Dubai Electronic Security Center

Dubai PKI

Dubai PKI Root CA

Certification Policy and Certificate Practice Statement

Project	DESC CA Project
Title	Dubai PKI Root CA, Certification Policy and Certificate Practice Statement
Classification	PUBLIC
File Name	DubaiPKI-DubaiRootCA-CertificationPracticeStatement_v1.5
Created on	18 May 2017
Revision	1.5
Modified on	11 April 2021

Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1	Khawla Hassan	Initial version
12 September 2017	0.2	Khawla Hassan	Minor modifications & Incorporation of Dubai government entity Root CA option
3 November 2017	0.3	Khawla Hassan	Minor modifications to reflect control environment
11 January 2018	0.4	Khawla Hassan	Update certificate profiles
18 January 2018	0.5	Khawla Hassan	Second revision of certificate profiles
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
07 August 2019	1.3	Khawla Hassan	Minor update on section 4.9 to enhance the readability
03 June 2020	1.4	Khawla Hassan	Updates based on regular review and removed unconstrained Root CA (Intermediate CA between Dubai PKI Root CA and Issuing CAs)
11 April 2021	1.5	Khawla Hassan	Annual review and updates to address Mozilla comments and clarify subordinate CAs governance and operating environment

Table of contents

1. Introduction

The present Certification Practice Statement (hereinafter, CPS) of the “Dubai PKI” Root Certification Authority (hereinafter, Dubai PKI Root CA or DESC Root CA) established by the Dubai Electronic Security Center (hereinafter, DESC).

This CPS addresses the technical, procedural and organizational policies and practices of the Dubai PKI Root CA with regard to all services available and during the complete lifetime of certificates issued by the Dubai PKI Root CA, including the certificates issued by the Dubai PKI Root CA to itself under the form of self-signed certificates.

This CPS is also a certificate policy (CP) in a broad sense. A CP is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.”

This CPS applies to the Dubai PKI Root CA and identifies the roles, responsibilities and practices of all its constitutive component services. This CPS also applies to all subscribers and relying parties, as well as any subordinate CAs signed by the Dubai PKI Root CA.

The provisions of the present CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including the Dubai PKI Root CA, subscribers and relying parties.

This CPS complies with the formal requirements of the Internet Engineering Task Force (IETF) RFC 3647 with regards to format and content. While certain section titles are included according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the PKI services of the Dubai PKI Root CA. Such sections are denoted as “Not applicable”.

Further information with regard to this CPS and the Dubai PKI Root CA can be obtained from DESC through the contact information as provided in the corresponding section.

1.1 Overview of Dubai PKI

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

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

CAs belonging to other entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai PKI Root CA. These issuing CAs will be directly signed by the Dubai PKI Root CA, which makes them subordinate CAs owned by the corresponding government or private sector entity but

operated by DESC. Policies and procedures of these Subordinate CAs must follow and be in full compliance with Dubai PKI Root CA CP/CPS.

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

1.1.1 Dubai PKI Hierarchy

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

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

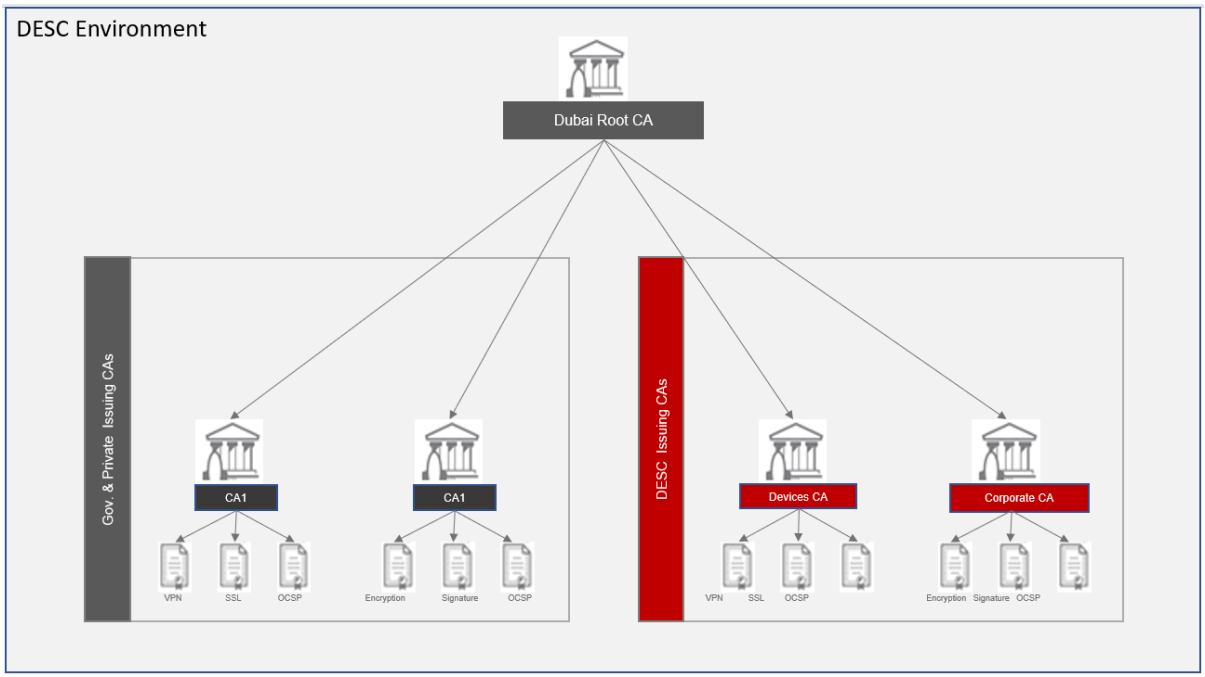

Figure 1: Trust Model for Dubai PKI

1.1.2 Certification Services

The Dubai PKI Root CA offers certification services for the underlying subordinate CAs in the Dubai PKI hierarchy. DESC has the business ownership and final responsibility in providing these

certification services, e.g., in issuing and managing its own subordinate CAs and supervising and operating the subordinate CAs issued to government or private sector entities in accordance to the present Dubai PKI Root CA Certification Practice Statement.

The CAs owned by other government or private sector entities shall be signed by the Dubai PKI Root CA. Any certificate delivered by the Dubai PKI Root CA SHALL be revoked when the agreement between DESC and the respective government or private sector entities has been cancelled by the Dubai PKI PA. The certificates issued by the Dubai PKI Root CA to government or private sector entities shall have a validity period of eight years.

1.2 Document Name and Identification

This document is named “Dubai PKI Root CA Certificate Practice Statement” and is referenced as such in related documents.

The Dubai PKI will identify this document using the Object Identifier (OID) 2.16.784.1.2.2.100.1.1.1.1.

1.3 PKI Participants

Several parties make up the participants of the Dubai PKI Root CA PKI. The parties mentioned hereunder, including the Dubai PKI Root CA, subscribers and relying parties are collectively called PKI participants.

