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_v2.1
Created on	18 May 2017
Revision	2.1
Modified on	08 Apr 2024

Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1	Khawla Hassan	Initial version
12 September 2017	0.2	Khawla Hassan	Minor modifications & Incorporation of Dubai government entity Root CA option
3 November 2017	0.3	Khawla Hassan	Minor modifications to reflect control environment
11 January 2018	0.4	Khawla Hassan	Update 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
1st April 2022	1.6	Khawla Hassan	• Annual review • General enhancements on the document
7 September 2022	1.7	Khawla Hassan	• Correct typographical errors and general enhancements
6 April 2023	1.8	Khawla Hassan	• Annual review • Align the definitions and log retention with the SSL BRs

2nd November 2023	1.9	Khawla Hassan	• Remove the references to SSL BRs and update Definitions • Update the certificates supported under the Devices CA in the PKI hierarchy • Limit permissible EKUs for Government or Private Sector Entity Issuing CA Certificates
10th February 2024	2.0	Khawla Hassan	• Add the authorityInfoAccess extension to the CRL
08 April 2024	2.1	Khawla Hassan	• Annual review • Updates to accommodate the CA/B Forum ballots CSCWG-18

Table of contents

Document History **2**

1. Introduction **10**

1.1 Overview **10**

1.1.1 Dubai PKI Hierarchy 11
1.1.2 Dubai PKI Policy Authority (PA) 12

1.2 Document Name and Identification **13**

1.3 PKI Participants **13**

1.3.1 Certification Authorities 13
1.3.2 Registration Authorities 13
1.3.3 Subscribers 13
1.3.4 Relying Parties 14
1.3.5 Other Participants 14

1.4 Certificate Usage **14**

1.4.1 Appropriate certificate usage 14
1.4.2 Prohibited Certificate Usage 14

1.5 Policy Administration **14**

1.5.1 Organization Administering the Document 15
1.5.2 Contact Person 15
1.5.3 Person Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval Procedures 15

1.6 Definitions and Acronyms **15**

1.6.1 Definitions 15
1.6.2 Acronyms 19

2. Publication and Repository Responsibilities **21**

2.1 Repositories **21**

2.2 Publication of Certificate Information **21**

2.3 Time or Frequency of Publication Repositories **21**

2.3.1 Certificates 21
2.3.2 CRLs 22

2.4 Access Controls on Repositories **22**

3. Identification and Authentication **23**

3.1 Naming **23**

3.1.1 Types of Names 23
3.1.2 Need for names to be meaningful 23
3.1.3 Anonymity and Pseudonymity of Subscribers 23
3.1.4 Rules for Interpreting Various Name Forms 24
3.1.5 Uniqueness of Names 24
3.1.6 Recognition, Authentication and Role of Trademarks 24

3.2 Initial Identity Validation **24**

3.2.1 Method to Prove Possession of Private Key 24
3.2.2 Authentication of Organization Identity 24
3.2.3 Authentication of Individual Identity 25
3.2.4 Non-verified Subscriber Information 25
3.2.5 Validation of Authority 25
3.2.6 Criteria for Interoperation 25

3.3 Identification and Authentication for Re-key Requests 25
3.3.1 Identification and Authentication for Routine Re-Keying 25
3.3.2 Identification and Authentication for Re-Key After Revocation 25
3.4 Identification and Authentication for Revocation Requests 26
4. Certificate Life-Cycle Operational Requirements 27
4.1 Certificate Application 27
4.1.1 Who Can Submit a Certificate Application 27
4.1.2 Enrolment Process and Responsibilities 27
4.2 Certificate Application Processing 29
4.2.1 Performing Identification and Authentication Functions 29
4.2.2 Approval or Rejection of Certificate Applications 29
4.2.3 Time to Process Certificate Applications 30
4.3 Certificate Issuance 30
4.3.1 CA Actions during Certificate Issuance 30
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 30
4.4 Certificate Acceptance 30
4.4.1 Conduct Constituting Certificate Acceptance 31
4.4.2 Publication of the Certificate by the CA 31
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 31
4.5 Key Pair and Certificate Usage 31
4.5.1 Subscriber Private Key and Certificate Usage 31
4.5.2 Relying Party Public Key and Certificate Usage 31
4.6 Certificate Renewal 32
4.6.1 Circumstance for certificate renewal 32
4.6.2 Who may request renewal 32
4.6.3 Processing certificate renewal requests 32
4.6.4 Notification of new certificate issuance to subscriber 32
4.6.5 Conduct constituting acceptance of a renewal certificate 32
4.6.6 Publication of the renewal certificate by the CA 32
4.6.7 Notification of certificate issuance by the CA to other entities 32
4.7 Certificate Re-key 32
4.7.1 Circumstance for Certificate Re-key 32
4.7.2 Who May Request Certification of a New Public Key 32
4.7.3 Processing Certificate Re-Keying Requests 33
4.7.4 Notification of New Certificate Issuance to Subscriber 33
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 33
4.7.6 Publication of the Re-Keyed Certificate by the CA 33
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 33
4.8 Certificate Modification 33
4.8.1 Circumstance for certificate modification 33
4.8.2 Who may request certificate modification 33
4.8.3 Processing certificate modification requests 33
4.8.4 Notification of new certificate issuance to subscriber 33
4.8.5 Conduct constituting acceptance of modified certificate 33
4.8.6 Publication of the modified certificate by the CA 33
4.8.7 Notification of certificate issuance by the CA to other entities 33
4.9 Certificate Revocation and Suspension 34
4.9.1 Circumstances for Revocation 34
4.9.2 Who Can Request Revocation 35
4.9.3 Procedure for Revocation Request 35

