



# Dubai Electronic Security Center

## Dubai PKI

### Corporate CA

## Certification Practice Statement

**Project** DESC CA Project

**Title** Corporate CA, Certification Practice Statement

**Classification** PUBLIC

**File Name** DubaiPKI-CorporateCA-CertificationPracticeStatement\_v1.61

**Created on** 18 May 2017

**Revision** 1.61

**Modified on** 13 July 2021

# Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1	Khawla Hassan	Initial version
12 September 2017	0.2	Khawla Hassan	Minor modifications & Incorporation of Dubai government entity Root CA option
3 November 2017	0.3	Khawla Hassan	Minor modifications to reflect control environment
11 January 2018	0.4	Khawla Hassan	Update certificates profiles
18 January 2018	0.5	Khawla Hassan	Second revision of certificates profile
30 January 2018	1.0	Khawla Hassan	Issue final version
25 February 2018	1.1	Khawla Hassan	Update publication of certificate information
16 October 2018	1.2	Khawla Hassan	<ul style="list-style-type: none"><li>• Updates based on regular review, in addition to explicitly documenting the email verification practice for certificates issued for email protection.</li><li>• Expand Dubai PKI services to cover an extended set of UAE government entities and documenting the relevant certificate management practices.</li></ul>
07 August 2019	1.3	Khawla Hassan	<ul style="list-style-type: none"><li>• Added contact and high-level procedure of Certificate Problem Report</li><li>• Aligned the circumstances of revocation with the BRs</li></ul>
3 June 2020	1.4	Khawla Hassan	<ul style="list-style-type: none"><li>• Updates based on regular review and addressing Mozilla Comments</li></ul>
26 November 2020	1.5	Khawla Hassan	<ul style="list-style-type: none"><li>• Depreciate the authentication certificate profile</li></ul>

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

			<ul style="list-style-type: none"><li>• Add new profile to replace deprecated profile section 7.1.1.4</li></ul>
18 February 2021	1.51	Khawla Hassan	<ul style="list-style-type: none"><li>• Add manual registration process for UAE PASS</li></ul>
11 April 2021	1.6	Khawla Hassan	<ul style="list-style-type: none"><li>• Annual review and updates to address Mozilla comments and clarify subordinate CAs governance and operating environment</li></ul>
13 July 2021	1.61	Khawla Hassan	<ul style="list-style-type: none"><li>• Add user authentication certificate profile (for natural persons)</li><li>• Increase the CRL lifetime to 72 hours</li></ul>

## Table of Contents

Document History .....	2
<b>1. Introduction .....</b>	<b>10</b>
<b>1.1 Overview of Dubai PKI.....</b>	<b>10</b>
1.1.1 Dubai PKI hierarchy .....	11
1.1.2 Certification services.....	12
1.1.3 Certificate Policy.....	12
1.1.4 Relationship Between the Corporate CA CP and this CPS .....	12
<b>1.2 Document name and identification .....</b>	<b>12</b>
<b>1.3 PKI participants.....</b>	<b>13</b>
1.3.1 Policy Authority (PA).....	13
1.3.2 Subordinate Certification Authorities.....	14
1.3.3 Registration Authorities.....	14
1.3.4 Local Registration Authority.....	15
1.3.5 Subscribers .....	15
1.3.6 Relying Parties .....	15
1.3.7 Other participants .....	15
<b>1.4 Certificate usage .....</b>	<b>15</b>
1.4.1 Appropriate certificate use.....	16
1.4.2 Prohibited certificate use.....	16
<b>1.5 Policy administration .....</b>	<b>16</b>
1.5.1 Organization administering the document .....	16
1.5.2 Contact details.....	17
1.5.3 Person determining CPS suitability for the policy.....	17
1.5.4 CPS approval procedures .....	17
<b>1.6 Definitions, acronyms and references .....</b>	<b>17</b>
1.6.1 Terminology and definitions.....	17
1.6.2 Acronyms .....	19
1.6.3 References.....	19
<b>2. Publication and repository responsibility.....</b>	<b>21</b>
<b>2.1 Repositories .....</b>	<b>21</b>
<b>2.2 Publication of certificate information.....</b>	<b>21</b>
<b>2.3 Time or frequency of publication repositories.....</b>	<b>21</b>
<b>2.4 Access controls on repositories .....</b>	<b>22</b>
<b>3. Identification and authentication.....</b>	<b>23</b>
<b>3.1 Naming .....</b>	<b>23</b>
3.1.1 Types of name.....	23
3.1.2 Meaningful names.....	23
3.1.3 Anonymity and pseudonymity of subscribers.....	23
3.1.4 Rules for interpreting various name forms.....	23
3.1.5 Uniqueness of names .....	24
3.1.6 Recognition, authentication and role of trademarks .....	24
<b>3.2 Initial identity validation .....</b>	<b>24</b>
3.2.1 Method to prove possession of private key.....	24

**Certification Practice Statement**

3.2.2	Authentication of Government entity identity .....	24
3.2.3	Authentication of individual identity .....	24
3.2.4	Non-verified subscriber information.....	25
3.2.5	Validation of authority.....	26
3.2.6	Criteria for interoperation.....	26
<b>3.3</b>	<b>Identification and authentication for re-keying requests.....</b>	<b>26</b>
3.3.1	Identification and authentication for routine re-keying .....	26
3.3.2	Identification and authentication for re-key after revocation.....	26
<b>3.4</b>	<b>Identification and authentication for revocation request.....</b>	<b>26</b>
<b>4.</b>	<b>Certificate Life Cycle Management.....</b>	<b>28</b>
<b>4.1</b>	<b>Certificate application .....</b>	<b>28</b>
4.1.1	Who can submit a certificate application .....	28
4.1.2	Enrolment process and responsibilities .....	28
<b>4.2</b>	<b>Certificate application processing .....</b>	<b>34</b>
4.2.1	Performing identification and authentication functions .....	34
4.2.2	Approval or rejection of certificate applications.....	34
4.2.3	Time to process certificate applications.....	34
<b>4.3</b>	<b>Certificate issuance.....</b>	<b>34</b>
4.3.1	CA actions during certificate issuance.....	34
4.3.2	Notification to the subscriber by the CA of issuance of certificate.....	35
<b>4.4</b>	<b>Certificate acceptance.....</b>	<b>36</b>
4.4.1	Conduct constituting certificate acceptance.....	36
4.4.2	Publication of the certificate by the CA.....	36
4.4.3	Notification of certificate issuance by the CA to other entities.....	36
<b>4.5</b>	<b>Key pair and certificate usage.....</b>	<b>36</b>
4.5.1	Subscriber private key and certificate usage .....	36
4.5.2	Relying party public key and certificate usage.....	36
<b>4.6</b>	<b>Certificate renewal.....</b>	<b>37</b>
<b>4.7</b>	<b>Certificate Re-key .....</b>	<b>37</b>
4.7.1	Circumstance for Certificate Re-key.....	37
4.7.2	Who may request certification of a new public key.....	37
4.7.3	Processing Certificate Re-keying requests.....	37
4.7.4	Notification of new certificate issuance to subscriber .....	37
4.7.5	Conduct constituting acceptance of a re-keyed certificate.....	37
4.7.6	Publication of the Re-keyed Certificate by the CA .....	37
4.7.7	Notification of certificate issuance by the CA to other entities.....	37
<b>4.8</b>	<b>Certificate modification .....</b>	<b>38</b>
4.8.1	Circumstance for certificate modification.....	38
4.8.2	Who may request certificate modification.....	38
4.8.3	Processing certificate modification requests.....	38
4.8.4	Notification of new certificate issuance to subscriber .....	38
4.8.5	Conduct constituting acceptance of modified certificate .....	38
4.8.6	Publication of the modified certificate by the CA.....	38
4.8.7	Notification of certificate issuance by the CA to other entities.....	38
<b>4.9</b>	<b>Certificate revocation and suspension .....</b>	<b>38</b>
4.9.1	Circumstances for revocation .....	38
4.9.2	Who can request revocation.....	39
4.9.3	Procedure for revocation request.....	40

**Certification Practice Statement**

4.9.4	Revocation request grace period .....	41
4.9.5	Revocation request response time.....	41
4.9.6	Revocation checking requirement for relying parties.....	41
4.9.7	CRL issuance frequency .....	42
4.9.8	Maximum latency for CRLs .....	42
4.9.9	Online revocation/status checking availability.....	42
4.9.10	Online revocation checking requirements.....	42
4.9.11	Other forms of revocation advertisements available .....	42
4.9.12	Special requirements – Key compromise .....	42
4.9.13	Circumstances for suspension.....	42
4.9.14	Who can request suspension .....	42
4.9.15	Procedure for suspension request .....	42
<b>4.10</b>	<b>Certificate Status Services .....</b>	<b>42</b>
4.10.1	Operational characteristics .....	42
4.10.2	Service availability .....	43
4.10.3	Optional features .....	43
<b>4.11</b>	<b>End of subscription .....</b>	<b>43</b>
<b>4.12</b>	<b>Key escrow and recovery .....</b>	<b>43</b>
<b>5.</b>	<b>Facility, Management and Operational Controls.....</b>	<b>44</b>
<b>5.1</b>	<b>Physical controls.....</b>	<b>44</b>
5.1.1	Site location and construction.....	44
5.1.2	Physical access .....	44
5.1.3	Water exposures.....	44
5.1.4	Fire prevention and protection .....	44
5.1.5	Media storage.....	45
5.1.6	Waste disposal .....	45
5.1.7	Off-site backup .....	45
<b>5.2</b>	<b>Procedural controls.....</b>	<b>45</b>
5.2.1	Trusted roles .....	45
5.2.2	Number of persons required per task.....	46
5.2.3	Identification and authentication for each role.....	46
5.2.4	Roles requiring separation of duties.....	46
<b>5.3</b>	<b>Personnel controls .....</b>	<b>46</b>
5.3.1	Qualifications, experience and clearance requirements .....	46
5.3.2	Background check procedures .....	47
5.3.3	Training requirements .....	47
5.3.4	Retraining frequency and requirements .....	47
5.3.5	Job rotation frequency and sequence .....	47
5.3.6	Sanctions for unauthorized actions .....	47
5.3.7	Independent contractor requirements .....	47
5.3.8	Documentation supplied to personnel .....	48
<b>5.4</b>	<b>Audit logging procedures .....</b>	<b>48</b>
5.4.1	Types of event recorded.....	48
5.4.2	Frequency of processing log.....	49
5.4.3	Retention period for audit log.....	50
5.4.4	Protection of audit log .....	50
5.4.5	Audit log backup procedures .....	50
5.4.6	Audit collection system (internal vs. external).....	50
5.4.7	Notification to event-causing subject.....	50

5.4.8	Vulnerability assessments .....	50
<b>5.5</b>	<b>Records archival .....</b>	<b>50</b>
5.5.1	Types of records archived .....	51
5.5.2	Retention period for archive .....	51
5.5.3	Protection of archive .....	51
5.5.4	Archive backup procedures .....	51
5.5.5	Requirements for time-stamping of records.....	52
5.5.6	Archive collection system (internal or external).....	52
5.5.7	Procedures to obtain and verify archive Information .....	52
<b>5.6</b>	<b>Key changeover.....</b>	<b>52</b>
<b>5.7</b>	<b>Compromise and disaster recovery .....</b>	<b>52</b>
5.7.1	Incident and compromise handling procedures .....	52
5.7.2	Computing resources, software/data corruption.....	52
5.7.3	Entity private key compromise procedures.....	52
5.7.4	Business continuity capabilities after a disaster.....	53
<b>5.8</b>	<b>CA or RA termination .....</b>	<b>53</b>
<b>6.</b>	<b>Technical Security Controls.....</b>	<b>55</b>
<b>6.1</b>	<b>Key pair generation .....</b>	<b>55</b>
6.1.1	Key pair generation.....	55
6.1.2	Private key delivery to subscriber .....	56
6.1.3	Public key delivery to certificate issuer.....	56
6.1.4	CA public key delivery to relying parties.....	56
6.1.5	Key sizes.....	56
6.1.6	Public key parameters generation and quality checking.....	56
6.1.7	Key usage purposes (as per X.509 v3 key usage field).....	57
<b>6.2</b>	<b>Private key protection and cryptographic module engineering controls.....</b>	<b>57</b>
6.2.1	Cryptographic module standards and controls.....	58
6.2.2	Private key multi-role control .....	58
6.2.3	Private key escrow.....	58
6.2.4	Private key backup.....	58
6.2.5	Private key archival.....	58
6.2.6	Private key transfer into or from an HSM.....	58
6.2.7	Private key storage on cryptographic module.....	58
6.2.8	Method of activating private key .....	58
6.2.9	Method of deactivating private key.....	58
6.2.10	Method of destroying private key .....	59
6.2.11	Cryptographic module rating.....	59
<b>6.3</b>	<b>Other aspects of key pair management .....</b>	<b>59</b>
6.3.1	Public key archival .....	59
6.3.2	Certificate operational periods and key pair usage periods .....	59
<b>6.4</b>	<b>Activation data.....</b>	<b>60</b>
6.4.1	Activation data generation and installation .....	60
6.4.2	Activation data protection .....	60
6.4.3	Other aspects of activation data .....	60
<b>6.5</b>	<b>Computer security controls .....</b>	<b>60</b>
6.5.1	Specific computer security technical requirements .....	60
6.5.2	Computer security rating .....	61
<b>6.6</b>	<b>Life cycle technical controls .....</b>	<b>61</b>