1.3.1 Policy Authority (PA)

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

- Specifying and approving the Dubai PKI infrastructure
- Approving government and private sector entities applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy
- Specifying, maintaining and approving the Dubai PKI practices and policies, in particular the Certification Practice Statements (CPS) and the related Certificate Policies (CP) when applicable
- Review annual audit report submitted by government or private sector entities CAs to ensure continuous compliance to Dubai PKI requirements
- Review quarterly audit reports of LRAs
- Enforcing CP /CPS and other policies applicable to Dubai PKI Environment
- Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CP/CPSs and related policies
- Defining the review process that ensures that the Dubai PKI properly implements the above practices
- Defining the review process that ensures that the related policies are supported by the Dubai PKI CP and CPSs
- Publication of CP and CPSs and of its revisions

- Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the Dubai PKI
- Evaluating the proper working of the Dubai PKI environment
- Allocating members to the key ceremonies as witness as well as trusted operatives and key custodians
- Evaluating changes to the Dubai PKI environment (management, operational, hardware, software and security)
- Evaluating case-by-case issues where key Dubai PKI staff/personnel did not respect the security and/or operational procedures, including ethics
- Deciding on critical issues in case of incidents, disasters and other severe problems with regards to the Dubai PKI.

1.3.2 Dubai PKI Root CA

The Dubai PKI Root CA is owned and operated by DESC. DESC makes available the Certificate lifecycle management processes, such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. DESC also provides Certificate status information using a Repository in the form of a Certificate Revocation List (CRL).

The Dubai PKI Policy Authority (PA) is responsible for maintaining this and other CP and CPS documents relating to certificates within the Dubai PKI hierarchy. For government or private sector entities issuing CAs, the particular government or private sector entity will maintain their own set of policies and practices that must comply with this CPS as well as the government or private sector entity issuing CA Certificate Policy. Through its Policy Authority, DESC has ultimate control over the lifecycle, management, and operations of the Root CA and any subsequent subordinate issuing CAs, including subordinate CAs issued to other government or private sector entities. The Dubai PKI PA has the right to conduct annual audits on subordinate CAs to ensure compatibility and compliance with Dubai PKI Root CA requirements.

The Dubai PKI is established in Dubai. It can be contacted at the address published in section 1.5 of this CPS. To deliver the Dubai PKI Root CA services, including the issuance, revocation, renewal, status verification of certificates to government entities, DESC operates a secure facility and provides for a disaster recovery facility in Dubai. See section 5 for further details.

1.3.3 Registration Authorities

DESC operates a single internal RA for the Dubai PKI Root CA, which is tasked to request issuance and revocation of a certificate under this CPS. The RA team is represented by its leader, acting as Registration Authority Officer (RAO). When a subscriber requests for the creation of a CA certificate under the Dubai PKI Root CA (either a subordinate CA owned by DESC or an authorized government or private sector entities requesting a subordinate CA), it is the DESC RAO that will validate the request and decide whether or not to request the creation of the CA certificate. See section 3 for further details.

1.3.4 Subscribers

The subscribers of the Dubai PKI Root CA services are DESC (for subordinate CAs owned by DESC) and authorized government or private sector entities for their certification services provided through the subordinate CA(s) signed by the Dubai PKI Root CA.

An authorized government or private sector entity issuing certificates from its own subordinate CA(s) that is signed by the Dubai PKI Root CA has responsibility on the issuance and life-cycle management of the certificates it issues. Certification authorities owned and operated by other government or private sector entities shall meet the contractual, audit and policy requirements applicable to Subordinate certification authorities (CA) as stated in this Certification Practice Statement. These certification authorities must perform regular compliance audits of their own Registration Authorities (RA) to ensure compliance with the applicable identity and authentication requirements.

All subscribers and their Dubai PKI Root CA signed certification services are identified in the Subject field of their certificate issued by the Dubai PKI Root CA and control the private key corresponding to the public key that is listed in the subscriber certificate.

For any certificate, the subscriber agrees to the terms and conditions of DESC subscriber agreement.

1.3.5 Relying Parties

Relying parties are entities, including natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate issued by the Dubai PKI Root CA they receive, relying parties must always verify such a certificate against the Dubai PKI Root CA Certificate Validation Service (i.e., CRL) prior to relying on information featured in such a received certificate.

1.3.6 Other Participants

There are no other participants within the Dubai PKI.

1.4 Certificate Usage

Certain limitations apply to the usage of certificates issued by the Dubai PKI Root CA that includes the ones stated hereunder.

1.4.1 Appropriate certificate usage

The Dubai PKI Root CA Certificate is a special class of self-signed certificate that is generated by the Dubai PKI Root CA to itself, as the highest trust point within the PKI. The root certificate can be used to:

- Sign subordinate certification authorities within a PKI hierarchy
- Sign certificate revocation lists (CRLs), containing the list of subscribers' revoked certificates and authority revocation lists (ARLs), containing the list of Dubai PKI Root CA revoked self-signed certificates

Subscribers' Certificates in the context of the Dubai PKI Root CA are a special class of certificates that are issued to DESC (for subordinate CA owned by DESC) or authorized government or private sector entities. These certificates are used by government or private sector entities to sign certificates for their subscribers, Online Certificate Status Protocol (OCSP) certificates, CRLs, and when relevant ARLs. Subscribers' Certificates may not be used for any other purpose.

1.4.2 Prohibited Certificate Usage

Certain limitations apply to the usage of certificates issued by the Dubai PKI Root CA as stated in this CPS.

The use of the Dubai PKI Root CA certificate to sign end-entity certificates is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Dubai PKI Policy Authority (further "PA"), is bearing responsibility for the drafting, publishing, OID registration, maintenance, and interpretation of this CPS, and other policies and practices within the realm of the Dubai PKI.

1.5.2 Contact Details

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

Dubai PKI Policy Authority

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

E-mail pa@desc.gov.ae

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

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

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

1.6 Definitions and Acronyms

1.6.1 Terminology and Definitions

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

Activation Data — Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected; for example, a PIN, a password or passphrase, or a manually held key share

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 — Certification Authority

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

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

CCTV — Closed Circuit TV

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

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

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

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

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

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

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

Issuer — The name of the CA that signs the certificate

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

ITU — International Telecommunications Union

Key Compromise — A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed

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

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

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

OSCP — Online Certificate Status Protocol

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

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

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

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

RA — Registration Authority

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

Relying Party — A recipient of a certificate who acts in reliance on that certificate/digital signatures verified using that certificate

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

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

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

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

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

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

SubjectAltName — A certificate attribute field that often contains the subject's e-mail address

Subject — A subject is the entity named in a certificate

Subscriber — A subject who is issued a certificate

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

UPS — Uninterruptible Power Supply

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

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

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

1.6.2 Acronyms

Please refer to section 1.6.1.

1.6.3 References

The Dubai PKI is committed to comply with the below requirements published at https://www.cpacanada.ca:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements

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

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for Code Signing ("Baseline Requirements for Code Signing")

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

The present CPS endorses the following standards:

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

2. Publication and Repository Responsibilities

2.1 Repositories

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

2.2 Publication of Certificate Information

In particular, DESC publishes a copy of its self-signed Dubai PKI Root CA certificate at this location. This Certification Practice Statement is at least updated annually. DESC reserves its rights to publish the certificate status information on third-party repositories.

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

DESC publishes digital certificate status information in frequent intervals as indicated in this CPS. The provision of the Dubai PKI Root CA issued electronic certificate validity status information is a 24/7 available service.

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

2.3 Time or Frequency of Publication Repositories

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

DESC maintains the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL until minimum 7 years after the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the Repository are uploaded within 24 hours. Dubai PKI Root CA shall publish certificates promptly following their generation and issuance. CRL information shall be published as set in section 4.9.7.

Due to their sensitivity, DESC refrains from making publicly available certain subcomponents and elements of such documents, including certain security controls, procedures related with the functioning of registration authorities and internal security policies. 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 regards to the Dubai PKI Root CA activities.

