Dubai Electronic Security Center

Dubai PKI

Corporate CA

Certification Practice Statement

Project	DESC CA Project
Title	Corporate CA, Certification Practice Statement
Classification	PUBLIC
File Name	DubaiPKI-CorporateCA-CertificationPracticeStatement_v2.1
Created on	18 May 2017
Revision	2.1
Modified on	10 Feb 2024

Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1	Khawla Hassan	Initial version
12 September 2017	0.2	Khawla Hassan	Minor modifications & Incorporation of Dubai government entity Root CA option
3 November 2017	0.3	Khawla Hassan	Minor modifications to reflect control environment
11 January 2018	0.4	Khawla Hassan	Update certificates profiles
18 January 2018	0.5	Khawla Hassan	Second revision of certificates profile
30 January 2018	1.0	Khawla Hassan	Issue final version
25 February 2018	1.1	Khawla Hassan	Update publication of certificate information
16 October 2018	1.2	Khawla Hassan	• Updates based on regular review, in addition to explicitly documenting the email verification practice for certificates issued for email protection. • Expand Dubai PKI services to cover an extended set of UAE government entities and documenting the relevant certificate management practices.
07 August 2019	1.3	Khawla Hassan	• Added contact and high-level procedure of Certificate Problem Report • Aligned the circumstances of revocation with the BRs
3 June 2020	1.4	Khawla Hassan	• Updates based on regular review and addressing Mozilla Comments
26 November 2020	1.5	Khawla Hassan	• Depreciate the authentication certificate profile

			• Add new profile to replace deprecated profile section 7.1.1.4
18 February 2021	1.51	Khawla Hassan	• Add manual registration process for UAE PASS
11 April 2021	1.6	Khawla Hassan	• Annual review and updates to address Mozilla comments and clarify subordinate CAs governance and operating environment
13 July 2021	1.61	Khawla Hassan	• Add user authentication certificate profile (for natural persons) • Increase the CRL lifetime to 72 hours
1st April 2022	1.7	Khawla Hassan	• Annual review • General enhancements on the document • Remove code signing certificates • Update Encryption certificates profile (removed emailprotection) • Add verification response signing certificate • Add signing and authentication certificates issued for UAE visitors
7th September 2022	1.8	Khawla Hassan	Correct typographical errors and general enhancements
6th April 2023	1.9	Khawla Hassan	• Annual review • Align the definitions and log retention with DESC Subordinate CAs, Certificate Policy Ver 1.8
2nd November 2023	2.0	Khawla Hassan	• Update the certificates supported under the Devices CA in the PKI hierarchy • Add LRA Certificate
10th February 2024	2.1	Khawla Hassan	• Add the authorityInfoAccess extension to the CRL

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). The Corporate CA is one of the subordinates CAs signed by the Dubai Root CA. This CPS complies with DESC Subordinate CAs Certificate Policy that applies to the provision of certification services offered by DESC through its Subordinate CAs (Issuing CAs).

This CPS covers the issuance and controls surrounding the following types of certificates issued by the Corporate CA:

- **Certificates for natural persons** – comprises certificates issued for citizens, residents, visitors and government employees of the UAE; these certificates are used for the following purposes:
    - **Signing certificate** – used to produce digital signatures on digital transactions and documents
    - **Encryption certificate** – used for data/document encryption
    - **Authentication certificate** – used for authentication of subscribers in online services
- **Certificates for government entities (eSeal certificates)** – Certificates used to apply eSeals on documents issued by an entity (legal person) to confirm the identity of the document issuer, the origin and integrity of the data source in these documents
- **Verification Response Signing Certificates** — Certificates for the Dubai PKI Signature Verification Service to sign verification responses related to certificates issued by the Dubai PKI.
- **LRA Certificates** — Certificates for authentication of Certificate Management requests received from LRAs.
- **OCSP certificates** – certificates for the Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by this CA

This CPS meets the formal requirements of Internet Engineering Task Force (IETF) [RFC 3647] regarding content, format and content. While certain clause titles are included according to the structure of [RFC 3647], the topic may not necessarily apply in the implementation of the Corporate CA, such sections state “No stipulation”. Additional information is presented in subsections of the standard structure where required.

This CPS aims to comply with the WebTrust Principles and Criteria for Certification Authorities requirements published at https://www.cpacanada.ca.

The Dubai PKI is committed to maintain this CPS in conformance with the current versions of the CA/Browser Forum Network and Certificate System Security Requirements published at http://www.cabforum.org.

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

Further information about this document and the Corporate CA can be obtained from the Dubai PKI Policy Authority (PA), which is representing the policy and governing body for the Dubai PKI including DESC Subordinate CAs. Contact information of the Dubai PKI PA is provided under section 1.5.

1.1 Overview

The “Dubai PKI” uses standard PKI technologies, policies and operating procedures and application interfaces. The Dubai PKI comprises the Dubai PKI Root CA that is the trust anchor of this PKI, which comes at the first level of the PKI hierarchy. The Dubai PKI also comprises currently multiple

Subordinate Certification Authorities (CAs): Corporate CA, Code Signing CA, Timestamping CA (hereinafter, DESC Subordinate CAs), which come at the second level of the PKI hierarchy. DESC owns and operates the Dubai PKI Root and the aforementioned Subordinate CAs to provide certification services that enable individuals and government entities in the UAE to conduct secure electronic transactions; this includes securing the machine-to-machine communication where devices can transact securely, leveraging the PKI signing and encryption capabilities.

Additionally, the Dubai PKI Root CA aims to sign subordinate CAs belonging to government or private sector entities. Such entities have their own custom needs and reasons to implement their own CAs rather than using a DESC Subordinate CAs.

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

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

1.1.1 Dubai PKI hierarchy

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

DESC is fulfilling the role of the Policy Authority (PA) for the Dubai PKI (hereinafter, Dubai PKI PA) shall authorize the Root certification services for DESC Subordinate CAs as well as the issuing CAs owned by other government or private sector entities.

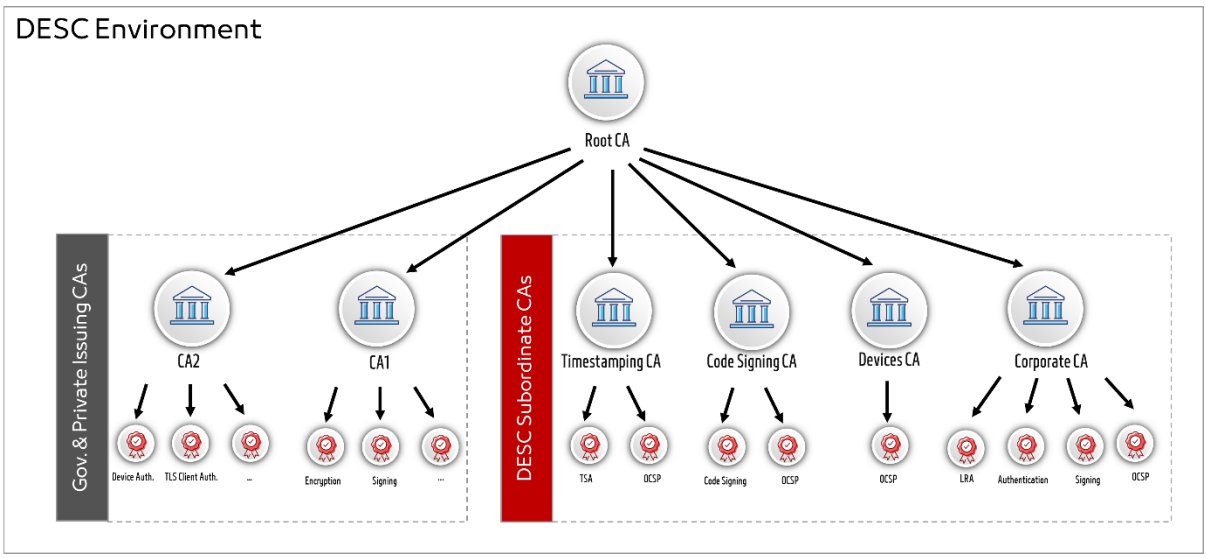

Figure 1: Trust Model for Dubai PKI

1.1.2 Dubai PKI Policy Authority (PA)

The Dubai PKI Policy Authority (PA), composed of appointed members of the DESC management and Dubai PKI team, is representing the policy and governing body for the Dubai PKI, including the Corporate CA. The PA is the highest-level management body with final authority and responsibility for:

- Specifying and approving the Dubai PKI infrastructure
- Approving government and private sector entities applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy
- Specifying, maintaining and approving the Dubai PKI practices and policies, in particular the Certification Practice Statements (CPS) and the related Certificate Policies (CP) when applicable
- Review annual audit report submitted by government or private sector entities CAs to ensure continuous compliance to Dubai PKI requirements
- Review regular audit reports of LRAs
- Enforcing CP/CPS and other policies applicable to Dubai PKI Environment
- Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CPs/CPSs and related policies
- Defining the review process that ensures that the Dubai PKI properly implements the above practices
- Defining the review process that ensures that the related policies are supported by the Dubai PKI CPs and CPSs
- Publication of CP and CPS documents
- Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the Dubai PKI
- Evaluating the proper working of the Dubai PKI environment
- Allocating members to the key ceremonies as witness as well as trusted operatives and key custodians
- Evaluating changes to the Dubai PKI environment (management, operational, hardware, software and security)
- Evaluating case-by-case issues where key Dubai PKI staff/personnel did not respect the security and/or operational procedures, including ethics
- Deciding on critical issues in case of incidents, disasters and other severe problems with regards to the Dubai PKI.