**Certification Practice Statement**

6.6.1	System development controls.....	61
6.6.2	Security management controls .....	61
6.6.3	Life cycle security controls.....	61
<b>6.7</b>	<b>Network security controls .....</b>	<b>61</b>
<b>6.8</b>	<b>Time-stamping.....</b>	<b>61</b>
<b>7.</b>	<b>Certificate, CRL and OCSP Profiles .....</b>	<b>62</b>
<b>7.1</b>	<b>Certificate profile .....</b>	<b>62</b>
7.1.1	Certificates for individuals.....	62
7.1.2	Certificates for Government entities.....	74
7.1.3	Version number .....	79
7.1.4	Certificate extensions.....	79
7.1.5	Algorithm object identifiers .....	79
7.1.6	Name forms.....	79
7.1.7	Name constraints.....	80
7.1.8	Certificate policy object identifier .....	80
7.1.9	Usage of policy constraints extension .....	80
7.1.10	Policy qualifiers syntax and semantics .....	80
7.1.11	Processing semantics for critical certificate extensions.....	80
<b>7.2</b>	<b>CRL profile.....</b>	<b>80</b>
7.2.1	Version number(s) .....	80
7.2.2	CRL and CRL entry extensions .....	80
7.2.3	CRL ASN1 description .....	80
<b>7.3</b>	<b>OCSP profile .....</b>	<b>82</b>
7.3.1	Version number(s) .....	82
7.3.2	OCSP extensions .....	82
7.3.3	OCSP Response Signing Certificate ASN1 Description .....	82
<b>8.</b>	<b>Compliance Audit and Other Assessments .....</b>	<b>84</b>
<b>8.1</b>	<b>Frequency or Circumstances of Assessments.....</b>	<b>84</b>
<b>8.2</b>	<b>Identity and Qualifications of the Assessor.....</b>	<b>84</b>
<b>8.3</b>	<b>Assessor’s Relationship to Assessed Party.....</b>	<b>85</b>
<b>8.4</b>	<b>Topics Covered by Assessment .....</b>	<b>85</b>
<b>8.5</b>	<b>Actions Taken as a Result of Deficiency.....</b>	<b>85</b>
<b>8.6</b>	<b>Communication of Results.....</b>	<b>85</b>
<b>9.</b>	<b>Other Business and Legal Matters.....</b>	<b>86</b>
<b>9.1</b>	<b>Fees .....</b>	<b>86</b>
<b>9.2</b>	<b>Financial Responsibility.....</b>	<b>86</b>
9.2.1	Insurance Coverage.....	86
9.2.2	Other Assets.....	86
9.2.3	Insurance or Warranty Coverage for End-Entities.....	86
<b>9.3</b>	<b>Confidentiality of Business Information.....</b>	<b>86</b>
<b>9.4</b>	<b>Privacy of Personal Information.....</b>	<b>87</b>
<b>9.5</b>	<b>Intellectual Property Rights.....</b>	<b>88</b>
<b>9.6</b>	<b>Representations and Warranties.....</b>	<b>88</b>
9.6.1	CA Representations and Warranties.....	88
9.6.2	RA Representations and Warranties.....	88
9.6.3	RA Representations and Warranties.....	88



**Certification Practice Statement**

9.6.4	Relying Party Representations and Warranties .....	89
9.6.5	Representations and Warranties of Other Participants .....	89
<b>9.7</b>	<b>Disclaimers of Warranties .....</b>	<b>89</b>
<b>9.8</b>	<b>Limitations of Liability.....</b>	<b>89</b>
<b>9.9</b>	<b>Indemnities .....</b>	<b>89</b>
<b>9.10</b>	<b>Term and Termination .....</b>	<b>89</b>
<b>9.11</b>	<b>Individual Notices and Communications with Participants .....</b>	<b>90</b>
<b>9.12</b>	<b>Amendments .....</b>	<b>90</b>
<b>9.13</b>	<b>Dispute Resolution Procedures .....</b>	<b>90</b>
<b>9.14</b>	<b>Governing Law .....</b>	<b>90</b>
<b>9.15</b>	<b>Compliance with Applicable Law .....</b>	<b>90</b>
<b>9.16</b>	<b>Miscellaneous Provisions .....</b>	<b>90</b>
<b>9.17</b>	<b>Other Provisions.....</b>	<b>91</b>

# 1. Introduction

This Certification Practice Statement (CPS) describes the certification practices that apply to the digital certificates issued by the Dubai PKI Corporate Certification Authority (CA). The Corporate CA is one of the subordinate CAs signed by the Dubai Root CA. This CPS covers the issuance and controls surrounding the following types of certificates:

- **Certificates for individuals** – comprises certificates issued for citizens, residents and government employees of the UAE; these certificates are used for the following purposes:
  - **Signing certificate** – used to produce digital signatures on digital transactions and documents
  - **Encryption certificate** – used for secure email and for data/document encryption
  - **Authentication certificate** – used for authentication of subscribers in online services
- **Signature Certificates for government entities** – comprises certificates issued for entities for the following purposes:
  - **Signing certificate** – used to produce digital signatures on digital transactions and documents on behalf on an entity
  - **Code signing certificate** – used to signing organization software
- **OCSP certificates** – certificates for the Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by this CA

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

## 1.1 Overview of Dubai PKI

The “Dubai PKI” uses standard PKI technologies, policies and operating procedures and application interfaces. The Dubai PKI comprises the Dubai PKI 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 currently two Subordinate Certification Authorities (CAs): Corporate CA and Devices CA, which come at the second level of the PKI hierarchy. DESC owns and operates the Dubai PKI Root and the two aforementioned Subordinate CAs to provide certification services that enable citizens, residents, government entities in the UAE 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 PKI Root CA aims to sign subordinate CAs belonging to government or private sector entities. Such entities have their own custom needs and reasons to implement their own CAs rather than using a DESC-operated subordinate CAs.

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

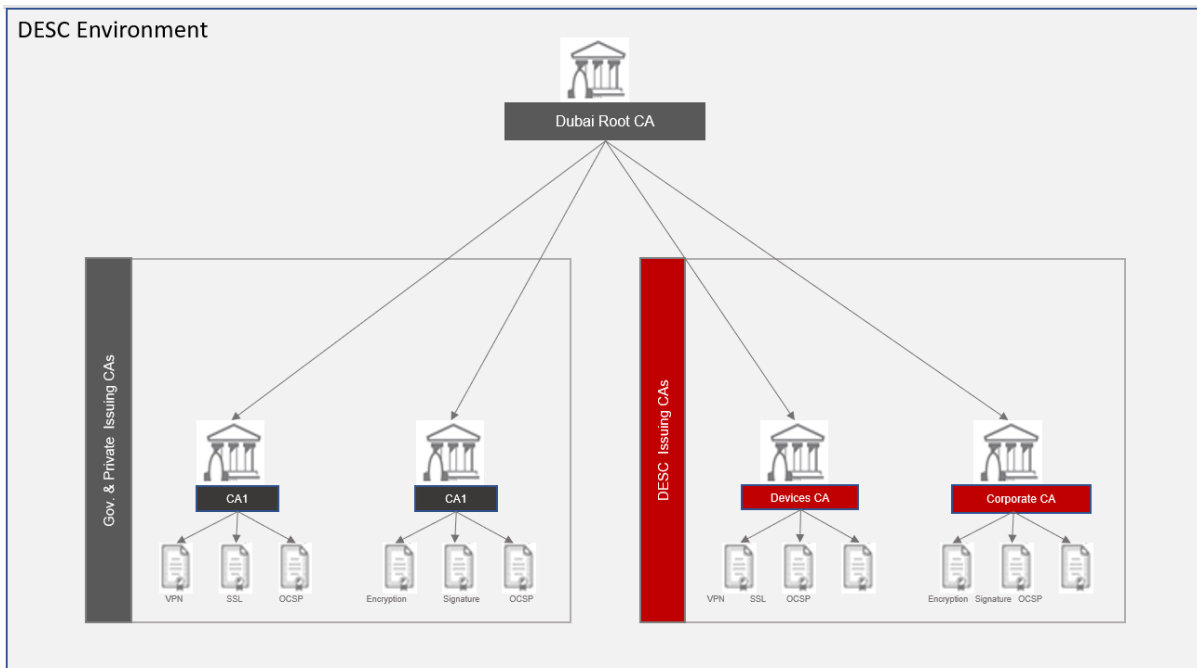
CAs belonging to other entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai PKI Root CA. These issuing CAs will be directly signed by the Dubai PKI Root CA, which makes them subordinate CAs owned by the corresponding government or private sector entity but operated by DESC. Policies and procedures of these Subordinate CAs must follow and be in full compliance with Dubai PKI Root CA CP/CPS.

The Dubai PKI Root CA and DESC Subordinate CAs are established and operated by DESC. DESC is the authority that has the final responsibility of providing governmental PKI certification services in Dubai, i.e., issuing and managing subordinate and end-entity certificates for Government 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 PKI Root CA is the top authority in this PKI with regard to the digital certification services offered by Dubai PKI. The Dubai PKI 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 government or private sector entities.

DESC is fulfilling the role of the Policy Authority (PA) for the Dubai PKI. Hence, DESC shall authorize the certification services from other government or private sector entities that aim to have their own subordinate CAs signed by Dubai PKI Root CA. Government or private sector entities plan to establish their own Subordinate CAs under Dubai PKI Root CA must be approved by Dubai PKI PA and their CP and CPS must also be approved by the same PA. Subordinate CAs must follow requirements set by the Dubai PKI PA. Dubai PKI PA requires subordinate CAs to go through an annual audit and submit annual audit reports to Dubai PKI PA. Any subordinate CA of Dubai PKI Root CA must be hosted in Dubai PKI environment and must be operated by Dubai PKI. Business practices and services of Subordinate CAs can be defined by Subordinate CA owners, but must be approved by Dubai PKI PA.



*Figure 1: Trust Model for Dubai PKI*

### 1.1.2 Certification services

The certification services offered by this CA are outlined as follows:

- **Registration services:** It 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:** It issues end-entity certificates based on the verification conducted by the registration service.
- **Dissemination service:** It disseminates, OCSP certificates, this CA 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:** It processes requests and reports revocation data for determining the appropriate action to be taken. The results of this service are available through the certificate validity status service.
- **Certificate validity status service:** It provides certificate validity status information to relying parties based on certificate suspension or revocation lists, and an OCSP responder service. The status information shall always reflect the current status of the certificates issued by this CA.

### 1.1.3 Certificate Policy

X.509 certificates issued by Corporate CA to subscribers will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a Certificate is trusted for a particular purpose. Subscriber Certificates issued by the Corporate CA will identify the applicable policy in the certificate Policies extension by including applicable OID(s).

### 1.1.4 Relationship Between the Corporate CA CP and this CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by Corporate CA as governed by the Corporate CA CP and related documents which describe Dubai PKI requirements and use of Certificates.

## 1.2 Document name and identification

This document is named and referred to as “Dubai PKI – Corporate CA Certificate Practice Statement”.

The object identifier (OID) of this CPS is 2.16.784.1.2.2.100.1.2.1.1.

Dubai PKI organizes the OID for the certificates that are issued by the Corporate CA as shown in the following table.

OID	Certificate type	Description
2.16.784.1.2.2.100.1.2.2.1.1	Encryption certificates	Encryption certificates for individuals (e.g., emails, documents)
2.16.784.1.2.2.100.1.2.2.1.2	<b>Deprecated:</b> Authentication certificates	Certificates for individual authentication purposes

2.16.784.1.2.2.100.1.2.2.1.6	Authentication certificates	Certificates for individual authentication purposes
2.16.784.1.2.2.100.1.2.2.1.3	Digital signature certificates (high assurance)	Digital signing certificates for individuals to be used for signing transactions that require a high assurance level of identity vetting
2.16.784.1.2.2.100.1.2.2.1.4	Digital signature certificates (moderate assurance)	Digital signing certificates for individuals to be used for transactions that does not require the highest assurance levels of identity vetting
2.16.784.1.2.2.100.1.2.2.1.5	Mobile Authentication certificates	Certificates for individuals installed on the mobile e.g. to trust personal smart device
2.16.784.1.2.2.100.1.2.2.2.1	Digital signature certificates (legal signing on behalf of government entity)	Digital signing certificates for organizations (signing for legal persons)
2.16.784.1.2.2.100.1.2.2.2.2	Code signing certificates	Certificates for (software) code signing purposes

## 1.3 PKI participants

Several parties are involved during the lifecycle management of the digital certificates issued by this CA. This include:

- Policy Authority (PA)
- Subordinate Certification Authorities (CA)
- Registration Authorities (RA)
- Local Registration Authority (LRA)
- Subscribers
- Relying Parties

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

### 1.3.1 Policy Authority (PA)

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

- Specifying and approving the Dubai PKI infrastructure
- Approving government and private sector entities applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy
- 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
- Review annual audit report submitted by government or private sector entities CAs to ensure continuous compliance to Dubai PKI requirements
- Review quarterly audit reports of LRAs

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- Enforcing CP /CPS and other policies applicable to Dubai PKI Environment
- Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CP/CPSs and related policies
- Defining the review process that ensures that the Dubai PKI properly implements the above practices
- Defining the review process that ensures that the related policies are supported by the Dubai PKI CP and CPSs
- Publication of CP and CPSs and of its revisions
- Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the Dubai PKI
- Evaluating the proper working of the Dubai PKI environment
- Allocating members to the key ceremonies as witness as well as trusted operatives and key custodians
- Evaluating changes to the Dubai PKI environment (management, operational, hardware, software and security)
- Evaluating case-by-case issues where key Dubai PKI staff/personnel did not respect the security and/or operational procedures, including ethics
- Deciding on critical issues in case of incidents, disasters and other severe problems with regards to the Dubai PKI.