4.9.4 Revocation Request Grace Period 36
4.9.5 Revocation Request Response Time 36
4.9.6 Revocation Checking Requirement for Relying Parties 36
4.9.7 CRL Issuance Frequency 36
4.9.8 Maximum Latency for CRLs 36
4.9.9 Online Revocation/Status Checking Availability 36
4.9.10 Online Revocation Checking Requirements 37
4.9.11 Other Forms of Revocation Advertisements Available 37
4.9.12 Special Requirements — Key Compromise 37
4.9.13 Who Can Request Suspension 37
4.9.14 Procedure for Suspension Request 37
4.9.15 Procedure for Suspension Request 37
4.9.16 Limits on Suspension Period 37
4.10 Certificate Status Services 37
4.10.1 Operational Characteristics 37
4.10.2 Service Availability 37
4.10.3 Optional Features 37
4.11 End of Subscription 37
4.12 Key Escrow and Recovery 38
4.12.1 Key Escrow and Recovery Policy and Practices 38
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 38
5. Management, Operational and Physical Controls 39
5.1 Physical Security Controls 39
5.1.1 Site Location and Construction 39
5.1.2 Physical Access 39
5.1.3 Power and air conditioning 39
5.1.4 Water Exposures 39
5.1.5 Fire Prevention and Protection 40
5.1.6 Media Storage 40
5.1.7 Waste Disposal 40
5.1.8 Offsite Backup 40
5.2 Procedural Controls 40
5.2.1 Trusted Roles 40
5.2.2 Number of Persons Required per Task 41
5.2.3 Identification and Authentication of Each Role 41
5.2.4 Roles Requiring Separation of Duties 41
5.3 Personnel Security Controls 41
5.3.1 Qualifications Experience and Clearance Requirements 42
5.3.2 Background Check Procedures 42
5.3.3 Training Requirements 42
5.3.4 Retraining Frequency and Requirements 42
5.3.5 Job Rotation Frequency and Sequence 42
5.3.6 Sanctions for Unauthorized Actions 42
5.3.7 Independent Contractor Requirements 43
5.3.8 Documentation Supplied to Personnel 43
5.4 Audit Logging Procedures 43
5.4.1 Types of Event Recorded 43
5.4.2 Frequency of Processing Log 45
5.4.3 Retention Period for Audit Log 45
5.4.4 Protection of Audit Log 45
5.4.5 Audit Log Backup Procedures 45

5.4.6 Audit Collection System (Internal vs. External) 45
5.4.7 Notification to Event-Causing Subject 46
5.4.8 Vulnerability Assessments 46
5.5 Records Archival 46
5.5.1 Types of Records Archived 46
5.5.2 Retention Period for Archive 46
5.5.3 Protection of Archive 46
5.5.4 Archive Backup Procedures 46
5.5.5 Requirements for Timestamping of Records 47
5.5.6 Archive Collection System (Internal or External) 47
5.5.7 Procedures to Obtain and Verify Archive Information 47
5.6 Key Changeover 47
5.7 Compromise and Disaster Recovery 47
5.7.1 Incident and Compromise Handling Procedures 47
5.7.2 Computing Resources, Software and/or Data Corruption 47
5.7.3 Entity Private Key Compromise Procedures 48
5.7.4 Business Continuity Capabilities after a Disaster 48
5.8 CA or RA Termination 49
6. Technical Security Controls 50
6.1 Key Pair Generation and Installation 50
6.1.1 CA Private Key Pair Generation 50
6.1.1.1 Dubai PKI Root CA 50
6.1.1.2 Subordinate CAs 51
6.1.2 Private Key Delivery to Subscriber 51
6.1.2.1 Dubai PKI Root CA 51
6.1.2.2 Subscribers (Subordinate CAs) 51
6.1.3 Public Key Provisioning 51
6.1.3.1 Dubai PKI Root CA 51
6.1.3.2 Subscribers (Subordinate CAs) 51
6.1.4 CA Public Key Delivery to Relying Parties 51
6.1.5 Key Sizes 51
6.1.6 Public Key Parameters Generation and Quality Checking 51
6.1.7 Key Usage Purposes (As per X.509 v3 Key Usage Field) 52
6.2 Private Key Protection and Cryptographic Module Engineering Controls 52
6.2.1 Cryptographic Module Standards and Controls 52
6.2.2 Private key (m out of n) multi-person control 52
6.2.3 Private Key Escrow 52
6.2.4 Private Key Backup 53
6.2.5 Private Key Archival 53
6.2.6 Private Key Transfer Into or From a Cryptographic Module 53
6.2.7 Private Key Storage on Cryptographic Module 53
6.2.8 Method of Activating Private Key 53
6.2.9 Method of Deactivating Private Key 53
6.2.10 Method of Destroying Private Key 53
6.2.11 Cryptographic Module Rating 54
6.3 Other Aspects of Key Pair Management 54
6.3.1 Public Key Archival 54
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 54
6.4 Activation Data 54
6.4.1 Activation Data Generation and Installation 54
6.4.2 Activation Data Protection 55
6.4.3 Other Aspects of Activation Data 55

6.5 Computer Security Controls 55
6.5.1 Specific Computer Security Technical Requirements 55
6.5.2 Computer Security Rating 55
6.6 Life Cycle Security Controls 55
6.6.1 System Development Controls 56
6.6.2 Security Management Controls 56
6.6.3 Life Cycle Security Controls 56
6.7 Network Security Controls 56
6.8 Timestamping 56
7. Certificates and CRL Profiles 57
7.1 Certificate Profile 57
7.1.1 Version Number(s) 57
7.1.2 Certificate Extensions 57
7.1.3 Algorithm Object Identifiers 57
7.1.4 Name Forms 57
7.1.5 Name Constraints 58
7.1.6 Certificate Policy Object Identifier 58
7.1.7 Usage of Policy Constraints Extension 58
7.1.8 Policy Qualifiers Syntax and Semantics 58
7.1.9 Processing Semantics for the Critical Certificate Policies 58
7.2 CRL Profile 58
7.2.1 Version Number(s) 58
7.2.2 CRL Entry Extensions 58
7.3 OCSP Profile 58
7.3.1 Version Number(s) 59
7.3.2 OCSP Extensions 59
8. Compliance Audit and Other Assessments 60
8.1 Frequency or Circumstances of Assessments 60
8.2 Identity and Qualifications of the Assessor 60
8.3 Assessor's Relationship to Assessed Entity 60
8.4 Topics Covered by Assessment 61
8.5 Actions Taken as a Result of Deficiency 61
8.6 Communication of Results 61
9. Other Business and Legal Matters 62
9.1 Fees 62
9.1.1 A Certificate Issuance or Renewal Fees 62
9.1.2 Certificate Access Fees 62
9.1.3 Revocation or Status Information Access Fees 62
9.1.4 Fees for Other Service 62
9.1.5 Refund Policy 62
9.2 Financial Responsibility 62
9.2.1 Insurance Coverage 62
9.2.2 Other Assets 62
9.2.3 Insurance or Warranty Coverage for End-Entities 62
9.3 Confidentiality of Business Information 63
9.3.1 Scope of Confidential Information 63
9.3.2 Information not within the scope of confidential information 63
9.3.3 Responsibility to protect confidential information 63