1.1.3 Certificate Policy

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

1.1.4 Relationship Between the DESC Subordinate CAs CP and this CPS

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

1.2 Document name and identification

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

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

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

OID	Certificate type	Description
2.16.784.1.2.2.100.1.2.2.1.1	Encryption certificates	Encryption certificates for individuals (e.g., data, documents)
2.16.784.1.2.2.100.1.2.2.1.2	**Deprecated:** Authentication certificates	Certificates for individual authentication purposes
2.16.784.1.2.2.100.1.2.2.1.6	Authentication certificates	Certificates for individual authentication purposes
2.16.784.1.2.2.100.1.2.2.1.3	Digital signature certificates (high assurance)	Digital signing certificates for individuals to be used for signing transactions that require a high assurance level of identity vetting
2.16.784.1.2.2.100.1.2.2.1.4	Digital signature certificates (moderate assurance)	Digital signing certificates for individuals to be used for transactions that does not require the highest assurance levels of identity vetting
2.16.784.1.2.2.100.1.2.2.1.5	Mobile authentication certificates	Certificates for individuals installed on the mobile e.g. to trust personal smart device
2.16.784.1.2.2.100.1.2.2.1.7	Visitors digital signature certificates (high assurance)	Digital signing certificates for individuals to be used for signing transactions that require a high assurance level of identity vetting. Issued for UAE visitors.
2.16.784.1.2.2.100.1.2.2.1.8	Visitors digital signature certificates (moderate assurance)	Digital signing certificates for individuals to be used for transactions that does not require the highest assurance levels of identity vetting. Issued for UAE visitors.
2.16.784.1.2.2.100.1.2.2.1.9	Visitors mobile authentication certificates	Certificates for individuals installed on the mobile e.g. to

		trust personal smart device. Issued for UAE visitors.
2.16.784.1.2.2.100.1.2.2.2.1	eSeal certificates (high assurance)	Certificates used to apply eSeals on documents issued by an entity (legal person) to confirm the identity of the document issuer, the origin and integrity of the data source in these documents
2.16.784.1.2.2.100.1.2.2.3.4	Signature verification service certificate	A certificate used to sign the verification responses generated by the DESC signature verification service
2.16.784.1.2.2.100.1.2.2.3.5	LRA certificate	Certificate used to authenticate certificate management requests sent by third-party LRAs

1.3 PKI participants

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

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

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

1.3.1 Certification Authorities

The Corporate CA (also referred to as “CA”) is the Certification Authority that issues Certificates in accordance with this CPS. The Corporate CA issues certificates (see section 1.2) for Government entities, Citizens, Residents, Visitors in addition to OCSP and signature verification response signing certificates. This includes the following tasks:

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

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

1.3.2 Registration Authorities

DESC RA

Duly authorized members part of Dubai PKI team act as Registration Authority (RA) for this CA. DESC RA function falls within the PKI operations structure and, it is responsible for accepting and validating certificate issuance and management operations, in addition to triggering related certification operations by this CA.

Local Registration Authority(LRA)

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

DESC accepts the following LRAs:

- Officer duly authorized by the government entity: This officer will be enrolled to DESC Corporate CA by DESC RA. He will receive credentials that allow to access the Corporate CA remotely through a dedicated Web RA application and manage the digital certificates of the government entity subscribers' community. Multi-factor authentication is implemented whenever RA/LRA officers approve certificate applications for issuance.
- System/application: Operated by the government entity and integrated with the Corporate CA through a secure interface exposed by the CA. The system/application is configured with dedicated credentials issued by DESC RA so that it can request certificates from Corporate CA and manage the subscribers' community certificates.
- The UAE national Authentication and Digital Signing platform (known as UAE PASS) is an example of an LRA application that is currently integrated with this CA to issue and manage Authentication and Signing certificates for Citizens, Residents and Visitors of the UAE.

Before authorizing an entity to operate an LRA, DESC RA validates the organization's identity as specified in section 3.2.2.3 and signs an LRA agreement through which the entity commits to operate their LRA in accordance with DESC Subordinate CA CP and this CPS.

The LRA agreement describes the LRA obligations/responsibilities for:

- Authenticating, approving, or rejecting certificate application requests
- Identify subscribers in accordance with naming conventions defined within the present CP and the applicable CPS to ensure uniqueness and unambiguity
- Submit certification requests to DESC Subordinate CAs only for the applications that have been validated and approved by the LRA
- Creating and maintaining an audit-log that records all significant events related to the RA's operations and fulfilment of the above-mentioned responsibilities
- Providing selective access to audit-log records as specified in this CP
- Implementing other operational controls as specified in this CP
- Ensuring that the information that it stores and processes is handled in a manner that is consistent both with the policies and procedures defined in this document and with the Dubai PKI security's regulations.

1.3.3 Subscribers

Subscribers of the Corporate CA are Government entities, Government employees and Citizens/Residents/Visitors of the UAE. In addition, the corporate CA OCSP responder as well as DESC signature verification service.

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

1.3.4 Relying Parties

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

Relying Parties are entities that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate issued by the Corporate CA.

Relying parties shall always verify the validity of a digital certificate issued by the Corporate CA using the Corporate CA Certificate Validations Services (e.g. CRL, OCSP), prior to relying on information featured in the certificate.

1.3.5 Other participants

There are no other participants for this CA.

1.4 Certificate usage

1.4.1 Appropriate certificate use

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

- Certificates for natural persons :
    - Encryption key pair with related certificate
        - Document/data encryption
    - Signature key pair and related certificate
        - Signing documents and digital transactions
    - Authentication key pair and related certificate
        - Authentication
- Certificates for government entities (legal persons):
    - Signature key pair and related certificate
        - eSeal documents issued by the entity (legal person)
- Signature verification service certificate:
    - Signature key pair and related certificate
        - Sign verification responses generated by DESC signature verification service
- LRA Certificates:
    - Authentication key pair and related certificate
        - Authenticate Certificate Management requests received from LRAs.
- OCSP certificates for OCSP responder delegated by this CA.

In accordance with its purpose of use, the certificate may be used without limitations.

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

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

1.4.2 Prohibited certificate use

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

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

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact Person

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

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

Email pa@desc.gov.ae

Certificate Problem Report

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

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

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

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

1.6 Definitions, acronyms and references

1.6.1 Definitions

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request. In the context of this CPS, the applicants are Government entities subscribing to the Corporate CA services.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information. In the context of this CPS, attestation letters are signed by Human Resource teams of government entities.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.)

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Root CAs and Subordinate CAs.

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of this CPS.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate Requester: An authorized administrator of a device or system who is responsible for submitting the certification requests to the CA/RA.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country: Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

CSPRNG: A random number generator intended for use in a cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Government Entity: A Dubai government entity or other government entities in the UAE authorized by Dubai PKI PA to consume the PKI services.

Hardware Security Module: a device designed to provide cryptographic functions, especially the safekeeping of private keys.

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Policy Qualifier: Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely- available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.
Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate. In the context of this CPS, the UAE official gazette is the reliable data source for government entities in UAE.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Requester.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Sovereign State: A state or country that administers its own government, and is not dependent upon, or subject to, another power.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Technically Constrained Subordinate CA Certificate: A Subordinate CA 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.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

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

Trustworthy System: Computer hardware, software, and procedures that are:
reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified by this CPS.

Validity Period: From RFC 5280 (http://tools.ietf.org/html/rfc5280): “The period of time from notBefore through notAfter, inclusive.”

1.6.2 Acronyms

CA — Certification Authority

CCTV — Closed circuit TV

CP — Certificate Policy

CPS — Certification Practice Statement

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

FQDN — Fully Qualified Domain Name

HSM — Hardware Security Module

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

ITU — International Telecommunications Union

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

DESC — Dubai Electronics Security Center

OID — Object Identifier

OSCP — Online Certificate Status Protocol

OTP — One Time Password

PA — Policy Authority of Dubai PKI

PIN — A Personal Identification Number or password used to protect the private information and keys on hardware tokens

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.

RA — Registration Authority

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

SCEP — Simple Certificate Enrolment Protocol

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

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

SubjectAltName — A certificate extension that contains FQDNs or authenticated domains or email addresses that are under the control of the Subscriber

SDG — Dubai Smart Government Establishment

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

2. Publication and repository responsibility

2.1 Repositories

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

2.2 Publication of certificate information

As part of the public repository, DESC publishes a copy of the Corporate CA certificates, OCSP certificates as well as this CPS.

DESC also retains other documents that make certain disclosures about the Corporate CA practices, procedures, and the content of certain of its policies as part of the public repository. DESC 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 24/7 available service offered as follows;

- Published CRLs including any changes since the publication of the previous CRL, at regular intervals. The Corporate CA adds a pointer (URL) to the relevant CRL to Subscribers' certificates as part of the CDP extension whenever this extension is present;
- An OCSP responder compliant with RFC 6960. The OCSP URL is referenced in the AIA extension of the Subscribers' certificates issued by the Corporate CA.

2.3 Time or frequency of publication repositories

Modified versions of this CPS and other published documents are published within five days maximum after the Dubai PKI PA approval.

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.

2.3.1 Certificates

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

2.3.2 CRLs

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.

The Corporate CA publishes CRLs at regular intervals according to the following rules:

- At the minimum, CRLs shall be refreshed every 26 hours, even if no changes have occurred since the last issuance.
- CRLs lifetime shall be set to 72 hours.

2.4 Access controls on repositories

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

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

3. Identification and authentication

3.1 Naming

3.1.1 Types of name

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

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

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

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

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

- **Certificates issued for individuals:**

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

- **Cerificate for the Signature verification service:**

  cn = DESC Signature Verification Service, o = DESC ,l = Dubai ,c = AE

- **OCSP responder:**

  cn = Corporate Certification Authority OCSP "C<n>", o = DESC, l = Dubai, c = AE
  Where "C<n>" is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.

3.1.2 Need for names to be meaningful

For certificates issued to natural persons: 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 certificate issued to the signature verification service: name is meaningful since it indicates the DESC signature verification service name which is "DESC Signature Verification Service".

For certificate issued to LRAs: name is meaningful since the CN contains the LRA Service name as agreed with during the LRA onboarding process.

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

3.1.3 Anonymity and pseudonymity of subscribers

This CA does not support the issuance of anonymous certificates.

3.1.4 Rules for interpreting various name forms

No stipulation – this section is intentionally left blank.

3.1.5 Uniqueness of names

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

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

3.1.6 Recognition, authentication and role of trademarks

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

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

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

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

3.2.2 Authentication of Organization identity

3.2.2.1 Identity

For certificates containing organization information, the applicant is required to provide the Government entity's name, organizational unit (if applicable) and official address. DESC RA verifies the Organization's identity as follows:

A. Presence / Legal standing

- Verify the existence of the Organization using an authoritative source that is expected to provide detailed information about the entity including its legal name and address, the most common authoritative source used by DESC RA is the UAE Official Gazette.

- Verify authority of the Organization's authorized representative requesting the certificate as specified in section 3.2.5.

