Dubai Electronic Security Center

Dubai PKI

DESC Subordinate CAs

Certificate Policy

Project	DESC CA Project
Title	DESC Subordinate CAs, Certificate Policy
Classification	PUBLIC
File Name	DubaiPKI-DESCSubordinateCAs-CertificatePolicy_v1.51
Created on	18 May 2017
Revision	1.51
Modified on	13 July 2021

Document History

Date	Revision	Author(s)	Summary
18 May 2017	0.1	Khawla Hassan	Initial version
12 September 2017	0.2	Khawla Hassan	Minor modifications & Incorporation of Dubai government entity Root CA option
3 November 2017	0.3	Khawla Hassan	Minor modifications to reflect control environment
11 January 2018	0.4	Khawla Hassan	Update certificate profiles
18 January 2018	0.5	Khawla Hassan	Second revision of certificate profiles
30 January 2018	1.0	Khawla Hassan	Issue final version
25 February 2018	1.1	Khawla Hassan	Update publication of certificate information
16 October 2018	1.2	Khawla Hassan	• Updates based on regular review, in addition to adding practices related to certificates issued for email protection. • Expand the government entities community to cover all UAE government entities.
07 August 2019	1.3	Khawla Hassan	Added a reference to the CPSs for the detailed list of circumstances of revocation
3 June 2020	1.4	Khawla Hassan	Updates based on regular review
11 April 2021	1.5	Khawla Hassan	Annual review and updates to address Mozilla comments and clarify subordinate CAs governance and operating environment
13 July 2021	1.51	Khawla Hassan	• Add user authentication certificate profile (for natural persons) • Increase the CRL lifetime to 72 hours

Table of Contents

1. Introduction

This Certificate Policy (CP) defines the requirements applicable to DESC Corporate and Devices Subordinate Certification Authorities, referred to as “Corporate and Devices CAs” or “DESC Subordinate CAs”, which come at the second level of the Dubai Public Key Infrastructure (PKI) hierarchy. Dubai PKI Subordinate CAs are owned by DESC. Dubai PKI Subordinate CAs are Certification Authorities under the Dubai PKI Root CA. This is achieved by the Dubai PKI Root CA issuing a digitally signed CA Certificates that authenticate the Public Key of the Corporate CA and Devices CA. DESC establishes and operates these subordinate CAs for issuing end-entity certificates (Corporate certificates and Device certificates) to the Government entities.

The Dubai PKI Policy Authority (PA), which is composed of appointed members of the DESC management and DESC PKI team, is representing the policy and governing body for the Dubai PKI, including DESC Subordinate CAs. This body is referred to in this CP document as the PA.

The PKI certification services are offered by DESC in accordance with the present CP and a dedicated Certification Practice Statement (CPS) for each Subordinate CA.

1.1 Overview of Dubai PKI

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

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

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

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

1.1.1 Dubai PKI Hierarchy

The below Figure depicts the Trust Model of the Dubai PKI. The Dubai PKI Root CA is the top authority in this PKI with regard to the digital certification services offered by Dubai PKI. The Dubai

PKI Root CA signs DESC Subordinate CAs, which come at the second level of the PKI hierarchy. In addition, the Root CA also signs subordinate CAs belonging to authorized government or private sector entities.

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

Figure 1: Trust Model for Dubai PKI

1.1.2 Certification Services

The certification services offered by the Corporate and Devices CA are broken down in this document as follows:

- **Registration service:** Verifies the identity and, if applicable, any specific attributes of end-entities applying for certificates. The results of this service are passed to the certificate generation service.
- **Certificate generation service:** Creates and signs end-entity certificates based on the verification conducted by the registration service.
- **Dissemination service:** Disseminates the end-entity certificates and makes them available to relying parties. This service also makes available any public policy and practice information to subscribers and relying parties.
- **Revocation management service:** Processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the certificate validity status service.
- **Certificate validity status service:** Provides certificate validity status information to relying parties. This shall be based upon certificate suspension/revocation lists. The status information shall always reflect the current status of the certificates issued by DESC Subordinate CAs.

1.1.3 Certificate Policy

X.509 certificates issued by Subordinate 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 Subordinate CAs CPSs establish the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by Subordinate Cas as governed by this CP and related documents which describe DESC PKI requirements and use of Certificates.

1.2 Document name and Identification

This document is named 'Dubai PKI DESC Subordinate CA Certificate Policy' and is referenced as such in related documents.

The Object Identifier (OID) of this document is 2.16.784.1.2.2.100.1.1.2.1.