### **1.3.2 Subordinate Certification Authorities**

The Corporate CA (further referred to as “CA”) issues certificates (see section 1.2) for Government entities, Citizens, and Residents in addition to OCSP response signing certificates. This includes the following tasks:

- 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 OCSP and Corporate CA certificates to a public repository
- Maintaining and providing certificates status information through publicly available CRL and OCSP mechanisms

### **1.3.3 Registration Authorities**

Duly authorized members part of Dubai PKI team act as Registration Authority (RA) for this CA. This team is involved in validating and accepting certificate issuance and management operations, in addition to triggering related certification operations by this CA.

Dubai PKI does not delegate the validation process of domain ownership or control (domain portion of an email address) to any third-party RA or LRA rather this process is performed only by DESC RA team.

### **1.3.4 Local Registration Authority**

Corporate CA allows government entities willing to manage the certificates life cycle for their own communities to set up and act as a Local Registration Authority (LRA). DESC accepts the following LRAs:

- Officer duly authorized by the government entity: This officer will be enrolled to DESC Corporate CA by DESC RA. He will receive credentials that allow to access the Corporate CA remotely through a dedicated Web RA application and manage the digital certificates of the government entity subscribers' community. Multi-factor authentication is implemented whenever RA/LRA officers approve certificate applications for issuance.
- System/application: Operated by the government entity and integrated with the Corporate CA through a secure interface exposed by the CA. The system/application is configured with dedicated credentials issued by DESC RA so that it can request certificates from Corporate CA and manage the subscribers' community certificates.

The entities willing to act as an LRA shall sign an agreement with DESC through which it commits to operate their LRA in accordance with DESC Subordinate CA CP and this CPS. In case DESC authorizes LRA to issue e-mail protection certificates to its employees, DESC first validates that the domain is owned/controlled by the subject entity (LRA) then hardens its dedicated Web RA application to issue e-mail protection certificates only if the domain portion of the email is in approved list.

The LRA agreement describes the LRA obligations/responsibilities for:

- The collection and validation of subscribers' identity data by the LRA
- The LRA conformance to DESC Subordinate CA CP and this CPS
- The request and management of certificates of the government entity subscribers' community
- The right for Corporate CA to quarterly audit the LRA to ensure compliance with registration processes highlighted in this CPS.

### **1.3.5 Subscribers**

Subscribers of the Corporate CA are Government entities, Government employees and Citizens/Residents in the UAE.

Before issuing any certificate, the subscriber shall agree to the terms and conditions of DESC subscriber agreement.

### **1.3.6 Relying Parties**

A Relying Party is any entity within UAE that processes a digital certificate issued by the Corporate CA.

### **1.3.7 Other participants**

There are no other participants for this CA.

## **1.4 Certificate usage**

### **1.4.1 Appropriate certificate use**

There are three categories of certificates issued by this CA which are:

- Certificates for individuals:
  - Encryption key pair with related certificate
    - Secure email
    - Document/data encryption
  - Signature key pair and related certificate
    - Signing documents and digital transactions
  - Authentication key pair and related certificate
    - Authentication
- Certificates for government entities
  - Code signing key pair and related certificate
    - Digitally signing code
  - Signature key pair and related certificate
    - Signing documents and digital transactions on behalf of an entity
- OCSP certificates for OCSP responder delegated by this CA.

In accordance with its purpose of use, the certificate may be used without limitations in the services provided by the Government entities.

DESC reserves the right to issue any of the above-mentioned certificates for DESC internal testing and quality assurance purposes. Test certificates will be issued by DESC RA that enforces the following rules:

- test certificates have a short lifetime (in days)
- certificate subject DN for test certificates always includes the word “TEST”

### **1.4.2 Prohibited certificate use**

Certificates referred to in this CPS document shall not be used for purposes other than the ones listed above under section 1.4.1 of this document. Using certificates for other purposes is explicitly prohibited.

Certificates referred to in this CPS document shall not be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

## **1.5 Policy administration**

### **1.5.1 Organization administering the document**

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



## **1.5.2 Contact details**

Inquiries, suggested changes or notices regarding this CP should be directed to **Dubai PKI Policy Authority**:

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

E-mail [pa@desc.gov.ae](mailto:pa@desc.gov.ae)

### **Certificate Problem Report**

Subscribers and Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to [pki.support@desc.gov.ae](mailto:pki.support@desc.gov.ae).

DESC or the designated RA will validate and investigate the revocation request before taking an action in accordance to section 4.9.

## **1.5.3 Person determining CPS suitability for the policy**

The Dubai PKI PA determines the suitability of any CPS part of the Dubai PKI.

## **1.5.4 CPS approval procedures**

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

In an effort to maintain credibility and promote trust in this CPS and better correspond to accreditation and legal requirements, the Dubai PKI PA shall review this CPS at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CPS.

# **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. E.g., 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

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

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

**Certification Practice Statement (CPS)** – A statement of the practices which a certification authority employs in issuing certificates

**CRL** – Certificate Revocation List

**DRP** – Disaster Recovery Plan

**DN** – Distinguished Name

**FIPS** – Federal Information Processing Standards

**Government entity** – A Dubai government entity or other government entities in the UAE authorized by Dubai PKI PA to consume the PKI services

**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

**Identity Provider** – In the context of this CPS, references to identity providers will be related to the government/federal identity providers including Smart Pass and Dubai ID.

**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

**Issuing Certification Authority (issuing CA)** – In the context of a particular certificate, the issuing CA is the CA which issued 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

**LRA** – Local Registration Authority

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

**OCSP** – Online Certificate Status Protocol

**PA** – Policy Authority of Dubai PKI

**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

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

**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 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 RSA algorithm –Ron Rivest, Adi Shamir and Leonard Adleman

**SCEP** – Simple Certificate Enrolment Protocol

**Secret Shares** – A set of devices, smartcards, PINs, etc.

**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 e-mail address

**Subject** – A subject is 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 Dubai PKI is committed to comply with the below requirements published at <https://www.cpacanada.ca>:

- WebTrust Principles and Criteria for Certification Authorities

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements

The Dubai PKI is committed to conform with the current versions of the below requirements published at <http://www.cabforum.org>:

- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing (“Baseline Requirements for Code Signing”)

If there is any inconsistency between this document and the Requirements above, the Requirements take precedence over this document.

The present CPS 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
- CA Security Council (CASC) Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

## 2. Publication and repository responsibility

### 2.1 Repositories

DESC publishes information about all digital certificates it issues in (an) online publicly accessible Certificate Dissemination Webpage at <https://ca-repository.desc.gov.ae/> and is provided on a 24/7 basis.

### 2.2 Publication of certificate information

DESC publishes a copy of the Corporate CA certificate and OCSP certificates at this website. An updated version of this CPS is published at least annually. DESC reserves its rights to publish certificate status information on third-party repositories.

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

DESC publishes digital certificate status information in frequent intervals as indicated in this CPS. The provision of the Corporate CA issued electronic certificate validity status information is a service available round-the-clock.

DESC operates the certificate status repository for the Corporate CA. This repository is a web server where the CA certificates and Certificate Revocation Lists (CRLs) are published in read-only mode.

### 2.3 Time or frequency of publication repositories

The Corporate CA certificate and OCSP certificates are published to the public repository (<https://ca-repository.desc.gov.ae/>) as soon as they are issued.

DESC publishes CRLs at regular intervals. A pointer (URL) to the relevant CRL is added by DESC to subscribers' certificates as part of the CDP extension whenever this extension is present.

DESC maintains the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL until minimum 7 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 Corporate CA:

- At the minimum, CRLs shall be refreshed every 26 hours, even if no changes have occurred since the last issuance.

- CRLs lifetime shall be set to 72 hours.

Owing to their sensitivity, DESC refrains 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 policies, etc. Such documents and documented practices are, however, conditionally available to designated authorized parties in the context of audit(s) that DESC owes duty to with regard to the Corporate CA activities.

## **2.4 Access controls on repositories**

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

Access controls are 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 name

This CA is identified in the Issuer's name field of the subscriber certificates as follows:

cn = Corporate Certification Authority, o = UAE Government, c = AE

The certificates issued by this CA contain X.500 Distinguished Names (DN) in English as follows.

- **Certificates issued for Government entities through DESC RA:**

cn=<Government entity name>, ou = <optional organizational unit within the government entity>, o =<Government entity meaningful unique name>, l =<Government entity locality information> , c = AE

- **Certificates issued for individuals:**

serialnumber=<optional serial number for each subscriber>, cn=<individual end user name>, ou = <optional organizational unit within the government entity>, o =<Government entity meaningful unique name>, l =<Government entity locality information>, c = AE

- **OCSP responder:**

cn = Corporate Certification Authority OCSP, o = DESC, l = Dubai, c = AE

### 3.1.2 Meaningful names

For certificates issued to individuals, names are meaningful since the CN contains the name of the subscriber.

For certificates issued to government entities, names are meaningful since the CN contains the name of the entity.

For certificates issued to the Corporate CA OCSP responder, the names are meaningful and indicate the OCSP name (Corporate CA OCSP).

### 3.1.3 Anonymity and pseudonymity of subscribers

This CA does not support the issuance of anonymous certificates.

### 3.1.4 Rules for interpreting various name forms

No stipulation – this section is intentionally left blank

### 3.1.5 Uniqueness of names

As per section 3.1.1 of this CPS, DESC enforces uniqueness of subject DNs are enforced as follows:

- **Certificates issued for individuals:** Uniqueness enforced through the “cn” attribute potentially combined with the “serialnumber” attribute.
- **Certificates issued for Government entities:** A convention for a meaningful name representing uniquely the Government entity is enforced by DESC.
- **Certificates issued for Corporate CA OCSP responder:** The OCSP responder unique name is included in the subject DN of issued OCSP certificate.

### 3.1.6 Recognition, authentication and role of trademarks

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. The Corporate CA does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The Corporate CA shall have the right to revoke a Certificate upon receipt of a properly authenticated order from DESC or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

## 3.2 Initial identity validation

### 3.2.1 Method to prove possession of private key

This CA always verifies that the certificate applicant possesses the private key corresponding to the public key being certified by performing signature verification on the certificate request received. The CA expects that the certificate request is signed by the private key associated to the public key being certified.

### 3.2.2 Authentication of Government entity identity

For all certificates that contain the identity of a Government entity, the applicant is required to provide the Government entity’s name, organizational unit (if applicable) and official address. DESC RA will verify this information against a trusted government register that lists entities and their representatives.

For certificates issued to DESC OCSP responder, the certification process is initiated by an authorized OCSP administrator under the supervision of the Dubai PKI PA. A dedicated operational key ceremony is documented by DESC.

The authority of the applicant to request a certificate on behalf of a Government entity is authenticated in accordance with section 3.2.5.

### 3.2.3 Authentication of individual identity

The below points describe the rules that apply for authentication of certificate applicants:

The applicant’s identity is established as follows:

- Certificates application through a government entity LRA officer (or DESC RA officer): The subscriber’s identity validation is performed by the RA/LRA officer according to the entity’s



applicable business rules. The Government entity ensures that the diligence and rigor of validation is equal to the face-to-face identity verification involving the presentation of a government issued ID card (e.g. Emirates ID).

For certificates issued for e-mail protection, the RA/LRA officer must use suitable methods to verify with reasonable assurance the email ownership of the e-mail to be included in the certificate. The verification could be made based on the entity's internal employee records where emails are formally assigned/specified for each employee.

Additionally, the RA/LRA officer shall use Challenge-Response mechanism to verify the applicant ownership of the e-mail to be included in the certificate. The RA/LRA officer sends an e-mail with a random, unique value to the e-mail address. If the applicant replies to the e-mail, and that e-mail includes the original random value as sent by the RA/LRA officer, the validation is passed. The reply should be within 3 days. Evidences on using the Challenge-Response mechanism are going to be verified as part of the Corporate CA quarterly audit on the LRA.

Domain control and ownership shall be done according to section 1.3.3.

- Certificates application through the UAE PASS system:
  - Authentication certificate and digital signature certificate for “moderate assurance” transactions through the UAE PASS enrolment application: The applicant is expected to have an existing account and authentication credentials from accepted Identity Providers in the UAE. Dubai PKI recognized Smart Pass and Dubai ID as trusted Identity Providers. The credentials from the existing Identity Provider are used by the applicant to authenticate to the UAE PASS enrolment application (2-factor authentication with static password and OTP). After a successful authentication to the UAE PASS enrolment application, the UAE PASS retrieves the applicant's identity data from the Identity Provider and uses this data to enroll the applicant into the UAE PASS system. As part of this process, the UAE PASS sends certificate requests to the Corporate CA requesting an authentication certificate and a signing certificate for “moderate assurance”.
  - Authentication certificate and digital signature certificate for “moderate assurance” transactions through the UAE PASS kiosk application: The applicant's identity verification is performed using biometric (fingerprint) verification against the fingerprints enrolled with the applicant's Emirates ID card. After successful biometric verification, the UAE PASS retrieves the applicant's identity data from the Emirates ID card then use this data to enroll the applicant into the UAE PASS system. As part of this process, the UAE PASS sends certificate requests to the Corporate CA requesting an authentication certificate and a signing certificate for “moderate assurance”.
  - Digital signature certificate for “high assurance” transactions: The applicant shall already be enrolled into the UAE PASS system with authentication and signing certificate (for “moderate assurance” transactions) already generated. The user is given the option by the UAE PASS to apply for a signing certificate for “high assurance” transactions. He applies for this signing certificate after a biometric (fingerprint) verification at the UAE PASS kiosk.