9.4 Privacy of Personal Information 63
9.4.1 Privacy plan 63
9.4.2 Information treated as Private 64
9.4.3 Information not Deemed Private 64
9.4.4 Responsibility to protect private information 64
9.5 Intellectual Property Rights 64
9.6 Representations and Warranties 64
9.6.1 CA Representations and Warranties 64
9.6.2 RA Representations and Warranties 65
9.6.3 Subscriber Representations and Warranties 65
9.6.4 Relying Party Representations and Warranties 66
9.6.5 Representations and Warranties of Other Participants 66
9.7 Disclaimers of Warranties 67
9.8 Limitations of Liability 67
9.9 Indemnities 67
9.10 Term and Termination 67
9.10.1 Term 67
9.10.2 Termination 67
9.10.3 Effect of Termination and Survival 67
9.11 Individual Notices and Communications with Participants 67
9.12 Amendments 68
9.12.1 Procedure for Amendment 68
9.12.2 Notification Mechanism and Period 68
9.12.3 Circumstances Under Which OID Must be Changed 68
9.13 Dispute Resolution Procedures 68
9.14 Governing Law 68
9.15 Compliance with Applicable Law 68
9.16 Miscellaneous Provisions 68
9.16.1 Entire Agreement 68
9.16.2 Assignment 68
9.16.3 Severability 69
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 69
9.16.5 Force Majeure 69
9.17 Other Provisions 69
Appendix I 70
The Dubai PKI Root CA Certificate profile 70
Devices CA Certificate Profile 73
Corporate CA Certificate Profile 76
Code Signing CA Certificate Profile 80
Timestamping CA Certificate Profile 83
Government or Private Sector Entity Issuing CA Certificate Profile 86
Appendix II: 90
CRL Profile 90
Appendix III: 92
OCSP Profile 92

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”.

This CPS aims 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 - Network Security
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements

The Dubai PKI is committed to maintain this CPS in conformance with the current versions of the below requirements published at http://www.cabforum.org:

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

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

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

1.1 Overview

The “Dubai PKI” uses standard PKI technologies, policies and operating procedures and application interfaces. The Dubai PKI comprises the Dubai PKI Root CA that is the trust anchor of this PKI, which

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

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

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

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

1.1.1 Dubai PKI Hierarchy

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

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

Issuing CAs that are owned by other Government or private sector entities shall be approved by the Dubai PKI PA under the following conditions:

- the issuing CA(s) must be hosted in Dubai PKI environment and must be operated under the supervision of the Dubai PKI PA,
- the business practices, and services of issuing CA(s) can be defined by owners under the following conditions:
    - the CPS shall comply with this CPS as well as the government or private sector entity issuing CAs CP,
    - the final CPS document but must be approved and published by the Dubai PKI PA.
- the issuing CA(s) must be technically constrained using a combination of extended key usage and name constraint extensions to limit the scope within which the issuing CA may issue end-user certificates,
- the government or private sector entity issuing certificates from its own issuing 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. Those entities must perform regular compliance audits of their own Registration Authorities (RA) to ensure compliance with the applicable identification and authentication requirements,

- the issuing CA(s) certificate(s) SHALL be revoked if the agreement between DESC and the respective government or private sector entities has been terminated,
- the issuing CA(s) certificate(s) validity period is eight years.

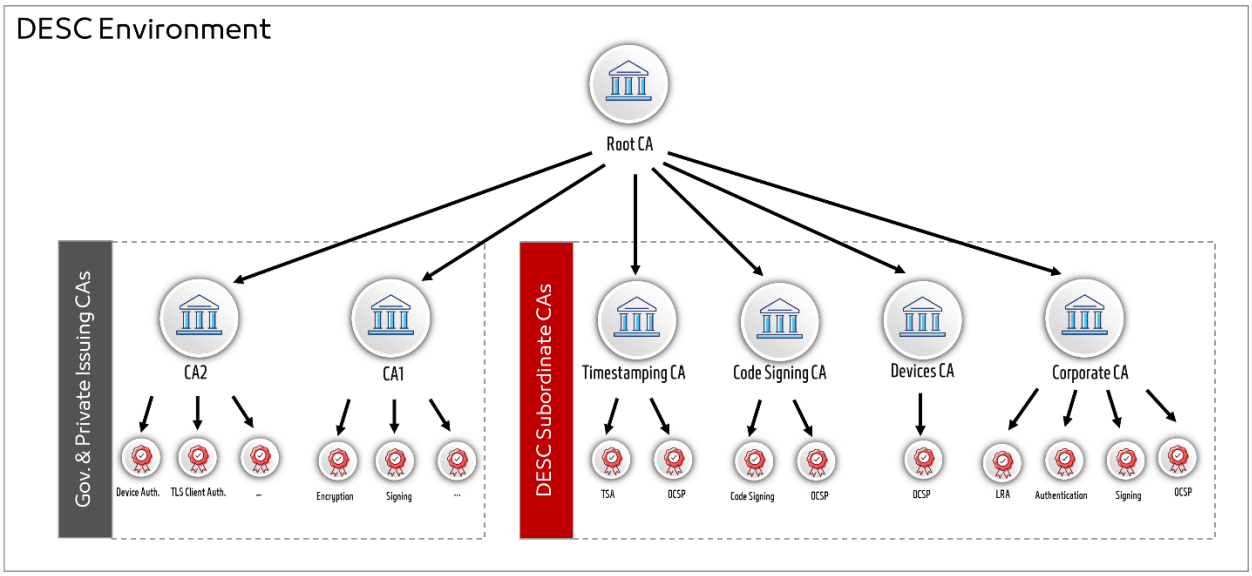

Figure 1: Trust Model for Dubai PKI

1.1.2 Dubai PKI Policy Authority (PA)

The Dubai PKI PA, composed of appointed members of the DESC management and the 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 the regular audit reports of LRAs,
- Enforcing CP/CPS and other policies applicable to Dubai PKI Environment,
- Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CPs/CPSs and related policies,
- Defining the review process that ensures that the Dubai PKI properly implements the above practices,
- Defining the review process that ensures that the related policies are supported by the Dubai PKI CP and CPS documents,
- Publication of CP and CPS documents,
- Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the Dubai PKI,
- Evaluating the proper working of the Dubai PKI environment,

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

1.2 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 Certification Authorities

The Dubai PKI Root CA is the Certification Authority that issues Certificates in accordance with this CP/CPS. The Dubai PKI Root CA is owned and operated by DESC, therefore 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 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 issuing CAs issued to government or private sector entities in accordance to the present Dubai PKI Root CA Certification Practice Statement.

