not addressed elsewhere
- Any other information that is indicated to be so in a field of a certificate

To incorporate information by reference, DESC uses computer-based and text-based pointers that include URLs and OIDs.

# 9.17 Other Provisions

Not applicable.