



# Dubai Electronic Security Center

## Dubai PKI

### DESC Subordinate CAs Certificate Policy

**Project** DESC CA Project

**Title** DESC Subordinate CAs, Certificate Policy

**Classification** PUBLIC

**File Name** Dubai PKI - DESC Subordinate CAs - Certificate Policy\_v1.0

**Created on** 18 May 2017

**Revision** 1.0

**Modified on** 30 January 2018

# Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1		Initial version
12 September 2017	0.2		Minor modifications & Incorporation of Dubai government entity Root CA option
3 November 2017	0.3		Minor modifications to reflect control environment
11 January 2018	0.4		Update certificate profiles
18 January 2018	0.5		Second revision of certificate profiles
30 January 2018	1.0		Issue final version

## Table of Contents

Document History.....	2
<b>1. Introduction.....</b>	<b>8</b>
<b>1.1 Overview of Dubai PKI .....</b>	<b>8</b>
1.1.1 Dubai PKI Hierarchy.....	8
1.1.2 Certification Services.....	9
<b>1.2 Document name and Identification.....</b>	<b>9</b>
<b>1.3 PKI Participants .....</b>	<b>10</b>
1.3.1 Subordinate Certification Authorities .....	11
1.3.2 Registration Authority .....	11
1.3.3 Local Registration Authority .....	11
1.3.4 Subscribers.....	12
1.3.5 Relying Parties.....	12
1.3.6 Other Participants.....	12
<b>1.4 Certificate Usage.....</b>	<b>12</b>
1.4.1 Appropriate Certificate Use.....	12
1.4.2 Prohibited Certificate Use .....	12
<b>1.5 Policy Administration .....</b>	<b>12</b>
1.5.1 Organization Administering the Document.....	12
1.5.2 Contact Details.....	13
1.5.3 Person Determining CPS Suitability for the Policy.....	13
1.5.4 CP Approval Procedures .....	13
<b>1.6 Definitions, Acronyms and References.....</b>	<b>14</b>
1.6.1 Terminology and definitions .....	14
1.6.2 Acronyms.....	16
1.6.3 References .....	16
<b>2. Publication and Repository Responsibility .....</b>	<b>17</b>
<b>2.1 Repositories.....</b>	<b>17</b>
<b>2.2 Publication of Certificate Information.....</b>	<b>17</b>
<b>2.3 Time or Frequency of Publication Repositories.....</b>	<b>17</b>
2.3.1 Certificates.....	17
2.3.2 CRLs .....	18
<b>2.4 Access Controls on Repositories.....</b>	<b>18</b>
<b>3. Identification and Authentication .....</b>	<b>19</b>
<b>3.1 Naming.....</b>	<b>19</b>
3.1.1 Types of Names .....	19
3.1.2 Meaningful Names .....	20
3.1.3 Anonymity and Pseudonymity of Subscribers .....	20
3.1.4 Rules for Interpreting Various Name Forms.....	20
3.1.5 Uniqueness of Names .....	20
3.1.6 Recognition, authentication and role of Trademarks.....	20
<b>3.2 Initial Identity Validation .....</b>	<b>21</b>
3.2.1 Method to Prove Possession of Private Key .....	21
3.2.2 Authentication of Organization Identity .....	21
3.2.3 Authentication of individual identity.....	21
3.2.4 Authentication of Domain name .....	21

**Certificate Policy**

3.2.5	Non-verified subscriber information .....	21
3.2.6	Validation of Authority.....	21
3.2.7	Criteria for Interoperation.....	21
<b>3.3</b>	<b>Identification and Authentication for Re-keying requests.....</b>	<b>22</b>
3.3.1	Identification and Authentication for Routine Re-Keying.....	22
3.3.2	Identification and Authentication for Re-Key after revocation.....	22
<b>3.4</b>	<b>Identification and Authentication for Revocation Requests .....</b>	<b>22</b>
<b>4.</b>	<b>Certificate Life Cycle Management .....</b>	<b>23</b>
<b>4.1</b>	<b>Certificate Application .....</b>	<b>23</b>
4.1.1	Who Can Submit a Certificate Application .....	23
4.1.2	Enrolment Process and Responsibilities.....	23
<b>4.2</b>	<b>Certificate Application Processing.....</b>	<b>23</b>
4.2.1	Performing Identification and Authentication Functions .....	23
4.2.2	Approval or Rejection of Certificate Applications.....	24
4.2.3	Time to Process Certificate Applications.....	24
<b>4.3</b>	<b>Certificate Issuance .....</b>	<b>24</b>
4.3.1	CA Actions during Certificate Issuance.....	24
4.3.2	Notification to Subscriber by the CA of Issuance of Certificate.....	24
<b>4.4</b>	<b>Certificate Acceptance.....</b>	<b>24</b>
4.4.1	Conduct Constituting Certificate Acceptance .....	24
4.4.2	Publication of the Certificate by the CA .....	24
4.4.3	Notification of Certificate Issuance by the CA to Other Entities .....	24
<b>4.5</b>	<b>Key Pair and Certificate Usage .....</b>	<b>25</b>
4.5.1	Subscriber Private Key and Certificate Usage .....	25
4.5.2	Relying on Party Public Key and Certificate Usage .....	25
<b>4.6</b>	<b>Certificate Renewal .....</b>	<b>25</b>
<b>4.7</b>	<b>Certificate Re-key.....</b>	<b>25</b>
4.7.1	Circumstance for Certificate Re-key .....	25
4.7.2	Who May Request Certification of a New Public Key .....	25
4.7.3	Processing Certificate Re-keying Requests.....	26
4.7.4	Notification of New Certificate Issuance to Subscriber .....	26
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate.....	26
4.7.6	Publication of the Re-keyed Certificate by the CA.....	26
4.7.7	Notification of Certificate Issuance by the CA to Other Entities .....	26
<b>4.8</b>	<b>Certificate Modification.....</b>	<b>26</b>
4.8.1	Circumstance for Certificate Modification.....	26
4.8.2	Who May Request Certificate Modification .....	26
4.8.3	Processing Certificate Modification Requests .....	26
4.8.4	Notification of New Certificate Issuance to Subscriber .....	26
4.8.5	Conduct Constituting Acceptance of Modified Certificate.....	26
4.8.6	Publication of the Modified Certificate by the CA.....	26
4.8.7	Notification of Certificate Issuance by the CA to Other Entities .....	26
<b>4.9</b>	<b>Certificate Revocation and Suspension .....</b>	<b>27</b>
4.9.1	Circumstances for Revocation .....	27
4.9.2	Who Can Request Revocation.....	27
4.9.3	Procedure for Revocation Request.....	27
4.9.4	Revocation Request Grace Period .....	27
4.9.5	Revocation Request Response Time .....	28
4.9.6	Revocation Checking Requirement for Relying Parties .....	28
4.9.7	CRL Issuance Frequency .....	28