B. Association

For eSeal and LRA certificates: The organization name to be inserted in the requested certificate must exactly match the legal name of the Government entity requesting the certificate unless there is an authentic proof linking the entity with the name to be included in the certificate.

For certificates issued to natural persons associated with an organization: The association between the Organization name to be inserted in the certificate and applicant needs to be established based on an authentic proof such as an HR Attestation Letter in the organization's letterhead is prepared confirming the relation between the applicant and the organization.

C. Authority of the applicant

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

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

3.2.2.2 DBA/Tradename

The use of DBA or Tradename in the Subject Identity Information is not supported by the Corporate CA.

3.2.2.3 Organizations applying to operate an LRA

When a government entity aims to issue and manage natural person certificates for their user base (e.g. employees), they communicate with DESC RA or the Dubai PKI PA to go through the following enrollment process:

(1) verify the presence / legal standing of the organization as specified under point A in section 3.2.2.1,

(2) an authorized representative of the Government entity signs the LRA agreement,

(3) DESC RA add the required configurations on the Corporate CA RA system to enroll the Government entity and their LRA officers. The information received from the Government entity during the enrolment process is used to populate this profile. The LRA officers are enrolled with multi-factor authentication credentials that are used to execute certificate requests and related certificate management operations.

3.2.3 Authentication of individual identity

3.2.3.1 Certificates issued through a government entity LRA officer (or DESC RA officer)

- **Certificates for "moderate assurance" transaction:** The RA/LRA verifies the applicant's Identity verification is performed as follows:
    - Obtain the following applicant's identity proofing evidence through the organization internal channels (e.g. from HR, from a direct line of business manager or from the applicant himself):
        - An attestation Letter confirming the affiliation of the applicant to the government entity and providing details such as employee ID, full name and date of birth,
        - Applicant's contact information if required (including phone number and email address)
        - An email from HR or a direct line of business manager requesting the RA/LRA to enroll the applicant into the PKI and issue him/her certificates of certain types (as per the business need).

- Verify the authenticity of the identity proofing documents through internal processes.

- **Certificates for "high assurance" transaction:** The RA/LRA verifies the applicant's identity through an in-person meeting with the applicant and involving the presentation of a government-issued photo ID (e.g. Emirates ID) in addition to supporting evidence. The verification process consists in the following steps:
  - Obtain the following supporting evidence through the organization internal channels (.g. from HR, from a direct line of business manager or from the applicant himself):
    - An attestation Letter in the organization's letterhead (or equivalent evidence such as an extract from the official gazette) confirming the affiliation of the applicant to the government entity and providing details such as employee ID, full name and date of birth,
    - An email from HR or a direct line of business manager requesting the RA/LRA to enroll the applicant into the PKI and issue him certificates of certain types (as per the business need).
  - Verify the authenticity of the identity proofing documents through internal processes,
  - Conduct an in-person meeting with the individual to complete the identity verification against the government-issued photo ID. During the meeting, the applicant presents his government-issued ID to RA/LRA officer that verifies that full name/date of birth of the individual from the attestation letter matches the full name/date of birth from the ID.

- **For certificates including email address(es):** The RA/LRA officer verifies ownership of the email to be included in the certificate as follows:

  (1) the entity's internal employee records where emails are formally assigned/specified for each employee.

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

3.2.3.2 Certificates issued through the UAE PASS system:

Refer to section 4.1.2.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

- **For Government entity certificates to be issued through DESC RA (including LRA certificates):** The authority of the certificate requestor to request a certificate on behalf of a Government entity will be performed through a reliable means of communication with the Government entity that include the following steps at minimum:

  (1) DESC RA receives a legible copy, which discernibly shows the requester's face, of at least one currently valid government-issued photo ID (Emirates ID, passport or a UAE driving license). DESC RA will then inspect the copy for any indication of alteration or falsification,

  (2) DESC RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized representative that attests the ability of the requestor to requests certificates on behalf of the government entity,

  (3) DESC RA verifies the authority of the authorized representative through the Official Gazette or through a formal communication of the Government entity HR, or based on a formal letter signed by the Organization's top authority (e.g. Director General).

- **For natural persons certificates to be issued through the government entity LRA:** The LRA officer/system (that was previously approved by The Dubai PKI PA) is authorized to submit certification requests on behalf of the Government Entity subscribers.

3.2.6 Criteria for interoperation

No stipulation – this section is intentionally left blank.

3.3 Identification and authentication for re-keying requests

3.3.1 Identification and authentication for routine re-keying

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

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

  Once the revocation request is successfully authenticated, DESC RA revokes the subject certificate through the relevant RA system.
- **Certificates issued to natural persons through a government entity LRA (including DESC RA):** The RA/LRA officer authenticates the revocation request through one of the following methods:
    - Receiving a revocation request from the subscriber through methods relevant to the RA/LRA and the government entity's internal processes. This may include a face to face, call from the subscriber and the RA/LRA asking relevant questions to identify the subscriber (e.g. employee ID, name, date of birth, ….) or email from the subscribe using an email address that can be verified by the RA/LRA and linked to the subscriber's identity.
    - Communication with the requesting party to provide reasonable assurances that the individual or department requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include telephone and/or email.
    - HR (or team within the entity with similar mandate) if the subscriber is terminated or changed role within the entity which would trigger the revocation request. The RA/LRA would have the internal means to confirm with HR the validity of the revocation request.
- **Certificates issued to natural persons through the UAE PASS system:** The following scenarios may trigger revocation requests from the UAE PASS system:

- A revocation request is triggered through the UAE PASS regular business processes. One example would be the subscriber renewing his UAE PASS PKI credentials before existing ones are expired. The UAE PASS system interacts with the subscriber and validates the subscriber's identity and confirms that a revocation request is required. The UAE PASS system interacts (through integration) with the Corporate CA to revoke the certificate and request new certificate for the subscriber.
- A revocation request is triggered through the UAE PASS helpdesk. A typical scenario would be subscriber who is terminated from the UAE PASS system (e.g. subscriber leaving the country). The UAE PASS helpdesk communicates with DESC RA through agreed channels (telephone, email) which results in the revocation request being authenticated by DESC RA which can then process it through their dedicated RA applications.

4. Certificate Life Cycle Management

4.1 Certificate application

4.1.1 Who can submit a certificate application

- **Certificates for Government entities issued through DESC RA (including LRA certificates):** An authorized person from the Government entity submits the certificate application as part of the certificate issuance process. Whoever is submitting the certificate request (requester) needs to sign the application form and ensure that the government entity authorized representative approves the certificate request by signing and stamping the certificate request form and the appended subscriber agreement.

  DESC maintains its own internal blacklist of applicants from which it will not accept certificate requests. DESC RA logs in this database previously rejected certificate requests due to suspected or fraudulent usage and revoked certificate requests from government entities. This internal blacklist database is queried by the DESC RA whenever it receives any certificate request.

- **Certificates for natural persons issued through the Government entity LRA (including DESC RA):** The entity LRA or DESC RA submits the certificate application.

  LRA maintains its own internal blacklist of applicants from which it will not accept certificate requests.

- **Certificates for natural persons issued through the UAE PASS:** The UAE PASS system is the interface through which certificate applications are triggered to the CA.

- **Certificates issued to the OCSP responder certificates and the signature verification service:** An authorized administrator under the supervision of the Dubai PKI PA initiates the certification process. A dedicated operational key ceremony is documented by DESC.

4.1.2 Enrolment process and responsibilities

Certificates issued to Government entities through DESC RA (including LRA certificates)

a) DESC RA shares the list of evidences required along with Subscriber Agreement and the certificate request form with the applicant,

b) the applicant prepares the list of evidences, fills the certificate request form and signs a Subscriber Agreement or ratify a certificate terms of use,

c) DESC RA receives the signed subscriber agreement, certificate application form along with the requests list of evidences (refer to section 3.2.2 for the evidences required),

d) DESC RA verifies the validity and authenticity of received documents,

e) One of DESC RA verifies the authorized representative, certificate requester and the organization's identity as described in section 3.2.2.

f) A second DESC RA officer (who was not involved in the collection of information from applicant) reviews the work done the first officer to conclude application's approval

g) Once the application is approved, DESC RA officer uses a dedicated RA application to enroll the applicant into this CA. The applicant's unique name from the application form is used to produce a unique distinguished name necessary for enrolment into the CA system.

h) As part of the enrolment, DESC RA generates a unique authorization code for this certificate application and submits this code to the certificate requester's email address (as provided in the certification application form).

i) The applicant generates a key pair on its own IT system or device. He then creates a CSR file using the received unique authorization code provided by DESC RA.

j) The CSR file is sent to DESC RA through the requester's email (as provided in the certificate application form). DESC RA processes the CSR and issue the certificate from the CA.

k) DESC RA send the certificate to the entity requester's email address.

For the eSeal certificates that are hosted within the UAE PASS Platform, DESC RA interacts with the UAE PASS team for certifying the eSeal keypair that is generated within the UAE PASS platform. I.e., the steps g to j executed with the UAE PASS team while the certificate requester is kept copied in the email communications. In this scenario, DESC signs a three-party Subscriber agreement with the Subscriber (the entity requesting an eSeal certificate) and SDG (UAE PASS team). The agreement specifies the roles and responsibilities of each party considering that the eSeal key/certificate will be hosted within the UAE PASS remote signing platform.

Certificates for natural persons issued through the Government entity LRA (including DESC RA)

Certificates issued to natural persons through DESC RA or a government entity LRA (DESC RA is responsible of issuing certificates to DESC employees. Government LRAs are only responsible for issuing certificates to their community that is agreed with DESC as per the LRA agreement):

a) The applicant initiates a request according to the applicable entity's internal processes for requesting a certificate(s) according to busines needs

b) The RA/LRA shares the Subscriber Agreement with the applicant to ratify

c) The RA/LRA officer verifies the applicant's identity as described in section 3.2.3

d) The RA/LRA officer uses DESC Web RA application to fill the certificate enrollment form after validating all data required for the enrollment

e) The Web RA application communicates with the CA to issue end-user certificates and make the certificate available for download on the applicant's cryptographic token

f) The applicant changes the PIN of cryptographic token using the supplied change PIN software.