DESC organizes the OID for the certificates it issues as depicted in the tables below:

Corporate CA

OID	Certificate type	Description
2.16.784.1.2.2.100.1.2.2.1.1	Encryption certificates	Encryption certificates for individuals (e.g., emails, documents)
2.16.784.1.2.2.100.1.2.2.1.2	**Deprecated:** Authentication certificates	Certificates for individual authentication purposes
2.16.784.1.2.2.100.1.2.2.1.6	Authentication certificates	Certificates for individual authentication purposes
2.16.784.1.2.2.100.1.2.2.1.3	Digital signature certificates (high assurance)	Digital signing certificates for individuals to be used for signing transactions that require a high assurance level of identity vetting
2.16.784.1.2.2.100.1.2.2.1.4	Digital signature certificates (moderate assurance)	Digital signing certificates for individuals to be used for transactions that does not require the highest assurance levels of identity vetting
2.16.784.1.2.2.100.1.2.2.2.1	Digital signature certificates (legal signing on behalf of government entity)	Digital signing certificates for organizations (signing for legal persons)
2.16.784.1.2.2.100.1.2.2.2.2	Code signing certificates	Certificates for (software) code signing purposes

Devices CA

OID	Certificate Type	Description
2.16.784.1.2.2.100.1.2.2.3.1	Device certificates	Certificates for general identification and authentication of devices
2.16.784.1.2.2.100.1.2.2.3.3	VPN certificates	Device identification and session data encryption for VPN (IPsec-based connections)
2.16.784.1.2.2.100.1.2.2.3.2	SSL certificates	SSL certificates used for server authentication and session data encryption

2.16.784.1.2.2.100.1.2.2.3.4	Signature verification service certificate	Certificate used to sign the verification responses generated by the DESC signature verification service
2.16.784.1.2.2.100.1.3.1.1	Time stamping certificates	Certificates intended for the Dubai PKI TSA (Time Stamping Authority)

1.3 PKI Participants

The participants within the context of the Corporate and Devices CA are as follows:

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

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

1.3.1 Policy Authority (PA)

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

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

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

1.3.2 Subordinate Certification Authorities

The table below lists the Dubai PKI Subordinate CAs operated by DESC and the certificates issued by these CAs.

Certification Authority	Supported certificates
Corporate CA	X.509 (V3) certificates for Government entities, Citizens and Residents in the UAE (encryption, signature, authentication and code signing) in addition to OCSP response signing certificates.

Certification Authority	Supported certificates
Devices CA	X.509 (V3) end-entity certificates for devices (generic device, SSL, VPN, signature verification service and time stamping service) in addition to OCSP response signing certificates.

The key responsibilities of DESC with regard to the operation of these Subordinate CAs are as follows:

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

All certificates issued by the Corporate and Devices CA shall conform to the rules and requirements as stated in this policy document.

1.3.3 Registration Authority

DESC shall set up an RA organization for the Corporate and Devices CAs. DESC does not delegate the validation process of domain ownership or control (domain portion of an email address) to any third-party RA or LRA, rather this process is performed only by DESC RA team. The RA shall comprise duly authorized individuals to be involved in validating the identity of individuals requesting certificates, as well as in issuing and managing these certificates.

1.3.4 Local Registration Authority

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

- Officer duly authorized by the government entity: DESC RA will enroll This LRA officer to DESC Corporate CA. He will receive credentials that allow to access the Corporate CA remotely through a dedicated Web RA application and manage the digital certificates of the government entity subscribers' community.
- System/application: Operated by the government entity and integrated with the Corporate CA through a secure interface exposed by the CA. The system/application is configured with dedicated credentials issued by DESC RA so that it can request certificates from Corporate CA and manage the subscribers' community certificates.
- .

  The UAE national Authentication and Digital Signing platform (known as UAE PASS) is an example of an LRA application that is currently integrated with this CA to issue and manage Authentication and Signing certificates for Citizens and Residents of the UAE.

The entities willing to act as an LRA shall sign an agreement with DESC through which it commits to operate their LRA in accordance with and this CP and DESC Subordinate CA CPS . In case DESC authorizes LRA to issue e-mail protection certificates to its employees, DESC shall first validates that the domain is owned/controlled by the subject entity (LRA) and shall hardens its dedicated Web RA application to issue e-mail protection certificates only if the domain portion of the email is in an approved list.

The LRA agreement describes the LRA obligations/responsibilities for:

- The collection and validation of subscribers' identity data by the LRA
- The LRA conformance to this CP and DESC Subordinate CA CPS
- The request and management of certificates of the government entity subscribers' community

1.3.5 Subscribers

Subscribers of the Corporate and Devices CA are listed in the below table:

Certification Authority	Subscribers
Corporate CA	Government entities, Government employees and the Citizens/Residents in the UAE
Devices CA	Government entity infrastructure devices such as VPNs, web servers, routers, switches and other devices

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

1.3.6 Relying Parties

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

1.3.7 Other Participants

There are no other participants within the context of the Corporate and Devices CA.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

Use of certificates issued from the Corporate and Devices CAs is restricted by using certificate extensions on key usage and extended key usage, which will be configured according to the certificate type. Please refer to the CPS of each respective subordinate CA for the specific restrictions that apply to each type of certificate.