2.4 Access Controls on Repositories

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

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

3. Identification and Authentication

DESC maintains documented practices and procedures to authenticate the identity and/or other attributes of a certificate subscriber. Prior to requesting the issuance of a certificate, DESC verifies the identity of the organization that requests a certificate under the Dubai PKI Root CA. See section 3.2 for further details.

DESC authenticates the requests of parties wishing the revocation of certificates under the provisions of the present CPS.

3.1 Naming

3.1.1 Types of Names

The certificates issued by the Dubai PKI Root CA shall contain X.500 Distinguished Names (DN) in English. The table below summarizes the DNs for the Dubai PKI Root CA.

Dubai PKI Root CA

The name of the Dubai PKI Root CA is defined as per the Issuer field of the Dubai PKI Root CA certificate (specified in section 7).

Field	Value
Country name	AE
Organization name	UAE Government
Common Name	UAE Global Root CA G4 E2

Subscribers

To identify the applicant certification service (here after referred to as the applicant), DESC follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names. These rules will be applied by the RA.

3.1.2 Meaningful Names

Names are meaningful since the CN (Common Name) contains the name of the subscriber.

Names do have to be meaningful or unique. Subscribers cannot be anonymous or pseudonymous. Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question.

3.1.3 Anonymity and Pseudonymity of Subscribers

This policy does not permit anonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

The naming conventio n used by Dubai PKI is ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 Uniqueness of Names

DESC enforces the controls necessary to guarantee that subject DN are unique.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringes upon the intellectual property rights of entities outside of their authority. As part of application process, the PA will validate the correctness of provided information as specified in section 3.1 and 3.2.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

DESC enforces that a Proof-of-Possession of the private key is submitted as part of certificate requests. A possible implementation would be to rely on certificate requests to be processed by DESC CAs and containing a Proof-of-Possession (e.g., PKCS#10, PKIX-CMP).

3.2.2 Authentication of Organization Identity

Dubai PKI Root CA

The Dubai PKI Root CA is fully controlled by Dubai PKI PA. It is specified and parameterized at the occasion of the Dubai PKI Root CA Bootstrap ceremony.

Subscribers

The Initial Identity Validation is done during the assessment of the applicant according to the DESC onboarding process.

3.2.3 Authentication of Individual Identity

3.2.4 The Dubai PKI Root CA does not issue end-entity certificates. Non-verified Subscriber Information

All subscriber information contained within certificate issued by the Dubai PKI Root CA shall be verified by the DESC RA. Non-verified information shall not be included in certificates issued by Dubai PKI Root CA.

3.2.5 Validation of Authority

No stipulation — this section intentionally left blank.

3.2.6 Criteria for Interoperation

No stipulation — this section intentionally left blank.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Keying

Same provisions as those defined in sections 3.1 and 3.2 apply. An authorized representative should request re-key of CA, in compliance with the Dubai PKI Root CA Operation Guidelines.

3.3.2 Identification and Authentication for Re-Key After Revocation

Same provisions as those defined in sections 3.1 and 3.2 apply. If the Root CA certificate is revoked, an authorized representative of the CA shall provide sufficient information before Dubai PKI Root CA initiates generation of the new CA certificate.

3.4 Identification and Authentication for Revocation Requests

Dubai PKI Root CA

In the event of a revocation due to a key compromise, internal procedures will be executed by the application of DESC Disaster Recovery and Business Continuity Plans.

Subscribers

For the identification and authentication procedures of revocation requests, a formal request is required to be addressed to DESC by the same government or private sector entity that performed the initial application. DESC has the final authority to cancel the authorization of that entity and to proceed to the subsequent certificate revocation when relevant.

4. Certificate Life-Cycle Operational Requirements

Dubai PKI Root CA

The operational requirements on the Dubai PKI Root CA certificates lifecycle are described in internal documents. Any event with regards to the Dubai PKI Root CA keys and certificates is decided, authorized and controlled by the PA. Such events must always be authorized in a written form by a document signed by at least two members of the PA.

When there is no further stipulation, the following subsections apply to subscribers.

Subscribers

Any of the certification services for which a certificate has been issued by the Dubai PKI Root CA (including government or private sector entity certificates) has a continuous obligation to inform DESC of all changes in the information featured in a certificate during the operational period of such certificate or of any other fact that materially affects the validity of a certificate.

DESC will then take appropriate measures to make sure that the situation is rectified (e.g., initiate the revocation of the existing certificates and the generation of new certificates with the correct data in case of an incorrectly issued certificate).

DESC issues or revokes certificates only at the request of the subscriber identified and authenticated as described in chapter 3, with the exception of a proven key compromise. In case of a proven CA key compromise, DESC will immediately revoke the concerned certificates

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate application is limited to government or private sector entities.

4.1.2 Enrolment Process and Responsibilities

The subscriber will issue to DESC its request for certificate issuance in a form of certificate application. DESC acts as the RA that has the authority and is designated to validate the certificate application details, including:

- The identification of the government or private sector entity
- The government or private sector entity CA CP & CPS. The CA Certificate Policy must be compliant with Dubai PKI Root CA CP. Guidelines on how to establish the CP are available at "https://ca-repository.desc.gov.ae/Repository/source/cp/DubaiPKI-DubaiGovernmententityissuingCA-CertificatePolicy_v1.3.pdf"
- Description of the applicant purpose

- Required applicant certificate profiles and the values of each attribute that should be present in the applicant's certificate

The above details together are further referred to as "Applicant Definition"; that is considered as integral part of the certificate request, and it is required by DESC in order to process the CA certificate request.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

As soon as a certificate application is received, DESC will evaluate whether the applicant is a valid government or private sector entity eligible to receive authorization to operate its own subordinate CA within the Dubai PKI. This evaluation is performed in accordance with internally defined process for the evaluation, acceptance and management of government or private sector entities, which includes among others the steps disclosed in this section.

DESC will validate the identity of the representative applying on behalf of a government or private sector entity to verify whether he/she is who he/she claims to be. This validation requires a face-to-face meeting where at least both the government or private sector entity representative and the DESC RA Officer are present.

Furthermore, DESC will assess all details about the applicant and its certification service, including compliance of the policies and practices with requirements defined by the applicable CP and CPS.

In the case where the applicant already was a subscriber desiring a certificate re-key (for renewing the CA certificate expiry date), all the above steps will be applicable. In addition, the existing certificate will be provided to DESC, as well, so that DESC can verify present subscriber information against those provided in the new PKCS#10 request to be provided by the applicant.

4.2.2 Approval or Rejection of Certificate Applications

Once the evaluation is complete, Dubai PKI PA will either approve or reject the certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

Upon final agreement of an Applicant Definition, the Applicant and DESC will agree upon a date and a backup date when the required people can make themselves available at the Dubai PKI Root CA premises to perform the subordinate CA signing key ceremony. Prior or at the ceremony date, the applicant generates and submits to DESC a PKCS#10 request for the certificate request. The request is signed by the private key, enabling the Subscriber to prove the possession of this key. A printout of the key to be certified is signed by the subscriber and Dubai-PKI PA and kept archived together with the Applicant Definition form.

4.2.3 Time to Process Certificate Applications

No stipulation — this section intentionally left blank.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The Dubai PKI Root CA trusted operatives and Dubai PKI Root CA key custodians gather at the Dubai PKI Root CA premises to activate the Dubai PKI Root CA keys prior to the commencement of the issuance procedure.

