Dubai Electronic Security Center

Dubai PKI

Government and Private Sector entity issuing CA Certificate Policy

Project	DESC CA Project
Title	Government and Private Sector entity issuing CA Certificate Policy
Classification	PUBLIC
File Name	Dubai PKI - Government and Private Sector entity issuing CA- Certificate Policy_v1.7
Created on	22 August 2017
Revision	1.7
Modified on	6th April 2023

Document History

Date	Revision	Author(s)	Summary
11 September 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 and naming conventions
30 January 2018	1.0	Khawla Hassan	Issue final version
25 April 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	Added the minimal restriction on subscriber key generation as per the BRs
11 April 2021	1.4	Khawla Hassan	Annual review, addressing Mozilla comments, and updating new delivery model for government and private sector SubCAs
1st April 2022	1.5	Khawla Hassan	• Annual review • General enhancements on the document
7th September 2022	1.6	Khawla Hassan	Correct typographical errors and general enhancements
6 April 2023	1.7	Khawla Hassan	• Annual review • Add more clarifications on the time limits for re-use of validation information

			• Align the definitions and log retention with the SSL BRs

Table of contents

1. Introduction

This Certificate Policy (CP) defines the requirements applicable to Government and Private Sector Entities Issuing CAs Government/Private entities, referred to as “Government and Private Sector Government/Private entity issuing CAs”. These are the Government and Private sector Entities that own their own subordinate CAs for issuing end-entity certificates to their subscribers (those entities are referenced hereinafter in this document as the Government/Private sector Entities). Operation of these CAs is the responsibility of DESC as part of the overall Dubai PKI infrastructure.

The PKI Certification services shall be offered by Government and Private sector entities CAs in accordance with the present CP and a dedicated Certification Practice Statement (CPS) for each Issuing CA.

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

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

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

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

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

Further information about this document can be obtained from the Dubai PKI Policy Authority (PA), which is representing the policy and governing body for the Dubai PKI including Government and Private Sector Government/Private entity issuing CAs. Contact information of the Dubai PKI PA is provided under section 1.5.

1.1 Overview of Dubai PKI

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

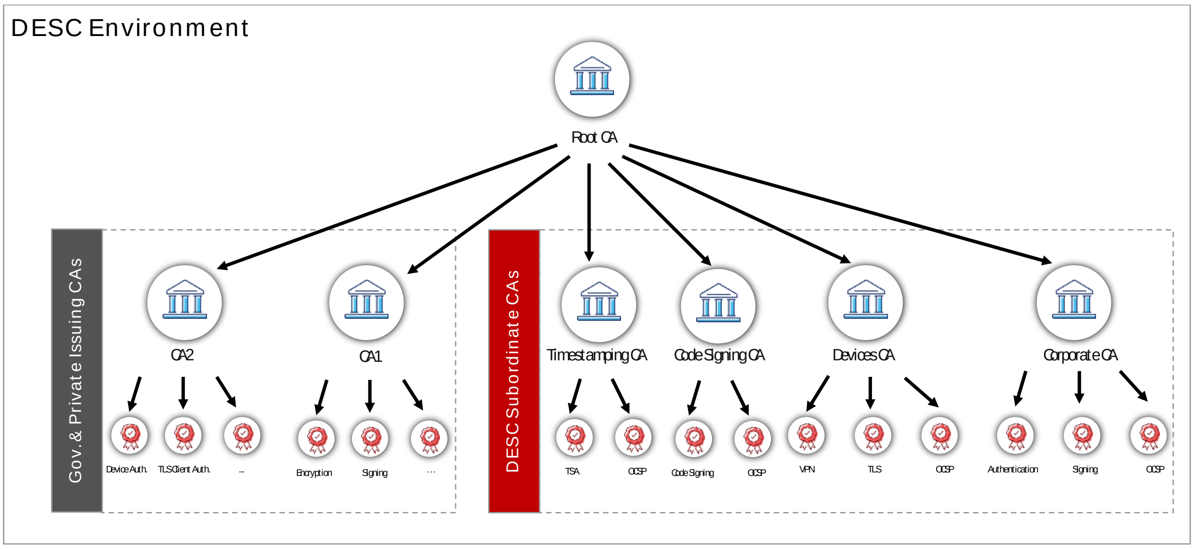

Figure 1: Trust Model for Dubai PKI

1.1.2 Dubai PKI Policy Authority (PA)

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

- Specifying and approving the Dubai PKI infrastructure,
- Approving Government/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,
- Enforcing CP/CPS and other policies applicable to Dubai PKI Environment,
- Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CPs/CPSs and related policies,
- Defining the review process that ensures that the Dubai PKI properly implements the above practices,
- Defining the review process that ensures that the related policies are supported by the Dubai PKI CPs and CPSs,
- Publication of CP and CPS documents,
- Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the Dubai PKI,
- Evaluating the proper working of the Dubai PKI environment,
- Allocating members to the key ceremonies as witness as well as trusted operatives and key custodians,
- Evaluating changes to the Dubai PKI environment (management, operational, hardware, software and security),
- Evaluating case-by-case issues where key Dubai PKI staff/personnel did not respect the security and/or operational procedures, including ethics,
- Deciding on critical issues in case of incidents, disasters and other severe problems with regards to the Dubai PKI.

1.1.3 Certificate Policy

X.509 certificates issued by the Government and Private Sector Government/Private entity issuing CAs to subscribers will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a Certificate is trusted for a particular purpose. Subscriber Certificates issued by the Subordinate CAs will identify the applicable policy in the certificate Policies extension by including applicable OID(s).

