Dubai Electronic Security Center

Dubai PKI

Corporate CA

Certification Practice Statement

Project	DESC CA Project
Title	Corporate CA, Certification Practice Statement
Classification	PUBLIC
File Name	Dubai PKI - Corporate CA - Certification Practice Statement_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 certificates profiles
18 January 2018	0.5		Second revision of certificates profile
30 January 2018	1.0		Issue final version

Table of Contents

1. Introduction

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

- **Corporate certificates for individuals** – comprises certificates issued for individuals acting on behalf of the Dubai Government entity they work for; those certificates are used for the following purposes:
  - **Signing certificate** – used to produce digital signatures on digital transactions and documents
  - **Encryption certificate** – used for secure email and for data/document encryption
  - **Authentication certificate** – used for authentication of subscribers in online services
- **Corporate certificates for government entities** – comprises one certificate with the following purpose:
  - **Code signing certificate** – used for digitally signing code
- **OCSP certificates** – certificates for the Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by this CA

The Dubai PKI Policy Authority (PA), composed of appointed members of the DESC management and 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 Dubai PKI Policy Authority (PA).

1.1 Overview of Dubai PKI

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

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

CAs belonging to other Dubai government entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai Root CA. There are two options for issuing these CAs: Option 1 is to directly issue a Dubai Government entity issuing CA from the Dubai Root CA, which is a technically constrained subordinate CA[1] owned and operated by a Dubai Government entity. Option 2

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

is for entities requiring more scalable hierarchy, met by issuing them two hierarchical levels of subordinate CAs — an unconstrained Dubai Government entity Root CA that comes directly under the Dubai Root CA, and a technically constrained Dubai Government entity issuing CA(s) that comes under the Dubai Government entity Root CA.

The Dubai Root CA and DESC Subordinate CAs are established and operated by DESC. DESC is the authority that has the final responsibility of providing governmental PKI certification services in Dubai, i.e., issuing and managing subordinate and end-entity certificates for 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.

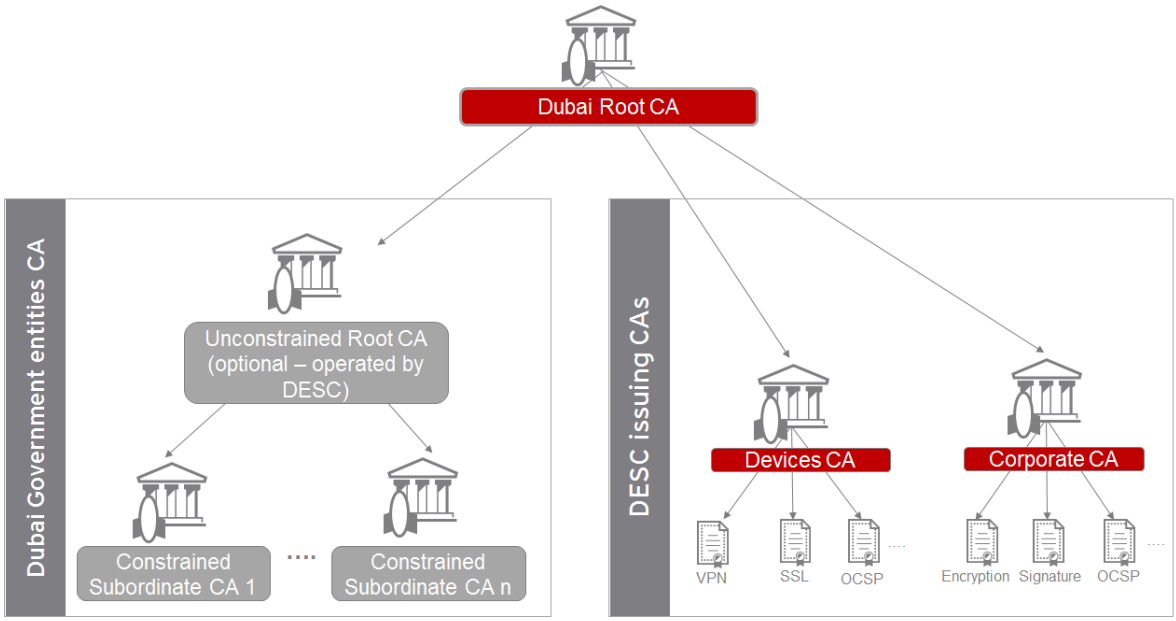

Figure 1: Trust Model for Dubai PKI.