The DESC RA officer (RAO) must be physically present at the Dubai PKI Root CA location and is duly authenticated through this physical presentation. The key ceremony authorization is verified by the Dubai PKI Root CA trusted operatives and Dubai PKI Root CA key custodians, so that the RAO can proceed further with the certificate issuance.

The CA processes certificate request from the RA provided that:

- The RA is authenticated
- The certificate request is validly formatted
- The certificate request contains valid subscriber data

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Once the certificate is issued, the RAO ensures that the certificate issued by the Dubai PKI Root CA contains all data that was presented to it in the request.

Following issuance of a certificate, DESC posts an issued certificate on the Certificate Repository, and the ROA then handovers the issued certificate to the subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber is responsible for checking the details associated with their certificate. Usage of the certificate by the Subscriber is considered as an acceptance of the issued certificate.

In case the Subscriber does not accept the certificate, the reason for non-acceptance will be discussed. If no measures can be agreed upon in order to obtain the acceptance, the certificate will be revoked.

Certificate acceptance is governed by the agreements set out between the Dubai PKI Root CA and applying CA's.

4.4.2 Publication of the Certificate by the CA

Following issuance of a certificate, DESC posts an issued certificate on the Certificate Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entities or organizations are notified directly of the certificate issuance. They are indirectly notified through the update of the Repository.

4.5 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below.

4.5.1 Subscriber Private Key and Certificate Usage

Unless otherwise stated in this CPS, subscribers' duties include the ones below and will be formally agreed upon through a subscriber agreement:

- Refraining from tampering with a certificate
- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to all government or private sector entities, and with its own CPS
- Using a certificate, as it may be reasonable under the circumstances
- Preventing the compromise, loss, disclosure, modification or otherwise, unauthorized use of their private keys
- Refrain from using the certificate outside its validity period or after it has been revoked

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by the Dubai PKI Root CA will:

- Use proper cryptographic tools to validate the certificate signature and validity period
- Validate the certificate by using a CRL or a web-based certificate validity status information service in accordance with the certificate path validation procedure
- Trust the certificate only if it has not been revoked and within the validity period
- Rely on the certificate, as may be reasonable under the circumstances
- Trust the certificate only for the signing of certificates and CRLs
- Relying parties shall use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

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.

Certificate Renewal is not be supported by this CA. Only certificate re-key is supported.

4.7 Certificate Re-key

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

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

4.7.1 Circumstance for Certificate Re-key

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

4.7.2 Who May Request Certification of a New Public Key

As per initial 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

The Dubai PKI Root CA does not allow certificate modification. The Subscriber must immediately inform DESC of any changes to the data on the Certificate, or when the certified data has become inaccurate or has changed in any way. The Subscriber must ask DESC to revoke the Certificate. The Certificate revocation process is then started immediately after identification and authentication of the requestor. The revocation procedures are set out in Section 4.9 of the present CPS.

In case the Subscriber wants to change the certified information or has requested the revocation of his/her Certificate due to circumstances mentioned in the previous paragraph, and wishes to be issued a new Certificate, the Subscriber shall process to a full Certificate application as for initial enrolment.

4.9 Certificate Revocation and Suspension

Suspension of certificates is not allowed.

Dubai PKI Root CA

The revocation of a Dubai PKI Root CA Key is a critical process and related procedures are described in internal documents related to business continuity and disaster recovery.

Subscribers

Suspension of a subscriber's certificate is not allowed.

Refer to the below subsections for further details.

4.9.1 Circumstances for Revocation

Government or private sector entities should obtain authorization from the Dubai PKI PA in order to be allowed to operate. This authorization and respective agreement will be delivered for a period of 8 years after which a renewal is required. Any certificate delivered by the Dubai PKI Root CA within this context SHALL be revoked when the agreement has been cancelled by DESC. For subordinate CA owned and operated by DESC, DESC unilaterally decides on revocation.

In the case of a subscriber termination, once the termination plan is completed and the agreement terminated, the certificate issued by the Dubai PKI Root CA to the terminated service, when not expired, shall be revoked.

In addition, revocation of a Subordinate CA certificate is initiated based on the following events:

- Having received a certificate revocation request from the subscriber
- Having received notice by the subscriber that there has been a loss, theft, modification, unauthorized disclosure or other compromise of the private key of the certificate subject
- Notification of the subscriber that the original certificate request was not authorized and does not retroactively grant authorization
- There has been a modification of the information contained in the certificate of the certificate subject
- DESC obtains evidence that the Certificate was misused
- DESC determines that any of the information appearing in the Certificate is inaccurate or misleading
- The Subordinate CA notifies DESC that the original certificate request was not authorized and does not retroactively grant authorization
- DESC obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6
- DESC is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement
- DESC ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
- The Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated
- Revocation is required by this Certificate Policy/Certification Practice Statement

- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g., the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk)
- Upon having a proof of compromise of the private key of the certificate subject, DESC will immediately request the revocation the relevant certificate

4.9.2 Who Can Request Revocation

The permanent revocation of a Certificate can be requested by:

- The Subscriber himself
- DESC at its own discretion (if for instance a compromise is known for this CA key)

Certification requests from subscribers are only accepted if the subscriber is authorized and authenticated to request revocation for the specific certificate (i.e., the subscriber is linked to the certificate through the certificate application request or other means).

The authority to revoke the Dubai PKI Root CA certificate rests within DESC.

4.9.3 Procedure for Revocation Request

The RA procedure for Subordinate-certificate revocation is as follows:

1. A request to revoke certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).
2. The Dubai PKI PA shall authenticate the request as well as the authorization of the request the revocation as per the agreement.
3. Looks up DN in a dedicated RA application
4. Selects the desired certificate
5. Selects “Revoke this certificate”
6. Enters revocation reason and submits it

4.9.4 Revocation Request Grace Period

There shall be no revocation grace period. Revocation requests shall be processed timely/ immediately by the RA.

The Dubai PKI Root CA shall maintain controls to provide reasonable assurance that the revocation process for the Subordinate CA Certificate be completed within 7 days.

4.9.5 Revocation Request Response Time

Authorized Certificate revocation should be processed within 24 hours. Certificate revocation problems must be reported within 24 hours.

DESC publishes notices of revoked certificates in the CRL.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

A CRL is issued minimum once every six months, at an agreed time. In addition, a new CRL will be generated and published following the revocation of any certificate. CRLs are signed and time-stamped by the Dubai PKI Root CA.

Revocation entries on a CRL are removed after eight years of the Expiry Date of the revoked Certificate.

4.9.8 Maximum Latency for CRLs

No stipulation — this section intentionally left blank.

4.9.9 Online Revocation/Status Checking Availability

Certificate status information is provided through the OCSP for the Dubai PKI Root CA.

4.9.10 Online Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation — this section intentionally left blank.

4.9.12 Special Requirements — Key Compromise

If DESC discovers, or has a reason to believe, that there has been a compromise of the private key of the Dubai PKI Root 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 Subordinate CAs, subscribers and potential relying parties that there has been a key compromise, and (4) generate new CA key pair as per Dubai PKI Root CA operation policies and procedures. Circumstances for Suspension

Certificate suspension is not supported by the Dubai PKI Root CA.

4.9.13 Who Can Request Suspension

Not applicable

4.9.14 Procedure for Suspension Request

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of public certificates is available from CRL's in the repositories and via an OCSP responder. CRLs and OCSP shall be published/accessed via public repository which is available to relying parties through HTTP protocol queries.