1.3.2 Registration Authorities

The Dubai PKI PA is bearing the responsibility of the RA for Dubai PKI Root CA, which is tasked to request issuance and revocation of a certificate under this CPS. 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 an issuing CA), it is the Dubai PKI PA that validates the request and decide whether or not to request the creation of the CA certificate. See section 3 for further details.

1.3.3 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 issuing CA(s) signed by the Dubai PKI Root CA.

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.

1.3.4 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 (e.g. OCSP or CRL) prior to relying on information featured in such a received certificate.

1.3.5 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 being the trust anchor of the Dubai PKI. The root certificate can be used to:

- Sign subordinate certification authorities within the Dubai 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,
- Sign OCSP certificates for the Dubai Root CA OCSP service.

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 CAs' certificates are used to sign end-entity certificates for the CAs' corresponding 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 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 Person

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.

Certificate Problem Report

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

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

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

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

1.6 Definitions and Acronyms

1.6.1 Definitions

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

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

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

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

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

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

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates as published by the CA/Browser Forum.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's

corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

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

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

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

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

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

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

1.6.2 Acronyms

CA — Certification Authority

CCTV — Closed circuit TV

CP — Certificate Policy

CPS — Certification Practice Statement

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

FQDN — Fully Qualified Domain Name

HSM — Hardware Security Module

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

ITU — International Telecommunications Union

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

DESC — Dubai Electronics Security Center

OID — Object Identifier

OSCP — Online Certificate Status Protocol

OTP — One Time Password

PA — Policy Authority of Dubai PKI

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

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

PKCS # 7 — Cryptographic Message Syntax

PKCS #10 — Certification Request Syntax Specification

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

PKE — Public Key Encryption

PKI — Public Key Infrastructure

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

RA — Registration Authority

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

SCEP — Simple Certificate Enrolment Protocol

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

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

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

SDG — Dubai Smart Government Establishment

UPS — Uninterruptible Power Supply

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

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

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

2. Publication and Repository Responsibilities

2.1 Repositories

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

2.2 Publication of Certificate Information

As part of the public repository, DESC publishes a copy of its self-signed Dubai PKI Root CA certificate, the Dubai Root CA OCSP certificate as well as this CPS.

DESC also retains other documents that make certain disclosures about the Dubai PKI Root CA's practices, procedures, and the content of certain of its policies as part of the public repository. DESC reserves its right to make available and publish information on its policies by any means it sees fit.

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

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

2.3 Time or Frequency of Publication Repositories

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

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.

2.3.1 Certificates

The Dubai Root CA certificate and OCSP Certificates are published to the Certificate Dissemination Webpage that is part of the public repository (https://ca-repository.desc.gov.ae/) as soon as they are issued.

2.3.2 CRLs

DESC maintains 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.

DESC publishes CRLs at regular intervals according to the following rules:

- At 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 lifetime shall be set to six months.

2.4 Access Controls on Repositories

Public read-only access to certificates, CRLs and documentations 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 Need for names to be meaningful

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 convention 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.

DESC Subordinate CAs

For DESC Subordinate CAs, it handled similar to the Dubai Root CA as part of approving the key generations ceremonies by the Dubai PKI PA.

Government and private sector entities CAs

The Dubai PKI PA verifies the Organization's identity as follows:

A. Presence / Legal standing

- Verify the existence of the Organization using an authoritative source that is expected to provide detailed information about the entity including its legal name and address, the most common authoritative source used by DESC RA is the UAE Official Gazette for Government entities and the Chamber of commerce for the private sector entities.
- Verify authority of the Organization's authorized representative requesting the certificate, that shall be an authorized representative from the entity. This can be established either based on the entity's record at the authoritative source or based on a formal communication between DESC and the Government Entity's HR. A face-to-face meeting where at least both the entity representative and a Dubai PKI PA representative are present.

B. Association

The organization name to be inserted in the requested certificate must exactly match the legal name of the entity requesting the CA certificate. The full name or the abbreviated version may be added to the certificate as agreed with the requesting entity.

C. Authority of the applicant

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

3.2.3 Authentication of Individual Identity

The Dubai PKI Root CA does not issue end-entity certificates.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

The authority of the certificate requestor to request a certificate on behalf of an entity will be performed through a reliable means of communication with the entity that include the following steps at minimum:

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

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

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

3.2.6 Criteria for Interoperation

The Dubai PKI Root CA conforms with the following standards to facilitate interoperation:

- X.509 certificates and CRLs in accordance with the profiles listed in this CPS,
- Offers certificate revocation information through X.509 CRLs, in addition to an OCSP responder that complies with RFC 6960.

Any CA wishing to interoperate, join or cross certify with the Dubai PKI Root CA shall adhere to the requirements specified above.

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. This is executed only as part of a regular re-key operation that is approved by the Dubai PKI PA.

3.3.2 Identification and Authentication for Re-Key After Revocation

Same provisions as those defined in sections 3.1 and 3.2 apply. This is executed only as part of a re-key operation that is approved after all investigations are performed by the Dubai PKI PA.

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.

DESC Subordinate CAs

Identification and authentication procedures of revocation requests go through an internal DESC process involving the PKI operations team and the Dubai PKI PA. An investigation report is delivered for the approval of the Dubai PKI PA. If the certificate revocation is due to a key compromise, DESC Disaster Recovery and Business Continuity plan will be executed.

Government and private sector entities Issuing CAs

A formal request is required to be addressed to DESC by the same government or private sector entity that performed the initial application. The revocation request is initiated by an authorized representative. Using an authoritative source (Official Gazette) or through formal communication with the applying entity, the Dubai PKI PA validate the representative's authority to request the CA certificate revocation.

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 Dubai PKI PA. Such events must always be authorized in a written form by a document signed by at least two members of the Dubai PKI 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, except for the circumstances specified in section 4.9.1 where DESC may decide on its own to revoke concerned certificate(s).

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

DESC Subordinate CAs

DESC Subordinate CAs are established as part of internal DESC processes. The Dubai PKI PA approves and plan the ceremonies for certification of DESC Subordinate CAs.

Government and private sector entities CAs

A dully authorized representative submits the certificate application as part of the overall process through which the entity is authorized by the Dubai PKI PA to have its issuing CA under the Dubai PKI Root CA.

4.1.2 Enrolment Process and Responsibilities

DESC Subordinate CAs

DESC Subordinate CAs are established as part of internal DESC processes. The Dubai PKI PA approves and plan the ceremonies for certification of DESC Subordinate CAs.