### **3.2.4 Non-verified subscriber information**

All fields constituting the subscriber information written in the certificate are verified by the relevant RA/LRA.

DESC does not delegate the validation process of domain ownership or control to any third-party RA or LRA rather this process is performed only by DESC PKI team.

### **3.2.5 Validation of authority**

- Government entity certificates to be issued through DESC RA: The authority of the certificate requestor to request a certificate on behalf of a Government entity will be performed through a reliable means of communication with the Government entity that include the following steps at minimum: (1) DESC RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized signatory that attests the ability of the requestor to requests certificates on behalf of the government entity. (2) DESC RA verifies the existence of the government entity and their authorized signatory against a trusted government register listing entity and their representatives.
- Individual certificates to be issued through the government entity LRA (including DESC RA): The RA/LRA officer/system (that is approved by DESC) is authorized to submit certification requests on behalf of the Government Entity subscribers.

### **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 for re-keying is performed as in initial registration.

### **3.3.2 Identification and authentication for re-key after revocation**

Identification and authentication for re-keying after revocation is performed as in initial registration.

## **3.4 Identification and authentication for revocation request**

- Certificates issued to Government entities through DESC RA: DESC RA verifies that an authorized representative has requested the revocation through one of the following methods:
  - Receiving a revocation request through email from the entity's authorized representative. The representative sends a completed and signed revocation request through the email. DESC RA verifies that the email originates from a legitimate entity's representative by using some of the available information (phone call, email)
  - Communication with the requesting entity to provide reasonable assurances that the individual or organization requesting revocation of the entity's certificate is who they claim to be. Such communication, depending on the circumstances, may involve DESC RA using telephone and email.

Once the revocation request is successfully authenticated, DESC RA revokes the subject certificate through the relevant RA system.

- Certificates issued to individuals through a government entity LRA (including DESC RA): The RA/LRA officer authenticates the revocation request through one of the following methods:
  - Receiving a revocation request from the subscriber through methods relevant to the RA/LRA and the government entity's internal processes. This may include a face to face, call from the subscriber and the RA/LRA asking relevant questions to identify the subscriber (e.g. employee ID, name, date of birth, ...) or email from the subscriber using an email address that can be verified by the RA/LRA and linked to the subscriber's identity.
  - Communication with the requesting party to provide reasonable assurances that the individual or department requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include telephone and/or email.
  - Human resource (or team within the entity with similar mandate) if the subscriber is terminated or changed role within the entity which would trigger the revocation request. The RA/LRA would have the internal means to confirm with HR the validity of the revocation request.
- Certificates issued to individuals through the UAE PASS system: The following scenarios may trigger revocation requests from the UAE PASS system:
  - A revocation request is triggered through the UAE PASS regular business processes. One example would be the subscriber renewing his UAE PASS PKI credentials before existing ones are expired. The UAE PASS system interacts with the subscriber and validates the subscriber's identity and confirms that a revocation request is required. The UAE PASS system interacts (through integration) with the Corporate CA to revoke the certificate and request new certificate for the subscriber.
  - A revocation request is triggered through the UAE PASS helpdesk. A typical scenario would be subscriber who is terminated from the UAE PASS system (e.g. subscriber leaving the country). The UAE PASS helpdesk communicates with DESC RA through agreed channels (telephone, email) which results in the revocation request being authenticated by DESC RA which can then process it through their dedicated RA applications.

# 4. Certificate Life Cycle Management

## 4.1 Certificate application

### 4.1.1 Who can submit a certificate application

- **Certificates for entities issued through DESC RA:** An authorized person from the Government entity submits the certificate application as part of the certificate issuance process.
- **Certificates for individuals issued through the Government entity LRA (including DESC RA):** The entity LRA or DESC RA submits the certificate application.
- **Certificates for individuals issued through the UAE PASS:** The UAE PASS system is the interface through which certificate applications are triggered to the CA.
- **OCSP responder certificates:** An authorized OCSP administrator can submit a certificate request.

### 4.1.2 Enrolment process and responsibilities

#### DESC RA Certificate Enrolment Process

- Certificates issued to Government entities through DESC RA:
  - The entity signs a Subscriber Agreement with DESC.
  - DESC RA receives a certificate application form. He then identifies the applicant as described in section 3.2.2.
  - DESC RA officer uses a dedicated RA application to enroll the applicant into this CA. The applicants' unique name from the application form is used to produce a unique distinguished name necessary for enrolment into the CA system. As part of the enrolment, DESC RA generates a unique authorization code for this certificate application and submits this code to the entity's representative email address (as provided in the certification application form).
  - The subscriber generates a key pair on its own IT system or device. He then creates a CSR file using the received unique authorization code provided by DESC RA.
  - The CSR file is sent to DESC RA through the entity representative email (as provided in the certificate application form). DESC RA processes the CSR and issue the certificate from the CA.
  - DESC RA send the certificate to the entity representative email address.

**Government LRA (including DESC RA)**

- Certificates issued to individuals through DESC RA or a government entity LRA (DESC RA is responsible of issuing certificates to DESC employees. Government LRAs are only responsible for issuing certificates to their community that is agreed with DESC as per the LRA agreement):
  - The applicant, who requires the PKI token with digital certificates, initiated a request according to the applicable entity's internal processes. He agrees to the subscriber agreement as part of this process. For updated list of approved PKI Tokens, refer to Dubai PKI dissemination website.
  - Certificate Key Pair are generated inside the PKI token.
  - The RA/LRA officer receives a request to enroll the applicant. He then identifies the applicant as described in section 3.2.3 then validates his/her identity according to the applicable Government entities' business rules.
  - The RA/LRA officer uses DESC Web RA application in order to fill the certificate enrollment form after validating all data required for the enrollment.
  - The Web RA application communicates with this CA in order to issue end-user certificates.
  - The CA generates the certificates and sends back to the Web RA application that installs the certificates on the PKI token.
  - The applicant is now a registered subscriber and is handed over his PKI token and Initial PIN.
  - The subscriber must immediately change the PIN using the supplied change PIN software.

**UAE PASS LRA - IDP Registered Users**

- Authentication certificate and digital signature certificate for “moderate assurance” transactions issued through the UAE PASS enrolment application:
  - The applicant is expected to have an existing account and authentication credentials from accepted Identity Providers (IDP) in the UAE. Approved IDPs are Dubai ID (SDG) and Smart PASS (TRA).
  - The credentials from the existing Identity Provider are used by the applicant to authenticate to the UAE PASS enrolment application (2-factor authentication) and also static password and OTP are used during this process.
  - After a successful authentication to the UAE PASS enrolment application, the UAE PASS retrieves the applicant's identity data from the Identity Provider and uses this data to enroll the applicant into the UAE PASS system. The applicant is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.
  - The UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the applicant's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA.
  - The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account.
- The applicant then triggers the signature key pair and certificate generation process with the UAE PASS. The UAE PASS securely generates the user's Signing key pair on an HSM and automatically submits Signing certificate request to DESC service for the Corporate CA .
- The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
- The UAE PASS validates the received certificate then stores it along with the applicant's account.

**UAE PASS LRA - New Users via KIOSK**

- Authentication certificate and digital signature certificate for “moderate assurance” transactions through the UAE PASS kiosk application:
  - The applicant attends to a UAE PASS kiosk.
  - The applicant's identity verification is performed using biometric (fingerprint) verification against the fingerprints enrolled with the applicant's Emirates ID card.
  - After successful biometric verification, the UAE PASS kiosk application retrieves the applicant's identity data from the Emirates ID card then use this data to enroll the applicant into the UAE PASS system. As part of this process the applicant is provided with a unique secret (i.e. QR code) to be used for the UAE PASS mobile app. He is also provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.
  - The applicant uses the unique secret code to access the UAE PASS mobile app. The UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the applicant's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA.
  - The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
  - The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account.
  - The applicant then triggers the signature key pair and certificate generation process with the UAE PASS. The UAE PASS securely generates the user's Signing key pair on an HSM and automatically submits Signing certificate request to DESC service for the Corporate CA.
  - The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
  - The UAE PASS validates the received certificate then stores it along with the applicant's account.

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- Digital signature certificate for “high assurance” transactions through the UAE PASS kiosk application:
  - The applicant shall already be enrolled into the UAE PASS system with authentication and signing certificate (for “moderate assurance” transactions) already generated.
  - The user attends to a UAE PASS kiosk. His identity is verified using biometric (fingerprint) verification. After successful biometric verification, the user is logged onto his UAE PASS account.
  - The user is given the option by the UAE PASS to apply for a signing certificate for “high assurance” transactions. He is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.
  - The UAE PASS generates the signature key pair on an HSM and creates a certificate request that is submitted to DESC service for the Corporate CA.
  - The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
  - The UAE PASS validates the received certificate then stores it along with the applicant’s account.

**UAE PASS LRA - New Users via Manual Registration**

- Authentication certificate and digital signature certificates for “high assurance” transactions through the UAE PASS manual registration:
  - The applicant attends to a UAE PASS Registration Authority Officer.
  - Subscriber fills and signs registration form and signs Certificate Issuance Terms and Conditions
  - RA officer collects a copy of Subscriber Emirates ID and validates Subscriber picture and information on the Emirates ID with information on the registration form
  - RA officer keeps original copy of the registration form and Terms and Conditions
  - RA Officer prepares a PDF file that contains Subscriber scanned copy of Emirates ID, signed Subscriber registration form, and signed Terms and Conditions.
  - RA Officer Digitally signs the PDF using his digital signature certificate (issued by DESC) through UAE PASS Application
  - RA Officer submits the signed pdf to business team for validation by email
  - Business team validates the identity of user by checking provided information against ICA through ICA webservices
  - If there is a match, the business team proceed with below , if no match then business team submits rejection email and process terminates at this step.
  - Business team takes/prints a screen shot of ICA response
  - Business officer fills approval form
  - Business officer prepares a pdf of ICA response and approval form
  - Business officer signs the PDF using his digital signature certificate (issued by DESC) through UAE PASS Application

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- Business officer sends approval (signed pdf) to the RA officer through email with link to complete the registration process
- At this stage, UAE PASS application will inform user to recover UAE PASS account
- If user agrees, the UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the Subscriber's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA.
- The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
- The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account.
- The RA officer in the presence of the Subscriber, clicks on the link provided by the business team
- The Subscriber is sent an authorization request to initiate certificate issuance
- User approves request through his UAE PASS application
- User will be asked to provide signing password
- This triggers the signature key pair and certificate generation process for "moderate assurance" and "high assurance" with the UAE PASS. The UAE PASS securely generates the user's Signing key pairs for both certificates on an HSM and automatically submits Signing certificate requests to DESC service for the Corporate CA.
- The CA validates the certificate requests, issues the certificates and sends the certificates back automatically to the UAE PASS.
- The UAE PASS validates the received certificates then stores it along with the applicant's account.
- The RA officer documents the serial numbers of issued certificates in the related section of Registration Form

**UAE PASS LRA - New Users via Digital Onboarding**

- Authentication certificate and digital signature certificate for "moderate assurance" transactions in addition to Mobile authentication certificate through the UAE PASS (Digital Onboarding Application):
  - The applicant presents his/her emirates ID (scanned by UAE PASS mobile app) and UAE PASS validates the identity status with ICA
  - The applicant then provides his/her personal email, mobile and confirms the OTP on both to prove the control on email and mobile provided.
  - The applicant performs a liveness test in UAE PASS mobile app and on successful verification the live photo (taken by UAE PASS mobile app) is submitted to UAE PASS
  - UAE PASS uses MOI service for the face recognition from the picture obtained in previous step after liveness verification.



*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- MOI identity verification is performed on UAE PASS submitted biometric and identity details using biometric verification against the federal government authorized Facial templates database After successful face verification, UAE PASS application uses the applicant's identity data to enroll the applicant into the UAE PASS system. The applicant is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.
- The UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the applicant's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA.
- The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
- The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account.
- The applicant then triggers the signature key pair and certificate generation process with the UAE PASS. The UAE PASS securely generates the user's Signing key pair on an HSM and automatically submits Signing certificate request to DESC service for the Corporate CA.
- The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.
- The UAE PASS validates the received certificate then stores it along with the applicant's account.