UAE PASS LRA - IDP Registered Users (for UAE Citizens and Residents)

Authentication certificate and digital signature certificate for "moderate assurance" transactions issued through the UAE PASS enrolment application:

a) The applicant is expected to have an existing account and authentication credentials from accepted Identity Providers (IDP) in the UAE. Approved IDPs are Dubai ID (SDG) and Smart PASS (TRA).

b) The credentials from the existing Identity Provider are used by the applicant to authenticate to the UAE PASS enrolment application (2-factor authentication) and also static password and OTP are used during this process.

c) After a successful authentication to the UAE PASS enrolment application, the UAE PASS retrieves the applicant's identity data from the Identity Provider and uses this data to enroll the applicant into the UAE PASS system. The applicant is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.

d) The UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the applicant's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA.

e) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

f) The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account.

g) The applicant then triggers the signature key pair and certificate generation process with the UAE PASS. The UAE PASS securely generates the user's Signing key pair on an HSM and automatically submits Signing certificate request to DESC service for the Corporate CA .

h) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

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

UAE PASS LRA - New Users via KIOSK (for UAE Citizens and Residents)

- Authentication certificate and digital signature certificate for "moderate assurance" transactions through the UAE PASS kiosk application:

  a) The applicant attends to a UAE PASS kiosk.

  b) The applicant's identity verification is performed using biometric (fingerprint) verification against the fingerprints enrolled with the applicant's Emirates ID card.

  c) After successful biometric verification, the UAE PASS kiosk application retrieves the applicant's identity data from the Emirates ID card then use this data to enroll the applicant into the UAE PASS system. As part of this process the applicant is provided with a unique secret (i.e. QR code) to be used for the UAE PASS mobile app. He is also provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.

  d) The applicant uses the unique secret code to access the UAE PASS mobile app. The UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the applicant's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA.

  e) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

  f) The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account.

  g) The applicant then triggers the signature key pair and certificate generation process with the UAE PASS. The UAE PASS securely generates the user's Signing key pair on an HSM and automatically submits Signing certificate request to DESC service for the Corporate CA.

  h) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

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

- Digital signature certificate for "high assurance" transactions through the UAE PASS kiosk application:

  a) The applicant shall already be enrolled into the UAE PASS system with authentication and signing certificate (for "moderate assurance" transactions) already generated.

  b) The user attends to a UAE PASS kiosk. His identity is verified using biometric (fingerprint) verification. After successful biometric verification, the user is logged onto his UAE PASS account.

  c) The user is given the option by the UAE PASS to apply for a signing certificate for "high assurance" transactions. He is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application.

d) The UAE PASS generates the signature key pair on an HSM and creates a certificate request that is submitted to DESC service for the Corporate CA.

e) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS.

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

UAE PASS LRA - New Users via Manual Registration (for UAE Citizens and Residents)

Authentication certificate and digital signature certificates for "high assurance" transactions through the UAE PASS manual registration:

a) The applicant attends to a UAE PASS Registration Authority Officer,

b) The applicant fills and signs registration form and signs Certificate Issuance Terms and Conditions,

c) RA officer collects a copy of applicant's Emirates ID and validates applicant's picture and information on the Emirates ID with information on the registration form,

d) RA officer keeps original copy of the registration form and Terms and Conditions,

e) RA Officer prepares a PDF file that contains Subscriber scanned copy of Emirates ID, signed Subscriber registration form, and signed Terms and Conditions,

f) RA Officer Digitally signs the PDF using his digital signature certificate (issued by DESC) through UAE PASS Application,

g) RA Officer submits the signed pdf to the UAE PASS business team for validation by email,

h) Business team validates the identity of user by checking provided information against ICA through ICA webservices,

i) If there is a match, the business team proceed with below, if no match then business team submits rejection email and process terminates at this step,

j) Business team takes/prints a screen shot of ICA response,

k) Business officer fills approval form,

l) Business officer prepares a pdf of ICA response and approval form,

m) Business officer signs the PDF using his digital signature certificate (issued by DESC) through UAE PASS Application,

n) Business officer sends approval (signed pdf) to the RA officer through email with link to complete the registration process,

o) At this stage, UAE PASS application will inform the applicant to recover UAE PASS account,

p) If applicant agrees, the UAE PASS securely generates the applicant's Authentication key pair through the UAE PASS Mobile App running on the Subscriber's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA,

q) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS,

r) The UAE PASS validates the received certificate then deploys it on the applicant's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account,

s) The RA officer in the presence of the applicant, clicks on the link provided by the business team,

t) The applicant is sent an authorization request to initiate certificate issuance,

u) The applicant approves request through his UAE PASS App,

v) The applicant will be asked to set a signing password through the UAE PASS App,

w) This triggers the signature key pair and certificate generation process for "moderate assurance" and "high assurance" with the UAE PASS. The UAE PASS securely generates the user's Signing key pairs for both certificates on an HSM and automatically submits Signing certificate requests to DESC service for the Corporate CA,

x) The CA validates the certificate requests, issues the certificates and sends the certificates back automatically to the UAE PASS,

y) The UAE PASS validates the received certificates then stores it along with the applicant's account,

z) The RA officer documents the serial numbers of issued certificates in the related section of Registration Form.

UAE PASS LRA - New Users via Digital Onboarding (for UAE Citizens, Residents and Visitors)

Authentication certificate and digital signature certificate for "moderate assurance" transactions in addition to Mobile authentication certificate through the UAE PASS (Digital Onboarding Application):

a) The applicant presents his/her identification documents (Emirates ID for UAE Citizens/Residents, and Passport & Visa page or UAE Visitors) to be scanned by UAE PASS mobile app for the UAE PASS to validate the identity status with ICA,

b) The applicant then provides his/her personal email, mobile and confirms the OTP on both to prove the control on email and mobile provided,

c) The applicant performs a liveness test in UAE PASS mobile app and on successful verification the live photo (taken by UAE PASS mobile app) is submitted to UAE PASS,

d) UAE PASS uses MOI service for the face recognition from the picture obtained in previous step after liveness verification,

e) MOI identity verification is performed on UAE PASS submitted biometric and identity details using biometric verification against the federal government authorized Facial templates database After successful face verification, UAE PASS application uses the applicant's identity data to enroll the applicant into the UAE PASS system. The applicant is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application,

f) The UAE PASS securely generates the user's Authentication key pair through the UAE PASS Mobile App running on the applicant's mobile and generate certificate request that is automatically sent to DESC service for Corporate CA,

g) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS,

h) The UAE PASS validates the received certificate then deploys it on the user's mobile device through the Mobile App. The UAE PASS also stores the authentication certificate along with the applicant's account,

i) The applicant then triggers the signature key pair and certificate generation process with the UAE PASS. The UAE PASS securely generates the user's Signing key pair on an HSM and automatically submits Signing certificate request to DESC service for the Corporate CA,

j) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS,

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

UAE PASS LRA – Existing Users via Digital Onboarding (for UAE Citizens, Residents and Visitors)

Digital signature certificate for "high assurance" transactions through the UAE PASS (Digital Onboarding Application. The applicant shall already be enrolled into the UAE PASS system with authentication and signing certificate (for "moderate assurance" transactions) already generated.

a) The applicant performs a liveness test in UAE PASS mobile app and on successful verification the live photo (taken by UAE PASS mobile app) is submitted to UAE PASS,

b) UAE PASS uses MOI service for the face recognition from the picture obtained in previous step after liveness verification,

c) MOI identity verification is performed on UAE PASS submitted biometric and identity details using biometric verification against the federal government authorized Facial templates database,

d) If Identity is verified, the user is given the option by the UAE PASS to apply for a signing certificate for "high assurance" transactions. He is provided with the option to accept subscriber agreement terms displayed to him by the UAE PASS application,

e) The UAE PASS generates the signature key pair on an HSM and creates a certificate request that is submitted to DESC service for the Corporate CA,

f) The CA validates the certificate request, issues the certificate and sends the certificate back automatically to the UAE PASS,

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

For certificates issued to the OCSP responder and the signature verification service

The certification process is initiated by an authorized 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, in addition to the backlist check that done by the RA/LRA according to its own internal blacklist. If the requestor/entity is in the blacklist, the certificate application is rejected.

All the activities comprising the certificate application processing (email communication, phone calls, vetting evidence) are stored along with the certificate application.

4.2.2 Approval or rejection of certificate applications

The certificate application based on the results of the identification and authentication specified in section 4.1.

For OCSP and signature verification service certificates: A certificate application is approved/rejected as part of the overall approval/rejection of the corresponding certification process.

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

4.2.3 Time to process certificate applications

No stipulation – this section is intentionally left blank.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

- **For certificates issued to Government entities through DESC RA (including LRA certificates):** Following the approval of the certificate application by the DESC RA, the CSR file is

uploaded and submitted to this CA by the DESC RA officer using a dedicated application. The CA then signs the certificate in accordance with the specified certificate template. The certificate is activated by the CA and is ready for usage. The certificate is then downloaded by DESC RA officer sent to the certificate requester email address.

- **For certificates issued to natural persons through the Government entity LRA (including DESC RA):** Following the approval of the certificate application by DESC RA / the government entity LRA, the certificate request is submitted to this CA by the RA/LRA officer using a dedicated application. The CA validates the format of the request then creates the certificate in accordance with the specified certificate template and is made available to the RA/LRA application. The certificate is activated by the CA and is ready for usage. The RA/LRA officer completes the process by installing the certificate on the target cryptographic device.
- **For certificates issued to natural persons through the UAE PASS:** The CA receives the certificate request from the UAE PASS system. The CA validates the format of the request then creates the certificate in accordance with the specified certificate template and automatically returns the certificate to the UAE PASS system. The certificate is activated by the CA and is ready for usage.
- **For OCSP and the signature verification service certificates:** An authorized administrator manually delivers the CSR file including the servers' public key to DESC RA team. DESC RA team submit the CSR file directly to the CA that will issue the certificate and makes it available to be downloaded by the PKI administrator who will then hand it over to the authrotized administrator.

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

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

When applicants (or the UAE PASS team in case of eSeal certificates) receive the certificate, they validate the certificate content against the request made earlier. In case of any discrepancies noted by the requester, he/she initiates a communication with the relevant RA\LRA, that may lead to initiation of the certificate revocation request by the applicant.

If no complaints were raised by the applicant within 10 business days from receiving the certificate, the certificate is deemed accepted by the applicant.

For OCSP and signature verification service certificates: A certificate is deployed on the target system as part of the overall DESC internal operational ceremony.