1.1.2 Certification services

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

- **Registration services:** It verifies the identity and, if applicable, any specific attributes of end-entities applying for certificates. The results of this service are passed to the certificate generation service.
- **Certificate generation service:** It creates and signs end-entity certificates based on the verification conducted by the registration service.
- **Dissemination service:** It disseminates end-entity encryption certificates, OCSP certificates, this CA certificates and makes them available to relying parties. This service also makes available any public policy and practice information to subscribers and relying parties.
- **Revocation management service:** It processes requests and reports revocation data for determining the appropriate action to be taken. The results of this service are available through the certificate validity status service.

- **Certificate validity status service:** It provides certificate validity status information to relying parties based on certificate suspension or revocation lists, and an OCSP responder service. The status information shall always reflect the current status of the certificates issued by this CA.

1.2 Document name and identification

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

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

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

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

1.3 PKI participants

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

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

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

1.3.1 Subordinate Certification Authorities

The Corporate CA (further referred to as “CA”) issues certificates code signing certificates and identity certificates for Dubai government entities in addition to OCSP response signing certificates. This includes the following tasks:

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

1.3.2 Registration Authorities

DESC shall set up a Registration Authority (RA) organization for this CA. The RA shall comprise 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).

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

The Dubai government entity that opts to operate an LRA appoints an LRA officer. He will be enrolled to DESC Corporate CA by the DESC RA 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 duties shall be as follows:

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

1.3.4 Subscribers

Subscribers of the Corporate CA, either Dubai government entities or employees acting on behalf of the entities they that they work for.

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 CA.

1.3.6 Other participants

There are no other participants for this CA.

1.4 Certificate usage

1.4.1 Appropriate certificate use

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

- Corporate certificates for individuals acting on behalf of the entity they work for
  - Encryption key pair with related certificate
    - Secure email
    - Document/data encryption
  - Signature key pair and related certificate
    - Signing digital transactions
  - Authentication key pair and related certificate
    - Authentication
- Corporate certificates for government entities
  - Code signing key pair and related certificate
    - Digitally signing code

This CA also issues OCSP certificates intended for Corporate CA OCSP responder.

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

1.4.2 Prohibited certificate use

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

1.5 Policy administration

1.5.1 Organization administering the document

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

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

a. Specifying and approving the Dubai PKI infrastructure

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

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

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

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

f. Defining the review process that ensures that the related policies are supported by the Dubai PKI CP and CPSs

g. Publication of CP and CPSs and of 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 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 regards 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 part of the Dubai PKI.

1.5.4 CPS approval procedures

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

1.6 Definitions, acronyms and references

1.6.1 Terminology and definitions

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

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

CA – Certification Authority

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

CCTV – Closed Circuit TV

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

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

CRL – Certificate Revocation List

DRP – Disaster Recovery Plan

DN – Distinguished Name

FIPS – Federal Information Processing Standards

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

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

ITU – International Telecommunications Union

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

LDAP – Lightweight Directory Access Protocol, a common standard for accessing directories

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

OCSP – Online Certificate Status Protocol

PA – Policy Authority

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 or digital signatures verified using that certificate

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

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

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

SCEP – Simple Certificate Enrolment Protocol

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

SHA – Secure Hash Algorithm

S/MIME – Secure Multipurpose Internet Mail Extensions

SSL/TLS – Secure Sockets Layer/Transport Layer Security

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

subjectAltName – A certificate attribute field that often contains the subject's e-mail address

Subject – A subject is the entity named in a certificate

Subscriber – A subject who is issued a certificate

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

UPS – Uninterruptible Power Supply

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

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

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

1.6.2 Acronyms

Please refer to section 1.6.1.

1.6.3 References

The Corporate CA conforms 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 CA conforms 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/ and is provided on a 24/7 basis.

2.2 Publication of certificate information

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

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

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

DESC operates the certificate status repository for the Corporate CA. This repository is an 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

The Corporate CA certificate, encryption certificates and OCSP certificates are published to the public repository (DESC Public LDAP) as soon as they are issued.

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

DESC maintains the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL until minimum 7 years after the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the Repository are uploaded within 24 hours.

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

- At the minimum, CRLs shall be refreshed every 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).

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

2.4 Access controls on repositories

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

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

3. Identification and authentication

3.1 Naming

3.1.1 Types of name

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

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

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

- **Certificates issued for Dubai government entities through DESC RA:**

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

- **Certificates issued for individuals of government entities through DESC RA or LRA:**

cn=<individual end user name>, ou = <optional organizational unit within the Dubai government entity>, o =<Dubai government entity meaningful unique name>, l =<Dubai government entity locality information>, s=Dubai, c = AE

- **OCSP responder:**

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

3.1.2 Meaningful names

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

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

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

3.1.3 Anonymity and pseudonymity of subscribers

This CA does not support the issuance of anonymous certificates.