**Certificate Policy**

4.9.8	Maximum Latency for CRLs.....	28
4.9.9	Online Revocation/Status Checking Availability .....	28
4.9.10	Online Revocation Checking Requirements .....	28
4.9.11	Other Forms of Revocation Advertisements Available .....	28
4.9.12	Special Requirements — Key Compromise.....	28
4.9.13	Circumstances for Suspension .....	28
4.9.14	Who Can Request Suspension.....	28
4.9.15	Procedure for Suspension Request .....	28
<b>4.10</b>	<b>Certificate Status Services.....</b>	<b>28</b>
4.10.1	Operational Characteristics .....	29
4.10.2	Service Availability .....	29
4.10.3	Optional Features .....	29
<b>4.11</b>	<b>End of Subscription .....</b>	<b>29</b>
<b>4.12</b>	<b>Key Escrow and Recovery .....</b>	<b>29</b>
4.12.1	Key Escrow and Recovery Policy and Practices .....	29
4.12.2	Session Key Encapsulation and Recovery Policy and Practices .....	29
<b>5.</b>	<b>Facility, Management and operational Controls.....</b>	<b>30</b>
<b>5.1</b>	<b>Physical Controls.....</b>	<b>30</b>
5.1.1	Site Location and Construction .....	30
5.1.2	Physical Access .....	30
5.1.3	Power and Air Conditioning.....	30
5.1.4	Water Exposures.....	30
5.1.5	Fire Prevention and Protection.....	30
5.1.6	Media Storage.....	30
5.1.7	Waste Disposal .....	30
5.1.8	Offsite Backup.....	31
<b>5.2</b>	<b>Procedural Controls.....</b>	<b>31</b>
5.2.1	Trusted Roles.....	31
5.2.2	Number of Persons Required Per Task .....	31
5.2.3	Identification and Authentication for Each Role .....	31
5.2.4	Roles Requiring Separation of Duties.....	32
<b>5.3</b>	<b>Personnel Controls .....</b>	<b>32</b>
5.3.1	Qualifications Experience and Clearance Requirements .....	32
5.3.2	Background Check Procedures.....	32
5.3.3	Training Requirements .....	32
5.3.4	Retraining Frequency and Requirements .....	32
5.3.5	Job Rotation Frequency and Sequence.....	32
5.3.6	Sanctions for Unauthorized Actions.....	33
5.3.7	Independent Contractor Requirements.....	33
5.3.8	Documentation Supplied to Personnel.....	33
<b>5.4</b>	<b>Audit Logging Procedures.....</b>	<b>33</b>
5.4.1	Types of Event Recorded .....	33
5.4.2	Frequency of Processing Log .....	34
5.4.3	Retention Period for Audit Log .....	34
5.4.4	Protection of Audit Log .....	34
5.4.5	Audit Log Backup Procedures.....	35
5.4.6	Audit Collection System (internal vs. external) .....	35
5.4.7	Notification to Event-causing Subject .....	35
5.4.8	Vulnerability Assessments .....	35
<b>5.5</b>	<b>Records Archival .....</b>	<b>35</b>
5.5.1	Types of Records Archived.....	35

**Certificate Policy**

5.5.2	Retention Period for Archive .....	36
5.5.3	Protection of Archive .....	36
5.5.4	Archive Backup Procedures.....	36
5.5.5	Requirements for timestamping of Records.....	36
5.5.6	Archive Collection System (internal or external).....	36
5.5.7	Procedures to Obtain and Verify Archive Information .....	37
<b>5.6</b>	<b>Key Changeover.....</b>	<b>37</b>
<b>5.7</b>	<b>Compromise and Disaster Recovery.....</b>	<b>37</b>
5.7.1	Incident and Compromise Handling Procedures .....	37
5.7.2	Computing Resources, Software and/or Data Corruption .....	37
5.7.3	Entity Private Key Compromise Procedures .....	37
5.7.4	Business Continuity Capabilities after a Disaster .....	38
<b>5.8</b>	<b>CA or RA Termination.....</b>	<b>38</b>
<b>6.</b>	<b>Technical Security Controls .....</b>	<b>39</b>
<b>6.1</b>	<b>Key Pair Generation and Installation.....</b>	<b>39</b>
6.1.1	Key Pair Generation.....	39
6.1.1.1	CA Key Pair Generation.....	39
6.1.1.2	Subscriber Key Pair Generation .....	39
6.1.2	Private Key Delivery to Subscriber .....	39
6.1.3	Public Key Delivery to Certificate Issuer .....	39
6.1.4	CA Public Key Delivery to Relying Parties .....	39
6.1.5	Key Sizes.....	39
6.1.6	Public Key Parameters Generation and Quality Checking .....	40
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field) .....	40
<b>6.2</b>	<b>Private Key Protection and Cryptographic Module Engineering Controls .....</b>	<b>40</b>
6.2.1	Cryptographic Module Standards and Controls.....	40
6.2.2	Private Key Multi-Role Control .....	40
6.2.3	Private Key Escrow .....	40
6.2.4	Private Key Backup.....	40
6.2.5	Private Key Archival .....	40
6.2.6	Private Key Transfer Into or From a HSM.....	40
6.2.7	Private Key Storage on Cryptographic Module .....	41
6.2.8	Method of Activating Private Key.....	41
6.2.9	Method of Deactivating Private Key.....	41
6.2.10	Method of Destroying Private Key.....	41
6.2.11	Cryptographic Module Rating .....	41
<b>6.3</b>	<b>Other Aspects of Key Pair Management.....</b>	<b>42</b>
6.3.1	Public Key Archival.....	42
6.3.2	Certificate Operational Periods and Key Pair Usage Periods.....	42
<b>6.4</b>	<b>Activation Data.....</b>	<b>42</b>
6.4.1	Activation Data Generation and Installation .....	42
6.4.1.1	CA Key Generation.....	42
6.4.1.2	Subscribers keys .....	42
6.4.2	Activation Data Protection.....	42
6.4.3	Other Aspects of Activation Data.....	43
<b>6.5</b>	<b>Computer Security Controls.....</b>	<b>43</b>
6.5.1	Specific Computer Security Technical Requirements .....	43
6.5.2	Computer Security Rating.....	43
<b>6.6</b>	<b>Life Cycle Technical Controls.....</b>	<b>43</b>
6.6.1	System Development Controls.....	43
6.6.2	Security Management Controls.....	43