4.4.2 Publication of the certificate by the CA

The Corporate CA and OCSP certificates shall be published on the dissemination page as described in section 2.2. The Corporate CA does not publish other end-user certificates apart from sharing it with the requester.

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:

- Comply with the terms of the Subscriber agreement,
- Use certificates exclusively for legal activities consistent with the CP and this CPS,
- Protect the private key (and related secrets) from compromise, loss, disclosure, or otherwise from unauthorized use,
- Discontinue the use of a private key following expiration or revocation of the corresponding certificate unless a subsequent unexpired or unrevoked certificate corresponding to that private key has been issued,
- Notify the RA/LRA immediately if any details in the certificate become invalid, or as a result of any compromise, loss, disclosure, or otherwise unauthorized use of their private keys,
- Avoid using the private key until after the CA has issued, and the Subscriber has accepted the corresponding certificate.

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.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

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 original certificate may be revoked after re-key is complete, however, the original certificate must not be further re-keyed.

4.7.2 Who may request certification of a new public key

As per initial certificate issuance.

4.7.3 Processing Certificate Re-keying requests

As per initial certificate issuance.

4.7.4 Notification of new certificate issuance to subscriber

As per initial certificate issuance.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As per initial certificate issuance.

4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certificate issuance.

4.7.7 Notification of certificate issuance by the CA to other entities

As per initial certificate issuance.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

This CPS does not provide provisions for certificate modification. If the Subscriber wants to change the information stored in the certificate or has requested revocation of his/her existing certificate and wishes to be issued a new certificate with modified information, the Subscriber shall submit a new certificate application.

4.8.2 Who may request certificate modification

Not applicable. Refer to section 4.8.1.

4.8.3 Processing certificate modification requests

Not applicable. Refer to section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

As per initial certificate issuance.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable. Refer to section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

As per initial certificate issuance.

4.8.7 Notification of certificate issuance by the CA to other entities

As per initial certificate issuance.

4.9 Certificate revocation and suspension

Suspension of a certificate is not allowed by this CA. Only permanent certificate revocation is allowed.

4.9.1 Circumstances for revocation

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

1. Received a written request from the Subscriber or an authorized representative;
2. The Subscriber discovers that the original certificate request was not authorized and does not retroactively grant authorization; or
3. The RA/LRA/CA discover or has reasons to believe that there has been a compromise of the private signing key,
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or
5. The information on the certificate is no longer accurate.

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

1. DESC obtains evidence that the certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
2. DESC obtains evidence that the Certificate was misused,
3. DESC is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use,
4. DESC is made aware of a material change in the information contained in the Certificate,
5. DESC is made aware that the Certificate was not issued in accordance with DESC CP/CPS,
6. Finding that the certificate was issued without the authorization of the individual named as the subject of such certificate,
7. DESC determines or made aware that any of the information appearing in the Certificate is inaccurate or misleading,
8. Revocation is required by DESC's CP and/or CPS,
9. The Government entity or the individual has been declared legally incompetent,
10. DESC is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed,
11. The Corporate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate, or

12. The Corporate CA's right to issue Certificates under the requirements defined in this CPS expires or is revoked or terminated, unless the Corporate CA has made arrangements to continue maintaining the CRL/OCSP Repository.

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

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

On the other hand, this CPS does not provide provisions for revoking an OCSP/signature verification service certificate apart from the compromise of the OCSP/ signature verification service key pair that is treated by DESC as per its Disaster Recovery and Business Continuity procedures.

The following sub-sections focus only on the revocation provisions that apply for the certificates issued by this CA.

4.9.2 Who can request revocation

- The individual to whom certificates were issued.
- The Government entity to whom certificates were issued.
- Any relying party possessing evidence of compromise of the subscriber's certificate .
- Revocations are directly initiated by DESC's RA officers in the cases described in section 4.9.1.
- For certificates issued through DESC RA (for DESC employees) or the LRA of the Government entity, the RA/LRA shall revoke digital certificates corresponding to its community when required by the entity's internal processes.
- The UAE PASS shall revoke digital certificates corresponding to its community when required by its relevant account management processes.
- DESC at its own discretion (if for instance a compromise is known for this CA key).

4.9.3 Procedure for revocation request

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

- **Revocation of certificates through DESC RA:**
    - The subscriber or an authorized representative can request the revocation of their certificate(s) to the DESC RA.
    - The DESC RA officer authenticates the subscriber's identity as described in section 3.4.
    - The DESC RA officer requests the subscriber to fill in and sign a revocation request form.
    - The DESC RA officer revokes the subscriber's certificate(s).
    - The CA generates an updated CRL and publishes it to the DESC public repository.
- **Revocation of certificates through Government LRA (including DESC RA):**
    - The RA/LRA receives a formal revocation request from the subscriber.
    - The RA/LRA validates the identity of the subscriber as done during initial certificate application.
    - The RA/LRA records the revocation request according to the Government entities' business rules.
    - The RA/LRA officer revokes the subscriber's certificates.
    - The CA generates an updated CRL and publishes it to the DESC public repository.

- **Revocation of certificates through UAE PASS:**
    - Revocation is requested as part of an account management process such as deletion or termination of UAE PASS Account. Certificates are revoked when user requests to renew certificate keys (through Kiosk), or call UAE PASS call center,
    - The UAE PASS validates the subscriber's identity using identification questions in addition to challenge-response authentication through the email or mobile number registered along with the account.
    - The UAE PASS records the revocation request according to its business rules.
    - The UAE PASS sends an automatic revocation request to the CA through the CA gateway service.
    - The CA revokes the certificate then generates an updated CRL and publishes it to the DESC public repository.
- **Revocation of OCSP and signature verification service certificates:**
    - The revocation is conducted as part of a PKI process internal to DESC and is approved by the Dubai PKI PA. For OCSP, the process will also involve communication with relying parties in order to update them with the OCSP certificate revocation.

Certificate Problem Report:

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

4.9.4 Revocation request grace period

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

4.9.5 Revocation request response time

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

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

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

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

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

4.9.6 Revocation checking requirement for relying parties

The Corporate CA provides revocation information to relying parties through CRLs published on a publicly available web server and through its publicly available OCSP responder.

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

4.9.7 CRL issuance frequency

CRLs are issued as per section 2.3.

4.9.8 Maximum latency for CRLs

The Corporate CA issues CRLs as per the CRL issuance frequency listed in section 2.3.

4.9.9 Online revocation/status checking availability

OCSP is supported within this PKI solution and is compliant with RFC 6960. OCSP information is available immediately to relying party applications based on the updates done by the CA on the certificates' status.

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

4.9.10 Online revocation checking requirements

The Corporate CA OCSP responder supports both HTTP GET and HTTP POST methods.

The Corporate CA OCSP responder's responses define value in the nextUpdate field which is not more than 8 hours after the thisUpdate field.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused" (i.e. not issued by) the Corporate CA, then the OCSP responder responds with a "revoked" status as defined by RFC 6960.

4.9.11 Other forms of revocation advertisements available

The Corporate CA only uses OCSP and CRL as methods for publishing certificate revocation information.

4.9.12 Special requirements – Key compromise

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

Parties may use the following methods to demonstrate key Compromise:

- Submission of a signed CSR, Private Key or other challenge response signed by the Private Key and verifiable by the Public Key, or
- The private key itself

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.

4.9.16 Limits on Suspension Period

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 through HTTP interface (an HTTP URL of the CRL distribution point is included in the certificate's CDP extension).

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

- it supports real-time revocation status i.e. for every revocation performed by this CA, revocation information is available to the OCSP service immediately,
- responses define value in the nextUpdate field which is not more than 8 hours after the thisUpdate field,
- the value in the nextUpdate field always before or equal to the notAfter date of all certificates included within the BasicOCSPResponse.certs field, or if the certs field is omitted, before or equal to the notAfter date of the CA certificate which issued the certificate that the BasicOCSPResponse is for.

4.10.2 Service availability

The repository including the latest CRL should be available 24X7 at least 99% per year.

The CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA maintains a 24X7 ability to respond internally to high-priority certificate problem report as described in section 4.9.3 of this CPS.

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.

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by this CA.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management and Operational Controls

5.1 Physical controls

5.1.1 Site location and construction

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

5.1.2 Physical access

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

The Dubai PKI systems are protected by six tiers of physical security, with access to the lower tier required before gaining access to the higher most restrictive tier. Sensitive CA operational activities related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is enforced through the use of two factor biometric authentication. Further, access to the enclave where the Dubai PKI systems are hosted is enabled only if two trusted employees are present to open the enclave's door.

Unauthorized personnel, including un-trusted or third-party employees or visitors, are not allowed into such secured areas without a prior approval and without an escort from one of trusted employees. Similar restrictions exist for the Disaster Recovery site.

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

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 data centers hosting the PKI systems are implementing reasonable precautions to minimize impact of water exposure. These include installing the PKI equipment on elevated floors with moisture detectors.

5.1.5 Fire prevention and protection

The secure enclave must is protected from fire, heat with a smoke detection equipment monitored on a 24*7*365. Fire suppression equipment are 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

Backups taken from the Dubai PKI systems provide sufficient recovery information to allow the recovery from system failure(s). Backups are made on a daily basis and copies are transferred to a secure offsite location on regular basis.

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

5.2 Procedural controls

DESC follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

DESC obtains a signed statement from each member of the staff concerned on not having conflicting interests with the Corporate CA activities, maintaining confidentiality and protecting personal data.

5.2.1 Trusted roles

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

- PKI Director
- PKI Deputy Director
- PKI Operation Manager
- Key Custodians
- Chief Information Security Officer (CISO)
- Registration Authority (RA) officer
- PKI operations manager
- PKI administrator

- System administrator
- PKI operator
- System administrator

DESC conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to ensure their trustworthiness and competence. Trusted roles individuals must go through an annual background checks.

5.2.2 Number of persons required per task

DESC maintains and enforces rigorous control procedures to ensure the segregation of duties, based on job responsibility, in order to prevent single trusted personnel to perform sensitive operations.

The most sensitive tasks such as the following require the involvement of two or more persons:

- physical access to the secure enclave where the CA systems are hosted,
- access to and management of CA cryptographic hardware security module (HSM),
- validate and authorize the issuance of end-entity certificates. This is enforced during the certificate application processing where an RA officer review and verify all the Applicant information and a second RA officer reviews and finally cross sign the application to get it approved.