1.1.4 Relationship Between the This CP and each Subordinate CA CPS

The Government and Private Sector Government/Private entity issuing CAs CPSs establish the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued those CAs as governed by this CP and related documents which describe the Dubai PKI requirements and use of Certificates.

1.2 Document name and Identification

This document is named ‘Dubai PKI - Government and Private Sector entity issuing CA Certificate Policy’ and is referenced as such in related documents.

The Object Identifier (OID) of this document is 2.16.784.1.2.2.100.1.1.2.2.

1.3 PKI Participants

The participants within the context of Government/Private sector Entities issuing CAs shall be as follows:

- The Dubai PKI Policy Authority (PA)
- Government/Private sector Entities issuing CA
- Registration Authority (RA)
- Subscribers
- Relying Parties

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

1.3.1 Certification Authorities

The Government/Private sector Entities issuing CAs are owned by the corresponding authorized Government/Private sector Entities. Each entity is required to define the practices and/or other requirements applicable to its issuing CA(s) that will be documented as part of a Certification Practice Statement, implementing this Certificate Policy. This CP is subject to approval by the Dubai PKI PA.

1.3.2 Registration Authority

The Government/Private sector Entities shall set up once or more RA for their issuing CAs. The RA shall comprise the individuals and systems involved in validating the identity of individuals requesting certificates, as well as in issuing and managing these certificates.

The RA consists in Registration Authority officers, products, systems, and procedures used to validate the identity of subscribers requesting the issuance of certificates from the issuing CAs. Involvement in the RA shall be limited to duly authorized individuals with the required clearance and other personal controls as stated in section 5.3 of this document.

1.3.3 Subscribers

Subscribers of the Government/Private sector Entities issuing CA must be listed within the Certification Practice Statement for the given CA.

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

1.3.4 Relying Parties

A Relying Parties are entities that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber’s certificate issued by the Government/Private sector Entities issuing CAs.

Relying parties shall always verify the validity of a digital certificate issued by the Government/Private sector Entities issuing CAs using the provided Certificate Validations Services (e.g. CRL, OCSP), prior to relying on information featured in the certificate.

1.3.5 Other Participants

There are no other participants within the context of the Government/Private sector Entities issuing CAs.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

Use of certificates issued from the Government/Private sector Entities issuing CAs is restricted by using certificate extensions on key usage and extended key usage, which will be configured according to the certificate type.

The CPS of each respective issuing CA shall specify the restrictions that apply to each type of certificate. The agreement between DESC and the Government/Private entity will specify the types of end-entity certificates allowed to be issued by each Government/Private entity.

1.4.2 Prohibited Certificate Use

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

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 CP only when they are addressed to the PA.

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CP Approval Procedures

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

In an effort to maintain credibility and promote trust in this CP and better correspond to accreditation and legal requirements, the Dubai PKI PA shall review this CP 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 CP.

1.6 Definitions, Acronyms and References

1.6.1 Definitions

Anti-Malware Organization: An entity that maintains information about Suspect Code and/or develops software used to prevent, detect, or remove malware.

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 CP, the applicants are Government entities subscribing to the 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 CP, 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.

Authorization Domain Name: Authorization Domain Name: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." From the left-most portion of the Wildcard Domain Name to yield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

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.

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

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

CAA: From RFC 8659 (http://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

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

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

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

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

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

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

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

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

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. E.g. a Section in a CA's CPS or a certificate template file used by CA software.

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%.

Code: A contiguous set of bits that has been or can be digitally signed with a Private Key that corresponds to a Code Signing Certificate.

Code Signature: A Signature logically associated with a signed Code.

Code Signing Certificate: A digital certificate issued by a CA that contains a Code
Signing EKU.

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.

Declaration of Identity: A written document that consists of the following:
1. the identity of the person performing the verification,
2. a signature of the Applicant,
3. a unique identifying number from an identification document of the Applicant,
4. the date of the verification, and

5. a signature of the Verifying Person.

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.

Domain Label: From RFC 8499 (http://tools.ietf.org/html/rfc8499): “An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in a portion of the graph of all possible domain names.”

DNS CAA Email Contact: The email address defined in Appendix A.1.1 of the CA/B Forum Baseline Requirements.

DNS CAA Phone Contact: The phone number defined in Appendix A.1.2 of the CA/B Forum Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Appendix A.2.1 of the CA/B Forum Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Appendix A.2.2. of the CA/B Forum Baseline Requirements.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Name: An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees).

Expiry Date: The “Not After” date in a Certificate that defines the end of a Certificate’s validity period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

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.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database. IP Address: A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.

IP Address: A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

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.

Platform: The computing environment in which an Application Software Supplier uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements.

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 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 CP, 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.

Reserved IP Address: An Ipv4 or Ipv6 address that is contained in the address block of any entry in either of the following IANA registries:
https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
https://www.iana.org/assignments/iana-ipv6-special-registry/ iana-ipv6-special-registry.xhtml

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.

Signature: An encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.

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.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the Platforms on which it executes.

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.

Timestamp Authority: A service operated by the CA or a delegated third party for its own code signing certificate users that timestamps data using a certificate chained to a public root, thereby asserting that the data (or the data from which the data were derived via a secure hashing algorithm) existed at the specified time.

Timestamp Certificate: A certificate issued to a Timestamp Authority to use to timestamp data.