**UAE PASS LRA – Existing Users via Digital Onboarding**

- Digital signature certificate for “high assurance” transactions through the UAE PASS (Digital Onboarding Application). The applicant shall already be enrolled into the UAE PASS system with authentication and signing certificate (for “moderate assurance” transactions) already generated.
  - The applicant performs a liveness test in UAE PASS mobile app and on successful verification the live photo (taken by UAE PASS mobile app) is submitted to UAE PASS
  - UAE PASS uses MOI service for the face recognition from the picture obtained in previous step after liveness verification.
  - MOI identity verification is performed on UAE PASS submitted biometric and identity details using biometric verification against the federal government authorized Facial templates database
  - If Identity is verified, the user is given the option by the UAE PASS to apply for a signing certificate for “high assurance” transactions. He is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.
  - The UAE PASS generates the signature key pair on an HSM and creates a certificate request that is submitted to DESC service for the Corporate CA.
  - The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

- The UAE PASS validates the received certificate then stores it along with the applicant's account

For certificates issued to the OCSP responder, the certification process is initiated by an authorized OCSP administrator under the supervision of the Dubai PKI PA. A dedicated operational key ceremony is documented by DESC.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

As described in section 4.1.

### 4.2.2 Approval or rejection of certificate applications

The approval or rejection of certificates applications is done as follows:

- **For certificates issued through the DESC RA:** The DESC RA officer approves or rejects the application for the certificate as part of the overall approval/rejection of the certificate issuance process.
- **For certificates issued through the Government entity LRA (including DESC RA):** The RA/LRA officer approves or rejects the certificate application as part of the overall approval/rejection of the certificate issuance process.
- **For individuals requesting certificates through the UAE PASS system:** The user's successful identity verification (with biometrics at the UAE PASS kiosk or through an identity provider) results in the UAE PASS triggering key pair generating and certification process for the user's keys.
- **For OCSP certificates:** A certificate application is approved/rejected as part of the overall approval/rejection of the OCSP certification process.

Multi-factor authentication is implemented whenever RA/LRA officers approve certificate applications for issuance.

### 4.2.3 Time to process certificate applications

No stipulation – this section is intentionally left blank.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

- **For certificates issued to Government entities through DESC RA:** Following the approval of the certificate application by the DESC RA, the CSR file is uploaded and submitted to this CA by the DESC RA officer using a dedicated application. The CA then signs the certificate in accordance with the specified certificate template. The certificate is activated by the CA and is ready for usage. The certificate is then downloaded by DESC RA officer and transferred back to the subscriber.
- **For certificates issued to individuals through the Government entity LRA (including DESC RA):** Following the approval of the certificate application by DESC RA / the

government entity LRA, the certificate request is submitted to this CA by the RA/LRA officer using a dedicated application. The CA validates the format of the request then creates the certificate in accordance with the specified certificate template and is made available to the RA/LRA application. The certificate is activated by the CA and is ready for usage. The RA/LRA officer completes the process by installing the certificate on the target device.

- **For certificates issued through the UAE PASS:** The CA receives the certificate request from the UAE PASS system. The CA validates the format of the request then creates the certificate in accordance with the specified certificate template and returns automatically the certificate to the UAE PASS system. The certificate is activated by the CA and is ready for usage.
- **For OCSP certificates:** The OCSP administrator manually delivers the CSR file including the servers' public key to the CA administrator. The CA administrator submits the CSR file directly to the CA that will sign and publish an OCSP certificate suitable for verification. The certificate is returned to the OCSP administrator.

#### **4.3.2 Notification to the subscriber by the CA of issuance of certificate**

- **For certificates issued to Government entities through DESC RA:** the applicant is notified of the certificate issuance once collecting his certificate from DESC RA.
- **For certificates issued to individuals through the Government entity LRA (including DESC RA):** The subscriber is notified once collecting his certificate from the RA/LRA officer.
- **For certificates issued through the UAE PASS system:** The UAE PASS notifies the user on certificate issuance once it receives the certificate from the CA. This is done through the interaction (message displayed) that the user has with the UAE PASS system.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

The user confirms certificate acceptance upon signing the subscriber agreement form.

OCSP certificates shall be issued as part of DESC internal processes and shall be approved by the Dubai PKI PA.

### 4.4.2 Publication of the certificate by the CA

The Corporate CA and OCSP certificates shall be published 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

When using a subscriber's private key and corresponding certificate, a subscriber is obligated to:

- Use certificates exclusively for legal activities consistent with this CPS
- Comply with the terms of the subscriber agreement
- Not use the private key until after the CA has issued, and the subscriber accepted the corresponding certificate
- The subscriber must discontinue the use of a private key following expiration or revocation of the corresponding certificate unless a subsequent un-expired or un-revoked certificate corresponding to that private key has been issued.

### 4.5.2 Relying party public key and certificate usage

When using a subscriber's public key and corresponding certificate, a relying party is obligated to:

- Validate the certificate path
- Ensure that the key is appropriate for the intended use as set forth in this CPS and that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage, certificate policies extension fields
- Check the status of the certificate in accordance with the requirements stated in Section 4.9.6 of this CPS. As part of the validation process, the authenticity of the revocation must be validated as follows:
  - In case of using CRLs, the digital signature of the CRLs is validated
  - In case of using OCSP, the digital signature of the OCSP response is validated

- Ensure that reliance was reasonable and made in good faith in light of all the circumstances that were known or should have been known to the relying party at the time of reliance

If a party relying on the Dubai PKI accepts a certificate that cannot be validated through the Corporate CA OCSP or CRL, it decides to do so completely at his own risk.

## **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; however, there is a different (longer) validity period.

This CA does not support certificate Renewal. Only certificate re-key is supported.

## **4.7 Certificate Re-key**

Certificate Re-key is the act of re-issuing a certificate for an existing subscriber such that all the identifying information from the old certificate is duplicated in the new certificate; however, there is a different public key and a different validity period.

Certificate Re-key is supported by this CA. The re-key process (including identity validation, issuance) is similar to the initial certificate application.

### **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 certification.

### **4.7.3 Processing Certificate Re-keying requests**

As per initial certification.

### **4.7.4 Notification of new certificate issuance to subscriber**

As per initial certification.

### **4.7.5 Conduct constituting acceptance of a re-keyed certificate**

As per initial certification.

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

As per initial certification.

### **4.7.7 Notification of certificate issuance by the CA to other entities**

As per initial certification.

## 4.8 Certificate modification

This CPS 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 CPS 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

The relevant RA/LRA revoke a certificate within 24 hours if one or more of the following occurs:

1. Received a written request from the Subscriber or an authorized representative;
2. The Subscriber discovers that the original certificate request was not authorized and does not retroactively grant authorization; or
3. The RA/LRA/CA discover or has reasons to believe that there has been a compromise of the private signing key.

This CA should ensure a certificate revocation is executed within 24 hours and shall revoke a certificate within 5 days if one or more of the following occurs:

1. DESC obtains evidence that the certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

2. DESC obtains evidence that the Certificate was misused;
3. DESC is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. DESC is made aware of a material change in the information contained in the Certificate;
5. DESC is made aware that the Certificate was not issued in accordance with DESC CP/CPS;
6. Finding that the certificate was issued without the authorization of the individual named as the subject of such certificate;
7. DESC determines or made aware that any of the information appearing in the Certificate is inaccurate or misleading;
8. Revocation is required by DESC's CP and/or CPS;
9. The Government entity or the individual has been declared legally incompetent
10. A third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code;
11. DESC is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>);
12. An Application Software vendor requests revocation of a code signing certificate
13. The Corporate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; or
14. The Corporate CA's right to issue Certificates under the requirements defined in this CPS expires or is revoked or terminated, unless the Corporate CA has made arrangements to continue maintaining the CRL/OCSP Repository.

In addition to the above circumstances, the below also apply:

- For certificates issued through DESC RA or the LRA of the Government entity, the RA/LRA shall revoke digital certificates corresponding to its community when required by the entity's internal processes.
- The UAE PASS shall revoke digital certificates corresponding to its community when required by its relevant account management processes.

On the other hand, this CPS does not provide provisions for revoking an OCSP certificate apart from the compromise of the OCSP key pair that is treated by DESC as per its Disaster Recovery and Business Continuity procedures. The following sub-sections focus only on the revocation provisions that apply for the other certificates issued by this CA.

#### **4.9.2 Who can request revocation**

- The individual to whom certificates were issued
- The Government entity to whom certificates were issued
- Any relying party possessing evidence of compromise of the subscriber's certificate
- Revocations are directly initiated by DESC's RA officers in the cases described in section 4.9.1.

- For certificates issued through DESC RA (for DESC employees) or the LRA of the Government entity, the RA/LRA shall revoke digital certificates corresponding to its community when required by the entity's internal processes.
- The UAE PASS shall revoke digital certificates corresponding to its community when required by its relevant account management processes.
- DESC at its own discretion (if for instance a compromise is known for this CA key).

#### **4.9.3 Procedure for revocation request**

A dedicated procedure has been setup by this CA for the revocation of certificates:

- **Revocation of certificates through DESC RA:**
  - The subscriber or an authorized representative can request the revocation of their certificate(s) to the DESC RA.
  - The DESC RA officer authenticates the subscriber's identity as described in section 3.4.
  - The DESC RA officer requests the subscriber to fill in and sign a revocation request form.
  - The DESC RA officer revokes the subscriber's certificate(s).
  - The CA generates an updated CRL and publishes it to the DESC public repository.
- **Revocation of certificates through Government LRA (including DESC RA):**
  - The RA/LRA receives a formal revocation request from the subscriber
  - The RA/LRA validates the identity of the subscriber as done during initial certificate application
  - The RA/LRA records the revocation request according to the Government entities' business rules
  - The RA/LRA officer revokes the subscriber's certificates
  - The CA generates an updated CRL and publishes it to the DESC public repository
- **Revocation of certificates through UAE PASS:**
  - Revocation is requested as part of an account management process such as deletion or termination of UAE PASS Account. Certificates are revoked when user requests to renew certificate keys (through Kiosk), or call UAE PASS call center,
  - The UAE PASS validates the subscriber's identity using identification questions in addition to challenge-response authentication through the email or mobile number registered along with the account.
  - The UAE PASS records the revocation request according to its business rules
  - The UAE PASS sends an automatic revocation request to the CA through the CA gateway service
  - The CA revokes the certificate then generates an updated CRL and publishes it to the DESC public repository
- **Revocation of OCSP certificates:**



- The revocation is conducted as part of a PKI process internal to DESC and is approved by the Dubai PKI PA. This process involves communication with relying parties in order to update them with the OCSP certificate revocation.

#### **4.9.4 Revocation request grace period**

There is no revocation grace period. Revocation requests are processed timely upon reception by the RA.

#### **4.9.5 Revocation request response time**

For all certificates except code signing certificates:

Certificate revocation requests received from subscribers, their representatives or initiated by DESC RA are processed within 24 hours.

For certificate problem reports, DESC RA begins investigations within 24 hours from receiving the report. DESC RA initiates communication with the Subscriber and where appropriate, with other concerned authorities (e.g. local regulator). A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

DESC RA performs further investigations involving the Dubai PKI PA, the subscriber and other relevant authorities (e.g. local regulator) to decide on the action to be taken on the subject certificate.

If the investigations results led to one of the certificate revocation circumstances listed in section 4.9.1, then the certificate will be revoked within the timeframe set forth in the aforementioned section.

Based on the revocation circumstance, DESC RA may agree with subscriber on a plan to issue a new certificate.

For code signing certificates, the following process applies for incidents involving malware:

- Within 1 business day of being made aware of the incident, the CA contacts the software publisher (a Government entity) and requests a response within 72 hours.
- Within 72 hours of being made aware of the incident, the CA determines the volume of relying parties impacted.
- If a response is received from the publisher, the CA and publisher determine a 'reasonable date' for revocation.
- If no response is received from the publisher, the CA notifies the publisher that the CA will revoke the certificate in 7 days unless it has documented evidence that this will cause significant impact to the general public.

For Integrated LRA systems, an interface for revocation is already enabled for registered LRAs to be used for revocation requests, which will be processed immediately by Corporate CA.

#### **4.9.6 Revocation checking requirement for relying parties**

This PKI offers revocation information to relying parties through CRLs published on a publicly available web server and through its publicly available OCSP responder.

Certificates issued by this CA (except OCSP certificates) include the name of the web-based distribution point and OCSP responder link from where a relying party could get revocation information. It is the relying party's obligation to retrieve and process the most up-to-date revocation information.

#### **4.9.7 CRL issuance frequency**

CRLs are issued as per section 2.3 or this document.

#### **4.9.8 Maximum latency for CRLs**

No stipulation – this section is intentionally left blank.

#### **4.9.9 Online revocation/status checking availability**

OCSP is supported within this PKI solution and is 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 referred to in the certificates.

#### **4.9.10 Online revocation checking requirements**

It is at the discretion of the relying party to decide whether using CRL or relying 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**

If DESC discovers, or has a reason to believe, that there has been a compromise of the private key of the Corporate CA, DESC will immediately declare a disaster and invoke Dubai PKI business continuity plan. DESC will (1) determine the scope of certificates that must be revoked, (2) publish a new CRL at the earliest feasible time, (3) use reasonable efforts to notify government entities, subscribers and potential relying parties that there has been a key compromise, and (4) generate new CA key pair as per DESC operations policies and procedures.

#### **4.9.13 Circumstances for suspension**

Certificate suspension is not supported by this CA.

#### **4.9.14 Who can request suspension**

Not applicable.

#### **4.9.15 Procedure for suspension request**

Not applicable.

## **4.10 Certificate Status Services**

Refer to section 4.9.6 of this document. In addition, the following provisions are made.