3.1.4 Rules for interpreting various name forms

No stipulation – this section is intentionally left blank

3.1.5 Uniqueness of names

Unique subject DNs are enforced as follows:

- **For certificates issued for individuals:** A convention for a meaningful name representing uniquely the individual and the Dubai government entity he works is enforced by DESC.
- **For certificates issued for Dubai government entities:** A convention for a meaningful name representing uniquely the Dubai government entity is enforced by DESC.
- **For certificates issued for corporate CA OCSP responder:** The OCSP responder unique name is included in the subject DN to ensure uniqueness.

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

- **Certificates issued for Dubai government entities:** Certificate Signing Requests (CSR) generated by IT systems contain a Proof-of-Possession (POP) of the private key as part of the PKCS#10 certificate requests submitted to this CA.
- **Certificates issued for individuals of Dubai government entities:** The token or smartcard that signs a proof of possession included in the PKIX-CMP request submitted to this CA.
- **Certificates issued for corporate CA OCSP:** Certificate Signing Requests (CSR) generated by the OCSP responder contains a Proof-of-Possession (POP) of the private key as part of the PKCS#10 request file submitted to this CA.

3.2.2 Authentication of Dubai government entity identity

For all certificates that contain the identity of a Dubai Government entity, the applicant is required to provide the Dubai government entities' name, organizational unit (if applicable) and officially recognized address. This will be verified by DESC RA against a trusted register of Dubai government entities and their representatives.

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

3.2.3 Authentication of individual identity

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

The subscriber's identity is established as follows:

- DESC RA
  - The subscriber provides a copy of his identity card, proof of employment by a Dubai government entity, hence providing evidence to establish the relation between the applicant and the Dubai government entity.
  - DESC RA validates the association between the applicant and the Dubai government entity.

- Dubai government entity LRA
  - The subscriber's identity verification is performed according to the applicable Dubai government entities' business rules.

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

3.2.4 Non-verified subscriber information

All subscriber information written in the certificate issued by corporate CAs is verified by the applicable RA.

3.2.5 Validation of authority

The authority of the applicant to request a certificate on behalf of a Dubai government entity will be performed through a reliable means of communication with the Dubai government entity. Examples include a formal letter signed by an official representative of the Dubai Government entity or a confirmation from the Dubai government entities HR department.

3.2.6 Criteria for interoperation

No stipulation – this section is intentionally left blank

3.3 Identification and authentication for re-keying requests

3.3.1 Identification and authentication for routine re-keying

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

Revocation through DESC RA can be requested by the initial certificate applicant, which will be authenticated as described in section 3.2. If revocation is requested by someone else, DESC RA will authenticate the requestor and its authority to request revocation on behalf of the applicant or the Dubai government entity as described in section 3.2.5.

For revocation of certificates through an LRA, the LRA of the Dubai government entity shall validate the identity of the applicant for a revocation request through a dedicated organizational process.

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

4. Certificate Life Cycle Management

4.1 Certificate application

4.1.1 Who can submit a certificate application

- **Certificates for Dubai government entities issued through DESC RA:** An authorized person from the Dubai government entity submits the certificate application as part of the certificate issuance process.
- **Certificates for individuals issued through DESC RA:** The Dubai government entity employee in need of a certificate submits the certificate application.
- **Certificates for individuals issued through DESC LRA:** The Dubai government entity LRA submits the certificate application for a Dubai government entity employee.
- **OCSP responder certificates:** An authorized OCSP administrator can submit a certificate request.

4.1.2 Enrolment process and responsibilities

Certificates issued by DESC RA for Dubai government entities and individuals using a CSR File:

- The DESC RA receives a certificate application form. He then identifies the applicant as described in section 3.2.3.
- If the certificate application is for a certificate for a Dubai government entity, the DESC RA will validate the authority of the applicant as described in section 3.2.5.
- The DESC RA asks the subscriber to sign the Subscriber Agreement and the certificate application form.
- The applicant submits the certificate application form to the DESC RA officer.
- The DESC RA officer uses a dedicated RA application to enroll the applicant into this CA. The applicants' unique name is used to produce a unique distinguished name identifying it within this CA system.
- The subscriber generates a key pair on the IT system or device. He then creates a CSR file using the received unique secret codes provided in the previous step.
- The CSR file is delivered to the DESC RA officer who uses the RA application to upload and submit the CSR file to the corporate CA. The certificate is issued and available for download as a file to the DESC RA officer.
- The DESC RA officer delivers the certificate to the subscriber. The certificate may be sent via email using the subscriber's email address known to the RA officer.