**Certificate Policy**

6.6.3	Life Cycle Security Controls.....	44
<b>6.7</b>	<b>Network Security Controls.....</b>	<b>44</b>
<b>6.8</b>	<b>Time-stamping.....</b>	<b>44</b>
<b>7.</b>	<b>Certificate, CRL profiles.....</b>	<b>45</b>
<b>7.1</b>	<b>Certificate Profile.....</b>	<b>45</b>
7.1.1	Version Number.....	45
7.1.2	Certificate Extensions.....	45
7.1.3	Algorithm Object Identifiers.....	45
7.1.4	Name Forms.....	45
7.1.5	Name Constraints.....	45
7.1.6	Certificate Policy Object Identifier.....	45
7.1.7	Usage of Policy Constraints Extension.....	46
7.1.8	Policy Qualifiers Syntax and Semantics.....	46
7.1.9	Processing Semantics for Critical Certificate Extensions.....	46
<b>7.2</b>	<b>CRL Profile.....</b>	<b>46</b>
7.2.1	Version Number(s).....	46
7.2.2	CRL and CRL Entry Extensions.....	46
<b>7.3</b>	<b>OCSP Profile.....</b>	<b>46</b>
<b>8.</b>	<b>Compliance Audit and Other Assessments.....</b>	<b>47</b>
<b>9.</b>	<b>Other Business and Legal Matters.....</b>	<b>48</b>
<b>9.1</b>	<b>Fees.....</b>	<b>48</b>
<b>9.2</b>	<b>Financial Responsibility.....</b>	<b>48</b>
9.2.1	Insurance Coverage.....	48
9.2.2	Other Assets.....	48
9.2.3	Insurance or Warranty Coverage for End-Entities.....	48
<b>9.3</b>	<b>Confidentiality of Business Information.....</b>	<b>48</b>
<b>9.4</b>	<b>Privacy of Personal Information.....</b>	<b>49</b>
<b>9.5</b>	<b>Intellectual Property Rights.....</b>	<b>50</b>
<b>9.6</b>	<b>Representations and Warranties.....</b>	<b>50</b>
<b>9.7</b>	<b>Disclaimers of Warranties.....</b>	<b>50</b>
<b>9.8</b>	<b>Limitations of Liability.....</b>	<b>51</b>
<b>9.9</b>	<b>Indemnities.....</b>	<b>51</b>
<b>9.10</b>	<b>Term and Termination.....</b>	<b>51</b>
<b>9.11</b>	<b>Individual Notices and Communications with Participants.....</b>	<b>51</b>
<b>9.12</b>	<b>Amendments.....</b>	<b>51</b>
<b>9.13</b>	<b>Dispute Resolution Procedures.....</b>	<b>51</b>
<b>9.14</b>	<b>Governing Law.....</b>	<b>51</b>
<b>9.15</b>	<b>Compliance with Applicable Law.....</b>	<b>51</b>
<b>9.16</b>	<b>Miscellaneous Provisions.....</b>	<b>52</b>
<b>9.17</b>	<b>Other Provisions.....</b>	<b>52</b>

# 1. Introduction

This Certificate Policy (CP) defines the requirements applicable to DESC Corporate and Devices Subordinate Certification Authorities, referred to as “Corporate and Devices CA” or “DESC Subordinate CAs”, which come at the second level of the Dubai Public Key Infrastructure (PKI) hierarchy. DESC establishes and operates these subordinate CAs for issuing end-entity certificates (corporate certificates and device certificates) to the Dubai government entities.

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

The PKI certification services are offered by DESC in accordance with the present CP and a dedicated Certification Practice Statement (CPS) for each Subordinate CA.

## 1.1 Overview of Dubai PKI

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

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

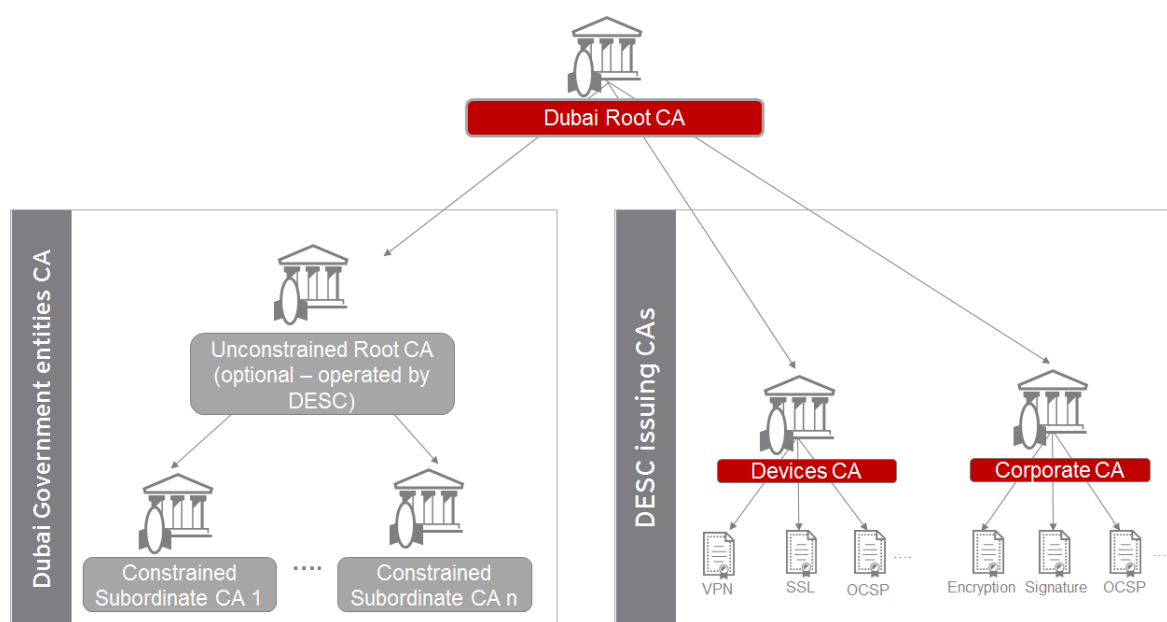
CAs belonging to other Dubai government entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai Root CA. Depending on the objectives of the Dubai government entity it will be issued one level of subordinate CA (technically constrained “Dubai Government entity issuing CAs”) or two levels of subordinate CA (an unconstrained “Dubai Government entity Root CA” and technically constrained “Dubai government entity issuing CAs”).

The Dubai Root CA and DESC Subordinate CAs are established and operated by DESC. DESC is the authority that has the final responsibility in providing the governmental PKI certification services in Dubai, i.e., issuing and managing subordinate and end-entity certificates for Dubai 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 Root CA is the top authority in this PKI with regard to digital certification services offered in Dubai. The Dubai Root CA signs DESC Subordinate Certification Authorities (CAs), which come at the second level of the PKI hierarchy. In addition, the Root CA also signs subordinate CAs belonging to authorized Dubai government entities.