Government and private sector entities CAs

The entity's authorized representative will issue to the Dubai PKI PA a request for certificate issuance in a form of certificate application submitted along with a signed subscriber agreement. The Dubai PKI PA acts as the RA that has the authority and is designated to approve the request under the following conditions:

- Authentication of the government or private sector entity and its authorized representative as specified in section 3.2.2,
- Proper justification of establishing a dedicated issuing CA(s) for the requesting entity,
- Issuing CA(s) must be hosted in Dubai PKI environment and must be operated under the supervision of the Dubai PKI PA,
- Business practices, and services of issuing CA(s) can be defined by owners under the following conditions:
    - the CPS shall comply with the Dubai PKI Root CA CPS (this document),
    - the final CPS document but must be approved and published by the Dubai PKI PA. Approval activities consist of evaluation of the policies and procedures defined by the certification authority, including but not limited to:
        - The certification authority hierarchy, certificate(s) type(s) and certificate(s) profile(s)
        - Processes and controls in place to maintain logical, physical and environmental security
        - Cryptographic modules used to generate, store and manage crypto keys
- Note: The Dubai PKI PA can alternatively take the ownership of producing the CPS according to the entity's business requirements.
- Issuing CA(s) must be technically constrained using a combination of Path Lengths, Extended Key Use and Name Constraints extensions to limit the scope within which the issuing CA may issue end-user certificates,
- The 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. These practices shall conform to the rules and requirements as stated in this policy document, compliance audit requirements and requirements of the applicable agreements,
- The government or private sector entity must perform regular compliance audits of their own Registration Authorities (RA) to ensure compliance with the applicable identification and authentication requirements. Audit results shall be shared with the Dubai PKI PA,
- The issuing CA(s) certificate(s) SHALL be revoked if the agreement between DESC and the respective government or private sector entities has been terminated,
- The issuing CA(s) certificate(s) validity period is eight years,
- The Government/Private entities is responsible for informing Dubai PKI in at least the following cases:
    - Significant changes to its certification requirements,
    - Incidents, termination or compromise related to the certification services.
- The key responsibilities of Dubai PKI regarding operation of issuing CAs are as follows:
    - Supervision of the certificates management operated by the entity and/or its RAs, including but not limited to all aspects related to application, issuance and revocation,

- Publication of public certificate information to a public repository as specified in section 2 of the Dubai Root CA CPS,
- Technical operations of the CA/RA systems,
- Maintaining and providing certificates status information through publicly available Certificate Revocation List (CRL) and OCSP mechanisms.

- The issuing CA(s) can support any of the following pre-defined certificate types for issuance:
  - SSL/TLS server authentication certificate for public Web Sites and IP addresses that belongs to the entity owning the CA,
  - Device certificates (non-SSL certificates) for general identification, authentication or session data encryption of generic devices owned or operated by Government/Private entities,
  - End-user certificates: certificates for encryption, authentication and digital signatures for individuals.

Where applicable, the above conditions shall be added to the subscriber agreement signed by the Entity Appling for the Issuing CA(s).

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

DESC Subordinate CAs

DESC Subordinate CAs are established as part of internal DESC processes. The Dubai PKI PA approves and plan the ceremonies for certification of DESC Subordinate CAs.

Government and private sector entities CAs

As soon as a certificate application is received, The Dubai PKI PA performs the following identification and authentication:

a) Blacklist check, If the requestor/entity is in the blacklist, the certificate application is rejected, *Any malicious certificate or revocation request or a request that fails multiple (more than 3) times is added to DESC blacklist.*

b) Verify the identity of the organization, authorized representative and the requester as specified in section 3.2.2,

c) Verify the signed approval is received from the authorized representation though a signed certificate request form and certificate subscriber agreement,

d) Verify that the legal name of the entity requesting a certificate and the organization name to be inserted in the requested certificate are matching. The full name or the abbreviated version may be added to the certificate as agreed with the requesting entity.

All above activities (e-mail communication, phone calls, vetting evidence) are stored along with the certificate application.

4.2.2 Approval or Rejection of Certificate Applications

DESC Subordinate CAs

DESC Subordinate CAs are established as part of DESC internal processes. The Dubai PKI PA authorizes the setup of these CAs after validating that all pre-requisites are met including the fulfilment of all compliance verifications.

Government and private sector entities CAs

Once the identification and authentication as done as described in section 4.2.1 and an authorization granted by the Dubai PKI PA as described in section 4.1.2, the Dubai PKI PA shall 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.

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 subordinate CA signing ceremony.

The Dubai PKI Root CA trusted operatives/key custodians 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 ceremony auditor/witness and Dubai PKI Root CA key custodians, so that the trusted operatives can proceed further with the certificate issuance.

The CA processes certificate request provided that:

- Identity verification is done for all the ceremony attendees,
- The certificate request is validly formatted (shall be in PKCS#10 format),
- The certificate request contains valid subscriber data as per the certificate application.

During the ceremony, the CA trusted operatives direct commands for the Dubai PKI Root CA to perform a certificate signing operation.

Following the successful completion of the ceremony and the issuance of the CA certificate, the CA trusted operatives and ceremony auditor/witness inspect the file contents and performs a verification against the expected certificate format. For the Government and private sector entities CAs, one or more entity representative will be attending the ceremony and will participate in reviewing the content of the certificate against the certificate request.

The certificate is then handed over to the PKI operations team for further processing and import into the target subordinate CA systems. A printout of the issued certificate footprint is added to the ceremony script before singing it off by all the ceremony attendees.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Once the certificate is issued, CA trusted operatives ensure 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 public repository and handover a copy to the subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Following the successful completion of the ceremony and the issuance of the CA certificate, the CA trusted operatives and ceremony auditor/witness inspect the file contents and performs a verification against the expected certificate format.

Further, the certificate is considered as formally accepted if successfully imported to the target subordinate CA systems. The certificate is then published on the public repository.

In case issues are raised in relation to certificate contents, or to the acceptance of the certificate by the target systems, The Dubai PKI PA will be notified to plan and execute another ceremony in coordination with all relevant parties.

4.4.2 Publication of the Certificate by the CA

Following issuance of a certificate, DESC posts an issued certificate on the public 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 the subscriber agreement:

- Providing correct and up-to-date information as part of its application,
- Refrain from using the certificate outside its validity period or after it has been revoked,
- 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,
- Notifying the Dubai PKI PA immediately if any details in the certificate become invalid,
- Not 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.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate Re-key

Certificate Re-key is the act of re-issuing a certificate for an existing subscriber such that all the identifying information from the old certificate is duplicated in the new certificate, however there is a different 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 original certificate may be revoked after re-key is complete, however, the original certificate must not be further re-keyed.