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

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

1.4.2 Prohibited Certificate Use

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

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

1.5.2 Contact Details

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

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

E-mail pa@desc.gov.ae

Certificate Problem Report
Refer to the applicable CPS.

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

Changes or updates to the Corporate CA CPS or Devices CA CPS documents must be made in accordance with the stipulations of the provisions contained in this CP and are subject to Dubai PKI Policy Authority approval. 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 CPS or an update notice. The PA formally approves the new version of the CPS.

1.6 Definitions, Acronyms and References

1.6.1 Terminology and definitions

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

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

CA — Certification Authority

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

CCTV — Closed Circuit TV

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

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

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

FQDN — Fully Qualified Domain Name

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

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

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

Identity Provider – In the context of this CPS, references to identity providers will be related to the government/federal identity providers including Smart Pass and Dubai ID.

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

Issuer — The name of the CA that signs the certificate

ITU — International Telecommunications Union

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

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

LRA – Local Registration Authority

DESC — Dubai Electronic Security Centre

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

OSCP — Online Certificate Status Protocol

PA — Policy Authority of the Dubai PKI

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

PKCS # 7 — Cryptographic Message Syntax

PKCS #10 — Certification Request Syntax Specification

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

PKE — Public Key Encryption

PKI — Public Key Infrastructure

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

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

RA — Registration Authority

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

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

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

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

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

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

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

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

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

Subject —The entity named in a certificate

Subscriber — A subject who is issued a certificate

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

UPS — Uninterruptible Power Supply

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

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

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

1.6.2 Acronyms

Please refer to section 1.6.1.

1.6.3 References

The Corporate CA (through its CPS) is committed to comply with the following requirements published at https://www.cpacanada.ca:

- WebTrust Principles and Criteria for Certification Authorities

The Devices CA (through its CPS) is committed to comply with the following 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 Devices CA (through its CPS) is committed to conforms to current versions of the following requirements published at http://www.cabforum.org:

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

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

The present CP endorses the following standards:

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

2. Publication and Repository Responsibility

2.1 Repositories

DESC publishes information about all digital certificates it issues in (an) online publicly accessible Certificate Dissemination Webpage at https://ca-repository.desc.gov.ae/.

2.2 Publication of Certificate Information

In particular, DESC publishes a copy of the subordinate CA certificates, OCSP certificates and TSA certificates at this location. This Certificate Policy is updated at the least, annually. DESC reserves its rights to publish certificate status information on third-party 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.

DESC publishes digital certificate status information in frequent intervals as indicated in this CP. The provision of the Devices and Corporate CA issued electronic certificate validity status information is a 24/7 available service.

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

2.3 Time or Frequency of Publication Repositories

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

2.3.1 Certificates

Corporate and Devices CA, TSA and OCSP certificates shall be published to the public repository (https://ca-repository.desc.gov.ae/) once they are issued.

2.3.2 CRLs

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

DESC maintains the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL 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 Corporate and Devices CA:

- 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 CP, CPS, certificates and CRLs 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 Corporate and Devices CA shall contain X.500 Distinguished Names (DNs) in English. The table below summarizes the DNs of the certificates issued by the Corporate and Devices CA.

Certification Authority	Distinguished name
Corporate CA CA DN: cn = Corporate Certification Authority, o = UAE Government, c = AE	• **Certificates issued for Government entities through DESC RA:** cn=<Government entity name>, ou = <optional organizational unit within the government entity>, o =<Government entity meaningful unique name>, l =<Government entity locality information> , c = AE • **Certificates issued for individuals:** serialnumber=<optional serial number for each subscriber>, cn=<individual end user name>, ou = <optional organizational unit within the government entity>, o =<Government entity meaningful unique name>, l =<Government entity locality information>, c = AE • **OCSP responder:** cn = Corporate Certification Authority OCSP, o = DESC, l = Dubai, c = AE
Devices CA CA DN: cn=Devices Certification Authority, o=UAE Government, c=AE	• **Devices** — The DN format is: cn = <System unique common name> or <unique device identifier> or <device IP address> ou = <optional organizational unit within the organization> o = <organization meaningful unique name> l = <organization's locality information> c = AE • **VPNs** — The DN format is: cn = <System unique common name> or <device DNS name> or <device IP address> ou = <optional organizational unit within the organization>

	o = <organization meaningful unique name> l = <organization's locality information> c = AE • **Web servers (SSL)** — The DN format is: cn = <web server DNS name> ou = <optional organizational unit within the organization> o = <organization meaningful unique name> l = <organization's locality information> c = AE • **OCSP responder** — The DN format is: cn = Devices Certification Authority OCSP o = DESC l = Dubai c = AE • **Signature verification**— The DN format is: cn = Dubai PKI Signature Verification Service o = DESC l = Dubai c = AE • **Dubai TSA** — The DN format is: cn = Dubai Timestamping Authority o = DESC l = Dubai, c = AE