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation — this section intentionally left blank.

4.11 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.12 Key Escrow and Recovery

Subscriber's key backup, escrow and key recovery are not applicable as these services are not provided by DESC in the context of the Dubai PKI Root CA activities.

5. Management, Operational and Physical Controls

This section describes security controls used by DESC to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit and archival.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

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

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

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

5.1.3 Water Exposures

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

5.1.4 Fire Prevention and Protection

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

5.1.5 Media Storage

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

5.1.6 Waste Disposal

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

5.1.7 Offsite Backup

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

Backup media shall be stored in a location separate from the DESC main site in accordance with the Dubai PKI Disaster Recovery plan and Procedures.

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

5.2 Procedural Controls

DESC follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of staff members, and 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 Dubai PKI Root 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 roles). The following are the trusted roles for a Dubai PKI Root CA: CA Administrator
- CA Security Officer
- CA Directory Administrator
- CA Database Administrator
- HSM Administrator
- HSM Partition Owner
- HSM Partition MofN Custodian
- HSM Security Officer

- System Administrator
- Internal Auditor
- External Auditor

DESC conducts an initial investigation on all staff members who are candidates to serve in trusted roles to ensure their trustworthiness and competence. Number of Persons Required per Task

Where dual or multiple control is required, at least two trusted members of the Dubai PKI Root CA staff need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

DESC ensures that all actions with respect to the Dubai PKI Root CA can be attributed to the system of the Dubai PKI Root CA and the member of the Dubai PKI Root CA staff that has performed the action.

5.2.2 Identification and Authentication of Each Role

Before exercising the responsibilities of a trusted role:

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

5.2.3 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 issuing Subordinate CA certificate, Root CA Key Backup, .etc.

- Dubai PKI Root CA operating personnel that manages operations on certificates
- Administrative personnel to operate the platform supporting the Dubai PKI Root CA
- Security personnel to enforce security measures

5.3 Personnel Security Controls

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

5.3.1 Qualifications Experience and Clearance Requirements

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

- Criminal convictions for serious crimes
- Misrepresentations by the candidate
- Appropriateness of references

- Any clearances as deemed appropriate

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

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

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

Independent Dubai PKI Root CA component services subcontractors and their personnel are subject to the same background checks as DESC employees. The background checks include:

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment.

5.4.1 Types of Event Recorded

DESC ensures that at least the following details are recorded:

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

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

- Start and stop of servers
- Outages and major problems
- Physical access of personnel and other persons to sensitive parts of the Dubai PKI Root CA site
- Backup and restore
- Report of disaster recovery tests

- Audit inspections
- Upgrades and changes to systems, software and infrastructure
- Security intrusions and attempts at intrusion
- System configuration changes and maintenance, as defined in the CPS
- CA personnel changes
- Discrepancy and compromise reports
- Information concerning the destruction of sensitive information
- Current and past versions of all Certificate Policies
- Current and past versions of Certification Practice Statements
- Vulnerability Assessment Reports
- Threat and Risk Assessment Reports
- Compliance Inspection Reports
- Current and past versions of Agreements
- Other documents that are required for audits include:
  - Infrastructure plans and descriptions
  - Physical site plans and descriptions
  - Configuration of hardware and software
  - Personnel access control lists

5.4.2 Frequency of Processing Log

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

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

All log entries include the following elements:

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the Dubai PKI Root CA audit log:

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

5.4.6 Audit Collection System (Internal vs. External)

No stipulation — this section intentionally left blank.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

Dubai PKI systems are subject to an annual assessment in line with DESC system assurance policy and this CP.

5.5 Records Archival

DESC keeps records of the following items:

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

The very last back up of the Dubai PKI Root CA archive will be retained for seven years following the issuance of the last certificate by the Dubai PKI Root CA.

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

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

Archives are accessible to authorized personnel of DESC.

5.5.1 Types of Records Archived

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

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

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for Timestamping of Records

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

5.5.6 Archive Collection System (Internal or External)

The Dubai PKI Root CA archive collection system is internal.

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 paper-based format.

5.6 Key Changeover

Dubai PKI Root CA private keys are maintained until such time as all relying certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In a separate internal document, DESC specifies applicable incident, compromise reporting and handling procedures. DESC specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing Resources, Software and/or Data Corruption

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

DESC establishes:

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

Disaster recovery infrastructure and procedures shall be fully tested at least once a year with the witnessing of more than one member of the Dubai PKI PA.

5.7.3 Entity Private Key Compromise Procedures

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

Compromise of the Dubai PKI Root CA private key(s) or of the associated activation data shall imply the immediate revocation of the certificate of the compromised key(s). The revocation of a Dubai PKI Root CA Key is a critical process and related procedures are described in internal documents.

DESC will additionally take the following measures:

- Notify the Dubai PKI Root CA community
- Notify all other PKI Participants
- List the certificate of the corrupted Dubai PKI Root CA in the CRL (in this case the CRL is called ARL. CRLs and ARLs can be merged within a single file, but revoked Dubai PKI Root CA certificate will be additionally listed on the Dubai PKI Root CA Certificate Dissemination Webpage)
- Revoke all the certificates signed by the corrupted Dubai PKI Root CA
- After assessing the reasons for corruption of the Dubai PKI Root CA private key and revocation of the Dubai PKI Root CA certificate, and after having taken all the necessary measures to avoid the cause of revocation in the future, and after obtaining authorization from Dubai PKII PA, a new key pair and the associated certificate may be generated

5.7.4 Business Continuity Capabilities after a Disaster

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

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

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

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

5.8 CA or RA Termination

In the case of Dubai PKI Root CA or RA termination, DESC shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

DESC shall inform within a reasonable delay, the following parties of the termination:

- All Subscribers
- All other PKI Participants
- Relying parties to the extent feasible

DESC shall terminate all authorization of sub-contractors to act on behalf of the terminated service (Dubai PKI Root CA or RA) in the performance of any functions related to the process of issuing certificates.

Before termination of the Dubai PKI Root CA activities, DESC will take measures to transfer the following information to a designated organization: all information, data, documents, repositories, archives and audit trails with regard to the Dubai PKI Root CA and shall maintain or transfer the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate.

6. Technical Security Controls

This section defines the security measures DESC takes to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key access tokens).

The security measures that are in place at subscribers are governed by their own CPS following this CPS as well as the government or private sector entity issuing CA Certificate Policy. When no other stipulation applies, the related subsections are not further specified with regards to Subscriber's obligations.

6.1 Key Pair Generation and Installation

DESC implements and documents key generation procedures in accordance with this CPS.

6.1.1 CA Private Key Pair Generation

6.1.1.1 Dubai PKI Root CA

DESC undertakes the generation of the Dubai PKI Root CA key pair(s) and protects its private key(s) in a Hardware Security Module certified against at least FIPS 140-2 level 3, using a trustworthy system and takes the required precautions to prevent compromise or unauthorized use, according to a documented procedure (i.e., the "DESC Dubai PKI Root CA Key Ceremony" document).