*Trust Model for Dubai PKI*

## 1.1.2 Certification Services

The certification services offered by the Corporate and Devices CA are broken down in this document as follows:

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

## 1.2 Document name and Identification

This document is named 'Dubai PKI DESC Subordinate CA Certificate Policy' and is referenced as such in related documents.

The Object Identifier (OID) of this document is 2.16.784.1.2.2.100.1.1.2.1.

DESC organizes the OID for the certificates it issues as depicted in the tables below:

*Corporate CA*

OID	Certificate type	Description
2.16.784.1.2.2.100.1.2.2.1.1	Encryption certificates	Encryption certificates for corporate individuals and organizations (e.g., emails, documents)
2.16.784.1.2.2.100.1.2.2.2.1	Digital signature certificates	Digital signing certificates for corporate individuals and organizations (e.g., emails, documents)
2.16.784.1.2.2.100.1.2.2.1.2	Authentication certificates	Certificates for authentication and identification purposes
2.16.784.1.2.2.100.1.2.2.2.2	Code signing certificates	Certificates for (software) code signing purposes
2.16.784.1.2.2.100.1.2.1.1	OCSP certificates	Certificates intended to sign OCSP tokens

*Devices CA*

OID	Certificate Type	Description
2.16.784.1.2.2.100.1.2.2.3.1	Device certificates	Certificates for general identification and authentication of devices
2.16.784.1.2.2.100.1.2.2.3.3	VPN certificates	Device identification and session data encryption for VPN (IPSec-based connections)
2.16.784.1.2.2.100.1.2.2.3.2	SSL certificates	SSL certificates used for server authentication and session data encryption
2.16.784.1.2.2.100.1.3.1.1	Time stamping certificates	Certificates intended for the Dubai PKI TSA (Time Stamping Authority)

## 1.3 PKI Participants

The participants within the context of the Corporate and Devices CA are as follows:

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

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

### 1.3.1 Subordinate Certification Authorities

The table below lists the Dubai PKI Subordinate CAs operated by DESC and the certificates issued by these CAs.

Certification Authority	Supported certificates
Corporate CA	X.509 (V3) certificates for Dubai government entities (encryption, signature, authentication and code signing) in addition to OCSP response signing certificates.

Certification Authority	Supported certificates
Devices CA	X.509 (V3) end-entity certificates for devices (generic device, SSL, VPN and time stamping certificates) in addition to OCSP response signing certificates.

The key responsibilities of DESC with regard to the operation of these Subordinate CAs are as follows:

- Management of certificates, including but not limited to all aspects related to application, issuance and revocation
- Identification and authentication of subscriber information according to the applicable certificate profile requirements
- Publication of public certificates to a public repository
- Maintaining and providing certificates status information through publicly available Certificate Revocation List (CRL) and OCSP mechanisms

All certificates issued by the Corporate and Devices CA shall conform to the rules and requirements as stated in this policy document.

### 1.3.2 Registration Authority

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

### 1.3.3 Local Registration Authority

DESC allows other Dubai government entities willing to manage the certificates life cycle for their own communities to set up and act as a Local Registration Authority (LRA). This is only allowed for certificates issued by the Corporate CA.

The Dubai government entities willing to act as LRA shall sign an agreement with DESC through which it commits to operate their LRA in accordance with this CP and Corporate CA CPS.

The Dubai government entity that opts to operate an LRA appoints an LRA officer. The DESC RA will enroll the officer to DESC Corporate CA, as an administrator having the credentials to enroll and manage the subscribers of the Dubai government entity that the LRA officer represents.

The LRA officer's duties shall be as follows:

- Collecting and validating the subscribers identity data
- Conforming to the rules of this CP and related CPS of the Corporate CA
- Issuing and managing certificates of the Dubai government entities subscribers

### **1.3.4 Subscribers**

Subscribers of the Corporate and Devices CA are listed in the below table:

<b>Certification Authority</b>	<b>Subscribers</b>
Corporate CA	Dubai government entities and their employees, for receiving identity certificates (authentication or signing) or code signing certificates
Devices CA	Dubai government entity infrastructure devices such as VPNs, web servers, routers, switches and other devices, Time-stamping Authority (TSA)

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

### **1.3.5 Relying Parties**

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

### **1.3.6 Other Participants**

There are no other participants within the context of the Corporate and Devices CA.

## **1.4 Certificate Usage**

### **1.4.1 Appropriate Certificate Use**

Use of certificates issued from the Corporate and Devices CA is restricted by using certificate extensions on key usage and extended key usage, which will be configured according to the certificate type. Please refer to the CPS of each respective subordinate CA for the specific restrictions that apply to each type of certificate.

### **1.4.2 Prohibited Certificate Use**

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

## **1.5 Policy Administration**

### **1.5.1 Organization Administering the Document**

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

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

- a. Specifying and approving the Dubai PKI infrastructure
- b. Approving Dubai government entity applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy

*Dubai PKI – DESC Subordinate CAs*  
**Certificate Policy**

- c. Specifying, maintaining and approving the Dubai PKI practices and policies, in particular, the Certification Practice Statements (CPS) and the related Certificate Policies (CP) when applicable
- d. Defining the review process for such practices and policies, including responsibilities for maintaining the Dubai PKI CP/CPSs and related policies
- e. Defining the review process that ensures that the Dubai PKI properly implements the above practices
- f. Defining the review process that ensures the Dubai PKI CP and CPSs support the related policies
- g. Publication of CP and CPSs and its revisions
- h. Specifying installation, key ceremonies, operation and life cycle management (including deprecation) procedures of the Dubai PKI
- i. Evaluating the proper working of the Dubai PKI environment
- j. Allocating members to the key ceremonies as witness, as well as trusted operatives and key custodians
- k. Evaluating of changes to the Dubai PKI environment (management, operational, hardware, software and security)
- l. Evaluating case-by-case issues where key DESC staff/personnel did not respect the security and/or operational procedures, including ethics
- m. Deciding on critical issues in case of incidents, disasters and other severe problems with regard to the Dubai PKI

### **1.5.2 Contact Details**

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 +97142512538

E-mail pa@desc.gov.ae

### **1.5.3 Person Determining CPS Suitability for the Policy**

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

### **1.5.4 CP Approval Procedures**

A dedicated process involves the PA reviewing the initial version of this 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.