Certificates issued by DESC RA for individuals on a PKI token:

- The DESC RA receives a certificate application form. He then identifies the applicant as described in section 3.2.3.
- If the certificate application is for a certificate for a Dubai government entity, the DESC RA will validate the authority of the applicant as described in section 3.2.5.
- The DESC RA asks the subscriber to sign the Subscriber Agreement and the certificate application form.
- The applicant submits the certificate application form to the DESC RA officer.
- The DESC RA uses a dedicated RA application in order to fill the certificate enrollment form after validating all data required for the enrollment.
- The RA application communicates with the corporate CA in order to issue end-user certificates.
- The CA generates the certificates and sends back to the RA application which installs the certificates on the PKI token.
- The applicant is now a registered subscriber and is handed over his PKI token, initial PIN label, a CD containing the device driver and change PIN software.

Certificates issued by a Dubai government entity LRA to individuals (only certificates for individuals may be requested through Dubai government entity LRAs):

- The applicant, who requires the PKI token with digital certificates, introduces himself to the local RA officer where they sign a Subscriber Agreement.
- The LRA officer validates the applicant's identity face-to-face and ensures the enrolment data is correct in addition to following business rules endorsed by business policy, procedure and process.
- The LRA officer uses a dedicated RA application in order to fill the certificate enrollment form after validating all data required for the enrollment.
- The RA application communicates with the corporate CA in order to issue end-user certificates.
- The CA generates the certificates and sends back to the RA application which installs the certificates on the PKI token.
- The applicant is now a registered subscriber and is handed over his PKI token, Initial PIN label, a CD containing the device driver and change PIN software.

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

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

As described in section 4.1.

4.2.2 Approval or rejection of certificate applications

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

- **For certificates issued through the DESC RA:** The DESC RA officer approves or rejects the application for the certificate as part of the overall approval/rejection of the certificate issuance process.
- **For certificates issued through a Dubai government entity LRA:** The LRA officer approves or rejects the certificate application as part of the overall approval/rejection of the certificate issuance process.
- **For OCSP certificates:** A certificate application is approved/rejected as part of the overall approval/rejection of the OCSP certification process.

4.2.3 Time to process certificate applications

No stipulation – this section is intentionally left blank.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

- **For certificates issued to Dubai government entities:** Following the approval of the certificate application by the DESC RA, the CSR file is uploaded and submitted to this CA by the DESC RA officer using a dedicated application. The CA then signs the certificate in accordance with the specified certificate template. The certificate is then downloaded by DESC RA officer and transferred back to the subscriber.
- **For certificates issued to individuals:** Following the approval of the certificate application by the DESC RA or Dubai government entity LRA, the certificate request is submitted to this CA by the DESC RA or Dubai government entity LRA officer using a dedicated application. The CA then signs the certificate in accordance with the specified certificate template. The certificate is then retrieved by the RA application and it is then either installed directly on a PKI device or downloaded by the DESC RA officer and transferred back to the subscriber. Additionally, if an encryption certificate is issued, the certificate is published on the public LDAP, as described in section 2.
- **For OCSP certificates:** The OCSP administrator manually delivers the CSR file including the servers' public key to the CA administrator. The CA administrator submits the CSR file directly to the CA that will sign and publish an OCSP certificate suitable for verification. The certificate is returned to the OCSP administrator.

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

The subscriber is notified by the DESC RA or Dubai government entity LRA officer for collecting his certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The user confirms certificate acceptance upon signing a dedicated form.

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

4.4.2 Publication of the certificate by the CA

Encryption certificates issued to end entities shall be published on the DESC certificate repository. The corporate CA and OCSP certificates shall be published on the dissemination page as described in section 2.2.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation – this section is intentionally left blank

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

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

4.5.2 Relying party public key and certificate usage

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

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

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

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

4.6 Certificate renewal

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

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

4.7 Certificate Re-key

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

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

4.7.1 Circumstance for Certificate Re-key

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

4.7.2 Who may request certification of a new public key

As per initial certification.

4.7.3 Processing Certificate Re-keying requests

As per initial certification.

4.7.4 Notification of new certificate issuance to subscriber

As per initial certification.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As per initial certification.

4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certification.

4.7.7 Notification of certificate issuance by the CA to other entities

As per initial certification.

4.8 Certificate modification

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

4.8.1 Circumstance for certificate modification

Not applicable beyond the normal certificate re-key operation.