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

- At least four trusted persons participate in the generation and installation of Dubai PKI Root CA private key(s); two trusted operatives and two key custodians
- The Dubai PKI Root CA Key Generation Ceremony will be witnessed by the CA's Qualified Auditor (see section 8 Compliance Audit and Other Assessments)
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians
- The PKI operations team and key custodians act upon authorization by DESC, who is the owner of the Dubai PKI Root CA private keys, to perform cryptographic operations using the Dubai PKI Root CA private key(s)
- The Qualified Auditor will then issue a report, covering that the Dubai PKI Root CA, during its Dubai PKI Root CA Key Pair and Certificate generation process:
  - Documented its Dubai PKI Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement
  - Included appropriate detail in its Dubai PKI Root CA Key Generation Script

- Maintained effective controls to provide reasonable assurance that the Dubai PKI Root CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Dubai PKI Root CA Key Generation Script
- Performed, during the Dubai PKI Root CA key generation process, all the procedures required by its Dubai PKI Root 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 Subordinate CAs

Government or private sector entity CA is generated by applying the same procedures as for the Dubai PKI Root CA. Key custodians will include trusted personnel from both DESC and the entity.

The security measures that are in place for key generation of other Subordinate CAs are governed by their own CPS.

6.1.2 Private Key Delivery to Subscriber

6.1.2.1 Dubai PKI Root CA

The private key is generated during the Key Ceremony procedure as ruled in a documented procedure (i.e., the “DESC Dubai PKI Root CA Key Ceremony" document).

6.1.2.2 Subscribers

Dubai PKI Root CA does not generate private keys for Subscribers (individuals). It issues certificates for approved Subordinate CAs

6.1.3 Public Key Provisioning

6.1.3.1 Dubai PKI Root CA

The public key is generated and certified during the same Key Ceremony procedure.

6.1.3.2 Subscribers (Subordinate CAs)

Subscribers bring the public key of their application of certification services to be certified physically by the face-to-face registration processes that is managed by Dubai PKI (see section 4.1 Certificate Application).

6.1.4 CA Public Key Delivery to Relying Parties

DESC will publish its public key(s) on its dedicated dissemination web page (see Section 2; Publication and Repository Responsibilities).

6.1.5 Key Sizes

The minimum size for the Dubai PKI Root CA Keys using the RSA SHA-256 algorithm is 4096 bits.

The minimum size for Subordinate CA Keys using the RSA SHA-256 algorithm is 4096 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key RSA exponents are chosen securely. Public Key module generation is done with state-of-the-art parameter generation technology. Parameter generation is implemented using state of the art technology and shall be regularly re-evaluated regarding new advances in cryptology.

6.1.7 Key Usage Purposes (As per X.509 v3 Key Usage Field)

The Dubai PKI Root CA uses private signing keys only for signing CRLs and applicant certification services certificates in accordance with the intended use of each of these keys. Other usages are restricted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

DESC uses a secure cryptographic device — Hardware Security Module (HSM) — to store the private keys meeting the appropriate FIPS 140-2 level 3 requirements.

The HSMs do not leave the secured environment of DESC. In case the HSMs require maintenance or repair, the HSMs will be securely transported to the manufacturer. The private keys will not be present in the HSM when brought outside the secured environment of DESC for maintenance or repair. When in use, the HSMs are physically present in the secured environment of DESC.

6.2.2 Private Key Multi-Role Control

Dubai PKI Root CAs keys are activated only during circumstances described in the “DESC Root CA Key Ceremony" document.

The Dubai PKI Root CA private keys remain controlled by multiple authorized persons, the Dubai PKI Root CA trusted operatives and key custodians, to safeguard and improve the trustworthiness of private keys. These trusted persons are assigned with the task to activate and deactivate the Dubai PKI Root CAs private keys.

A certain number of persons ‘m’ (at least 2), out of ‘n’ persons (3 persons), the total number of key custodians, need to be present concurrently together with two (2) Dubai PKI Root CA trusted operatives to activate or re-activate the Dubai PKI Root CA private key.

The Dubai PKI PA 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 will keep track of the renewed tokens and/or password distribution.

More than one member of the Dubai PKI PA makes authorization of Dubai PKI Root CA private key protection tokens and related password distribution and assigned personnel in writing.

6.2.3 Private Key Escrow

Private keys of the Dubai PKI Root CA may not be escrowed. DESC implements internal disaster recovery measures.

6.2.4 Private Key Backup

The private key(s) is (are) backed up, stored and recovered by multiple and appropriately authorized members of Dubai PKI Root CA staff serving in trustworthy positions. More than one member of the Dubai PKI PA makes authorization of key back up and assigned personnel in writing.

A backup of the generated key material is taken and stored under the same security measures as the primary key material.

The procedures are described in an internal document.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from an HSM

See section 6.2.4 Private Key Backup.

6.2.7 Private Key Storage on Cryptographic Module

See section 6.2.1 Cryptographic Module Standards and Controls.

6.2.8 Method of Activating Private Key

The Dubai PKI Root CA private keys remain under m out of n multi-personnel control. Dubai PKI Root CA trusted operatives and key custodians are assigned with the task to activate and deactivate the Dubai PKI Root CA private keys. Dubai PKI Root CA keys are then active only for defined time periods.

Subscriber's private key activation is the responsibility of the Subscriber.

6.2.9 Method of Deactivating Private Key

The Dubai PKI Root CA private keys remain under m out of n multi-personnel control. Dubai PKI Root CA trusted operatives and key custodians are assigned with the task to deactivate the Dubai PKI Root CA private keys.

6.2.10 Method of Destroying Private Key

At the end of their lifetime, taking into account business purpose and legal obligations, the private keys are destroyed by at least three trusted Dubai PKI Root CA staff members at the presence of 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 Dubai PKI Root CA keys are destroyed by permanently removing the keys from any hardware modules the keys are stored on, together with all associated activation data or hardware that could be used for recovering the private key.

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

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

DESC archives its own Dubai PKI Root CA public keys. See section 5.5 of the present CPS for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Dubai PKI Root CA Certificate shall have a validity period greater than the maximum lifetime of the Subscriber certificate after the latest Subscriber certificate issuance, augmented with a period taking into account the Dubai PKI Root CA private key usage period and re-key activities.

The certificate validity and key usage periods within DESC hierarchy are defined as follows:

- Dubai PKI Root CA certificates are valid for 25 years, with a key usage period of 15 years. Relevant parties will be noticed in advance to avoid disruption of CA services
- Subscriber certificates' validity is aligned to the validity period of the CA(s) issued to the government or private sector entities. These certificates are valid for eight years by default. However, if a new certificate is issued to the Subscriber during the period of validity of the entity Subordinate CA (e.g., if the Subscriber renews its key pair), the new certificate validity will be aligned to the remaining duration lifetime of the entity Subordinate CA.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 CA Key Generation

DESC ensures that activation data associated to Dubai PKI Root CAs private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of Sections 6.1 and 6.2.

6.4.2 Activation Data Protection

Subscriber's activation data protection is the responsibility of the Subscriber. This should be managed in accordance with the requirements specified in their own CPS, in accordance with applicable DESC policies and following the minimal requirements stipulated within the agreement between DESC and the government or private sector entity.

6.4.3 Other Aspects of Activation Data

No stipulation — this section intentionally left blank.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

DESC ensures that computer security controls are implemented in compliance with technical standards and vendor security hardening guidelines as a minimum. Detailed description of implemented computer security controls is available as internal document(s).

Throughout the environment, the following computer security controls are implemented as a combination of operating system, hardened module and software-based controls:

- Access controls, including identification and authentication of PKI roles
- Network or system-based controls supporting integrity and isolation of systems and services
- Cryptographic controls for ensuring secure session and trusted path communication
- Controls limiting the accounts and network services on CA-related systems
- Audit logging of performed activities on CA-related systems
- Controls enforcing segregation of duties for applicable activities

6.5.2 Computer Security Rating

No stipulation — this section intentionally left blank.