Trusted Platform Module: A microcontroller that stores keys, passwords and digital certificates, usually affixed to the motherboard of a computer, which due to its physical nature makes the information stored there more secure against external software attack or physical theft.

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.

UAE PASS: The UAE national digital identity for citizens and residents, and visitors enabling them to access many online services across various sectors, sign and authenticate documents as well as transactions digitally, request a digital version of their official documents, and use the official documents to request services from service providers.

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 CP/applicable 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."

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

Wildcard Domain Name: A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

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

UPS — Uninterruptible Power Supply

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

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

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

1.6.3 References

The present CP endorses the following standards:

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

2. Publication and Repository Responsibility

2.1 Repositories

DESC retains an online repository of documents where it makes certain disclosures about the practices, procedures and content of certain of its policies, including the present CP. It reserves its right to make available and publish information on its policies by any means it sees fit. The URL of DESC online repository is https://ca-repository.desc.gov.ae/.

DESC publishes a copy of this CP at this location. This CP is updated at the least, annually. DESC reserves its rights to publish certificate status information on third-party repositories.

The Government/Private sector Entities shall publish and maintain the applicable CPS and certificate information about all digital certificates they issue through its Subordinate CA, in (an) online publicly accessible Certificate Dissemination Webpage as defined in the applicable CPS.

2.2 Publication of Certificate Information

A copy of the issuing CA certificates shall be published and an online repository shall be retained where it makes certain disclosures about the practices, procedures and content of certain of its policies.

Digital certificate status information shall be published in frequent intervals as indicated in this CP. The provision of the issued electronic certificate validity status information is a 24/7 available service.

DESC shall operate the certificate status repository for the Government/Private sector Entities Subordinate CAs.

2.3 Time or Frequency of Publication Repositories

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

Due to their sensitivity, DESC and the Government/Private sector Entities shall refrain from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the functioning of registration authorities, internal security polices, etc. Such documents and documented practices shall, however, conditionally available to designated authorized parties in the context of audit(s) that DESC and/or Government/Private sector Entities owes duty to with regard to its CA activities.

2.3.1 Certificates

Government/Private sector Entities issuing CA and OCSP certificates shall be published to the public repository once they are issued.

2.3.2 CRLs

CRLs shall be published at regular intervals and add a pointer (URL) to the relevant CRL to subscribers' certificates as part of the CDP extension whenever this extension is present.

A Certificate Dissemination Webpage shall be maintained, the CRL distribution point and the information on this URL for a minimum of seven years after the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the repository are uploaded within 24 hours.

The following rules shall apply for the CRL issued by the Government/Private sector Entities issuing CAs:

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

2.4 Access Controls on Repositories

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

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

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The certificates issued by the Government/Private sector Entities issuing CAs shall contain X.500 Distinguished Names (DNs) in English. The table below summarizes the DN formats allowed for certificates issued by the Government/Private sector Entities issuing CAs.

Certification Authority	Distinguished name
Government/Private sector Entities issuing CA CA DN: cn=<Government/Private sector Entities certification authority name>, l=<Dubai Government locality name>, o=<Government/Private entity meaningful unique name>, ou=<Government/Private sector Entities organizational unit>, c=AE	• **Web servers (SSL)** — The DN format is: *cn = <web server DNS name>, ou = <optional organizational unit within the organization>, o = < Government/Private entity Government/Private entity unique name>, l = < Government/Private entity Government/Private entity locality information>, c = AE* • ***Device certificates (non-SSL):*** *The DN format is:* *cn = <System unique common name> or<device external IP address>, ou = <optional organizational unit within the Dubai Government Entity>, o = <Government/Private entity Government/Private entity meaningful unique name>, l = <Government/Private entity locality name>, c = AE* • ***End user certificates:*** *The DN format is:* *cn=<individual unique name>, ou = <optional organizational unit within the Government/Private entity>, o = <Dubai government entity meaningful unique name>, l = <Government/Private entity locality name>, c = AE* • ***OCSP Responder*** *cn = < Government/Private entity certification authority OCSP responder name>, ou= <optional organizational unit within the Dubai Government Entity>, o = <Government/Private entity meaningful unique name>, l = <Government/Private entity locality name>, c = AE*

3.1.2 Need for names to be meaningful

All end-entity certificates issued by the Government/Private sector Entities issuing CA shall be meaningful and uniquely identify the subject.

3.1.3 Anonymity and Pseudonymity of Subscribers

This policy does not permit anonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation — this section is intentionally left blank.

3.1.5 Uniqueness of Names

The Government/Private sector Entities shall enforce the controls necessary to guarantee that subject Distinguished Name (DN) are unique. The table below summarizes the minimum controls enforced.

Distinguished Name
For certificates issued to individuals, the Government/Private sector Entities shall enforce a convention for a meaningful representation uniquely identifying the individual.
Certificates issued to devices shall uniquely identify the device. Options could be to use the registered public DNS name, public IP address or unique device identifier. For SSL certificates, the Subject Alternative Name extension must be used to define the applicable domain and one or more additional domain names for the certificate.

3.1.6 Recognition, authentication and role of Trademarks

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. the Government/Private sector Entities issuing CAs do not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The Government/Private sector Entities issuing CAs shall have the right to revoke a Certificate upon receipt of a properly authenticated order from DESC or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The Government/Private sector Entities RA shall enforce submission of a Proof-of-Possession of the private key as part of certificate requests. A possible implementation would be to rely on certificate requests containing a Proof-of-Possession (e.g., PKCS#10, PKIX-CMP).