All operational activities performed by the personnel having trusted roles are logged and maintained in a verifiable and secure audit trail.

5.2.3 Identification and authentication for each role

Before carrying out the responsibilities of a trusted role:

- DESC confirms the identity of the employee by carrying out background checks,
- DESC issues access credentials to the individual who needs to access equipment located in the secure enclave,
- DESC provides the required dedicated credentials that allow designated individuals to conduct their functions.

5.2.4 Roles requiring separation of duties

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

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

5.3 Personnel controls

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

5.3.1 Qualifications, experience and clearance requirements

Prior to the commencement of employment of a DESC PKI personnel, whether as an employee, agent, or an independent contractor, 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 checks include:

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:
    - The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
    - The verification of well-recognized forms of government-issued photo identification (e.g., Emirates ID); and
2. Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:
    A. Criminal convictions for serious crimes,
    B. Misrepresentations by the candidate,
    C. Appropriateness of references,
    D. Any clearances as deemed appropriate.

5.3.2 Background check procedures

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

5.3.3 Training requirements

DESC makes available relevant technical training for their personnel to perform their functions.

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

The required skills and knowledge for validation specialists are tested through an examination on the information verification requirements outlined in this CPS.

5.3.4 Retraining frequency and requirements

The training content is reviewed and amended on a yearly basis to reflect latest leading practices, CA configuration changes and relevant updates on applicable requirements.

5.3.5 Job rotation frequency and sequence

The Dubai PKI PA ensures that any change or rotation in staff shall not affect the operational effectiveness, continuity and integrity of the Corporate CA services.

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 the applicable Dubai Law.

5.3.7 Independent contractor requirements

Independent subcontractors and their personnel are subject to the same background checks as DESC employees. The background checks include:

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of event recorded

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

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

DESC ensures that at least the following details are recorded:

- CA key lifecycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction,
    - Cryptographic device lifecycle management events.
- CA and subscriber certificate lifecycle management events, including:
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles,
    - 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 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,
- System configuration changes and maintenance, as defined in the CPS,
- CA personnel changes,
- Discrepancy and compromise reports,
- Information concerning the destruction of sensitive information,
- Current and past versions of all Certificate Policies,
- Current and past versions of Certification Practice Statements,
- Vulnerability Assessment Reports,
- Threat and Risk Assessment Reports,
- Compliance Inspection Reports,
- Current and past versions of Agreements,
- Other documents that are required for audits include:
    - Infrastructure plans and descriptions,
    - Physical site plans and descriptions,
    - Configuration of hardware and software,
    - Personnel access control lists.

5.4.2 Frequency of processing log

DESC ensures that designated personnel reviews log files at regular intervals in order to validate log integrity and ensure timely identification of anomalous events.

Designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity as per the following audit log review cycle:

- On a monthly basis, the PKI operations management reviews the CA applications and security logs to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly

- On a quarterly basis, the PKI operation management reviews the physical access logs and the user management on the CA systems with an objective to continuously validate the ongoing physical and logical access policies
- Evidence of audit log reviews, outcome of the review process, and executed remediation actions are collected and archived for inspection by authorized DESC personnel.

5.4.3 Retention period for audit log

The audit logs are retained for at least two years:

- CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) after the later occurrence of:
    - destruction of the CA Private Key; or
    - revocation or expiration of the CA certificate.
- Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the revocation or expiration of the Subscriber Certificate;
- Any security event records (as set forth in Section 5.4.1) after the event occurred.

These may be made available to auditors upon request.

5.4.4 Protection of audit log

Audit logs shall be protected by a combination of physical and procedural security controls, this includes:

- The CA generates a message authentication code for each audit log file it keeps,
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived,
- Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective trusted operative personnel.

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)

Automatic audit processes are initiated at system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, DESC determines whether to suspend the CA's or RA's operations until the problem is fixed.

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

DESC conducts an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes, and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DESC has in place to counter such threats.

DESC also performs regular vulnerability assessment and penetration testing covering the Dubai PKI systems. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the certificate issuance process. Evidence of the vulnerability assessment and penetration testing activities' execution are collected and archived by the Dubai PKI PA Information Security function.

5.5 Records archival

5.5.1 Types of records archived

DESC archives the audit logs set forth in Section 5.4.1, in addition to the following:

1. Documentation related to the security of their Certificate Systems, Certificate Management Systems, and Root CA Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention period for archive

DESC retains audit logs (as set forth in Section 5.4.1) and records (as set forth in Section 5.5.1) for 7 years after any certificate based on that documentation/logs ceases to be valid.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

The PKI operations team use backup, restore and archive procedures that document how the archive information is created, transmitted and stored.

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

To minimize impact of key compromise, Corporate CA private key is periodically changed over as specified in section 6.3.2.

To support revocation management of issued certificate, the old 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

If DESC detects a potential hacking attempt or other form of compromise to the CA, it shall perform an investigation to determine the nature and the degree of damage. If the CA Private key is suspected of compromise, the procedures outlined in DESC's Business continuity and disaster recovery plan shall be followed. Otherwise, the scope of potential damage shall be assessed to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised. DESC also specifies applicable compromise reporting and relevant communications as part of the Business continuity and disaster recovery plan.

Apart from the circumstance of key compromise, 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 the Corporate CA services in case of a disaster, corrupted servers, software or data.

DESC establishes:

- Disaster recovery resources in a location sufficiently distant from the regular 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 subscriber's key compromise, see section 4.9 of the present CPS.

In the event of a key compromise of the Corporate CA, or of the associated activation data, DESC triggers the Key compromise and CA termination plans detailed as part of DESC Business continuity and disaster recovery plan.

As part of the Key compromise and CA termination plan, the Dubai PKI PA will be invited for an emergency meeting to take decisions and handle communications as required with law enforcement authorities and other relevant stakeholders such as Root Programs and Relying Parties.

5.7.4 Business continuity capabilities after a disaster

DESC establishes the necessary measures to full and automatic recovery of the online services such as the OCSP and the public repository hosting CRLs in case of a disaster, in addition to 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.

Failover scenarios to the Corporate CA disaster recovery location are made possible considering the Corporate CA backup system that enables the continuous replication of critical Corporate CA data from the primary site to the disaster recovery site.

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 of this CA services are deemed necessary, the CA termination plan shall be executed and it shall cover the following actions:

1. Minimize disruption caused by the termination of an Issuing CA is minimized as much as possible,

2. ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings. The retention of archived data specified in Section 5.5,
3. ensure Certificate status information services are maintained for the applicable period,
4. terminate all authorization of sub-contractors to act on behalf of the terminated service (Corporate CA and RA/LRAs) in the performance of any functions related to the process of issuing certificates,
5. notify subscribers, relying parties and other stakeholders (e.g. auditors and root programs). Notification procedures shall exist for informing affected entities and transferring archived CA records to an appropriate custodian.

6. Technical Security Controls

6.1 Key pair generation

The requirements for key generation and delivery are stated in the following sections.

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

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

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

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

- The key generation ceremony is subject to the formal authorization of the Dubai PKI PA,
- The key generation ceremony is conducted in presence of a combination of authorized personnel with trusted roles including the Dubai PKI PA representatives,
- The Corporate CA Key Generation Ceremony is witnessed by DESC internal auditor,
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians,
- DESC internal auditor issues a report, covering that the Corporate CA, during its Key Pair and Certificate generation process:
    - Documented its Corporate CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement,
    - Included appropriate detail in its Corporate CA Key Generation Script,
    - Maintained effective controls to provide reasonable assurance that the Corporate CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Corporate CA Key Generation Script,
    - Performed, during the Corporate CA key generation process, all the procedures required by its Corporate CA Key Generation Script,
- A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes.

6.1.1.2 Subscriber key pair generation

The Corporate CA does not perform subscriber key generation.

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

Certificate type	Key generation requirements
Encryption certificates	Key pair is generated using a [FIPS 186-4] or [ETSI TS 119 312] approved methods for key generation
Digital signature certificates	Key pair is generated on a hardware based cryptographic modules using a [FIPS 186-4] or [ETSI TS 119 312] approved methods for key generation
Authentication certificates	Key pair is generated using a [FIPS 186-4] or [ETSI TS 119 312] approved methods for key generation
Signature Verification Service certificates	Key generation is done using a dedicated verification services key management utility. The verification services key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module
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. The Corporate CA does not perform Subscriber key generation.

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

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

6.1.5 Key sizes

This Corporate CA key pair is 4096-bit RSA.

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

6.1.6 Public key parameters generation and quality checking

The Corporate CA relies on off-the-shelf implementation of key PKI functionality including public key parameters generations. The Corporate CA HSMs and associated software meet FIPS 186-2 requirements for random generation and primality checks.

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

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

6.1.7.1 Corporate CA

Corporate CA key usage.

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

6.1.7.2 Certificates for individuals

Certificates issued to subscribers contain a key usage extension depending on their intended usage in accordance with RFC 5280. Refer to section 7.1 and 7.3 of this CPS.

6.1.7.3 Certificates for government entities

Subscriber's key usage.

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

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

DESC generates the CAs' key pairs and store their private keys within a Cryptographic Device that is certified according to the rating specified in 6.2.11.

The Cryptographic modules used for Subscribers' key generation and storage are at least compliant to FIPS 140-2 Level 2.

6.2.2 Private key (n out of m) multi-person control

DESC implements technical and procedural mechanisms that implement the principles of dual control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with the CA cryptographic hardware.

DESC keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it keeps track of the renewed tokens and/or password distribution.

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. Backup operations are executed as part of the Corporate CA key generation ceremonies. The Corporate CA key is backed up under the same dual control and split knowledge as the primary key.

The Corporate CA key backup is physically transported from the primary site to the DR site as part of the overall Corporate CA key ceremony procedure.

Trusted operatives or key custodians participate in the transport operation, which is escorted by an auditor. The backup is 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 Cryptographic Module

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

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

CA Key backups are generated with the enforcement of dual control and split knowledge mechanisms. The transfer of the CA Key backups to the DR site is subject to the same dual control and split knowledge principles.

6.2.7 Private key storage on cryptographic module

No further stipulation other than those stated in sections 6.2.1, 6.2.2, 6.2.4 and 6.2.6.

6.2.8 Method of activating private key

6.2.8.1 CA keys

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.