## 1.6 Definitions, Acronyms and References

### 1.6.1 Terminology and definitions

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

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

**CA** — Certification Authority

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

**CCTV** — Closed Circuit TV

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

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

**CRL** — Certificate Revocation List

**DRP** — Disaster Recovery Plan

**DN** — Distinguished Name

**FIPS** — Federal Information Processing Standards

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

**HTTP** — Hyper Text Transfer Protocol

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

**IEC** — International Electro-technical Commission

**IETF** — Internet Engineering Task Force

**IPSEC** — Internet Protocol Security

**ISO** — International Standards Organization

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

**ITU** — International Telecommunications Union

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

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

**DESC** — Dubai Electronic Security Centre

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

**OSCP** — Online Certificate Status Protocol

**PA** — Policy Authority

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

**PKCS # 7** — Cryptographic Message Syntax

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

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

**PKE** — Public Key Encryption

**PKI** — Public Key Infrastructure

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

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

**RA** — Registration Authority

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

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

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

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

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

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

**SHA** — Secure Hash Algorithm

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

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

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

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

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

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

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

**UPS** — Uninterruptible Power Supply

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

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

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

## **1.6.2 Acronyms**

Please refer to section 1.6.1.

## **1.6.3 References**

The Corporate and Devices CA conform to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at <http://www.cabforum.org>. In the event of any inconsistency between this document and those requirements, the requirements take precedence over this document.

The Corporate and Devices CA conform to the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at <https://aka.ms/csbr>. If there is any inconsistency between this document and those requirements, the requirements take precedence over this document.

The present CP endorses the following standards:

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

### 2.2 Publication of Certificate Information

In particular, DESC publishes a copy of the subordinate CA certificates, encryption certificates, OCSP certificates and TSA certificates at this location. This Certificate Policy is updated at the least, annually. DESC reserves its rights to publish certificate status information on third-party repositories.

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

DESC publishes digital certificate status information in frequent intervals as indicated in this CP. The provision of the Devices and Corporate CA issued electronic certificate validity status information is a 24/7 available service.

DESC operates the certificate status repository for the Devices and Corporate CA. This repository is a Lightweight Directory Access Protocol (LDAP) directory server where the CA certificates and Certificate Revocation Lists (CRLs) are published in read-only mode.

### 2.3 Time or Frequency of Publication Repositories

Due 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 and Devices CA activities.

#### 2.3.1 Certificates

Corporate and Devices CA, TSA and OCSP certificates shall be published to the public repository (DESC Public LDAP) once they are issued.

### **2.3.2 CRLs**

DESC publishes CRLs at regular intervals. DESC adds a pointer (URL) to the relevant CRL 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 for a minimum of seven years after the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the repository are uploaded within 24 hours.

The following rules shall apply for the CRL issued by the Corporate and Devices CA:

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

## **2.4 Access Controls on Repositories**

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

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

# 3. Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

The certificates issued by the Corporate and Devices CA shall contain X.500 Distinguished Names (DNs) in English. The table below summarizes the DN formats of the certificates issued by the Corporate and Devices CA.

Certification Authority	Distinguished name
<p><b>Corporate CA</b></p> <p>CA DN: cn=Corporate Certification Authority, l=Dubai, s=Dubai, o=Dubai Government, ou=DESC, c=AE</p>	<ul style="list-style-type: none"> <li> <p><b>Certificates issued for Dubai government entities through DESC RA:</b></p> <p>cn=&lt;individual unique name  Dubai Government entity meaningful unique name &gt;, ou = &lt;optional Dubai government entity unit within the organization&gt;, o = &lt;Dubai Government entity meaningful unique name&gt;, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE</p> </li> <li> <p><b>Certificates issues for Dubai government entities through LRA:</b></p> <p>cn=&lt;individual unique name&gt;, ou = &lt;optional organizational unit within the Dubai government entity&gt;, o = &lt;Dubai government entity meaningful unique name&gt;, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE</p> </li> <li> <p><b>OCSP Responder</b></p> <p>cn = OCSP, ou= Corporate Certification Authority, o = DESC, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE</p> </li> </ul>
<p><b>Devices CA</b></p> <p>CA DN: cn=Devices Certification Authority, l=Dubai, s=Dubai, o=Dubai Government, ou=DESC, c=AE</p>	<ul style="list-style-type: none"> <li> <p><b>Devices:</b> The DN format is:</p> <p>cn = &lt;System unique common name&gt; or &lt;device DNS name&gt; or &lt;device external IP address&gt;, ou = &lt;optional organizational unit within the Dubai Government Entity&gt;, o = &lt;Dubai Government entity meaningful unique name&gt;, l = &lt;Dubai Government entity locality name&gt;, s = Dubai , c = AE</p> </li> <li> <p><b>VPN:</b> The DN format is:</p> <p>cn = &lt;System unique common name&gt; or &lt;device DNS name&gt; or &lt;device external IP address&gt;, ou = &lt;optional organizational unit within the Dubai Government entity&gt;, o = &lt;Dubai Government entity meaningful unique name&gt;, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE</p> </li> </ul>

Certification Authority	Distinguished name
	<ul style="list-style-type: none"> <li> <b>Web server (SSL):</b> The DN format is:                      cn = &lt;web server DNS name&gt;, ou = &lt;optional organizational unit within the organization&gt;, o = &lt;organization meaningful unique name&gt;, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE                 </li> <li> <b>OCSP Responder:</b> The DN format is:                      cn = OCSP, ou = Devices Certification Authority, o = DESC, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE                 </li> <li> <b>Dubai TSA:</b> The DN format is:                      cn = Dubai TSA, ou = Devices Certification Authority, o = DESC, l = &lt;Dubai Government entity locality name&gt;, s = Dubai, c = AE                 </li> </ul>

### 3.1.2 Meaningful Names

Names are meaningful, since the CN contains the name of the subscriber.

All end-entity certificates issued by the Corporate and Devices CA shall be meaningful and shall contain the subject’s legal name in English.

OCSP and TSA certificates names shall indicate the service name operated by DESC.

Devices certificates issued by the DESC Devices CA shall include the name of the device.

### 3.1.3 Anonymity and Pseudonymity of Subscribers

This policy does not permit anonymous subscribers.

### 3.1.4 Rules for Interpreting Various Name Forms

No stipulation — this section is intentionally left blank.

### 3.1.5 Uniqueness of Names

DESC shall enforce the controls necessary to guarantee that subject Distinguished Name (DN) are unique. The table below summarizes the minimum controls enforced for each CA.

Certification Authority	Distinguished Name
<b>Corporate CA</b>	For certificates issued to Dubai government entities, DESC shall enforce a convention for a meaningful representation uniquely identifying the individual and the entity he or she works for.
<b>Devices CA</b>	Certificates issued by the Devices CA shall uniquely identify the device. Options could be to use the registered public DNS name or public IP address.