4.8.2 Who may request certificate modification

Not applicable beyond the normal certificate re-key operation

4.8.3 Processing certificate modification requests

Not applicable beyond the normal certificate re-key operation

4.8.4 Notification of new certificate issuance to subscriber

Not applicable beyond the normal certificate re-key operation

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable beyond the normal certificate re-key operation

4.8.6 Publication of the modified certificate by the CA

Not applicable beyond the normal certificate re-key operation

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable beyond the normal certificate re-key operation

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

An individual or an authorized Dubai Government entities' representative may request a revocation of his certificate if:

- It is discovered or there are reasons to believe that there has been a compromise or loss of his private signing key.
- The information on the certificate is no longer accurate; for example a change of name or if an employee left his position at the Dubai Government entity.

The LRA of the Dubai Government entity shall revoke digital certificates corresponding to his Dubai Government entity when required by the Dubai Government entities' internal processes.

This CA will revoke the certificate upon:

- The request of the individual or an authorized Dubai Government entities' representative
- Knowing that the information on the certificate is no longer accurate
- Discovering that the certificate was issued in a manner not materially in accordance with the procedures required by the CPS
- Determination that the certificate was issued to an entity other than the one named as the subject of the certificate
- Finding that the certificate was issued without the authorization of the individual named as the subject of such certificate
- The Dubai Government entity or the individual has been declared legally incompetent
- A third party provides information that leads the CA to believe that the certificate is compromised or is being used for Suspect Code; or
- An Application Software vendor requests revocation of a code signing certificate

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

4.9.2 Who can request revocation

- The individual to whom certificates were issued

- The Dubai government entity to whom certificates were issued
- Any relying party possessing evidence of compromise of the subscriber's certificate
- Revocations are directly initiated by DESC's RA officers in the cases described in section 4.9.1.
- The LRA of the Dubai Government entity shall revoke digital certificates corresponding to his Dubai Government entity when required by the Dubai Government entities' internal processes.
- DESC at its own discretion (if for instance a compromise is known for this CA key).

4.9.3 Procedure for revocation request

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

- **Revocation of certificates through DESC RA:**
  - The subscriber or an authorized representative requests the revocation of their certificate(s) to the DESC RA.
  - The DESC RA officer authenticates the subscriber's identity as described in section 3.4.
  - The DESC RA officer requests the subscriber to fill in and sign a revocation request form.
  - The DESC RA officer revokes the subscriber's certificate(s).
  - The CA generates an updated CRL and publishes it to the DESC public repository.
- **Revocation of certificates through an LRA:**
  - The LRA receives a revocation request from the subscriber
  - The LRA validates the identity of the subscriber as done during initial certificate application
  - The LRA records the revocation request according to the Dubai government entities' business rules
  - The LRA officer revokes the subscriber's certificates
  - The CA generates an updated CRL and publishes it to the DESC public repository
- **Revocation of OCSP certificates:**
  - The revocation is conducted as part of a PKI process internal to DESC and is approved by the Dubai PKI PA. This process involves communication with relying parties in order to update them with the OCSP certificate revocation.

4.9.4 Revocation request grace period

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

4.9.5 Revocation request response time

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

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

- Within 1 business day of being made aware of the incident, the CA contacts the software publisher (a Dubai Government entity) and requests a response within 72 hours.

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

4.9.6 Revocation checking requirement for relying parties

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

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

4.9.7 CRL issuance frequency

CRLs are issued as per section 2.3 or this document.

4.9.8 Maximum latency for CRLs

No stipulation – this section is intentionally left blank.

4.9.9 Online revocation/status checking availability

OCSP is supported within this PKI solution and is compliant with RFC 2560. OCSP information is available immediately to relying party applications.

The actual OCSP URL to be queried by relying party organizations is referred to in the certificates.

4.9.10 Online revocation checking requirements

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

4.9.11 Other forms of revocation advertisements available

No stipulation – this section is intentionally left blank.

4.9.12 Special requirements – Key compromise

No stipulation – this section is intentionally left blank.

4.9.13 Circumstances for suspension

Certificate suspension is not supported by this CA.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.10 Certificate Status Services

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

4.10.1 Operational characteristics

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

The DESC OCSP responder exposes 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

Key escrow and recovery are not supported by this CA.

5. Facility, Management and Operational Controls

5.1 Physical controls

5.1.1 Site location and construction

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

5.1.2 Physical access

Physical security controls include security guard controlled building access, man traps, biometric IRIS access and CCTV monitoring. These physical controls protect the hardware and software from unauthorized access, furthermore these controls are monitored on a 24*7*365 basis.

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site 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 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 deliver the necessary credentials that allow Administrators to conduct their functions.

5.2.4 Roles requiring separation of duties

DESC ensures separation among the following discreet work groups:

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

5.3 Personnel controls

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

5.3.1 Qualifications, experience and clearance requirements

DESC ensures that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such background checks include:

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

5.3.2 Background check procedures

DESC 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 to avoid dependency on key staff members.