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Identity

For certificates containing organization information, the identity and related information of the organization shall be verified through a reliable data source that allows the RA to verify at least the legal name, legal representatives (e.g. the UAE Official Gazette).

In summary, the validation of Organization identity consists in two parts:

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,
- Verify authority of the Organization’s authorized representative requesting the certificate. The requestor shall be an authorized representative from the entity.

B. Association

The organization name to be inserted in the requested certificate must exactly match the legal name of the entity requesting the certificate unless there is an authentic proof linking the entity with the name to be included in the certificate.

3.2.2.2 DBA/Tradename

The use of DBA or Tradename in the Subject Identity Information is not supported by the Government/Private sector Entities issuing CAs.

3.2.2.6 Data Source Accuracy

The RA shall document the processes followed to check the accuracy of information and documents received as part of the certificate enrolment process.

3.2.2.7 CAA records

The CAA records check procedure is documented in the issuing CA CPS.

3.2.3 Authentication of individual identity

The Government/Private sector Entities RA shall validate the identity of the certificate applicant in a way such that the diligence and rigor of validation is equal to the face-to-face identity verification involving the presentation of a government issued ID card (e.g. Emirates ID).

Further, if applicable, the RA shall also validate the association between the applicant and the organization, and the association between the applicant and the subject.

3.2.4 Non-verified subscriber information

All subscriber information contained within certificate issued by the Government/Private sector Entities issuing CA shall be verified by the Government/Private sector Entities RA.

3.2.5 Validation of Authority

For certificates containing organization information: The authority of the certificate requestor to request a certificate on behalf of the applying entity shall be performed through a reliable means of communication with the entity to establish the authority of the applicant to request a certificate on behalf of the entity.

For certificates issued to individuals: The RA officer/system (that is appointed by the Government/Private sector Entities issuing CA owner) is authorized to submit certification requests on behalf of the defined/agreed CA subscribers.

3.2.6 Criteria for Interoperation

No stipulation — this section is intentionally left blank.

3.3 Identification and Authentication for Re-keying requests

3.3.1 Identification and Authentication for Routine Re-Keying

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

3.3.2 Identification and Authentication for Re-Key after revocation

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

3.4 Identification and Authentication for Revocation Requests

The Government/Private sector Entities RA shall authenticate all revocation requests that are at the Subscriber’s request. The RA may authenticate revocation requests by referencing the Certificate’s Public Key, regardless of whether the associated Private Key is compromised.

4. Certificate Life Cycle Management

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate application shall be limited to applicants associated to the Government/Private sector Entities issuing CA . Further details shall be specified in the applicable CPS.

4.1.2 Enrolment Process and Responsibilities

For any requested certificate, the certificate applicant shall agree to a dedicated subscriber agreement. Further details on the enrollment process shall be specified in the applicable CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Refer to section 3.2 of this CP. In addition, the following requirements shall also apply:

Certification Authority	Acceptance/rejection of certificate applications
General requirements for all certificate applications	• Blacklist check according to the RA's own blacklist • Verify the association between the certificate requester and the applicant (in case the applicant is not applying for the certificate himself/herself)
For certificates issued to legal persons	• Establish the entity existence based on a trusted authoritative source • Verify the association between the authorized representative and the entity based on a trusted authoritative source or a formal communication with the entity's HR. • Verify the association between the certificate requester and the entity based on a proof of employment or a formal communication with the entity's HR. For Code Signing certificates, the use of the documents and data provided to verify certificate information in accordance to section 3.2 shall be valid for a period no more than a specific period, prior to issuing the Certificate. This specific period shall not be more than the maximum validity period of the Code Signing certificate. Any issuance

	exceeding such period, shall relay on new validation evidence as specified in section 3.2.
For certificates issued to a natural person	• Identify the person (as described in section 3.2.2) • For certificates issued to a natural person with association to a legal person: Verify the association between the applicant and the organization (legal person) based on a proof of employment or a formal communication with the organization's HR.
For certificates issued to a non-natural person	• Verify that the organization field of the subject DN value (from CSR) matches the name of the entity • Verify the association between the IT system or device for which the certificate is requested and the entity.
For TLS/SSL and Server Authentication certificates	• CAA records shall be checked to verify the authority of the CA to issue Certificates for the subject domain, details shall be documented in the applicable CPS. The Government/Private sector Entity shall identify High Risk Certificate Requests and determine require additional verifications prior to the Certificate Request approval. The use of the documents and data provided to verify certificate information in accordance to section 3.2 shall be valid for a period no more than a specific period, prior to issuing the Certificate. This specific period shall not be more than the maximum validity period of the SSL/VPN certificates. Any issuance exceeding such period, shall relay on a fresh validation evidence as specified in section 3.2.

For further details, please refer to the applicable CPS.

4.2.2 Approval or Rejection of Certificate Applications

Approval of certificate applications is subject to the results of the identification and authentication described under section 4.2.1.

Refer to the applicable CPS for further details and conditions.

4.2.3 Time to Process Certificate Applications

No stipulation — this section is intentionally left blank.

4.3 Certificate Issuance

The Government/Private sector Entities shall process a certificate issuance request as follows:

- Verify that the certificate request originated from a valid RA
- Issue the required digital certificates that contain the information provided in the certificate request
- If applicable, publish the issued certificates on the Government/Private sector Entities public repository

For further details, please refer to the applicable CPS.