### 3.1.6 Recognition, authentication and role of Trademarks

No stipulation — this section is intentionally left blank.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

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

### 3.2.2 Authentication of Organization Identity

For certificates containing organization information, the identity and related information of the organization shall be verified through a reliable data source that allows the RA to verify at least the legal name, form and address of the organization.

### 3.2.3 Authentication of individual identity

The table below describes the rules that apply for authentication of certificate applicants:

Certification Authority	Method of authentication of individual identity
Corporate CA	<ul style="list-style-type: none"><li>• <b>Certificates issued for Dubai government entities through DESC RA:</b> Any applicant for certificates through the DESC RA shall undergo the following identity validation steps:<ul style="list-style-type: none"><li>○ Appear in person before the DESC RA and bring paper work related to the certificate application, and providing evidence on the link between the applicant and the Dubai government entity.</li><li>○ The DESC RA validates the association between the applicant and the organization.</li></ul></li><li>• <b>Certificates issued for Dubai government entities through an LRA:</b> The LRA of the Dubai government entity shall validate the identity of the applicant and confirm if he or she is authorized to receive PKI credentials from the organization.</li></ul>
Devices CA	For any issued Devices Certificate, the DESC RA shall validate the identity (proof of system ownership) of the certificate applicant.

### 3.2.4 Authentication of Domain name

For SSL certificates, the control or ownership of the domain name(s) which is/are specified in the certificate application must be verified.

### 3.2.5 Non-verified subscriber information

All subscriber information contained within certificate issued by the Corporate and Devices CA shall be verified by the DESC RA or Dubai Government entity LRA.

### 3.2.6 Validation of Authority

No stipulation — this section is intentionally left blank.

### 3.2.7 Criteria for Interoperation

No stipulation — this section is intentionally left blank.

## 3.3 Identification and Authentication for Re-keying requests

### 3.3.1 Identification and Authentication for Routine Re-Keying

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

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

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

## 3.4 Identification and Authentication for Revocation Requests

The table below summarizes the methods that shall be enforced for identification and authentication for revocation requests:

Certification Authority	Method of identification and authentication of revocation of revocation requests
Corporate CA	<ul style="list-style-type: none"><li>• <b>Revocation of Corporate certificates through DESC RA:</b> any request for certificate revocation requires the authorized applicant from the Dubai government entity to appear in person before the DESC RA and request revocation. The identity of the applicant is validated by the DESC RA as part of this process.</li><li>• <b>Revocation of Corporate certificates through an LRA:</b> the LRA of the Dubai government entity shall validate the identity of the applicant for a revocation request through a dedicated organization process.</li></ul>
Devices CA	The DESC RA is the single channel for the revocation of Devices Certificates. The RA shall validate the validation request and the identity of the revocation request applicant.

OCSP and TSA certificate revocation shall be conducted as part of DESC internal processes and the Dubai PKI PA shall approve it.

# 4. Certificate Life Cycle Management

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

Certificate application is limited to Dubai government entities. For further details, please refer to the applicable CPS.

### 4.1.2 Enrolment Process and Responsibilities

For any certificate issued by the Corporate or Devices CA, the certificate applicant shall sign a dedicated subscriber agreement.

For further details on the enrollment process, please refer to the applicable CPS.

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

Refer to section 3.2 of this CP.

Certification Authority	Acceptance/rejection of certificate applications
Corporate CA	<ul style="list-style-type: none"><li>• <b>Certificates issued for Dubai government entities through DESC RA:</b> Any applicant for certificates through the DESC RA shall undergo the following enrolment process:<ul style="list-style-type: none"><li>○ Identity validation process by the DESC RA</li><li>○ The DESC RA validates the association between the applicant and the Dubai government entity</li><li>○ If all verifications are successful, the DESC RA accepts the certificate application, and issues the required PKI credentials and related certificates</li></ul></li><li>• <b>Certificates issued for Dubai government entities through an LRA:</b> The LRA of the Dubai government entity shall validate the identity of the applicant and confirm if he is authorized to receive PKI credentials from the Dubai government entity. If all verifications by LRA are successful, the LRA accepts the certificate application. The LRA enrolls the individual to the PKI, and issues related PKI credentials and certificates.</li></ul>
Devices CA	For any issued Devices Certificate, the DESC RA shall validate the identity of the certificate applicant who needs to proof ownership of the device. The DESC RA shall then enroll the infrastructure device and issue related digital certificate.

For SSL certificate applications, Certificate Authority Authorization (CAA) records shall be verified.

For further details, please refer to the applicable CPS.

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

OCSP and TSA certificate certifications shall be conducted as part of DESC internal processes and shall be approved by the Dubai PKI PA.

For further details, please refer to the applicable CPS.

#### **4.2.3 Time to Process Certificate Applications**

No stipulation — this section is intentionally left blank.

### **4.3 Certificate Issuance**

DESC shall process a certificate issuance request as follows:

- Verify that the certificate request originated from a valid (L)RA
- Issue the required digital certificates that contain the information provided in the certificate request
- If applicable, publish the issued certificates on the DESC public repository

For further details, please refer to the applicable CPS.

#### **4.3.1 CA Actions during Certificate Issuance**

Refer to the applicable CPS.

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

For further details, please refer to the applicable CPS.

### **4.4 Certificate Acceptance**

#### **4.4.1 Conduct Constituting Certificate Acceptance**

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

OCSP and TSA certificates shall be issued as part of DESC internal processes and the Dubai PKI PA shall approve it.

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

Encryption certificates shall be published on the DESC certificate repository. TSA 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

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

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

### 4.5.2 Relying on Party Public Key and Certificate Usage

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

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

## 4.6 Certificate Renewal

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

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

## 4.7 Certificate Re-key

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

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

Re-key for OCSP and TSA certificates shall happen as part of internal DESC processes and approved by the Dubai PKI PA.