6.2.8.2 Subscribers keys

Subscribers are responsible for activating and protecting their private key according to the obligations articulated in the Subscriber Agreement.

6.2.9 Method of deactivating private key

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

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

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

6.2.10 Method of destroying private key

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

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

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

6.2.11 Cryptographic module rating

6.2.11.1 Corporate CA

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

6.2.11.2 Subscribers

The Cryptographic modules used for Subscribers' key generation and storage are at least compliant to FIPS 140-2 Level 2.

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 five years i.e., 60 months

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1.1 Corporate CA

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

During the key generation ceremony of the Corporate CA, trusted individuals (key custodians) are instructed to use strong passwords and PINs. A password policy, that meet the requirements specified by the CAB Forums Network Security Requirements, is distributed to the trusted roles as part of the key ceremony documentation.

6.4.1.2 Subscribers keys

Subscribers shall set and protect the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure and use of these private keys. Such obligation is articulated as part of the Subscriber Agreement.

6.4.2 Activation data protection

6.4.2.1 Corporate CA

The Corporate CA activation data consists of PINs, passwords and accounts that are used to activate the HSMs hosting the CA keys. Activation data is protected by same security controls used for the CA private key protection. A combination of physical security, technical and procedural controls ensure that the CA private keys and activation data is always protected. Refer to section 6.2 of this CPS for further details.

6.4.2.2 Subscribers

Refer to section 6.4.1.2 of this CPS.

6.4.3 Other aspects of activation data

No stipulation – this section intentionally left blank.

6.5 Computer security controls

The Corporate CA performs all CA and RA functions using trustworthy systems that meet DESC security in addition to the present requirements.

6.5.1 Specific computer security technical requirements

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

- Physical access control to CA servers shall be enforced,
- Separation of duties and dual controls for CA sensitive operations,
- Identification and authentication of PKI roles and their associated identities,
- Archival of CA history and audit data,
- Audit of security-related events,
- Automatic and regular validation of CA systems integrity,
- Recovery mechanisms for keys and CA systems,
- Hardening CA servers operating system according to best practices and PKI vendor requirements,
- Network protection, including intrusion detection systems,
- Proactive patch management for the CA systems,
- Multi-factor authentication for all accounts capable of directly causing certificate issuance.

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

Purchased hardware or software shall be shipped or delivered in a sealed, tamper-proof container and be installed by trained and trusted personnel. Hardware and software updates shall be handled in the same manner as the original equipment.

The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operations.

The CA hardware or software shall be tested, deployed and configured in accordance with industry best practices and vendor recommendations. All changes are controlled through the Dubai PKI change management processes.

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.

A change management process is enforced to ensure that the CA systems configuration, modification and upgrades are documented and controlled by the PKI operations management.

A vulnerability management process is enforced to ensure that the CA systems are scanned for malicious code on first use and periodically thereafter. The vulnerability management process supports the processing within 96 hours of discovery of critical vulnerabilities not previously met by the PKI operations team.

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 a highly secure network zone .

6.8 Time stamping

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

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

7.1.1 Version number

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

7.1.2 Certificate extensions

X.509 v3 extensions are supported as specified in sections 7.1.10 and 7.1.12 of this CPS for.

7.1.3 Algorithm object identifiers

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

7.1.4 Name forms

As per the naming conventions and constraints listed in Section 3.1.1 of this CPS, that is followed while defining the certificate profiles in sections 7.1.10 and 7.1.12 of this CPS.

The certificate subject attributes shall not contain values as meta data of period, hyphen, empty space, etc (Eg: '.' OR '-' OR ' ') indicating the attribute as blank or not applicable.

7.1.5 Name constraints

Name constraints extension is not supported.

7.1.6 Certificate policy object identifier

The Corporate CA uses certificate policy object identifiers that are defined as part of OID scheme for the Dubai PKI. Refer to sections 7.1.10 and 7.1.12 of this CPS for the profiles of the certificates issued by the Corporate CA including the values of the OID identifiers.

7.1.7 Usage of policy constraints extension

Policy constraints extension is not supported.

7.1.8 Policy qualifiers syntax and semantics

The use of policy qualifiers as per the RFC 5280 is supported. Refer to sections 7.1.10 and 7.1.12 of this CPS for the profiles of the certificates issued by the Corporate CA including the used policy qualifiers.

7.1.9 Processing semantics for critical certificate extensions

Processing of certificate policies extensions shall conform with the RFC 5280.

7.1.10 Certificates for natural persons

7.1.1.1 Subscriber's encryption certificate ASN1 description

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

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

CE = Critical Extension.
O/M: O = Optional, M = Mandatory.
CO = Content: S = Static, D = Dynamic

						alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	<optional organizational unit name> as agreed during onboarding process	UTF8 encoded
	organizationName		M	D	<Government entity meaningful name> or as agreed during onboarding process	UTF8 encoded
	localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user name>	UTF8 encoded
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
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	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	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						

keyUsage		True	M			
	keyEncipherment		M	S	True	
	dataEncipherement		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	

7.1.1.2 Subscriber's signing certificate ASN1 description

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

Field		CE[4]	O/M[5]	CO[6]	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	(2) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer		False	M			
	countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationName		M	S	UAE Government	UTF8 encoded
	commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[60]** Months	

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

subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	<optional organizational unit name> or as agreed during onboarding process	UTF8 encoded
	organizationName		M	D	<Government entity meaningful name> or as agreed during onboarding process	UTF8 encoded
	localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user name>	UTF8 encoded
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	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	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-calssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA certificate download URL
cRLDistributionPoints		False	O			

	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
keyUsage		True	M			
	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	<For Citizens/Resident certificates issued for high assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.3> <For Visitors certificates issued for high assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.7> <For Citizens/Resident certificates issued for moderate assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.4> <For Visitors certificates issued for moderate assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.8>	

7.1.1.3 Subscriber's authentication certificate ASN1 description (Deprecated)

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

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

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

	localityName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	Allocated during LRA onboarding process	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Individual end user's name>	UTF8 encoded
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-calssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA Certificate download URL.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
subjectAltName		Falise	O			
	GeneralName			D	RFC822 Name	Email address
Key Usage Properties						
keyUsage		True	M			

	digitalSignature		M	S	True	
	keyEncipherment		M	S	True	Not to be included for ECDSA keys
	dataEncipherement		M	S	True	Not to be included for ECDSA keys
Extended Key Usage Properties						
extKeyUsage		False	M			
	clientAuth		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	

7.1.1.4 Subscriber's mobile authentication certificate ASN1 description

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

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

10 CE = Critical Extension.

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

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

	AccessMethod		M	S	Id-ad-2 2 *id-ad-calssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA Certificate download URL.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
keyUsage		True	M			
	digitalSignature		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	<For Citizens/Resident certificates issued for moderate assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.5> <For Visitors certificates issued for moderate assurance transactions, the OID value will be 2.16.784.1.2.2.100.1.2.2.1.9>	

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

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

Field	CE[13]	O/M[14]	CO[15]	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

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

SerialNumber		False				
	CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature		False	M			
	algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer		False	M			
	countryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationName		M	S	UAE Government	UTF8 encoded
	commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[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	<optional organizational unit name> or as agreed during onboarding process	UTF8 encoded
	organizationName		M	D	<Entity meaningful name> or as agreed during onboarding process	UTF8 encoded
	localityName		M/O	D	User’s locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	commonName		M	D	<Individual end user’s name>	UTF8 encoded
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for

					self-signed certificates
keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess	False	M			
AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	S	Id-ad-2 2 *id-ad-calssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA Certificate download URL.
cRLDistributionPoints	False	O			
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
keyEncipherment		M	S	True	Not to be included for ECDSA keys
Extended Key Usage Properties					
extKeyUsage	False	M			
clientAuth		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	2.16.784.1.2.2.100.1.2.2.1.6	

7.1.11 Certificates for Government entities

7.1.11.1 Subscriber's signing certificate (eSeal) ASN1 description

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

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

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

	localityName		M/O	D	<Government entity locality>	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	<Government entity State or Province>	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
	commonName		M	D	<Government Entity Service Name as agreed during subscriber registration process >	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
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	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA certificate download URL
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
(6)	keyUsage	True	M			
	(7) 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	

7.1.12 Verification Response Signing Certificate ASN1 Description

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

Field	CE[19]	O/M [20]	CO [21]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2
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
TBS Certificate					
Version	False				
		M	S	2	Version 3
Serial Number	False				
certificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates
Signature	False	M			
algorithm		M	S	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”. Printable String, size 2 (rfc5280)
organizationName		M	S	UAE Government	UTF8 encoded
CommonName		M	S	Corporate Certification Authority	UTF8 encoded

[19] CE = Critical Extension.
[20] O/M: O = Optional, M = Mandatory.
[21] 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 **[36]** Months	
Subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280)
	commonName		M	S	DESC Signature Verification Service	
	organizationName		M	S	DESC	
	localityName		M	S	Dubai	
subjectPublicKeyInfo		False	M			
	Algorithm		M	S	RSA	
	subjectPublicKey		M	D	Public key length: 2048 or 4096 (RSA)	
Extensions			M			
Authority Properties						

authorityKeyIdentifier	False	O			Mandatory in all certificates except for self-signed CA certificates
keyIdentifier		M	S	SHA-1 Hash of the Corporate CA public key	When this extension is used, this field MUST be supported at minimum
cRLDistributionPoints	False	O			
distributionPoint		O	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	S	SHA-1 Hash	
Key Usage Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
nonrepudiation		M	S	True	
Certificate Policy Property					
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 Corporate CA's CPS	
certificatePolicies	False	M			
policyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.3.4	

7.1.13 LRA certificate ASN1 description

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

Field	CE[22]	O/M[23]	CO[24]	Value	Comment
Certificate		M			

[22] CE = Critical Extension.
[23] O/M: O = Optional, M = Mandatory.
[24] CO = Content: S = Static, D = Dynamic

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	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer		False	M			
	countryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationName		M	S	UAE Government	UTF8 encoded
	commonName		M	S	Corporate Certification Authority	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[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	<optional organizational unit name within the RA entity>	UTF8 encoded
	organizationName		M	D	<LRA meaningful name>	UTF8 encoded
	localityName		M/O	D	<LRA locality>	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
	stateOrProvinceName		M/O	D	<LRA State or Province>	UTF8 encoded
	commonName		M	D	<LRA Service Name as agreed during LRA onboarding process >	PrintableString encoded
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key	

					Key length: 2048 or 4096 (RSA) / 256 or 384 (ECDSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the Corporate CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	S	Id-ad-2 2 *id-ad-calssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		M	S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA Certificate download URL.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Corporate/corporate_certification_authority_uae_government_ae_crlfile<CRL Number>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
	keyEncipherment		M	S	True	Not to be included for ECDSA keys
Extended Key Usage Properties						
extKeyUsage		False	M			
	clientAuth		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	2.16.784.1.2.2.100.1.2.2.3.5	

7.2 CRL profile

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). Please refer to section 7.2.3 below for the other supported extension in the CRLs issued by the Corporate CA.