4.3.1 CA Actions during Certificate Issuance

Refer to the applicable CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Refer to the applicable CPS.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

The CA may publish the issued certificates on the dissemination page as described in section 2.2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation — this section is intentionally left blank.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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

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

4.5.2 Relying on Party Public Key and Certificate Usage

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

- Ensure that the key is appropriate for the intended use as set forth in this CP and the applicable CPS. And that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage and certificate policies extension fields
- Check the status of the certificate against the appropriate and current CRLs or through the OCSP service offered by the Government/Private entity issuing CA.

4.6 Certificate Renewal

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

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

4.7 Certificate Re-key

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

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

4.7.1 Circumstance for Certificate Re-key

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

4.7.2 Who May Request Certification of a New Public Key

As per initial certificate issuance

4.7.3 Processing Certificate Re-keying Requests

As per initial certificate issuance

4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

As per initial certificate issuance

4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certificate issuance

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate issuance

4.8 Certificate Modification

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

4.8.1 Circumstance for Certificate Modification

Not applicable beyond the normal certificate re-key operation

4.8.2 Who May Request Certificate Modification

Not applicable beyond the normal certificate re-key operation

4.8.3 Processing Certificate Modification Requests

Not applicable beyond the normal certificate re-key operation

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable beyond the normal certificate re-key operation

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable beyond the normal certificate re-key operation

4.8.6 Publication of the Modified Certificate by the CA

Not applicable beyond the normal certificate re-key operation

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable beyond the normal certificate re-key operation

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Circumstances for revocation
The RA of the Government/Private sector Entities shall revoke certificates when required by the organization internal processes and under the circumstances mentioned in the applicable CPS.

This CP does not provide provisions for revoking an OCSP certificate apart from the compromise of the OCSP key pair which shall be considered by the Government/Private sector Entities as per its disaster recovery and business continuity procedures.

The following sub-sections focus only on the revocation provisions that apply for end-user and device certificates issued by the Government/Private sector Entities issuing CA.

4.9.2 Who Can Request Revocation

A subscriber shall be able to request the revocation for its certificate.

The RA shall be able to request the revocation for the certificates that they manage.

Only authorized revocation requests shall be accepted.

For further details, please refer to the applicable CPS.

4.9.3 Procedure for Revocation Request

Refer to the applicable CPS.

4.9.4 Revocation Request Grace Period

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

4.9.5 Revocation Request Response Time

Certificate revocation requests and problem reports shall be processed within 24 hours from their reception, problem reports processing may require additional time for investigation and involvement of relevant parties. More details on the procedure and involved parties shall be documented in the applicable CPS.

4.9.6 Revocation Checking Requirement for Relying Parties

Revocation information is offered to relying parties through CRLs published on a publicly available repository or through its OCSP responder. Relying parties shall use any of these methods while processing a certificate issued by a Government/Private entity issuing CA.

4.9.7 CRL Issuance Frequency

CRLs are issued as per section 2.3 of this CP.

4.9.8 Maximum Latency for CRLs

No stipulation — this section is intentionally left blank.

4.9.9 Online Revocation/Status Checking Availability

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

The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by a Dubai government entity issuing CA.

4.9.10 Online Revocation Checking Requirements

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

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation — this section is intentionally left blank.

4.9.12 Special Requirements — Key Compromise

No stipulation — this section is intentionally left blank.

4.9.13 Circumstances for Suspension

Certificate suspension shall not be supported by the Government/Private sector Entities issuing CA.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.10 Certificate Status Services

Refer to section 4.9.6 of this CP.

4.10.1 Operational Characteristics

CRLs shall be published by the Government/Private sector Entities issuing CA on a public repository which is available to relying parties through HTTP protocol queries.

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

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation — this section is intentionally left blank.

4.11 End of Subscription

No stipulation — this section is intentionally left blank.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow shall not be supported by the Government/Private sector Entities issuing CA.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation — this section is intentionally left blank.

5. Facility, Management and operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

All critical components related to the issuing CA shall be housed within a highly secure enclave within Dubai PKI facilities. Physical access controls shall be in place to protect the infrastructure, management systems and related operational activities of the issuing CA.

5.1.2 Physical Access

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

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

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

5.1.8 Offsite Backup

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

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

5.2 Procedural Controls

The DESC and Government/Private sector Entities shall follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of Certificate Authorities and electronic signature-related technologies.

The DESC and Government/Private sector Entities shall obtain a signed statement from each member of the staff concerned on not having conflicting interests with the CA activities, maintaining confidentiality and protecting personal data.

5.2.1 Trusted Roles

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

The DESC and Government/Private sector Entities shall conduct an initial investigation of all members of staff who are candidates, to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

5.2.2 Number of Persons Required Per Task

The DESC and Government/Private sector Entities shall maintain and enforce 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 access to and management of CA cryptographic hardware security module (HSM) shall require the involvement of two or more persons.

5.2.3 Identification and Authentication for Each Role

Before exercising the responsibilities of a trusted role:

- The DESC and Government/Private sector Entities shall confirm the identity of the employee by carrying out background checks.
- The DESC and Government/Private sector Entities shall issue access credentials to individual who needs to access equipment located in the secure enclave.
- The DESC and Government/Private sector Entities shall provide the required credentials that allow designated individuals to conduct their functions.

5.2.4 Roles Requiring Separation of Duties

The DESC and Government/Private sector Entities shall ensure separation among the following discreet work groups:

- Personnel managing operations on certificates
- Administrative personnel who operate the supporting platform
- Security personnel who enforce security measures.