4.7.2 Who May Request Certification of a New Public Key

As per initial certificate issuance.

4.7.3 Processing Certificate Re-Keying Requests

As per initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per initial certificate issuance.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

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

4.8.2 Who may request certificate modification

Not applicable. Refer to section 4.8.1.

4.8.3 Processing certificate modification requests

Not applicable. Refer to section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

As per initial certificate issuance.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable. Refer to section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

As per initial certificate issuance.

4.8.7 Notification of certificate issuance by the CA to other entities

As per initial certificate issuance.

4.9 Certificate Revocation and Suspension

Suspension of 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 valid 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 DESC subordinate CAs, 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 by the Dubai PKI PA based on the following events:

1. Having received a certificate revocation request from the subscriber,
2. Notification of the subscriber that the original certificate request was not authorized and does not retroactively grant authorization,
3. Obtained an evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate is no longer complies with the requirements of Baseline Requirements Sections 6.1.5 and 6.1.6,
4. There has been a loss, theft, modification, unauthorized disclosure or other compromise of the private key of the certificate subject,
5. Obtained an evidence that the Certificate was misused,
6. Got notified that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the applicable Certificate Policy or Certification Practice Statement,
7. Determined that any of the information appearing in the Certificate is inaccurate or misleading,
8. DESC ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate,
9. The Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated,
10. There has been a modification of the information contained in the certificate of the certificate subject,
11. Revocation is required by this Certificate Policy/Certification Practice Statement,

12. 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),
13. The Government Or the private sector entity did not successfully complete the regular compliance audits of their own Registration Authorities (RA), and there is documented evidence shows that the entity misused its issuing CA certificate, or didn't operate continuously in accordance with the provisions of this CPS and the government or private sector entity issuing CAs CP, leading the Dubai PKI PA to conclude that the identified issues cause an unacceptable risk to the compliance of the Dubai PKI against applicable requirements (WebTrust / CA/Browser Forum).

Whenever any of the above circumstances occur, a PA meeting is organized no later than twenty-four (24) hours after the circumstances of certificate revocation were identified. The outcome of this meeting is the validation of the circumstances triggering the Subordinate CA certificate revocation request and the related revocation reason. The Dubai PKI PA may request additional information/evidence which shall be provided within a maximum of seventy-two (72) hours by the operations team. At the end of this process, the Subordinate CA certificate revocation is approved by the Dubai PKI PA.

The certificate revocation ceremony is planned and executed no later than seventy-two (72) hours after the CA certificate revocation is approved by the Dubai PKI PA. The outcome of the ceremony shall be as follows:

- The Subordinate CA certificate is revoked (with the decided revocation reason),
- A CRL is generated by the Dubai PKI Root CA, placed on the public repository, and made immediately available for relying parties,
- The Dubai PKI PA publishes a notice on its repository containing the details of the certificate being revoked and the revocation circumstances,
- The Dubai PKI PA communicates with the subscriber (CA owner) and other relevant stakeholders,
- The Dubai PKI Root CA ensure that all communication, reports, and evidence in relation to the certificate revocation operation is recorded and archived for future use as part of audit processes.

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 the CA key).

Revocation 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 procedure for a 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. A Dubai PKI PA meeting is organized as described in section 4.9.1 to authenticate the request then plan the revocation ceremony involving the Dubai PKI Root CA,
3. The CA produces a new CRL which is published to its repository, the CA also pushes the revocation status to the OCSP service,
4. DESC notifies the subscriber via email on the completion of revocation,
5. If applicable based on the circumstance of revocation, DESC may update their internal blacklist with details of the revoked certificate and/or the subscriber's details.

4.9.4 Revocation Request Grace Period

There shall be no revocation grace period. Revocation requests are processed by DESC RA timely after a decision for revocation is made and within the timeframes listed under section 4.9.1.

4.9.5 Revocation Request Response Time

For certificate problem reports, The Dubai PKI PA begins investigations within 24 hours from receiving the report. DESC initiates communication with the Subscriber and where appropriate, with other concerned authorities. A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

The Dubai PKI PA performs further investigations involving the subscriber and other relevant authorities to decide on the action to be taken on the subject certificate. If the investigations results led to one of the certificate revocation circumstances listed in section 4.9.1, then the certificate within the timeframe set forth in Section 4.9.1.

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

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

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

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

4.9.10 Online Revocation Checking Requirements

The Dubai PKI Root CA OCSP responder supports both HTTP GET and HTTP POST methods.

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation — this section intentionally left blank.

4.9.12 Special Requirements — Key Compromise

If the Dubai PKI PA discovers, or has a reason to believe, that there has been a compromise of the Dubai PKI Root CA private key, this will be considered as a disaster scenario where DESC Disaster Recovery and Business Continuity plan is invoked.

4.9.13 Who Can Request Suspension

Not applicable.

4.9.14 Procedure for Suspension Request

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

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 at least 99% per year.

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

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.

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by this CA.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. 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. Further, access to the enclave where the Dubai PKI systems are hosted is enabled only if two trusted employees are present to open the enclave's door.

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

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

5.1.3 Power and air conditioning

The secure enclave 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.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Offsite Backup

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

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, and security officers or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives). The following are the trusted roles for a Dubai PKI Root CA:

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

- PKI administrator
- System administrator
- PKI operator
- System administrator

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

5.2.2 Number of Persons Required per Task

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

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

- physical access to the secure enclave where the CA systems are hosted,
- access to and management of CA cryptographic hardware security module (HSM),
- validate and authorize the issuance of certificates.

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

5.2.3 Identification and Authentication of Each Role

Before carrying out the responsibilities of a trusted role:

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

5.2.4 Roles Requiring Separation of Duties

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

Prior to the commencement of employment of a DESC PKI personnel, whether as an employee, agent, or an independent contractor, DESC ensures that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such checks include:

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

5.3.2 Background Check Procedures

DESC conducts background investigations for 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 and vetting (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

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

DESC sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the Dubai PKI Root CA personnel, as it

might be appropriate under the circumstances and as per the prevailing HR Policy and the applicable Dubai Law.

5.3.7 Independent Contractor Requirements

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

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

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

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

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

DESC ensures that at least the following details are recorded:

- CA key lifecycle management events, including:
    - Key generation, backup, storage, recovery, archival and destruction,
    - Cryptographic device lifecycle management events.
- CA and Subscriber Certificate lifecycle management events, including:
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles,
    - Certificate requests, 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.