### 4.7.1 Circumstance for Certificate Re-key

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

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

As per initial certificate issuance

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

As per initial certificate issuance

### **4.7.4 Notification of New Certificate Issuance to Subscriber**

As per initial certificate issuance

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

As per initial certificate issuance

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

As per initial certificate issuance

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

As per initial certificate issuance

## **4.8 Certificate Modification**

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

### **4.8.1 Circumstance for Certificate Modification**

Not applicable beyond the normal certificate re-key operation

### **4.8.2 Who May Request Certificate Modification**

Not applicable beyond the normal certificate re-key operation

### **4.8.3 Processing Certificate Modification Requests**

Not applicable beyond the normal certificate re-key operation

### **4.8.4 Notification of New Certificate Issuance to Subscriber**

Not applicable beyond the normal certificate re-key operation

### **4.8.5 Conduct Constituting Acceptance of Modified Certificate**

Not applicable beyond the normal certificate re-key operation

### **4.8.6 Publication of the Modified Certificate by the CA**

Not applicable beyond the normal certificate re-key operation

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

Not applicable beyond the normal certificate re-key operation

## 4.9 Certificate Revocation and Suspension

### 4.9.1 Circumstances for Revocation

Certification Authority	Circumstances for revocation
Corporate CA	<ul style="list-style-type: none"><li>• <b>Circumstances of revocation of Dubai government entity certificates through DESC RA:</b> The authorized Dubai government entity representative may approach the DESC RA for certificate revocation under the following circumstances:<ul style="list-style-type: none"><li>○ The subscriber discovers or has reason to believe that there has been a compromise of the corresponding private keys.</li><li>○ The subscriber no longer requires the keys and certificates.</li><li>○ The information in the certificates is no longer valid and requires to be changed.</li></ul></li><li>• <b>Circumstance for revocation of Dubai government entity certificates through an LRA:</b> The LRA of the Dubai government entity shall revoke digital certificates corresponding to his organization when required by the organization internal processes. The LRA shall submit a signed certificate revocation request to the RA in an authenticated manner.</li></ul>
Devices CA	<p>The DESC RA is the single channel for the revocation of Devices Certificates. An Devices Certificate may be revoked under the following circumstance:</p> <ul style="list-style-type: none"><li>• The subscriber discovers or has reason to believe that there has been a compromise of the corresponding private keys.</li><li>• The system or device no longer requires the certificate.</li><li>• The information on the certificate is no longer accurate and a new certificate with updated data is required.</li></ul>

This CP does not provide provisions for revoking an OCSP/TSA certificate apart from the compromise of the OCSP/TSA key pair which shall be considered by DESC as per its disaster recovery and business continuity procedures. The following sub-sections focus only on the revocation provisions that apply for individual and device certificates issued by the Corporate or Devices CA.

### 4.9.2 Who Can Request Revocation

Refer to section 4.9.1.

Only authorized revocation requests shall be accepted.

For further details, please refer to the applicable CPS.

### 4.9.3 Procedure for Revocation Request

Refer to the applicable CPS.

### 4.9.4 Revocation Request Grace Period

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

#### **4.9.5 Revocation Request Response Time**

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

#### **4.9.6 Revocation Checking Requirement for Relying Parties**

Revocation information is offered to relying parties through CRLs published on a publicly available LDAP or through its OCSP responder. Relying parties shall use any of these methods while processing a certificate issued by the Corporate or Devices CA.

#### **4.9.7 CRL Issuance Frequency**

CRLs are issued as per section 2.3 of this CP.

#### **4.9.8 Maximum Latency for CRLs**

No stipulation — this section is intentionally left blank.

#### **4.9.9 Online Revocation/Status Checking Availability**

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

The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by the Corporate or Devices CA.

#### **4.9.10 Online Revocation Checking Requirements**

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

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

No stipulation — this section is intentionally left blank.

#### **4.9.12 Special Requirements — Key Compromise**

No stipulation — this section is intentionally left blank.

#### **4.9.13 Circumstances for Suspension**

Certificate suspension is not supported by the Corporate and Devices 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 CP.

### **4.10.1 Operational Characteristics**

CRLs shall be published by the Corporate and Devices CA on a public repository which is available to relying parties through LDAP protocol queries.

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

### **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**

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

Key escrow is not supported by the Corporate and Devices CA.

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

No stipulation — this section is intentionally left blank.

# 5. Facility, Management and operational Controls

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

All critical components of the PKI solution are housed within a highly secure enclave within a DESC building. 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, man traps, biometric IRIS access and Closed Circuit TV (CCTV) monitoring. These physicals controls protect the hardware and software from unauthorized access and shall be monitored on a 24x7x365 basis.

### 5.1.3 Power and Air Conditioning

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

### 5.1.4 Water Exposures

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

### 5.1.5 Fire Prevention and Protection

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

### 5.1.6 Media Storage

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

### 5.1.7 Waste Disposal

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

### **5.1.8 Offsite Backup**

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

Backup media shall be stored in a location separate from the DESC 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 the DESC'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 Devices and 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).

DESC conducts an initial investigation of all members of staff who are candidates, to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

### **5.2.2 Number of Persons Required Per Task**

DESC shall maintain and enforce rigorous control procedures to ensure the segregation of duties, based on job responsibility, in order to prevent a 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 provide 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:

- Personnel managing operations on certificates
- Administrative personnel who operate the supporting platform
- Security personnel who 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 regards to the Devices and 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 makes the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

### **5.3.3 Training Requirements**

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 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 DESC 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**

For details on the audit logging procedures, refer to the applicable CPSs. The following provisions are made in this CP.

### **5.4.1 Types of Event Recorded**

Following events occurring on the Corporate and Devices CA shall be recorded:

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

*Dubai PKI – DESC Subordinate CAs*  
**Certificate Policy**

- 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, DESC maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

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

#### **5.4.2 Frequency of Processing Log**

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

Log files and audit trails are periodically archived for inspection by authorized DESC personnel 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 and Devices 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 CP.

## **5.5 Records Archival**

DESC keeps records of the following items:

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

The very last back up of the Subordinate CA archive will be retained for seven 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. DESC ensures that at least the following records are archived:

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

## **Certificate Policy**

- 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**

Only the records administrator (member of staff assigned with the records retention duty) may access an archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium
- Protection against deletion of archive
- Protection against deterioration and/or obsolescence of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media

### **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 timestamping 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 shall be allowed to handle archived 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 archived information. DESC retains records in electronic or paper-based format.

## **5.6 Key Changeover**

DESC Subordinate CAs 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, DESC specifies applicable incident, compromise reporting and handling procedures. DESC 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 and/or Data Corruption**

DESC and all other PKI Participants (other than Subscribers and Relying Parties) establish the necessary measures to ensure full recovery of DESC Subordinate CAs services in case of a disaster, and corrupted servers, software or data.

DESC establishes:

- Disaster recovery resources in a location sufficiently distant from the regular DESC 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 more than one member of the Dubai PKI PA as the witness.

### **5.7.3 Entity Private Key Compromise Procedures**

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

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

- All active certificates issued by the Subordinate CA shall be revoked.
- Organizations holding Client and Device Certificates shall be notified.
- A new Subordinate CA key pair shall be generated and certificate produced by the Dubai Root CA.
- A Subordinate CA compromise notice shall be published toward relevant relying parties.
- After DESC 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 CP document.

#### **5.7.4 Business Continuity Capabilities after a Disaster**

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

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

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

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

## **5.8 CA or RA Termination**

If DESC determines that termination of its PKI and Subordinate CA services are deemed necessary, DESC 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. DESC shall arrange for the retention of archived data specified in section 5.5 of this CP, taking into account the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate.