7.2.3 CRL ASN1 description

This is the complete ASN1 description of the CRL certificate.

Field	CE[25]	CO[26]	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	(8) 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 + 3 days + 2 hours	
revokedCertificates				
Certificate				

[25] CE = Critical Extension.
[26] CO = Content: S = Static, D = Dynamic

	CertificateSerial		D	Serial of the revoked certificate	
	revocationDate		D	UTC Time of revocation (Optional)	
crlExtensions					
authorityKeyIdentifier		False		This MUST be the same value as the subject Key Identifier field in the CRL Issuer's certificate. Non-critical <subject key identifier CA>	SHA-1 Hash of the Corporate CA public key
crlNumber		False			Sequential CRL number
IssuingDistributionPoint		True			Mandatory for Partitioned RLs
	DistributionPoint		D	CN=CRL<*CRL Number*> CN=Corporate Certification Authority O=UAE Government C=AE	Partitioned CRL directory address, *where <CRL Number> a dedicated sequence number that the CA uses for CRL file naming*
	DistributionPoint		*D*	*http://ca-repository.desc.gov.ae/CRL/Corporate/Corporate_certification_authority_uae_government_ae_crlfilec<CRL Number>.crl*	*CRL hosting URL, where <CRL Number> a dedicated sequence number that the CA uses for CRL file naming*
	onlyContainsCACerts		S	No	
	onlyContainsUserCerts		S	Yes	
	IndirectCRL		S	No	
expiredCertsOnCRL (2.5.29.60)		False	D	< a date-time value specifies the date on or after which revoked certificates are retained on the CRL>	
authorityInfoAccess		False	S		
	AccessMethod		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		S	http://ca-repository.desc.gov.ae/certificate/corporate.crt	Corporate CA certificate download URL

7.3 OCSP profile

7.3.1 Version number(s)

The OCSP responder issues OCSP responses of version 1.

7.3.2 OCSP extensions

No stipulation – this section intentionally left blank.

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[27]	O/M[28]	CO[29]	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	(9) 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 **[3]** 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 "C<n>"	"C<n>" is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over
	organizationName		M	S	DESC	
	localityName		M	S	Dubai	
subjectPublicKeyInfo		False	M			
	algorithm		M	S	RSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions			M			

[27] CE = Critical Extension.
[28] O/M: O = Optional, M = Mandatory.
[29] CO = Content: S = Static, D = Dynamic

Authority Properties						
authorityKeyIdentifier		False	M			
	KeyIdentifier		M	S	SHA-1 Hash of the Corporate CA public key	When this extension is used, this field MUST be supported at minimum
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
Key Usage		True	M			
	digitalSignature		M	S	True	
	nonRepudiation		M	S	True	
extKeyUsage		False	M			
	id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck		False	M	S	05 00	
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessments

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

8.2 Identity and Qualifications of the Assessor

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

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

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

8.3 Assessor’s Relationship to Assessed Party

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

8.4 Topics Covered by Assessment

The Corporate CA is audited for compliance to WebTrust Principles and Criteria for Certification Authorities.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

The results of the audit are reported to the Dubai PKI PA for analysis and resolution of findings. The results can also be made available to any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement.

The external audit reports are published through the CA repository no later than three months after the end of the audit period .

9. Other Business and Legal Matters

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

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fees

No fee will be charged for Certificate revocation or status information access.

9.1.4 Fees for Other Service

DESC may charge for other services depending on business needs and subject to the Dubai PKI PA approval.

9.1.5 Refund Policy

Charged fees cannot be refunded.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

DESC ensures that this CA is covered by existing government insurance provisions. Details of coverage are specified in the applicable agreements.

9.2.2 Other Assets

DESC maintains sufficient financial resources to maintain operations and fulfill duties of this CA.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

DESC considers the following as confidential information:

- Subscriber's personal information that are not part of certificates or CRLs issued by the Corporate CA,
- Correspondence between the subscribers and DESC RA during the certificate management processing (including the collected subscribers data),
- Contractual agreements between DESC and its suppliers,
- The Dubai PKI internal documentation (technical documentation, operational processes, ….).

9.3.2 Information not within the scope of confidential information

Any information not defined as confidential (refer to section 9.3.1) is deemed public. This includes the information published at the CA repository.

9.3.3 Responsibility to protect confidential information

DESC guarantees the protection of confidential information according to the applicable laws on privacy.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

DESC observes personal data privacy rules and confidentiality rules as described in this CPS. Refer to section 9.4.2 for the cope of private information.

Both private and non-private information can be subject to data privacy rules if the information contains personal data.

Only limited trusted personnel are permitted to access subscribed private information for the purpose of certificate lifecycle management.

DECS does not release any confidential information without the consent of the legitimate data owner or explicit authorization by a court order. When DESC releases private information, DESC ensures through reasonable means that this information is not used for any purpose apart from the requested purposes. 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 UAE applicable laws.

DESC respects 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.

All communications channels with DESC/RA/LRA shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the Corporate CA systems. This shall include:

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

9.4.2 Information treated as Private

All personal information that is not publicly available in the content of a certificate or CRL are considered as private information.

9.4.3 Information not Deemed Private

Information included in the certificate or CRL is not considered as private.

9.4.4 Responsibility to protect private information

DESC employees, suppliers and contractors handle personal information in strict confidence under DESC contractual obligations that at least as protective as the terms specified in section 9.4.1..

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the Dubai PKI CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement,
- All Application Software Suppliers with whom the Dubai PKI Root CA will enter into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier,
- and all Relying Parties who reasonably rely on a Valid Certificate.

DESC represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the Corporate CA has complied with its CPS in issuing and managing the Certificate.
The Certificate Warranties specifically include, but are not limited to, the following:

- **Authorization for Certificate:** That, at the time of issuance, the Corporate CA
  I. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject,
  II. followed the procedure when issuing the Certificate, and
  III. accurately described the procedure in this CPS.
- **Accuracy of Information:** That, at the time of issuance, the Corporate CA

I. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate,

II. followed the procedure when issuing the Certificate, and

III. accurately described the procedure in this CPS.

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the Corporate CA

  I. implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2,

  II. followed the procedure when issuing the Certificate,

  III. accurately described the procedure in this CPS.

- **Subscriber Agreement:** That, if the Corporate CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use.
- **Status:** That the Corporate CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.
- **Revocation:** That the Corporate CA will revoke the Certificate for any of the reasons specified in these Requirements.

9.6.2 RA Representations and Warranties

DESC RA warrant that it performs registration functions as per the stipulations specified in the applicable CP and this CPS.

The LRAs warrant (through signing an LRA agreement with DESC) that they perform RA functions as per the stipulations specified in this CPS.

9.6.3 Subscriber Representations and Warranties

DESC requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant makes the commitments and warranties in this section for the benefit of the Corporate CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, DESC shall obtain, for its express benefit and the Certificate Beneficiaries, either:

- The Applicant's agreement to the Subscriber Agreement with DESC, or
- The Applicant's acknowledgement of the Terms of Use.

DESC implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request.

The Subscriber Agreement or Terms of Use contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to DESC, both in the certificate request and as otherwise requested by DESC in connection with the issuance of the Certificate(s) to be supplied by the Corporate CA,

- **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token),
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy,
- **Use of Certificate:** When TLS server certificates are requested, an obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use,
- **Reporting and Revocation:** An obligation and warranty to:
    - promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
    - promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness:** An obligation to respond to DESC's instructions concerning Key Compromise or Certificate misuse within a specified time period**.**
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that DESC is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CPS.

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under the Corporate CA shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension),
- Verify the Validity by ensuring that the Certificate has not Expired,
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment,
- Ensure that the Certificate has not been revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon, and
- Determine that such Certificate provides adequate assurances for its intended use.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

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

9.8 Limitations of Liability

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

9.9 Indemnities

Not applicable.

9.10 Term and Termination

9.10.1 Term

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”).

9.10.2 Termination

Amendments to this document are applied and approved by the Dubai PKI PA and marked by an indicated new version of the document. Upon publishing on the Corporate CA repository, the newer version becomes effective. The older versions of this document are also archived on the Corporate CA repository.

9.10.3 Effect of Termination and Survival

The Dubai PKI PA will communicate the conditions and effect of this CPS termination via appropriate mechanisms.

9.11 Individual Notices and Communications with Participants

Notices related to this CPS can be addressed to the Dubai PKI PA contact address as stated in section 1.5.

9.12 Amendments

9.12.1 Procedure for Amendment

When changes are required to be done on this CPS. The Dubai PKI PA will incorporate any such change into a new version of this document and, upon approval, publish the new version. The new document will carry a new version number.

9.12.2 Notification Mechanism and Period

The Dubai PKI PA reserve the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors or minor enhancements. The decision to designate amendments as material or non-material shall be at the Dubai PKI PA sole discretion.

9.12.3 Circumstances Under Which OID Must be Changed

Major changes to this CPS that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the OID or qualifier (URL).

9.13 Dispute Resolution Procedures

Any dispute arising out of or related to the digital certificates issued by the Dubai PKI shall be first addressed to the Dubai PKI PA. If mediation is not successful, then the dispute will escalated to the relevant court in 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

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate rights or duties under this CPS, without the prior written consent of DESC.

9.16.3 Severability

If any provision of this CPS is determined to be invalid or unenforceable, the other sections shall remain in effect until this CPS is updated.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

DESC shall not be liable for any failure or delay in their performance under the provisions of this CPS due to causes that are beyond their reasonable control, including, but not limited to unavailability of interruption or delay in telecommunications services.

9.17 Other Provisions

Not applicable.