5.4.3 Retention Period for Audit Log

The audit logs are retained for at least two years:

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

These may be made available to auditors upon request.

5.4.4 Protection of Audit Log

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

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

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the 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)

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

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

DESC conducts an annual Risk Assessment that:

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

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

5.5 Records Archival

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for 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

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

To support revocation management of issued certificate, the old CA private keys are maintained until such time as all relying certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

Apart from the circumstance of key compromise, DESC specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing Resources, Software 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, DESC triggers the Key compromise and CA termination plans detailed as part of DESC Business continuity and disaster recovery plan.

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

5.7.4 Business Continuity Capabilities after a Disaster

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

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

Failover scenarios to the Dubai PKI Root CA disaster recovery location are made possible considering the policy in place for replicating the Dubai PKI Root CA backup to the disaster recovery site as part of any ceremony involving the Dubai PKI Root CA.

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:

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

5.8 CA or RA Termination

If DESC determines that termination of this CA services is deemed necessary, the CA termination plan shall be executed and it shall cover the following actions:

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

6. Technical Security Controls

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

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

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:

- The key generation ceremony is subject to the formal authorization of the Dubai PKI PA
- The key generation ceremony is conducted in presence of a combination of authorized personnel with trusted roles including the Dubai PKI PA representatives
- The 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 Qualified Auditor issues 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

The 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 the corresponding 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 (Subordinate CAs)

The Subordinate CA private key is generated during the Key Ceremony procedure as ruled in a documented procedure.

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)

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

6.1.4 CA Public Key Delivery to Relying Parties

DESC will publish the CAs’ 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)

Private Keys corresponding to the Dubai Root CA Certificates are not used to sign Certificates except in the following cases:

- Self-signed Certificates to represent the Dubai Root CA itself,
- Certificates for Subordinate CAs,
- And certificates for the Dubai Root CA OCSP responder.

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 (m out of n) multi-person 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 Dubai PKI Root CA private keys shall be backed up within backup devices that meet the same certification level as the Dubai PKI Root CA HSM and as described in section 6.2.1. Backup operations are executed as part of the Dubai PKI Root CA generation ceremonies. The Dubai PKI Root CA key is backed up under the same multi-person control and split knowledge as the primary key.

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

Trusted operatives or key custodians participate in the transport operation, which is escorted by an auditor. The backup is be stored in a locked safe at the disaster recovery site.

6.2.5 Private Key Archival

No stipulation – this section is intentionally left blank.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The Dubai PKI Root CA key shall only be transferred to another hardware cryptographic device, for backup purposes, of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control. At no time should the CA private key be copied to disk or other media during this operation.

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

The Dubai PKI Root CA private keys remain under m out of n multi-person 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.

6.2.9 Method of Deactivating Private Key

The HSMs used for the Dubai PKI Root CA key ceremony are deactivated at the end of the ceremony which prevents any further use of the Dubai PKI Root CA private keys. This activity applies to the principles of dual control and split knowledge and shall always be witnessed by the relevant personnel (The Dubai PKI PA, auditor). The HSMs are safely powered off at the end of the ceremony, and all material used during the ceremony are stored inside a dedicated safes inside the secure enclave.

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,
- The Subordinate CAs' certificates are valid for eight years by default. However, if a new certificate is issued to a Subscriber during the period of validity of the Subordinate CA (e.g., if a Subscriber renews its key pair), the new certificate validity will be aligned to the remaining duration lifetime of the Subordinate CA.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

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.

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

6.4.2 Activation Data Protection

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

6.4.3 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:

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

6.5.2 Computer Security Rating

No stipulation — this section 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

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

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

The CA hardware or software shall be tested, deployed and configured in accordance with industry best practices and vendor recommendations. All changes on the Dubai PKI Root CA systems is done as part of the a formal ceremony approved and planned by the Dubai PKI PA.

6.6.2 Security Management Controls

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

The Dubai PKI Root CA equipment is scanned for malicious code on first use and periodically thereafter. Authorized personnel must ensure up-to-date virus definition databases in place before each NR-CA usage.

Refer to section 6.6.1 for further details.

6.6.3 Life Cycle Security Controls

No stipulation — this section intentionally left blank.

6.7 Network Security Controls

The Dubai PKI 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 online systems supporting the Root CA operations such as the public repository and OCSP responder, 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.

The Dubai PKI PA ensures regular vulnerability testing is conducted on the Dubai Root CA online services. The Dubai PKI PA also ensures that at least once a year, a penetration testing is conducted on the online services by an independent third-party.

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

The Dubai PKI Root CA meets the technical requirements set forth in Section 2.2 – Publication of Information, Section 6.1.5 – Key Sizes, and Section 6.1.6 – Public Key Parameters Generation and Quality Checking of the CA/Browser Baseline Requirements.

The Dubai PKI Root CA generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

Certificate profiles are specified in Appendix–I.

7.1.1 Version Number(s)

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

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 CPS. 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

X.509v3 standard OIDs is used. Algorithm must be RSA encryption for the subject key and SHA256withRSA encryption for the certificate signature.

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, yet it will used for the issuing CAs owned by government and private sector entities where the CA certificate will support of id-kp-serverAuth usage to its subscribers.

Appendix I shows detailed profiles.

7.1.6 Certificate Policy Object Identifier

The Dubai PKI Root CA uses certificate policy object identifiers that are defined as part of OID scheme for the Dubai PKI.

Refer to Appendix I of this CPS for the profiles of the certificates issued by the Dubai PKI Root CA including the values of the OID identifiers.

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.

Refer to Appendix I of this CPS for the profiles of the certificates issued by the Dubai PKI Root CA including the used policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies

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

7.2 CRL Profile

Certification status information is provided through certificate revocation lists (CRLs), in conformance with RFC 5280.

CRL profiles are described in Appendix–II.

7.2.1 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

The CRL extensions contain the CRL Number (a sequential number incremented with each new CRL produced). Please refer to Appendix–II of this CPS for the other supported extension in the CRLs issued by the Dubai PKI Root CA.

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960.

OCSP certificate profile is described in Appendix–III.

7.3.1 Version Number(s)

The OCSP responder issues OCSP responses of version 1.

7.3.2 OCSP Extensions

No stipulation — this section intentionally left blank.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessments

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

DESC also perform an internal audit at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. This internal audit is part of the Dubai PKI management cycle, and remediation for the audit findings is implemented by the CA operations team in a timely manner.