# 6. Technical Security Controls

## 6.1 Key Pair Generation and Installation

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

### 6.1.1 Key Pair Generation

#### 6.1.1.1 CA Key Pair Generation

The Subordinate CAs 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).

#### 6.1.1.2 Subscriber Key Pair Generation

Subscriber key generation is not performed for the Corporate and Devices CA. Subscribers must generate their keys in a manner that is appropriate for the certificate type.

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

### 6.1.4 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 (DESC Public LDAP).

### 6.1.5 Key Sizes

The Corporate CA key pair shall be at least 4096 bit RSA.

The Devices CA key pair shall be at least 4096 bit RSA.

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

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

The Corporate and Devices 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)**

Certificates issued by the Corporate and Devices should always contain a key usage bit string in accordance with RFC 5280.

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

### **6.2.1 Cryptographic Module Standards and Controls**

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

### **6.2.2 Private Key Multi-Role Control**

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 CAs cryptographic hardware.

### **6.2.3 Private Key Escrow**

Not applicable

### **6.2.4 Private Key Backup**

The Corporate and Devices CA private keys shall be backed up within backup tokens 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 tokens shall be conducted using the principles of dual controls and split knowledge, involving at least two PKI officers. At least one backup of the Subordinate CAs keys shall be taken. This backup shall be stored in a locked safe at the disaster recovery site.

### **6.2.5 Private Key Archival**

Not applicable.

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

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

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



### **6.2.7 Private Key Storage on Cryptographic Module**

No further stipulation other than those stated in 6.2.1.

### **6.2.8 Method of Activating Private Key**

Private keys for the Corporate and Devices 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 and Devices CA.

### **6.2.9 Method of Deactivating Private Key**

Private keys for the Corporate and Devices shall be deactivated in situations such as:

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

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

### **6.2.10 Method of Destroying Private Key**

At the end of their lifetime, taking into account business purpose and legal obligations, the Corporate and Devices 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 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 shall use an HSM certified to FIPS 140-2 Level 3 or ISO 15408 Common Criteria (CC) EAL 4+ or above.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

Refer to section 5.5 of this CP.

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

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

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

#### 6.4.1.1 CA Key Generation

The Corporate and Devices CAs 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 a Corporate or Devices 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 or Devices CA shall register its subscribers prior to issuing digital certificates to the subscribers.

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

### 6.4.2 Activation Data Protection

Activation data for 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 one of the following means:

- For corporate certificates: automated process through the secure exchange of activation data between the Subordinate CAs and RA applications.
- For devices and any OCSP certificates: at the discretion of DESC guaranteeing that only the legitimate subscriber organization representative receives the activation data.

### 6.4.3 Other Aspects of Activation Data

No stipulation — this section is intentionally left blank.

## 6.5 Computer Security Controls

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

### 6.5.1 Specific Computer Security Technical Requirements

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

- Physical access control to the CA servers shall be enforced
- Separation of duties and dual controls for CA sensitive operations
- Identification and authentication of PKI roles and their associated identities
- Archival of CAs history and audit data
- Audit of security-related events
- Automatic and regular validation of the CA systems' integrity
- Recovery mechanisms for keys and CA systems
- Hardening CA servers' operating system according to best practices and PKI vendor requirements
- Network protection, including intrusion detection systems

### 6.5.2 Computer Security Rating

No stipulation — this section is intentionally left blank.

## 6.6 Life Cycle Technical Controls

### 6.6.1 System Development Controls

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

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

### 6.6.2 Security Management Controls

The hardware and software used to set up the Dubai PKI 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 and Devices CA and RAs functionality shall be scanned for malicious code on first use and periodically afterward.

Upon installation, and at least once a week, the integrity of the DESC Subordinate CAs databases shall be validated.

### **6.6.3 Life Cycle Security Controls**

No stipulation — this section is 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 CAs servers' internal clock shall be synchronized using Network Time Protocol.

# 7. Certificate, CRL profiles

## 7.1 Certificate Profile

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

For further details, please refer to the applicable CPS.

### 7.1.1 Version Number

The Corporate and Devices CA shall issue X.509 version 3 certificates as defined in RFC 5280.

### 7.1.2 Certificate Extensions

End-entity certificates require at least the use of the following extensions. For the complete profile, refer to the applicable CPS.

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

### 7.1.3 Algorithm Object Identifiers

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

### 7.1.4 Name Forms

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

### 7.1.5 Name Constraints

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

### 7.1.6 Certificate Policy Object Identifier

Refer to the ASN1 definitions described in the below subsections.

### **7.1.7 Usage of Policy Constraints Extension**

No stipulation — this section is intentionally left blank.

### **7.1.8 Policy Qualifiers Syntax and Semantics**

No stipulation — this section is intentionally left blank.

### **7.1.9 Processing Semantics for Critical Certificate Extensions**

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

## **7.2 CRL Profile**

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

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

For further details, please refer to the applicable CPS.

### **7.2.1 Version Number(s)**

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

### **7.2.2 CRL and CRL Entry Extensions**

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

## **7.3 OCSP Profile**

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

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

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

For further details, please refer to the applicable CPS.

## 8. Compliance Audit and Other Assessments

DESC 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.

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

The Devices and Corporate CA are 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 who fulfill the following requirements:
- Independence from the subject of the audit
- The ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities v2.0
- Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the 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 US\$1m 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.

# 9. Other Business and Legal Matters

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

## 9.1 Fees

Refer to the applicable CPS.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

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

### 9.2.2 Other Assets

Not applicable.

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

Not applicable.

## 9.3 Confidentiality of Business Information

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

DESC guarantees the confidentiality of any data not published in the certificates issued by the CAs implementing this CP, according to the applicable laws on privacy.



## 9.4 Privacy of Personal Information

DESC observes personal data privacy rules and confidentiality rules as described in this CP. Confidential information includes:

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

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

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 its activities. It owes such a duty to the RA and promptly responds to any such requests
- A court order

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

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

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

DESC 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 Dubai PKI 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 Dubai PKI 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 DESC and the (L)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 CAs' digital certificates and any other publication whatsoever originating from the Dubai PKI including this CP.

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**

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

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

## **9.7 Disclaimers of Warranties**

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

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

## **9.8 Limitations of Liability**

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

## **9.9 Indemnities**

Not applicable.

## **9.10 Term and Termination**

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

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

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

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

## **9.12 Amendments**

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

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

## **9.13 Dispute Resolution Procedures**

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

## **9.14 Governing Law**

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

## **9.15 Compliance with Applicable Law**

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

## 9.16 Miscellaneous Provisions

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

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

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

## 9.17 Other Provisions

Not applicable.