#### **4.10.1 Operational characteristics**

CRLs are published by this CA on a public repository which is available to relying parties. Apart from CRLs distributed at distribution points, the DESC also publishes combined (uniform) CRLs on its public repository

It provides revocation information as below:

- CRL must be reissued at least every 26 hours
- value in the nextUpdate field does not exceed 72 hours beyond the value of the thisUpdate field

The Corporate CA OCSP responder exposes an HTTP interface accessible to relying parties. It provides revocation information as below:

- it supports real-time revocation status i.e. for every revocation performed by this CA, revocation information is available to the OCSP service immediately.
- responses define value in the nextUpdate field which is not more than 8 hours after the thisUpdate field
- the value in the nextUpdate field always before or equal to the notAfter date of all certificates included within the BasicOCSPResponse.certs field, or if the certs field is omitted, before or equal to the notAfter date of the CA certificate which issued the certificate that the BasicOCSPResponse is for.
- The Corporate CA updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

#### **4.10.2 Service availability**

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

#### **4.10.3 Optional features**

No stipulation – this section is intentionally left blank.

## **4.11 End of subscription**

No stipulation – this section is intentionally left blank.

## **4.12 Key escrow and recovery**

Key escrow and recovery are not supported by this CA.

# 5. Facility, Management and Operational Controls

## 5.1 Physical controls

### 5.1.1 Site location and construction

All critical components of the PKI system are housed within a highly secure enclave within Dubai PKI Data Center premises. Physical access controls are in place to protect the infrastructure, management systems and related operational activities of the PKI solution.

### 5.1.2 Physical access

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

The Dubai PKI systems are protected by six tiers of physical security, with access to the lower tier required before gaining access to the higher most restrictive tier. Sensitive CA operational activities related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is enforced through the use of two factor biometric authentication. Unauthorized personnel, including un-trusted or third-party employees or visitors, are not allowed into such secured areas without a prior approval and without an escort from one of trusted employees. Similar restrictions exist for the Disaster Recovery site.

All the Networking and systems components including the certification components are located in secure Data cabinets with locks from both sides. To prevent tampering, cryptographic hardware is stored in the most secure area, with access limited to authorized personnel. Power and air conditioning

The secure enclave must be furnished with an uninterruptible power supply (UPS), heating ventilating and air conditioning (HVAC) sufficient to maintain the computer equipment within the manufacturers recommended range of operating temperatures and humidity.

### 5.1.3 Water exposures

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

### 5.1.4 Fire prevention and protection

The enclave must be protected from fire, heat with a smoke detection equipment monitored on a 24\*7\*365. Fire suppression equipment must be installed within the enclave.

### **5.1.5 Media storage**

Electronic optical and other media must be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains security audit archive and backup information must be stored in a secure fire-protected safe while within the enclave.

### **5.1.6 Waste disposal**

All obsolete paper, magnetic media, optical media, etc. created within the enclave must 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.

### **5.1.7 Off-site backup**

Dubai PKI systems 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 theDubai PKI main site in accordance with the Dubai PKI Disaster Recovery plan and Procedures.

Facilities used for offsite backup and archives shall have the same level of security as theDubai PKI's main site.

## **5.2 Procedural controls**

DESC follows 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.

DESC obtains a signed statement from each member of the staff concerned on not having conflicting interests with the Corporate 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 following are the trusted roles for a Corporate CA:

- CA Administrator
- CA Security Officer
- CA Directory Administrator
- CA Database Administrator
- HSM Administrator
- HSM Partition Owner
- HSM Partition MofN Custodian
- HSM Security Officer

- System Administrator
- Internal Auditor
- External Auditor

DESC conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to ensure their trustworthiness and competence.

### **5.2.2 Number of persons required per task**

DESC 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:

- DESC shall confirm the identity of the employee by carrying out background checks.
- DESC shall issue an access card to Administrators who need to access equipment located in the secure enclave.
- DESC shall deliver the necessary credentials that allow Administrators to conduct their functions.

### **5.2.4 Roles requiring separation of duties**

DESC ensures separation among the following discreet work groups to ensure no one individual can complete any of critical transactions such as revocation of Subordinate CA certificate:

- Personnel that manages operations on certificates
- Administrative personnel to operate the supporting platform
- Security personnel to enforce security measures

## **5.3 Personnel controls**

DESC ensures implementation of security controls with regard to the duties and performance of the members of its staff with regard to the Corporate CA activities. These security controls are documented in an internal confidential policy and include the areas below.

### **5.3.1 Qualifications, experience and clearance requirements**

DESC ensures 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**

DESC conducts background investigations for all Dubai PKI personnel, contractors, trusted roles and management positions. Additionally, Dubai PKI staff who have Trusted roles go through an annual background check to ensure continuous trustworthiness of those employees

### **5.3.3 Training requirements**

DESC makes 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 are tested through an examination on the information verification requirements outlined in the Baseline Requirements.

### **5.3.4 Retraining frequency and requirements**

Periodic training will 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**

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

### **5.3.6 Sanctions for unauthorized actions**

DESC sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the DESC Subordinate CAs 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 PKI Subordinate CAs component services subcontractors and their personnel are subject to the same background checks as DESC 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

DESC makes available documentation to personnel, during initial training and retraining.

## 5.4 Audit logging procedures

### 5.4.1 Types of event recorded

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. At a minimum, each audit record includes the following:

- The type of event
- The date and time the event occurred
- A success or failure indicator of the event (e.g. CA signing event, revocation event, certificate validation event)
- The identity of the entity and/or operator that caused the event.
- Description of the event.

DESC ensures that at least the following details are recorded:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device lifecycle management events
- CA and subscriber certificate lifecycle 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, Dubai PKI maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:



*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

- Start and stop of servers
- Outages and major problems
- Physical access of personnel and other persons to sensitive parts of theDubai PKI 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
  - System configuration changes and maintenance, as defined in the CPS
  - CA personnel changes
  - Discrepancy and compromise reports
  - Information concerning the destruction of sensitive information
  - Current and past versions of all Certificate Policies
  - Current and past versions of Certification Practice Statements
  - Vulnerability Assessment Reports
  - Threat and Risk Assessment Reports
  - Compliance Inspection Reports
  - Current and past versions of Agreements
- 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**

DESC ensures that 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 are periodically archived for inspection by authorizedDubai PKIpersonnel and designated auditors. The log files are properly protected by an access control mechanism, so that no others can have access. Log files and audit trails are 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 Corporate CA audit log:

- Backup media shall be stored locally in DESC's main site in a secure location.
- A second copy of the audit log data and files shall be stored outside DESC'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 PKI systems are subject to an annual assessment in line with DESC system assurance policy and this CPS.

## **5.5 Records archival**

DESC keeps records of the following items:

- All certificates for a minimum period of 7 years after the expiration of that certificate.
- Audit trails on the issuance of certificates for a minimum period of 7 years after issuance of a certificate.
- Audit trail of the revocation of a certificate for a minimum period of 7 years after revocation of a certificate.
- CRLs for a minimum period of 7 years after publishing.

The very last back up of the Subordinate CA archive will be retained for 7 years following the issuance of the last certificate by the Subordinate CA.

DESC archives audit logging data on a regular basis and keeps archived data in a retrievable format.

DESC ensures the integrity of the physical storage media and implements proper backups to prevent data loss.

Archives are accessible to authorized personnel of DESC.

### **5.5.1 Types of records archived**

DESC retains in a trustworthy manner records of digital certificates, audit data, systems information and documentation. Dubai PKI ensures that at least the following records are archived:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival and destruction
  - Cryptographic device lifecycle management events
- CA and Subscriber Certificate lifecycle 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**

DESC retains 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 are 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 is taken at each key ceremony.

### **5.5.5 Requirements for time-stamping of records**

All recorded events include the date and time of when the event took place, based on the time of the operating system. Procedures are 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 is allowed to handle archive material.

### **5.5.7 Procedures to obtain and verify archive Information**

Only DESC staff members with a clear hierarchical control and a definite job description may obtain and verify archive information. DESC retains records in electronic or in paper-based format.

## **5.6 Key changeover**

The Corporate CA private keys are 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, Dubai PKI specifies applicable incident, compromise reporting and handling procedures. Dubai PKI specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

### **5.7.2 Computing resources, software/data corruption**

DESC and all other PKI Participants (other than subscribers and relying parties), establishes the necessary measures to ensure full recovery of the Corporate CA services in case of a disaster, corrupted servers, software or data.

DESC establishes:

- Disaster recovery resources in a location sufficiently distant from the regular Dubai PKI Subordinate CAs 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 with witnessing of more than one member of the Dubai PKI PA.

### **5.7.3 Entity private key compromise procedures**

For subscriber's key compromise, see section 4.9 of the present CPS.

In the event of a key compromise of the Corporate, the following actions shall be taken by DESC:

- All active certificates issued by the Corporate CA shall be revoked.
- Organizations holding Client Certificates shall be notified.

- A new Corporate CA key pair shall be generated and certificate produced by the Dubai Root CA.
- A Corporate CA compromise notice shall be published toward relevant relying parties.
- After Dubai PKI has identified the compromise scenario and established proper remedies, issuing certificates for existing and new entities may start. This shall happen according to the certificate management procedures listed in this CPS document.

#### **5.7.4 Business continuity capabilities after a disaster**

DESC establishes the necessary measures to full and automatic recovery of the on-line services such as CRL availability in case of a disaster, corrupted servers, software or data.

DESC establishes the necessary measures to ensure full recovery of the off-line services service in case of a disaster, corrupted servers, software or data.

A **Business Continuity Plan** has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document. It includes the following:

1. Conditions for activating the plan
2. Emergency procedures
3. Fallback procedures
4. Resumption procedures
5. A maintenance schedule for the plan
6. Awareness and education requirements
7. Responsibilities of individuals
8. Recovery time objective (RTO)
9. Regular testing of contingency plans
10. Plan to maintain or restore 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. 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 Dubai PKI determines that termination this CA is deemed necessary, Dubai PKI 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. Dubai PKI shall arrange for the retention of archived data specified in

*Dubai PKI – Corporate CA*  
***Certification Practice Statement***

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.

If an LRA decides to terminate operations, the Agreement between Dubai PKI and the LRA shall set forth what actions are to be taken to ensure continued support for certificates previously issued by the Corporate CA. Upon termination of the RA Agreement, the RA certificate shall be revoked, and Dubai PKI will be the custodian of LRA archival records in case of termination.

# 6. Technical Security Controls

## 6.1 Key pair generation

The requirements for generating and installing the Corporate CA are stated in the following sections.

### 6.1.1 Key pair generation

#### 6.1.1.1 CA key pair generation

The Corporate CA keys shall be generated as part of a key ceremony produced by the PA and executed under the supervision of the PA.

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).

DESC ensures the implementation and documentation of key generation procedures in line with this CPS. It acknowledges public, international and WebTrust and CA/Browser Forum Guidelines on trustworthy systems, incorporating the following requirements:

- At least four trusted persons participate in the generation and installation of Corporate CA private key(s); two trusted operatives and two key custodians
- The Corporate CA Key Generation Ceremony will be witnessed by the CA's Qualified Auditor (see section 8 Compliance Audit and Other Assessments)
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians
- The PKI operations team and key custodians act upon authorization by DESC, who is the owner of the Corporate CA private keys, to perform cryptographic operations using the Corporate CA private key(s)
- The Qualified Auditor will then issue a report, covering that the Corporate CA, during its Corporate CA Key Pair and Certificate generation process:
  - Documented its Corporate CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement
  - Included appropriate detail in its Corporate CA Key Generation Script
  - Maintained effective controls to provide reasonable assurance that the Corporate CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Corporate CA Key Generation Script
  - Performed, during the Corporate CA key generation process, all the procedures required by its Corporate CA Key Generation Script

- A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes

### **6.1.1.2 Subscriber key pair generation**

The Corporate CA does not perform subscriber key generation.

The LRA or the subscribers themselves as per the table below can generate subscribers' keys:

<b>Certificate type</b>	<b>Key generation requirements</b>
Encryption certificates	Key pair is generated using a FIPS-approved methods for key generation
Digital signature certificates	Key pair is generated on a hardware based cryptographic modules using FIPS-approved methods
Authentication certificates	Key pair is generated using a FIPS-approved methods for key generation
Code signing certificates	Key pair is generated using a FIPS-approved methods for key generation
OCSP certificates	Key generation is done using a dedicated OCSP key management utility. The OCSP key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module

### **6.1.2 Private key delivery to subscriber**

Not applicable.

### **6.1.3 Public key delivery to certificate issuer**

Public keys shall be delivered to the CA 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).

### **6.1.4 CA public key delivery to relying parties**

The CA should make its certificates available to subscribers and relying parties by publishing them in a public repository (<https://ca-repository.desc.gov.ae/>).

### **6.1.5 Key sizes**

This Corporate CA key pair is 4096-bit RSA.

The subscriber key pair must be at least 2048-bit RSA, recommended 4096-bit RSA or at least 256-bit ECDSA, recommended 384-bit ECDSA.

### **6.1.6 Public key parameters generation and quality checking**

The Corporate 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).



### 6.1.7 Key usage purposes (as per X.509 v3 key usage field)

The certificates will always contain a KeyUsage bit string in accordance with RFC 5280. The below tables elaborate further on the KeyUsage of the CA certificate and the end-entity certificates issued by this CA.

#### 6.1.7.1 Corporate CA

Corporate CA key usage.