8.2 Identity and Qualifications of the Assessor

To carry out the audits, there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with DESC or any person having any conflicting interests thereof.

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 WebTrust criteria specified in section 8.4,
- 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.

8.3 Assessor’s Relationship to Assessed Entity

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

8.4 Topics Covered by Assessment

The Dubai PKI Root CA is audited for compliance to the following standards:

- WebTrust Principles and Criteria for Certification Authorities,
- WebTrust Principles and Criteria for Certification Authorities — Network Security,
- WebTrust Principles and Criteria for Certification Authorities — Publicly Trusted Code Signing Certificates.

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

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

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

9. Other Business and Legal Matters

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

9.1 Fees

9.1.1 A Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Service

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

9.1.5 Refund Policy

Charged fees cannot be refunded.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

DESC considers the following as confidential information:

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

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of Personal Information

9.4.1 Privacy plan

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

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

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

DECS does not release any confidential information without the consent of the legitimate data owner or explicit authorization by a court order. When DESC releases private information, DESC ensures through reasonable means that this information is not used for any purpose apart from the requested purposes. Parties requesting and receiving confidential information are granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third-parties. Also, these parties are bound to observe personal data privacy rules in accordance with the UAE applicable laws.

DESC respects all applicable privacy, confidential information, and trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention and disclosure of non-public information.

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

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

9.4.2 Information treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to protect private information

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

9.5 Intellectual Property Rights

DESC owns and reserves all intellectual property rights associated with its own databases, web sites, the 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

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

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

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

- **Compliance:** The Dubai PKI Root CA has complied with the Baseline Requirements for Code Signing and the applicable Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate and operating its PKI or Signing Service;
- **Identity of Subscriber:** At the time of issuance, the Code Signing CA represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 3.2 of this document, (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the applicable Certificate Policy or Certification Practice Statement;

- **Authorization for Certificate:** That, at the time of issuance, the Dubai Root CA
  I. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject,
  II. followed the procedure when issuing the Certificate, and
  III. accurately described the procedure in this CPS.
- **Accuracy of Information:** That, at the time of issuance, the Dubai Root CA
  I. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate,
  II. followed the procedure when issuing the Certificate, and
  III. accurately described the procedure in this CPS.
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the Dubai PKI Root CA
  I. implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2,
  II. followed the procedure when issuing the Certificate,
  III. accurately described the procedure in this CPS.
- **Subscriber Agreement:** That, if the Dubai Root CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use.
- **Status:** That the Dubai Root CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.
- **Revocation:** That the Dubai Root CA will revoke the Certificate for any of the reasons specified in these Requirements.

9.6.2 RA Representations and Warranties

The Dubai PKI PA warrant that it performs registration functions as per the stipulations specified in this CPS.

9.6.3 Subscriber Representations and Warranties

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

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

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

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

The Subscriber Agreement or Terms of Use contains provisions imposing the following obligations and warranties:

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to DESC, both in the certificate request and as otherwise requested by DESC in connection with the issuance of the Certificate(s) to be supplied by the Dubai PKI Root CA,
- **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the activation data under the subscriber's custody for Private Key that corresponds to the Public Key to be included in the requested Certificate(s),
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy,
- **Use of Certificate**: To use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement,
- **Reporting and Revocation:** An obligation and warranty to:
    - promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
    - promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness:** An obligation to respond to DESC's instructions concerning Key Compromise or Certificate misuse within a specified time period**.**
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that DESC is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CPS, or the Baseline Requirements.

9.6.4 Relying Party Representations and Warranties

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

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

- Profit loss,
- Loss of data,
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures,
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant or if it is the result of negligence or with intent to deceive DESC, the 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

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

In the event of a conflict between the Baseline Requirements and any regulation in Dubai, DESC may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Dubai. This applies only to operations or certificate issuances that are subject to that Law. In such event, DESC will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by DESC. DESC will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS. Any modification to DESC practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other Provisions

Not applicable.

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-alpha-2 code elements”.

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

						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_root_ca_g4_e2_uae_government_ae_crlfile.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	
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)
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

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

					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-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.crt	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	
extendedKeyUsage		False	M			
	serverAuth		M	S	True	
	clientAuth		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

Field	CE[7]	O/M[8]	CO[9]	Value	Comment
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.crt	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	
ExtendedKeyUsage	False	M			

Field	CE[7]	O/M[8]	CO[9]	Value	Comment
clientAuth		M	S	True	
Microsoft Document Signing (1.3.6.1.4.1.311.10.3.12)		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	

Code Signing CA Certificate Profile

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

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	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			

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

Field	CE[10]	O/M[11]	CO[12]	Value	Comment
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	PrintableString
commonName		M	S	Code Signing Certification Authority	PrintableString
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.crt	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	
ExtendedKeyUsage	False	M			

Field	CE[10]	O/M[11]	CO[12]	Value	Comment
codeSigning		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	
certificatePolicies	False	O			
policyIdentifier		M	S	2.23.140.1.4.1	
BasicConstraints	True				
cA		M	S	True	TRUE for CA Certificates
pathLenConstraint		M	S	0	

Timestamping CA Certificate Profile

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

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

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

Field	CE[13]	O/M[14]	CO[15]	Value	Comment
countryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	UAE Government	PrintableString
commonName		M	S	Timestamping Certification Authority	PrintableString
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	

Field	CE[13]	O/M[14]	CO[15]	Value	Comment
ExtendedKeyUsage	False	M			
timeStamping		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	
certificatePolicies	False	O			
policyIdentifier		M	S	2.23.140.1.4.2	
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[16]	O/M [17]	CO [18]	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
CommonName		M	S	UAE Global Root CA G4	UTF8 encoded

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

					E2	
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 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-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.crt”	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			
	clientAuthentication | Microsoft Document Signing (1.3.6.1.4.1.311.10.3.12)		M	S	True	**Technical constraint will be applied based on the agreement with the CA business owner**
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[19]	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>	
crlExtensions	M		

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

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>	
authorityInfoAccess	M		
AccessMethod	M	Id-ad-2 2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
accessLocation	M	http://ca-repository.desc.gov.ae/certificate/root.crt	Root CA certificate download URL

Appendix III:

OCSP Profile

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

Field	CE[20]	O/M[21]	CO[22]	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
CommonName		M	S	UAE Global Root CA G4	UTF8 encoded

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

					E2	
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	