6.6 Life Cycle Security Controls

DESC ensures that periodic development control, security management and life cycle security controls are implemented in compliance with technical standards and vendor security hardening guidelines as a minimum. Detailed description of implemented life cycle technical controls is available as internal document(s) for any tools whose development is under control of DESC.

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

Formal procedures are in place to document and maintain the configuration of CA-related systems, including configuration modifications and/or upgrades. The configuration integrity of systems and applications is verified on a regular basis using automated tools for detecting malicious configuration changes.

6.6.3 Life Cycle Security Controls

No stipulation — this section intentionally left blank.

6.7 Network Security Controls

Root CA systems are located in a high security zone and in an offline state or air-gapped from all other networks. The Dubai PKI Root CA machine is offline and kept in a secure safe within DESC secure premises.

For the systems supporting the Dubai PKI and Dubai PKI Root CA, DESC ensures maintenance of network security, including managed firewalls and intrusion detection systems.

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

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

6.8 Timestamping

The Dubai PKI Root CA is offline and therefore, relies on its internal clock for time-stamping the archive records as required by section 5.5.5 of the present CPS in the context of "audit logging procedures" and any purposes or activities for which time is a critical element.

7. Certificates and CRL Profiles

7.1 Certificate Profile

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions.

Certificate profiles are described in Appendix–I.

7.1.1 Version Number(s)

X.509 v3 is supported and used for all certificates related to the Dubai PKI Root CA.

7.1.2 Certificate Extensions

X.509 v3 extensions are supported and used as indicated in the Certificates profiles as described in section 7.1 of the present CPS.

Subordinate CA certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CPS.

7.1.3 Algorithm Object Identifiers

Algorithms OID are conforming to IETF RFC 3279 and RFC 5280.

7.1.4 Name Forms

Name forms are in the X.500 distinguished name form as implemented in RFC 3739. The following Subject Attributes are used:

- Country (country codes MUST follow the format of two letter country codes, specified ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions — 1997)
- Organization
- Organizational unit
- Common name

7.1.5 Name Constraints

X.509 v3 Name Constraints extension will not be included in the Dubai PKI Root CA certificate and DESC Subordinate CAs i.e. Corporate Certification Authority and Devices Certification Authority, yet it

will used for the subordinate CAs owned by government and private sector entities where the CA certificate will support of id-kp-serverAuth or id-kp-emailProtection usage to its subscribers.

Appendix I shows detailed profiles.

7.1.6 Certificate Policy Object Identifier

The Dubai PKI will identify this document using the Object Identifier (OID) 2.16.784.1.2.2.100.1.1.1.1.

7.1.7 Usage of Policy Constraints Extension

Usage of Policy Constraints extension is supported as per RFC 5280.

7.1.8 Policy Qualifiers Syntax and Semantics

The use of policy qualifiers defined in RFC 5280 is supported.

7.1.9 Processing Semantics for the Critical Certificate Policies

Not applicable.

7.2 CRL Profile

Certification status information is provided through certificate revocation lists (CRLs), in conformance with IETF PKIX RFC 5280. CRL profiles are described in Appendix–II.

7.2.1 The profile of the CRL is provided in Version Number(s)

See section 7.2. The Dubai PKI Root CA will support X.509 version 2 CRLs.

7.2.2 CRL Entry Extensions

See Section 7.2.

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960. OCSP profiles are described in Appendix–III.

7.3.1 Version Number(s)

The OCSP responder issues OCSP responses of version 1.

7.3.2 OCSP Extensions

- The OCSP response signing authority is designated to the DESC OCSP responder; therefore, the OCSP certificate contains the id-kp-OCSP Signing OID in the extended key usage extension.
- The certificate will include the extension id-pkix-ocsp-nocheck as a non-critical extension, which indicates that an OCSP relying party can trust an OCSP response signing certificate for its lifetime.

8. Compliance Audit and Other Assessments

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

8.1 Frequency or Circumstances of Assessments

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

Identity and Qualifications of 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 or any person having any conflicting interests thereof.

The Dubai PKI Root CA is audited for compliance to the latest version of one or more of the following standards:

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

These audits will be performed by Qualified Auditors who fulfils the following requirements:

- Independence from the subject of the audit
- The 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 the third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics

- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors and Omissions insurance with policy limits of at least US$1m in coverage

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

8.2 Assessor's Relationship to Assessed Entity

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

8.3 Topics Covered by Assessment

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

8.4 Actions Taken as a Result of Deficiency

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

8.5 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being

taken by the audited party, shall be provided to DESC PKI PA. The audit Report shall be publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9. Other Business and Legal Matters

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

9.1 Fees

An entity can only apply for a certificate issued by the Dubai PKI Root CA if authorized by the Dubai PKI PA. Fees may be applicable to obtain this authorization.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

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

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

9.4 Privacy of Personal Information

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

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

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

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

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

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

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

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

Disclosure Conditions

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

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

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

- Themselves
- Persons in their custody

Only the RA is permitted to access confidential information.

DESC properly manages the disclosure of information to the Dubai PKI Root CA personnel.

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

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

All communications of confidential information are encrypted, including:

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

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

9.6.2 RA Representations and Warranties

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

9.6.3 RA Representations and Warranties

Subscribers shall represent to DESC that the Subscriber will:

- Securely generate its Private Keys and protect its Private Keys from compromise (including protecting any tokens or corresponding activation data that provides access to Private Keys),
- Provide accurate and complete information and communication to this CA and the RA,
- Confirm the accuracy of certificate data prior to using the certificate,
- Promptly cease using a certificate and notify DESC if (i) any information that was submitted to the CA or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate, and
- Use the certificate only for authorized and legal purposes, consistent with this CPS and the applicable agreement with DESC

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

- Profit loss
- Loss of data
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant or if it is the result of negligence or with intent to deceive DESC, the Dubai PKI Root 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 Dubai PKI Root CA does not offer any guarantees or warranties or enter into agreements that could be the subject of performance penalties, that could lead to legal actions on behalf of subscribers or relying parties.

9.9 Indemnities

Not applicable.

9.10 Term and Termination

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

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

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

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

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

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

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

9.17 Other Provisions

Not applicable.

Appendix I

The Dubai PKI Root CA Certificate profile

The Dubai PKI Root CA Certificate profile is further described in the following table. All fields of type Directory String are of type UTF8String.

Dubai PKI Root CA Certificate Profile					
Field	CE[1]	O/M[2]	CO[3]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280 Also see next part of the table
Signature	False	M			
Algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Root CA Signature.	CA signature value
TBSCertificate					
Version	False	M			
		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	S		
CountryName		M	S	AE	Encoded according to "ISO 3166-1-

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

						alpha-2 code elements". PrintableString, size 2 (rfc5280)
	OrganizationName		M	S	UAE Government	UTF8 encoded
	CommonName		M	S	UAE Global Root CA G4 E2	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 + **[300]** Months	
Subject		False	M			
	CountryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	OrganizationName		M	S	UAE Government	UTF8 encoded
	CommonName		M	S	UAE Global Root CA G4 E2	UTF8 encoded
SubjectPublicKeyInfo		False	M			
	Algorithm		M	S	RSA	
	SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions			M			
Authority Properties						
crlDistributionPoints		False	O			
	DistributionPoint		O	D	**Example value:** http://ca-repository.desc.gov.ae/CRL/Root/uae_global_	CRL download URL.

					root_ca_g4_e2_uae_government_ae_crlfile.crl	
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	SHA-1 Hash	
Policy Properties						
KeyUsage		True	M			
	KeyCertSign		M	S	True	
	cRLSign		M	S	True	
BasicConstraints		True	M			This extension MUST be marked CRITICAL
	CA		M	S	True	TRUE for CA Certificates

Devices CA Certificate Profile

This is the complete ASN1 description of the certificate associated to the Devices CA.