CA signing
Corporate CA signing keys are the only keys permitted to be used for signing certificates and CRLs.
The Certificate KeyUsage field must be set to: KeyCertSign and cRLSign

#### 6.1.7.2 Certificates for individuals

Subscriber’s key usage.

Signing	Encryption	Authentication
Keys may be used to produce digital signatures on digital transactions and for document signing.	Key will be used for secure email and for document encryption	Key will be used for subscriber authentication
The Certificate KeyUsage field will be set to:	The Certificate KeyUsage field will be set to:	The Certificate KeyUsage field will be set to:
Key usage: Bitstring {nonRepudiation}	Key usage: Bitstring {keyEncipherment, dataEncipherment}	Key usage: Bitstring {digitalSignature, keyEncipherment}

#### 6.1.7.3 Certificates for government entities

Subscriber’s key usage.

Legal Signing	Code Signing
Keys may be used to digitally sign documents on behalf of government entity.	Keys may be used to digitally sign code.
The Certificate KeyUsage field will be set to:	The Certificate KeyUsage field will be set to:
Key usage: Bitstring { nonRepudiation }	Key usage: Bitstring {digitalSignature}

## 6.2 Private key protection and cryptographic module engineering controls

### **6.2.1 Cryptographic module standards and controls**

DESC shall generate subordinate key pairs and store their private keys within a Cryptographic Device that is certified according to the rating specified in 6.2.11.

Subscriber and RA key pairs shall be generated in cryptographic modules at least compliant to FIPS 140-2 Level 2 or higher.

### **6.2.2 Private key multi-role control**

DESC 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 the CA cryptographic hardware.

### **6.2.3 Private key escrow**

Not applicable.

### **6.2.4 Private key backup**

The Corporate CA private keys shall be backed up within backup devices that meet the same certification level as the subordinate CA HSM and as described in section 6.2.1.

The creation of key backups on backup devices 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**

No stipulation – this section is intentionally left blank.

### **6.2.6 Private key transfer into or from an HSM**

The Corporate CA key pairs shall only be transferred to another hardware cryptographic device, for backup purposes, 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 should the CA private key be copied to disk or other media during this operation. LRA and Subscriber private keys shall not be transferred from the module they are generated in.

### **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 Corporate CA are 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.

Subscriber's private keys are not generated and managed by the Corporate CA.

### **6.2.9 Method of deactivating private key**

This CA's private key is deactivated in the following situations:

- The CA service is shut down.
- The CA HSM is manually stopped.
- 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 are cleared from memory before the memory is de-allocated. Any disk space where keys were stored must 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 Corporate CA private keys shall be destroyed by multi-person presence including at least one representative of the Dubai PKI PA, in order to ensure that these private keys cannot ever be retrieved and used again.

The key destruction process is documented in Cryptographic Devices Lifecycle Management Policy and Procedure. Any associated records are archived.

The decision for private key destruction outside the context of the end of its lifetime needs to be authorized in writing by multiple members of the Dubai PKI PA. This decision includes the assignment of the personnel.

### **6.2.11 Cryptographic module rating**

The CA must use a Cryptographic Device certified to FIPS 140-2 Level 3 or ISO 15408 Common Criteria (CC) EAL 4+ or above. Subscriber certificates must be generated in a FIPS 140-2 Level 2 or higher compliant devices.

## **6.3 Other aspects of key pair management**

### **6.3.1 Public key archival**

Refer to section 5.5 of this CPS.

### **6.3.2 Certificate operational periods and key pair usage periods**

- The maximum operational period of the CA's key pair must be set for eight (8) years.
- The maximum operational period for a subscriber's key pair must be five (5) years.

<b>Key certificate type</b>	<b>Maximum validity period</b>
Certification Authority Certificate and associated keys	Recommended 96 months, re-key at 37% lifetime i.e., 36 months
Certificates for individuals and associated keys	Maximum operational period for a subscriber's key pair must be five years i.e., 60 months
Certificates for government entities and associated keys	Maximum operational period for a subscriber's key pair must be five years i.e., 60 months

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

#### 6.4.1.1 CA key generation

The Corporate CA activation data 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 the Corporate 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 Corporate CA shall register its subscribers prior to issuing digital certificates to the subscribers.

The enrolment of a subscriber shall result in activation data to be 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 CA 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 via an automated process through the secure exchange of activation data between the Corporate CA and RA applications.

### 6.4.3 Other aspects of activation data

No stipulation – this section intentionally left blank.

## 6.5 Computer security controls

The Corporate CA shall perform all CA and RA functions using trustworthy systems that meet Dubai PKI security and audit requirements.

### 6.5.1 Specific computer security technical requirements

The Corporate CA shall be operated according to the following security controls:

- Physical access control to 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 CA history and audit data
- Audit of security-related events
- Automatic and regular validation of 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 this 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 Corporate CA and RAs functionality shall be scanned for malicious code on first use and periodically afterwards.

Upon installation, and at least once a week, the integrity of this CA database shall be validated.

### **6.6.3 Life cycle security controls**

No stipulation – this section intentionally left blank.

## **6.7 Network security controls**

DESC ensures maintenance of network security, including managed firewalls and intrusion detection systems.

The network is segmented into several zones, based on their functional, logical and physical relationship. Network boundaries are 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 are 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 and OCSP Profiles

## 7.1 Certificate profile

### 7.1.1 Certificates for individuals

#### 7.1.1.1 Subscriber's encryption certificate ASN1 description

This is the complete ASN1 description of the certificate associated to the encryption key of the subscriber.

Field	CE <sup>1</sup>	O/M <sup>2</sup>	CO <sup>3</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(1) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded

<sup>1</sup> CE = Critical Extension.

<sup>2</sup> O/M: O = Optional, M = Mandatory.

<sup>3</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than <b>[60]</b> Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	<optional organizational unit name> as agreed during onboarding process	UTF8 encoded
	organizationName		M	D	<Government entity meaningful name> or as agreed during onboarding process	UTF8 encoded
	localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user name>	UTF8 encoded
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA / ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
<b>Authority Properties</b>						
authorityKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field

Dubai PKI – Corporate CA  
**Certification Practice Statement**

accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2.2 id-ad-ca/issuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints		False	M		
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRLNumber>.crl	CRL download URL.
<b>Subject Properties</b>					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>					
keyUsage	True	M			
keyEncipherment		M	S	True	
dataEncipherment		M	S	True	
<b>Extended Key Usage Properties</b>					
extKeyUsage	False	M			
emailProtection		M	S	True	
<b>Certificate Policy Properties</b>					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.1	

### 7.1.1.2 Subscriber's signing certificate ASN1 description

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE <sup>4</sup>	O/M <sup>5</sup>	CO <sup>6</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				

<sup>4</sup> CE = Critical Extension.

<sup>5</sup> O/M: O = Optional, M = Mandatory.

<sup>6</sup> CO = Content: S = Static, D = Dynamic



Dubai PKI – Corporate CA  
**Certification Practice Statement**

CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature		False	M		
algorithm		M	S	(2) OID 1.2.840.113549.1.1.11	=SHA256 with RSA Encryption
issuer		False	M		
countryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity		False	M		Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than <b>[60]</b> Months	
subject		False	M		
countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationUnitName		O	D	<optional organizational unit name> or as agreed during onboarding process	UTF8 encoded
organizationName		M	D	<Government entity meaningful name> or as agreed during onboarding process	UTF8 encoded
localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
commonName		M	D	<Individual end user name>	UTF8 encoded
SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M		
algorithm		M	D	RSA/ECDSA	

Dubai PKI – Corporate CA  
**Certification Practice Statement**

subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions		M			
<b>Authority Properties</b>					
authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed certificates
keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M		
AccessMethod		M	S	Id-ad-2 1 id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2 2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA certificate download URL
cRLDistributionPoints		False	O		
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crfile<CRL Number>.crl	CRL download URL.
<b>Subject Properties</b>					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>					
keyUsage	True	M			
nonRepudiation		M	S	True	
<b>Certificate Policy Properties</b>					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.3 <For certificates issued for moderate assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.4>	

### 7.1.1.3 Subscriber's authentication certificate ASN1 description (Deprecated)

This is the complete ASN1 description of the certificate associated to the authentication key of the subscriber.

Field	CE <sup>7</sup>	O/M <sup>8</sup>	CO <sup>9</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(3) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M			
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than <b>[60]</b> Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationUnitName		O	D	<optional organizational unit name> or as agreed during onboarding process	UTF8 encoded

<sup>7</sup> CE = Critical Extension.

<sup>8</sup> O/M: O = Optional, M = Mandatory.

<sup>9</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

organizationName		M	D	<Government entity meaningful name> or as agreed during onboarding process	UTF8 encoded
localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
commonName		M	D	<Individual end user's name>	UTF8 encoded
SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M		
algorithm		M	D	RSA/ECDSA	
subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M		
<b>Authority Properties</b>					
authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed certificates
keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M		
AccessMethod		M	S	Id-ad-2 1 id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2 2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	<a href="http://ca-repository.desc.gov.ae/certificate/corporate.p7b">http://ca-repository.desc.gov.ae/certificate/corporate.p7b</a>	Corporate CA Certificate download URL.
cRLDistributionPoints		False	O		
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crfile<CRL Number>.crl	CRL download URL.
<b>Subject Properties</b>					
subjectKeyIdentifier	False	M			

Dubai PKI – Corporate CA  
**Certification Practice Statement**

keyIdentifier		M	D	SHA-1 Hash	
subjectAltName	False	O			
GeneralName			D	RFC822 Name	Email address will be included if the certificate is used for email signing
<b>Key Usage Properties</b>					
keyUsage	True	M			
digitalSignature		M	S	True	
keyEncipherment		M	S	True	
dataEncipherment		M	S	True	
<b>Extended Key Usage Properties</b>					
extKeyUsage	False	M			
clientAuth		M	S	True	
emailProtection		M	S	True	
<b>Certificate Policy Properties</b>					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.2	

#### 7.1.1.4 Subscriber's mobile authentication certificate ASN1 description

This is the complete ASN1 description of the certificate associated to the authentication key of the subscriber.

Field	CE <sup>10</sup>	O/M <sup>11</sup>	CO <sup>12</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(4) OID 1.2.840.113549.1.1.11	=SHA256 with RSA Encryption
Issuer	False	M			

#### 10 CE = Critical Extension.

<sup>11</sup> O/M: O = Optional, M = Mandatory.

<sup>12</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

countryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than <b>[60]</b> Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationUnitName		O	D	<optional organizational unit name> or as agreed during onboarding process	UTF8 encoded
organizationName		M	D	<Government entity meaningful name> or as agreed during onboarding process	UTF8 encoded
localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
commonName		M	D	<Individual end user’s name>	UTF8 encoded
SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo	False	M			
algorithm		M	D	RSA/ECDSA	
subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions		M			
Authority Properties					

Dubai PKI – Corporate CA  
**Certification Practice Statement**

authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed certificates
keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess	False	M			
AccessMethod		M	S	Id-ad-2 1 id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2 2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints	False	O			
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
<b>Subject Properties</b>					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>					
keyUsage	True	M			
digitalSignature		M	S	True	
<b>Certificate Policy Properties</b>					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.5	

**7.1.1.5 Subscriber's authentication certificate ASN1 description (for natural persons)**

This is the complete ASN1 description of the certificate associated to the authentication key of the subscriber.

Field	CE <sup>13</sup>	O/M <sup>14</sup>	CO <sup>15</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			

<sup>13</sup> CE = Critical Extension.

<sup>14</sup> O/M: O = Optional, M = Mandatory.

<sup>15</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

<b>Signature</b>		False	M			
algorithm			M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue			M	D	Corporate CA Signature.	CA signature value
<b>TBSCertificate</b>						
<b>Version</b>		False				
			M	S	2	Version 3
<b>SerialNumber</b>		False				
CertificateSerialNumber			M	D		At least 64 bits of entropy Validated on duplicates.
<b>signature</b>		False	M			
algorithm			M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
<b>issuer</b>		False	M			
countryName			M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationName			M	S	UAE Government	UTF8 encoded
commonName			M	S	Corporate Certification Authority	UTF8 encoded
<b>Validity</b>		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore			M	D	Certificate generation process date/time.	
NotAfter			M	D	Certificate generation process date/time + not more than <b>[36]</b> Months	
<b>subject</b>		False	M			
countryName			M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationUnitName			O	D	<optional organizational unit name> or as agreed during onboarding process	UTF8 encoded
organizationName			M	D	<Entity meaningful name> or as agreed during onboarding process	UTF8 encoded
localityName			M/O	D	User’s locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
commonName			M	D	<Individual end user’s name>	UTF8 encoded
SERIALNUMBER			O	D	<Identifier for each individual>	PrintableString encoded



Dubai PKI – Corporate CA  
**Certification Practice Statement**

subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
<b>Authority Properties</b>						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 <i>id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1</i> (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 <i>id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2</i> (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crfile<CRL Number>.crl	CRL download URL.
<b>Subject Properties</b>						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>						
keyUsage		True	M			
	digitalSignature		M	S	True	
	keyEncipherment		M	S	True	
<b>Extended Key Usage Properties</b>						
extKeyUsage		False	M			
	clientAuth		M	S	True	
<b>Certificate Policy Properties</b>						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.6	

## 7.1.2 Certificates for Government entities

### 7.1.2.1 Subscriber's signing certificate (eSeal/legal signing certificate) ASN1 description

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE <sup>16</sup>	O/M <sup>17</sup>	CO <sup>18</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(5) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M			
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than <b>[60]</b> Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

<sup>16</sup> CE = Critical Extension.