5.3 Personnel Controls

The DESC and Government/Private sector Entities shall ensure implementation of security controls with regard to the duties and performance of the members of its staff with regards to the CA activities. These security controls shall be 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 PKI personnel, whether as an employee, agent, or an independent contractor, DESC and Government/Private shall verify the background, qualifications and experience needed to perform within the competence context of the specific job.

5.3.2 Background Check Procedures

The DESC and Government/Private sector Entities shall make the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

5.3.3 Training Requirements

The DESC and Government/Private sector Entities shall make available relevant technical training for their personnel to perform their functions.

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

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

The DESC and Government/Private sector Entities shall sanction personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the DESC and Government/Private sector Entities personnel, as it might be appropriate under the circumstances, and as per the prevailing HR policy and country law.

5.3.7 Independent Contractor Requirements

Independent Government/Private sector Entities issuing CA component services subcontractors and their personnel are subject to the same background checks as Government/Private sector Entities 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

The DESC and Government/Private sector Entities shall make available documentation to personnel, during initial training and retraining.

5.4 Audit Logging Procedures

Details on the audit logging procedures shall be defined in the applicable CPSs. The following provisions are made in this CP.

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.

The Government/Private sector Entities issuing CA shall ensure that at least the following details are recorded:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival and destruction
  - Cryptographic device life cycle management events
- CA and Subscriber Certificate life cycle management events, including:
  - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
  - Certificate requests, re-key requests, and revocation
  - All verification activities stipulated in these requirements and the CA’s Certification Practice Statement
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls

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

In addition, the following internal logs and audit trails of relevant operational events shall also be maintained, 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 Government/Private sector Entities issuing 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
- 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

A designated personnel shall review 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.

5.4.3 Retention Period for Audit Log

The audit logs are retained for at least two years, details the retention criteria shall be specified in the applicable according to applicable requirements.

5.4.4 Protection of Audit Log

Audit logs shall be protected by a combination of physical and procedural security controls.

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the Government/Private sector Entities issuing CA audit log:

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

5.4.6 Audit Collection System (internal vs. external)

No stipulation — this section is intentionally left blank.

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

Government/Private sector Entities issuing CA systems shall be subject to an annual assessment in line with DESC system assurance policy and this CP.

The Dubai PKI systems are subject to regular vulnerability assessment and penetration testing covering the Dubai PKI systems.

5.5 Records Archival

5.5.1 Types of Records Archived

DESC and the Government/Private sector Entities shall archive 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, and Certificate Management Systems; and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

The Government/Private sector Entities shall retain 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 is able to manage the archive without modifying integrity, authenticity and confidentiality of the contained records.

5.5.4 Archive Backup Procedures

A backup, restore and archive procedures shall be documented, including how the archive information is created, transmitted and stored.

5.5.5 Requirements for timestamping of Records

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

5.5.6 Archive Collection System (internal or external)

Only authorized and authenticated staff shall be allowed to handle archived material.

5.5.7 Procedures to Obtain and Verify Archive Information

Only Government/Private sector Entities staff members with a clear hierarchical control and a definite job description may obtain and verify archived information. The Government/Private sector Entities shall retain records in electronic or paper-based format.

5.6 Key Changeover

To minimize impact of key compromise, Government/Private sector Entities issuing 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 and/or the Government/Private entity detects a potential hacking attempt or other form of compromise to the CA, DESC 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 with the Government/Private 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, the Government/Private sector Entities and all other PKI Participants (other than Subscribers and Relying Parties) shall establish the necessary measures to ensure full recovery of the CA services in case of a disaster, and corrupted servers, software or data.

DESC and the Government/Private sector Entities shall establish:

- Disaster recovery resources in a location sufficiently distant from the regular Government/Private sector Entities issuing 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.

5.7.3 Entity Private Key Compromise Procedures

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

In the event of a key compromise for any of a Government/Private entity Issuing CA, or of the associated activation data, DESC triggers the Key compromise and CA termination plans detailed as part of DESC Business continuity and disaster recovery plan.

As part of the Key compromise and CA termination plan, the Dubai PKI PA shall 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 and the Government/Private entity shall establish the necessary measures to ensure full recovery of the offline services service in case of a disaster, and corrupted servers, software or data.

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

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

5.8 CA or RA Termination

If DESC and or the Government/Private entity determines that termination of this CA services are deemed necessary, the CA termination plan shall be executed and it shall cover the following actions:

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

6. Technical Security Controls

6.1 Key Pair Generation and Installation

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

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

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

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

DESC shall ensure the implementation and documentation of key generation procedures in line with this CP. 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 key Generation Ceremony is witnessed by DESC internal auditor
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians
- DESC internal auditor then issues a report, covering that the CA, during its Key Pair and Certificate generation process:
    - Documented its key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement
    - Included appropriate detail in its Key Generation Script
    - Maintained effective controls to provide reasonable assurance that the key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Key Generation Script
    - Performed, during the key generation process, all the procedures required by its Key Generation Script
- A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes.

6.1.1.2 Subscriber Key Pair Generation

Sufficient security shall be maintained during the subscriber key generation process and delivery of these keys and corresponding certificate to the subscriber. Cryptographic algorithms shall be approved by FIPS and specified in FIPS 186-4.

6.1.2 Private Key Delivery to Subscriber

The generated key pair shall be encrypted with a passcode provided by the subscriber and keys shall be delivered using a secure communication channel.