5.3.6 Sanctions for unauthorized actions

DESC sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the DESC Subordinate CAs personnel, as it might be appropriate under the circumstances and as per the prevailing HR Policy and Country Law.

5.3.7 Independent contractor requirements

Independent 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

5.4.1 Types of event recorded

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. DESC ensures that at least the following details are recorded:

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

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

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

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

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

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

Archives are accessible to authorized personnel of DESC.

5.5.1 Types of records archived

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

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

5.5.2 Retention period for archive

DESC retains in a trustworthy manner, records of digital certificates for a term as indicated under article 5.5 in this CP.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

Only authorized and authenticated staff is allowed to handle archive material.

5.5.7 Procedures to obtain and verify archive Information

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

5.6 Key changeover

Corporate CA private keys are maintained until such time as all relying certificates have expired.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In a separate internal document, 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/data corruption

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

DESC establishes:

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

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, the following actions shall be taken by DESC:

- All active certificates issued by the corporate CA shall be revoked.
- Organizations holding Client Certificates shall be notified.
- A new corporate CA key pair shall be generated and certificate produced by the Dubai Root CA.

- A corporate CA compromise notice shall be published toward relevant relying parties.
- After 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 CPS document.

5.7.4 Business continuity capabilities after a disaster

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

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

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

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

5.8 CA or RA termination

If DESC determines that termination this CA is 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

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

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

The corporate 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 CA. Subscribers must generate their keys as specified in the below table:

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

6.1.2 Private key delivery to subscriber

Not applicable.

6.1.3 Public key delivery to certificate issuer

Public keys shall be delivered to 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

This corporate CA key pair is 4096 bit RSA.

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

6.1.6 Public key parameters generation and quality checking

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

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

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

6.1.7.1 Corporate CA

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

Corporate CA key usage.

6.1.7.2 Certificates for individuals

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

Subscriber's key usage.

6.1.7.3 Certificates for government entities

Signing
Keys may be used to digitally sign code. The Certificate KeyUsage field will be set to: Key usage:: Bitstring {digitalSignature}

Subscriber's key usage.

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

The creation of key backups on backup devices shall be conducted using the principles of dual controls and split knowledge, involving at least two PKI officers. At least one backup of the 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

No stipulation – this section is intentionally left blank.

6.2.6 Private key transfer into or from a HSM

The corporate CA key pairs shall only be transferred to another hardware cryptographic device 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 CA are activated by a minimum of two privileged users using the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the CA HSM.

Subscriber’s private keys are not generated and managed by the corporate CA.

6.2.9 Method of deactivating private key

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

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

When private keys are deactivated, they are cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system.

6.2.10 Method of destroying private key

At the end of their lifetime, taking into account business purpose and legal obligations, the corporate CA private keys shall be destroyed by multi-person presence including at least one representative of the Dubai PKI PA, in order to ensure that these private keys cannot ever be retrieved and used again.

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

6.2.11 Cryptographic module rating

The CA must use 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 CPS.

6.3.2 Certificate operational periods and key pair usage periods

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

Key certificate type	Maximum validity period
Certification Authority Certificate and associated keys	Recommended 96 months, re-key at 37% lifetime i.e., 36 months
Certificates for individuals and associated keys	Maximum operational period for a subscriber's key pair must be five years i.e., 60 months
Certificates for government entities and associated keys	Maximum operational period for a subscriber's key pair must be 39 months

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1.1 CA key generation

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

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

6.4.1.2 Subscribers keys

The corporate CA shall register its subscribers prior to issuing digital certificates to the subscribers.

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

6.4.2 Activation data protection

Activation data for CA subscribers shall be generated randomly. Any activation data shall be bound to one subscriber only and shall have a limited lifetime. Activation data shall be transmitted via an automated process through the secure exchange of activation data between the corporate CA and RA applications.

6.4.3 Other aspects of activation data

No stipulation – this section intentionally left blank.

6.5 Computer security controls

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

6.5.1 Specific computer security technical requirements

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

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

6.5.2 Computer security rating

No stipulation – this section is intentionally left blank.

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

6.6.2 Security management controls

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

The corporate CA and RAs functionality shall be scanned for malicious code on first use and periodically afterwards.

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

6.6.3 Life cycle security controls

No stipulation – this section intentionally left blank.