<sup>17</sup> O/M: O = Optional, M = Mandatory.

<sup>18</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

organizationUnitName		O	D	<optional organizational unit name within the Government entity>	UTF8 encoded
organizationName		M	D	<Government entity meaningful name>	UTF8 encoded
localityName		M/O	D	<Government entity locality>	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName		M/O	D	<Government entity locality>	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
commonName		M	D	<Government Entity Service Name as agreed during subscriber registration process >	UTF8 encoded
subjectPublicKeyInfo	False	M			
algorithm		M	D	RSA/ECDSA	
subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions		M			
<b>Authority Properties</b>					
authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed certificates
keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess	False	M			
AccessMethod		M	S	Id-ad-2.1 id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2.2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA certificate download URL
cRLDistributionPoints	False	O			
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
<b>Subject Properties</b>					
subjectKeyIdentifier	False	M			

Dubai PKI – Corporate CA  
**Certification Practice Statement**

	keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>						
(6)	keyUsage	True	M			
(7)	nonRepudiation		M	S	True	
<b>Certificate Policy Properties</b>						
	certificatePolicies	False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
	certificatePolicies	False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1	

**7.1.2.2 Subscriber's code signing certificate ASN1 description**

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE <sup>19</sup>	O/M <sup>20</sup>	CO <sup>21</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(8) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than [36] Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

<sup>19</sup> CE = Critical Extension.

<sup>20</sup> O/M: O = Optional, M = Mandatory.

<sup>21</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

organizationUnitName		O	D	<Government Entity Organization Unit Name> as agreed during subscriber registration process	UTF8 encoded
organizationName		M	D	<Government Entity Organization Name> as agreed during subscriber registration process	UTF8 encoded
localityName		M/O	D	<Government entity locality> as agreed during subscriber registration process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
commonName		M	D	<Government Entity Organization Unit Name> as agreed during subscriber registration process >	UTF8 encoded
subjectPublicKeyInfo	False	M			
algorithm		M	D	RSA/ECDSA	
subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions		M			
<b>Authority Properties</b>					
authorityKeyIdentifier	False	O			
keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	
authorityInfoAccess	False	M			
AccessMethod		M	S	Id-ad-2.1 id-ad-ocsp OID i.e.1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2.2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints	False	M			
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crfile<CRL Number>.crl	CRL download URL.
<b>Subject Properties</b>					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>					
keyUsage	True	M			
digitalSignature		M	S	True	
<b>Extended Key Usage Properties</b>					

*Dubai PKI – Corporate CA*  
**Certification Practice Statement**

extKeyUsage	False	M				
codeSigning		M	S	True		
certificatePolicies	False	M				
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1		
policyQualifiers:policyQualifierId		M	S	id-qt 1		
policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS		
certificatePolicies	False	M				
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.2.2		
certificatePolicies	False	M				
PolicyIdentifier		M	S	2.23.140.1.4.1		Code Signing Certificate issued in compliance with the Code Signing Baseline Requirements

### 7.1.3 Version number

This CA issues X.509 version 3 certificates as defined in RFC 5280.

### 7.1.4 Certificate extensions

The Corporate CA subscriber certificates require the use of the following extensions:

- CertificatePolicies (not critical)
  - policyIdentifier
  - policyQualifiers
    - policyQualifierId
- cRLDistributionPoints (not critical)
- authorityInformationAccess (not critical)
  - URL of the Issuing CA's OCSP responder
  - URL of the Issuing CA's certificate
- KeyUsage (critical)
- extKeyUsage (not critical)
- authorityKeyIdentifier (not critical)

### 7.1.5 Algorithm object identifiers

X.509v3 standard OIDs is used. Algorithm must be RSAencryption for the subjectkey and SHA256withRSA encryption for the certificate signature.

### 7.1.6 Name forms

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

### 7.1.7 Name constraints

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

### 7.1.8 Certificate policy object identifier

Refer to the ASN1 definitions described in this chapter.

### 7.1.9 Usage of policy constraints extension

No stipulation – this section is intentionally left blank.

### 7.1.10 Policy qualifiers syntax and semantics

No stipulation – this section intentionally left blank.

### 7.1.11 Processing semantics for critical certificate extensions

Critical extensions, when marked, is interpreted by relying parties accordingly.

## 7.2 CRL profile

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

### 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 contain the CRLNumber (a sequential number incremented with each new CRL produced).

### 7.2.3 CRL ASN1 description

This is the complete ASN1 description of the CRL certificate.

Field	CE <sup>22</sup>	CO <sup>23</sup>	Value	Comment
CertificateList				
TBSCertificate				
Signature	False			
algorithm		S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		D	Corporate CA Signature.	CA signature value
TbsCertList				
Version	False			
		S	2	V2
SerialNumber	False			

<sup>22</sup> CE = Critical Extension.

<sup>23</sup> CO = Content: S = Static, D = Dynamic



Dubai PKI – Corporate CA  
**Certification Practice Statement**

CertificateSerialNumber		F		At least 64 bits of entropy Validated on duplicates.
signature		False		
algorithm		S	(9) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer		False S		
countryName		S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		S	UAE Government	UTF8 encoded
commonName		S	Corporate Certification Authority	UTF8 encoded
Validity		False		
				Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		D	CRL generation date/time	
nextUpdate		D	CRL generation date/time + 1 day + 2 hours	
revokedCertificates				
Certificate				
CertificateSerial		D	Serial of the revoked certificate	
revocationDate		D	UTC Time of revocation (Optional)	
crlExtensions				
authorityKeyIdentifier	False		This MUST be the same value as the subject Key Identifier field in the CRL Issuer's certificate. Non-critical <subject key identifier CA>	SHA-1 Hash of the Corporate CA public key
crlNumber	False			Sequential CRL number
IssuingDistributionPoint		True		
DistributionPoint		D	CN=CRL1 CN=UAE Global Root CA G4 E2 O=UAE Government C=AE	Partitioned CRL directory address
DistributionPoint		D	<i>http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea&lt;CRLNumber&gt;.crl</i>	<i>CRL hosting URL, where &lt;CRL Number&gt; a dedicated sequence number that the CA uses for CRL file naming</i>
onlyContainsCACerts		S	No	
onlyContainsUserCerts		S	Yes	
IndirectCRL		S	No	

expiredCertsOnCRL (2.5.29.60)	False	D	< a date-time value specifies the date on or after which revoked certificates are retained on the CRL>
-------------------------------	-------	---	--

## 7.3 OCSP profile

### 7.3.1 Version number(s)

The OCSP responder issues OCSP responses of version 1.

### 7.3.2 OCSP extensions

- The OCSP response signing authority is designated to the DESC OCSP responder therefore; the OCSP certificate contains the id-kp-OCSPSigning OID in the extended Key Usage extension.
- The certificate will include the extension id-pkix-ocsp-nocheck as a none-critical extension, which indicates that an OCSP relying party can trust an OCSP response signing certificate for its lifetime.

### 7.3.3 OCSP Response Signing Certificate ASN1 Description

This is the complete ASN1 description of the certificate associated to the OCSP response signing private key.

Field	CE <sup>24</sup>	O/M <sup>25</sup>	CO <sup>26</sup>	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(10) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded

<sup>24</sup> CE = Critical Extension.

<sup>25</sup> O/M: O = Optional, M = Mandatory.

<sup>26</sup> CO = Content: S = Static, D = Dynamic

Dubai PKI – Corporate CA  
**Certification Practice Statement**

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than [12] Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	commonName		M	S	Corporate Certification Authority OCSP	
	organizationName		M	S	DESC	
	localityName		M	S	Dubai	
subjectPublicKeyInfo		False	M			
	algorithm		M	S	RSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions			M			
<b>Authority Properties</b>						
authorityKeyIdentifier		False	M			
	KeyIdentifier		M	S	SHA-1 Hash of the Corporate CA public key	When this extension is used, this field MUST be supported at minimum
<b>Subject Properties</b>						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
<b>Key Usage Properties</b>						
Key Usage		True	M			
	digitalSignature		M	S	True	
	nonRepudiation		M	S	True	
extKeyUsage		False	M			
	id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck		False	M	S	05 00	
<b>Certificate Policy Properties</b>						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	

## 8. Compliance Audit and Other Assessments

DESC organizes compliance audits to ensure that it meets requirements, standards, procedures and service levels according to this CPS at least on an annual basis. DESC accepts this auditing of its own practices and procedures and will make the audit report publicly available no later than three months after the end of the audit period. The Dubai PKI PA evaluates the results of such audits before further implementing them.

### 8.1 Frequency or Circumstances of Assessments

The Corporate CA shall be subjected to periodic compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques. DESC also performing internal audit at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. Moreover, DESC may require ad-hoc compliance audits of Dubai Root CA to validate that it is operating in accordance with the respective CP, PDS, CPS, and other supporting operational policies and procedures.

### 8.2 Identity and Qualifications of the Assessor

To carry out the audits, there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with DESC nor any person having any conflicting interests thereof.

The Corporate CA is audited for compliance to one or more of the following standards

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities – SSL Baseline with Network Security
- AICPA/CICA WebTrust for Certification Authorities – Publicly Trusted Code Signing Certificates

These audits will be performed by qualified auditors that fulfil the following requirements:

- Independence from the subject of the audit
- Ability to conduct an audit that addresses the criteria specified in the latest version of WebTrust for Certification Authorities

- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

If irregularities are detected, the auditor will submit a report to the Dubai PKI PA, stating the measures that will be taken to rectify the situation and ensure compliance. If the proposed measures are deemed insufficient, a second audit will be carried out to ensure compliance.

## **8.3 Assessor’s Relationship to Assessed Party**

The entity that performs the annual audit SHALL be completely independent of the CA.

## **8.4 Topics Covered by Assessment**

The compliance audits will verify whether the CA PKI operations environment is in compliance with the Corporate CA CP/CPS and supporting operational policies and procedures.

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

Deficiencies identified by the auditor during the compliance audit will determine the actions to be taken. The PA is responsible for ensuring that remediation actions are documented taken within an adequate timeframe corresponding to the significance of identified matters.

## **8.6 Communication of Results**

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to Dubai PKI PA. The audit Report shall be publicly available no later than three months after the end of the audit period.

# 9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of certificates issued by the Corporate CA under this CPS as described in this section.

## 9.1 Fees

Fee details will be provided at the time of certificate issuance.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

This CPS 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 DESC.

DESC guarantees the confidentiality of any data not published in the certificates issued by the Corporate CA, according to the applicable laws on privacy.

## 9.4 Privacy of Personal Information

DESC observes personal data privacy rules and confidentiality rules as described in this CPS. 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 the Corporate CA services
- Corporate CA Private key(s)

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

DESC 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 DESC owes a duty to keep information confidential with regards to the Corporate CA activities. It owes such a duty to the RA and promptly responds to any such requests
- A court order

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 Corporate CA 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 DESC holds about it in the context of the Corporate CA activities

Confidential information will not be disclosed by the DESC 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.

DESC properly manages the disclosure of information to the Corporate CA personnel.

DESC 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 Corporate CA and the RA.
- Sessions to deliver certificates and certificate status information

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

## **9.5 Intellectual Property Rights**

DESC owns and reserves all intellectual property rights associated with its own databases, web sites, the Corporate CA digital certificates and any other publication whatsoever originating from the Corporate CA, including this CPS.

When DESC uses 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**

### **9.6.1 CA Representations and Warranties**

DESC warrant that their procedures are implemented in accordance with this CPS, and that any certificates issued under this CPS are in accordance with the stipulations specified.

### **9.6.2 RA Representations and Warranties**

An RA/LRA that performs registration functions as described in this CPS shall comply with the stipulations specified in the applicable CP and this CPS. An RA/LRA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

### **9.6.3 RA Representations and Warranties**

Subscribers shall represent to DESC that the Subscriber will:

- Securely generate its Private Keys and protect its Private Keys from compromise (including protecting any tokens or corresponding activation data that provides access to Private Keys),
- Provide accurate and complete information and communication to this CA and RA/LRA,
- Confirm the accuracy of certificate data prior to using the certificate,
- Promptly cease using a certificate and notify DESC / the government entity through which the certificate was issued if (i) any information that was submitted to the CA or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate, and



- Use the certificate only for authorized and legal purposes, consistent with this CPS and Subscriber Agreement

#### **9.6.4 Relying Party Representations and Warranties**

No stipulation.

#### **9.6.5 Representations and Warranties of Other Participants**

No stipulation.

## **9.7 Disclaimers of Warranties**

Within the limitations of the laws in Dubai, 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, the Corporate CA, 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**

The Corporate CA 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 CPS 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 CPS can be addressed to DESC contact address as stated in section 1.5.

## 9.12 Amendments

Minor changes to this CPS 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 CPS do not require a change in the CPS OID or the CPS 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 CPS OID or CPS pointer qualifier (URL).

## 9.13 Dispute Resolution Procedures

All disputes associated with this CPS 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 CPS.

## 9.15 Compliance with Applicable Law

The present CPS and provision of Corporate CA certification services are 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 CPS
- Any other applicable certificate policy as may be stated on a certificate issued by the Corporate CA
- 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.