6.1.3 Public Key Delivery to Certificate Issuer

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

The Government/Private sector Entities issuing CAs MUST NOT generate the key pairs for end-entity certificates that have an EKU extension containing the Key Purpose Ids id-kp-codeSigning, id-kp-timeStamping or anyExtendedKeyUsage.

6.1.4 CA Public Key Delivery to Relying Parties

The Government/Private sector Entities issuing CA certificates shall be available to subscribers and relying parties by publishing them in a public repository (https://ca-repository.desc.gov.ae/).

6.1.5 Key Sizes

The Government/Private sector Entities issuing CA key pair shall be at least 4096 bit RSA.

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

Certificates issued by the Government/Private sector Entities issuing CA should always contain a key usage bit string in accordance with RFC 5280.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The Government/Private sector Entities subordinate key pairs shall be generated and stored within a HSM that is certified according to the rating specified in 6.2.11.

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

6.2.2 Private Key Multi-Role Control

Technical and procedural mechanisms shall be implemented to enforce principles of dual control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with CAs cryptographic hardware.

6.2.3 Private Key Escrow

Not applicable

6.2.4 Private Key Backup

The Government/Private sector Entities issuing CA private keys shall be backed up within backup tokens that meet the same certification level as the CA HSM and as described in section 6.2.1.

The creation of key backups on backup HSMs shall be conducted using the principles of dual controls and split knowledge.

At least one backup of the CA keys shall be taken. This backup shall be stored in a locked safe at the disaster recovery site.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The Government/Private sector Entities issuing CA key pairs shall only be transferred to another hardware cryptographic token of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control.

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

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

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

Private keys for the Government/Private sector Entities issuing CA shall be activated by a minimum of two privileged users using the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the CA HSM.

Subscribers are responsible for activating and protecting their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

6.2.9 Method of Deactivating Private Key

Private keys for the Government/Private sector Entities issuing CA shall be deactivated in situations such as:

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

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

6.2.10 Method of Destroying Private Key

At the end of their lifetime, taking into account business purpose and legal obligations, the Government/Private sector Entities issuing CA private keys shall be destroyed by multi-person presence, in order to ensure that these private keys cannot ever be retrieved and used again.

6.2.11 Cryptographic Module Rating

The Government/Private sector Entities issuing CA shall use an HSM certified to FIPS 140-2 Level 3 or ISO 15408 Common Criteria (CC) EAL 4+ or above.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to section 5.5 of this CP.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 CA Key Generation

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

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

6.4.1.2 Subscribers keys

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

6.4.2 Activation Data Protection

6.4.2.1 CA Key Activation Data

The CA activation data consists of PINs, passwords and accounts that are used to activate the HSMs hosting the CA keys and 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 CP for further details.

6.4.2.2 Subscribers

Refer to section 6.4.1.2 of this CP.

6.4.3 Other Aspects of Activation Data

No stipulation — this section is intentionally left blank.

6.5 Computer Security Controls

The Government/Private sector Entities issuing CA shall perform all CA and RA functions using trustworthy systems that meet DESC security in addition to the present requirements.

6.5.1 Specific Computer Security Technical Requirements

The Government/Private sector Entities issuing CA shall be operated according to the following security controls:

- Physical access control to the CA servers shall be enforced
- Separation of duties and dual controls for CA sensitive operations

- Identification and authentication of PKI roles and their associated identities
- Archival of CAs history and audit data
- Audit of security-related events
- Automatic and regular validation of the CA systems' integrity
- Recovery mechanisms for keys and CA systems
- Hardening CA servers' operating system according to best practices and PKI vendor requirements
- Network protection, including intrusion detection systems
- Proactive patch management for the CA systems
- DESC shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation — this section is intentionally left blank.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

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

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

6.6.3 Life Cycle Security Controls

No stipulation — this section is intentionally left blank.

6.7 Network Security Controls

The Government/Private sector Entities shall ensure maintenance of network security, including managed firewalls and intrusion detection systems.

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

Issuing Systems, Certificate Management Systems, and Security Support Systems shall be maintained and protected in a highly secure network zone.

6.8 Time-stamping

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

7. Certificate, CRL profiles

7.1 Certificate Profile

The Certificates and CRLs issued by the Government/Private sector Entities issuing CAs shall comply with the requirements of RFC 5280.

For further details, please refer to the applicable CPS.

7.1.1 Version Number

The Government/Private sector Entities issuing CAs shall issue X.509 version 3 certificates as defined in RFC 5280.

7.1.2 Certificate Extensions

The Government/Private sector Entities issuing CAs shall issue certificates with X.509 v3 extensions as defined in RFC 5280 in addition to extensions indorsed by the browsers' root programs. Further, the values allowed for the key usage and extended key usage field depend on the type of certificate:

Certificate type	Key Usage	Extended Key Usage
SSL/TSL server Auth	• digitalSignature • keyEncipherment	• serverAuth
Device certificate (non-SSL)	• digitalSignature • keyEncipherment	• clientAuth
End-user certificate	• digitalSignature • nonRepudiation • keyEncipherment • dataEncipherement	• clientAuth

Refer to section 7.1 of the applicable CPS for the details of the contents of the certificates issued by the CA.

7.1.3 Algorithm Object Identifiers

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

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

7.1.6 Certificate Policy Object Identifier

The Government/Private sector Entities issuing CAs shall use certificate policy object identifiers that are defined as part of OID scheme for the Dubai PKI. Refer to the ASN1 definitions described section 7.1 of the applicable CPS.

7.1.7 Usage of Policy Constraints Extension

Policy constraints extension is not supported.