6.7 Network security controls

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

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

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

6.8 Time-stamping

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

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

7.1.1 Certificates for individuals

7.1.2.1 Subscriber's encryption certificate ASN1 description

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

Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(1) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded

[2] CE = Critical Extension.
[3] O/M: O = Optional, M = Mandatory.
[4] CO = Content: S = Static, D = Dynamic

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[60]** Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	Allocated as per certificate request	UTF8 encoded
	organizationName		M	D	Allocated as per certificate request	UTF8 encoded
	localityName		M/O	D	Dubai	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Dubai	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user name>	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm			D	RSA / ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field

	accessLocation		M	D	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints		False	M			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRLNumber>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(2)	keyUsage	True	M			
	(3) keyEncipherment		M	S	True	
	(4) dataEncipherement		M	S	True	
Extended Key Usage Properties						
(5)	extKeyUsage	False	M			
	(6) emailProtection		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.1	

7.1.2.2 Subscriber's signing certificate ASN1 description

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

Field	CE[5]	O/M[6]	CO[7]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(7) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		

[5] CE = Critical Extension.
[6] O/M: O = Optional, M = Mandatory.
[7] CO = Content: S = Static, D = Dynamic

	countryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationName		M	S	UAE Government	UTF8 encoded
	commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[60]** Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	<optional organizational unit name within the Dubai government entity>	UTF8 encoded
	organizationName		M	D	<Dubai government entity meaningful name>	UTF8 encoded
	localityName		M/O	D	Dubai	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Dubai	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user name>	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm			D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			

	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		O	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	D	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA certificate download URL
cRLDistributionPoints		False	O			
	distributionPoint		O	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(8) keyUsage		True	M			
	(9) nonRepudiation		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.3	

7.1.2.3 Subscriber's authentication certificate ASN1 description

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

Field	CE[8]	O/M[9]	CO[10]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(10) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore			D	Certificate generation process date/time.	
NotAfter			D	Certificate generation process date/time + not more than **[60]** Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationUnitName		O	D	<optional organizational unit name within the Dubai government entity>	UTF8 encoded
organizationName		M	D	<Dubai government entity meaningful name>	UTF8 encoded

[8] CE = Critical Extension.
[9] O/M: O = Optional, M = Mandatory.
[10] CO = Content: S = Static, D = Dynamic

	localityName		M/O	D	Dubai	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Dubai	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user name>	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm			D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		O	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	D	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints		False	O			
	distributionPoint		O	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(11)	keyUsage	True	M			
	(12) digitalSignature		M	S	True	
	(13) keyEncipherment		M	S	True	
	(14) dataEncipherement		M	S	True	
Extended Key Usage Properties						
(15)	extKeyUsage	False	M			

	(16) clientAuth		M	S	True	
	(17) emailProtection		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.1.2	

7.1.2 Certificates for Dubai government entities

7.1.3.1 Subscriber's signing certificate ASN1 description

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

Field	CE[11]	O/M[12]	CO[13]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(18) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than **[60]** Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationUnitName		O	D	<optional organizational unit name within the Dubai government entity>	UTF8 encoded

[11] CE = Critical Extension.
[12] O/M: O = Optional, M = Mandatory.
[13] CO = Content: S = Static, D = Dynamic

	organizationName		M	D	<Dubai government entity meaningful name>	UTF8 encoded
	localityName		M/O	D	Dubai	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Dubai	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Dubai Government Entity Organization Unit Name>	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm			D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		O	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	D	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA certificate download URL
cRLDistributionPoints		False	O			
	distributionPoint		O	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(19)	keyUsage	True	M			
	(20) nonRepudiation		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	M			

	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.2.1	

7.1.3.2 Subscriber's code signing certificate ASN1 description

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

Field	CE[14]	O/M[15]	CO[16]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(21) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore			D	Certificate generation process date/time.	
NotAfter			D	Certificate generation process date/time + not more than **[36]** Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationUnitName		O	D	<Dubai Government Entity Organization Unit Name>	UTF8 encoded
organizationName		M	D	<Dubai Government Entity Organization Name>	UTF8 encoded

[14] CE = Critical Extension.
[15] O/M: O = Optional, M = Mandatory.
[16] CO = Content: S = Static, D = Dynamic

	localityName		M/O	D	Dubai	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Dubai	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Dubai Government Entity Organization Unit Name>	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm			D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	D	http://ca-repository.desc.gov.ae/certificate/corporate.p7b	Corporate CA Certificate download URL.
cRLDistributionPoints		False	M			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(22)	keyUsage	True	M			
	(23) digitalSignature			S	True	
Extended Key Usage Properties						
(24)	extKeyUsage	False	M			
	(25) codeSigning			S	True	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			

	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.2.2	

7.1.3 Version number

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

7.1.4 Certificate extensions

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

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

7.1.5 Algorithm object identifiers

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

7.1.6 Name forms

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

7.1.7 Name constraints

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

7.1.8 Certificate policy object identifier

Refer to the ASN1 definitions described in the below subsections.