Field	CE[4]	O/M[5]	CO[6]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280 Also see next part of the table
Signature	False	M			
Algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	UAE Global Root CA G4 E2 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	S		
CountryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)

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

	OrganizationName		M	S	UAE Government	UTF8 encoded
	CommonName		M	S	UAE Global Root CA G4 E2	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using Generalized Time
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + **[96]** Months	
subject		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	Devices Certification Authority	UTF8 encoded
subjectPublicKeyInfo		False	M			
	Algorithm		M	S	RSA	
	SubjectPublicKey		M	D	Public key length: 4096 (RSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	O			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	SHA-1 Hash of the UAE Global Root CA G4 E2 public key	When this extension is used, this field MUST be supported at the 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		O	S	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	S	http://ca-repository.desc.gov.ae/certificate/root.p7b	Root CA Certificate download URL
cRLDistributionPoints		False	M			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea<CRLNumber>.crl	CRL download URL
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
keyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.1.1.1	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	URL location of Root CA CPS	
Basic Constraints		True				
	cA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		M	S	0	

Corporate CA Certificate Profile

This is the complete ASN1 description of the certificate associated to the Corporate CA.

Field	CE[7]	O/M[8]	CO[9]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280 Also see next part of the table
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	UAE Global Root CA G4 E2 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	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	UAE Global Root CA G4 E2	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 + **[96]** Months	
subject	False	M			

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

	countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationName		M	S	UAE Government	UTF8 encoded
	commonName		M	S	Corporate Certification Authority	UTF8 encoded
subjectPublicKeyInfo		False	M			
	algorithm			S	RSA	
	subjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates
	keyIdentifier		M	D	SHA-1 Hash of the UAE Global Root CA G4 E2 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		O	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	S	http://ca-repository.desc.gov.ae/certificate/root.p7b	Root CA Certificate download URL.
cRLDistributionPoints		False	M			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea<CRLNumber>.crl	CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	

	cRLSign		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.1.1.1	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	URL location of Root CA CPS	
BasicConstraints		True				
	cA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		M	S	0	

Government or Private Sector Entity Issuing CA Certificate Profile

The Subscribers' Certificate profile is further described in the following table. All fields of type Directory String are of type UTF8String.

Subordinate CA Certificate Profile					
Field	CE[10]	O/M [11]	CO [12]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280 Also see next part of the table
Signature	False	M			
Algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Issuing 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	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

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

	CommonName		M	S	UAE Global Root CA G4 E2	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 + **[96]** Months	
Subject		False	M			
	Country Name		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	OrganizationUnitName		O	D	Allocated as per certificate request	UTF8 encoded
	OrganizationName		M	D	Allocated as per certificate request	UTF8 encoded
	LocalityName		O	D	Allocated as per certificate request	UTF8 encoded
	CommonName		M	D	Allocated as per certificate request	UTF8 encoded
SubjectPublicKeyInfo		False	M			
	Algorithm		M	S	RSA	
	SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions			M			
Name Constraints					Allocated as per certificate request and subscriber agreement	
NameConstraints		True	O			Mandatory only if Extended Key Usage have id-kp-serverAuth or id-kp-emailProtection bit
permittedSubtrees			M	S	[Permitted Subtrees to be decided case by case based on the end user base of each CA]	
excludedSubtrees			M	S	[Excluded Subtrees to be decided case by case based on the end user base of	

				each CA]	
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash of the Government Entity Root 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		O	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		O	S	“http://ca-repository.desc.gov.ae/certificate/root.p7b”	Root CA Certificate download URL.
cRLDistributionPoints	False	M			
DistributionPoint		M	D	“http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea<CRLNumber>.crl”	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	
Policy Properties					
KeyUsage	True	M			
KeyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage	False	O			
serverAuth I timeStamping I emailProtection I codesigning		M	S	True	**Technical constraint will be applied based on the agreement with the CA business owner**
clientAuthentication		O	S	True	**As per subscriber agreement**
OCSPSigning		O	S	True	**As per subscriber agreement**

CertificatePolicies		False	M			
	PolicyIdentifier		M	D	2.16.784.1.2.2.100.<TBD> Value inserted here dependent on given OID	This is to be discussed at the time of certification
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	HTTP URL location of Root CA CPS	
BasicConstraints		True	M			This extension MUST be marked CRITICAL
	cA		M	S	True	TRUE for CA Certificates
	pathLenConstraint		M	S	0	

Appendix II:

CRL Profile

Certificate List Component	O/M[13]	Value	Comments
CertificateList	M		
tBSCertList	M		see next part of the table
SignatureAlgorithm	M	SHA-256	
SignatureValue	M	Value inserted here dependent on algorithm selected	
tBSCertList			
Version	M	v2	
Signature	M	value inserted here dependent on algorithm selected	
Issuer	M		The issuer field is defined as the X.501 type Name, and MUST follow the encoding rules for the issuer name field in the certificate
CountryName	M	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". Printable String, size 2 (rfc5280)
OrganizationName	M	UAE Government	UTF8 encoded
CommonName	M	UAE Global Root CA G4 E2	UTF8 encoded
ThisUpdate	M	<creation time>	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NextUpdate	M	<creation time + six months>	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
revokedCertificates	O	When there are no revoked certificates, the revoked certificates list MUST BE absent (as per RFC 5280)	
userCertificate		<certificate serial number>	
revocationDate		<Optional revocation time>	

[13] O/M: O = Optional, M = Mandatory.

crlExtensions	M		
authorityKeyIdentifier	M	This MUST be the same value as thez subject Key Identifier field in the CRL Issuer's certificate. Non-critical <subject key identifier CA>	
cRLNumber	M	Non-critical <CA assigned unique number>inversion avec AKI	Monotonically increasing
IssuingDistributionPoint	O		Mandatory for Partitioned RLs
DistributionPoint	M	CN=CRL1 CN=UAE Global Root CA G4 E2 O=UAE Government C=AE	Partitioned CRL directory address
DistributionPoint	M	http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea<CRLNumber>.crl	CRL hosting URL, where <CRL Number> a dedicated sequence number that the CA uses for CRL file naming
onlyContainsCACerts	M	Yes	
onlyContainsUserCerts	M	No	
IndirectCRL	M	No	
expiredCertsOnCRL (2.5.29.60)	O	< a date-time value specifies the date on or after which revoked certificates are retained on the CRL>	

Appendix III:

OCSP Profile

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

Field	CE[14]	O/M[15]	CO[16]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280 Also see next part of the table
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Root 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”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	UAE Government	UTF8 encoded

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

	CommonName		M	S	UAE Global Root CA G4 E2	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 **[12]** 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 OCSP	UTF8 encoded.
	organizationName		M	S	DESC	UTF8 encoded.
	LocalityName		M	S	Dubai	UTF8 encoded.
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	D	SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported at minimum
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	
Ext Key Usage		False	M			
	OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck		False	M	S	05 00	
Certificate Policy Property						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.1.1.1	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	URL location of Root CA CPS	