7.1.8 Policy Qualifiers Syntax and Semantics

The Government/Private sector Entities issuing CAs shall use policy qualifiers as per the RFC 5280. Refer to the ASN1 definitions described section 7.1 of the applicable CPS.

7.1.9 Processing Semantics for Critical Certificate Extensions

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

7.2 CRL Profile

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

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

For further details, please refer to the applicable CPS.

7.2.1 Version Number(s)

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

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

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

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

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

For further details, please refer to the applicable CPS.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessments

DESC shall organize compliance audits to ensure that it meets requirements, standards, procedures and service levels according to this CP at least on an annual basis. DESC shall accept 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 shall evaluate the results of such audits before further implementing them.

8.2 Identity and Qualifications of the Assessor

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

These audits will be performed by qualified auditors who fulfill the following requirements:

- Independence from the subject of the audit
- The ability to conduct an audit that addresses the WebTrust criteria specified above
- Employs individuals who have proficiency in examining PKI technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation, or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least US$1m in coverage.

8.3 Assessor’s Relationship to Assessed Party

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

8.4 Topics Covered by Assessment

The compliance audits will verify whether the Dubai PKI operations environment is in compliance with the this CP, the applicable CPS and supporting operational policies and procedures.

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 external Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to Dubai PKI PA. The audit Report shall be publicly available through the CA repository no later than three months after the end of the audit period.

8.7 Self-audits

The Dubai PKI PA, through its compliance function, monitors and strictly controls its adherence to the procedures listed in this CP document and to the Baseline Requirements by performing self-audits on at least a quarterly basis against a randomly selected samples at least 3 percent of the ServerAuth Certificates, and 6 percent of the Code Signing and Timestamping Certificates.

9. Other Business and Legal Matters

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

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Refer to the applicable CPS.

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fees

Refer to the applicable CPS.

9.1.4 Fees for Other Service

Refer to the applicable CPS.

9.1.5 Refund Policy

Refer to the applicable CPS.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The Government/Private sector Entities issuing CAs consider the following as confidential information:

- Subscriber’s personal information that are not part of certificates or CRLs issued by The Government/Private sector Entities issuing CAs,
- Correspondence between the subscribers and RAs during the certificate management processing (including the collected subscribers data)
- Contractual agreements between DESC, the Government/Private sector Entities and their suppliers
- The CAs’ 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 and the Government/Private sector Entities guarantee the protection of confidential information according to the applicable laws on privacy.

9.4 Privacy of Personal Information

9.4.1 Privacy plan

DESC and the Government/Private sector Entities observe personal data privacy rules and confidentiality rules as described in this CP. 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.

DESC and the Government/Private sector Entities don't not release any confidential information without the consent of the legitimate data owner or explicit authorization by a court order. When DESC and/or the Government/Private sector Entities release private information, it 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 and the Government/Private sector Entities respect all applicable privacy, confidential information, and trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention and disclosure of non-public information.

All communications channels with DESC/the Government/Private sector Entities/RAs shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with Government/Private sector Entities issuing CAs systems. This shall include:

- The communications link between the CAs 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/Government/Private sector Entities employees, suppliers and contractors handle personal information in strict confidence under the applicable contractual obligations that at least as protective as the terms specified in section 9.4.1.

9.5 Intellectual Property Rights

The Government/Private sector Entities and DESC own and reserve all intellectual property rights associated with its own databases, web sites, the CAs' digital certificates and any other publication whatsoever originating from the Dubai PKI including this CP.

When the Government/Private sector Entities or DESC use software from suppliers, it is possible that this software remains intellectual property of the supplier. This is defined in the license agreement of contract of this supplier.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

DESC and the Government/Private sector Entities shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued under this CP are in accordance with the stipulations of this Policy.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this Policy, and comply with the applicable CPS approved by the Dubai PKI PA. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.3 Subscriber Representations and Warranties

Government/Private sector Entities require, 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 Government/Private sector Entities issuing CAs and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the Government/Private sector Entities shall obtain, for its express benefit and the Certificate Beneficiaries, either:

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

Government/Private sector Entities shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request.

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

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the CA/RA, both in the certificate request and as otherwise requested by CA/RA in connection with the issuance of the Certificate(s) to be supplied by the Government/Private sector Entities CAs,
- **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token),
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy,

- **Use of Certificate:** When TLS server certificates are requested, an obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use,
- **Reporting and Revocation:** An obligation and warranty to:
  - promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
  - promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise,
- **Responsiveness:** An obligation to respond to instructions concerning Key Compromise or Certificate misuse within a specified time period,
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the Government/Private sector Entities issuing CA 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 the applicable CPS, or the Baseline Requirements.

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under Government/Private sector Entities issuing CAs 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

CAs operating under this policy may not disclaim any responsibilities described in this CP.

9.8 Limitations of Liability

The Dubai government issuing CAs may limit their liability to any extent not otherwise prohibited by this CP, if the Issuing CA remains responsible for complying with this CP and the Issuing CA's CPS.

9.9 Indemnities

Not stipulation.

9.10 Term and Termination

9.10.1 Term

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

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 CP termination via appropriate mechanisms.

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

When changes are required to be done on this CP. 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 CP 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 CP 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 CP.

9.15 Compliance with Applicable Law

The present CP is 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 CP, 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/the Government/Private sector Entities. 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 CP. Any modification to DESC/the Government/Private sector Entities 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 CP 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 CP 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 stipulation.