7.1.9 Usage of policy constraints extension

No stipulation – this section is intentionally left blank.

7.1.10 Policy qualifiers syntax and semantics

No stipulation – this section intentionally left blank.

7.1.11 Processing semantics for critical certificate extensions

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

7.2 CRL profile

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

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

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

7.2.3 CRL ASN1 description

This is the complete ASN1 description of the CRL certificate.

Field	CE[17]	CO[18]	Value	Comment
CertificateList				
TBSCertificate				
Signature	False			
algorithm		S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		D	Corporate CA Signature.	CA signature value
TbsCertList				
Version	False			
		S	2	V2
SerialNumber	False			
CertificateSerialNumber		F		At least 64 bits of entropy Validated on duplicates.
signature	False			
algorithm		S	(26) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	S		
countryName		S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
organizationName		S	UAE Government	UTF8 encoded
commonName		S	Corporate Certification Authority	UTF8 encoded
Validity	False			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		D	CRL generation date/time	
nextUpdate		D	CRL generation date/time + 1 day + 2 hours	

[17] CE = Critical Extension.
[18] CO = Content: S = Static, D = Dynamic

revokedCertificates					
	Certificate				
	CertificateSerial		D	Serial of the revoked certificate	
	revocationDate		D	UTC Time of revocation (Optional)	
Extensions					
crlEntryExtensions					
authorityKeyIdentifier		False		This MUST be the same value as the subject Key Identifier field in the CRL Issuer's certificate. Non-critical <subject key identifier CA>	SHA-1 Hash of the Corporate CA public key
crlEntryExtensions					
crlNumber		False			Sequential CRL number

7.3 OCSP profile

7.3.1 Version number(s)

The OCSP responder issues OCSP responses of version 1.

7.3.2 OCSP extensions

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

7.3.3 OCSP Response Signing Certificate ASN1 Description

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

Field	CE[19]	O/M[20]	CO[21]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Corporate CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			

[19] CE = Critical Extension.
[20] O/M: O = Optional, M = Mandatory.
[21] CO = Content: S = Static, D = Dynamic

	algorithm		M	S	(27) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer		False	M	S		
	countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationName		M	S	UAE Government	UTF8 encoded
	commonName		O	S	Corporate Certification Authority	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore			D	Certificate generation process date/time.	
	NotAfter			D	Certificate generation process date/time + not more than **[36]** Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	commonName		M	S	Corporate Certification Authority OCSP	
	organizationName		M	S	DESC	
	localityName		M	S	Dubai	
subjectPublicKeyInfo		False	M			
	algorithm			S	RSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions			M			
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(28) Key Usage		True	M			
	(29) digitalSignature		M	S	True	
	(30) nonRepudiation		M	S	True	
(31) extKeyUsage		False	M			
	(32) id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck		False	M	S	05 00	
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	(33) policyQualifiers:policyQualifierId		O	S	id-qt 1	
	(34) policyQualifiers:qualifier:cPSuri		O	D	URL location of this CPS	

8. Compliance Audit And Other Assessments

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

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

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

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

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

- Independence from the subject of the audit
- Ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities v2.0
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

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

9. Other Business and Legal Matters

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

9.1 Fees

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

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

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

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

9.4 Privacy of Personal Information

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

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

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

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

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

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

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

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

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

Disclosure Conditions

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

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

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

- Themselves
- Persons in their custody

Only the RA is permitted to access confidential information.

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

DESC authenticates itself to any party requesting the disclosure of information by:

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

All communications of confidential information are encrypted, including:

- The communications link between the Corporate CA and the RA.
- Sessions to deliver certificates and certificate status information

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

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

The Corporate CA warrants to the Subject, Subscriber, Relying parties and all Application Software Suppliers with whom the Corporate CA 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, the Corporate CA, or any person receiving or relying on the certificate
- Any liability incurred as a result of the applicant breaking any laws applicable in Dubai, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- Other damage

9.8 Limitations of Liability

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

9.9 Indemnities

Not applicable.

9.10 Term and Termination

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

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

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

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The present CPS and provision of Corporate CA certification services are compliant to relevant, and applicable laws of Dubai.

9.16 Miscellaneous Provisions

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

- Terms and conditions in this CPS
- Any other applicable certificate policy as may be stated on a certificate issued by the Corporate CA
- The mandatory elements of applicable standards
- Any non-mandatory, but customized elements of applicable standards
- Content of extensions and enhanced naming not addressed elsewhere
- Any other information that is indicated to be so in a field of a certificate

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

9.17 Other Provisions

Not applicable.