3.1.2 Meaningful Names

Certification Authority	Meaningful Names
Corporate CA	For certificates issued to individuals, names are meaningful since the CN contains the name of the subscriber. For certificates issued to government entities, names are meaningful since the CN contains the name of the entity.
Devices CA	Distinguished Names (DN) shall be used to identify both the subject and the issuer of the certificate. DESC shall issue certificates to subscribers that demonstrate ownership and control on the domain names, IP addresses mentioned in the Subject DN.

OCSP, TSA and Signature Verification Service, certificates names shall indicate the service name operated by DESC.

3.1.3 Anonymity and Pseudonymity of Subscribers

This policy does not permit anonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

DESC shall enforce the controls necessary to guarantee that subject Distinguished Name (DN) are unique. The table below summarizes the minimum controls enforced for each CA.

Certification Authority	Distinguished Name
Corporate CA	DESC shall enforce a convention for a meaningful representation uniquely identifying the individual or the Government entity to which the certificate issued. For certificates issued for Corporate CA OCSP responder: The OCSP responder unique name shall be included in the subject DN to ensure uniqueness.
Devices CA	Certificates issued by the Devices CA shall uniquely identify the system/device. Options could be to use Fully Qualified Domain Names (FQDNs), unique device identifier, IP address or unique system common names. 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. For certificates issued for OCSP, TSA and Signature Verification Service, a service unique name shall be included in the subject DN to ensure uniqueness.

3.1.6 Recognition, authentication and role of Trademarks

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

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The CA shall verify that the certificate applicant possesses the private key corresponding to the public key being certified by performing signature verification on the certificate request received. The CA shall always expect the certificate request to be signed by the private key associated to the public key being certified.

3.2.2 Authentication of Organization 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, organizational unit (if applicable) and official address of the organization.

The authority of the applicant to request a certificate on behalf of a Government entity is authenticated in accordance with section 3.2.6.

3.2.3 Authentication of individual identity

The table below describes the rules that apply for authentication of certificate applicants:

Certification Authority	Method of authentication of individual identity
Corporate CA	• **Certificates application through a government entity LRA officer (or DESC RA officer)**: The subscriber's identity validation shall be performed by the RA/LRA officer according to the government entity's applicable business rules. The Government entity shall ensure that the diligence and rigor of validation is based on face-to-face identity validation or equal to the face-to-face identity verification involving the presentation of a government issued ID card (e.g. Emirates ID). • **Certificates application through the UAE PASS system:** The LRA of the Government entity shall validate the identity of the applicant as follows: o Authentication certificate and digital signature certificate for "High assurance" transactions: Identity validation shall be performed within a controlled environment (e.g. through dedicated kiosk), involving a government issued ID and biometric verification or through use of and approved technology that can verify user through use of biometric information (e.g. fingerprint or face verification) o For signing certificates for "Moderate assurance" transactions, identity validation can be performed either as mentioned above or based existing authentication credentials from accepted Identity Providers in the UAE provided that the following requirements are met: o Existence of ID proofing artifacts substantiate the antecedent verification outcome o Mechanisms are in place that bind the individual to the asserted identity Dubai PKI recognized Smart Pass and Dubai ID as trusted Identity Providers
Devices CA	For any Devices Certificate, DESC RA shall undergo the following identity validation steps for the applicant: • Identity validation through one of the following methods:

	○ Face-to-face verification against a government issued photo ID ○ Remote verification involving a government issued ID and biometric verification • Validation of association between the applicant and the government entity to which he/she belongs • Validation of the system/device/domain ownership

3.2.4 Authentication of Domain name

For SSL certificates, the control or ownership of the domain name(s) which is/are specified in the certificate application must be verified. Refer to the Devices CA CPS for more details on the domain ownership verification.

3.2.5 Non-verified subscriber information

subscriber information contained within certificate issued by the Corporate and Devices CA shall be verified by the relevant RA/LRA. Non-verified information shall not be included in certificates issued by Dubai PKI Subordinate CAs.

Note: DESC does not delegate the validation process of domain ownership or control to any third-party RA or LRA rather this process is performed only by DESC RA team.

3.2.6 Validation of Authority

Certification Authority	Validation of authority
Corporate CA	• Government entity certificates to be issued through DESC RA: The authority of the certificate requestor to request a certificate on behalf of a Government entity shall be performed through a reliable means of communication with the Government entity to establish the authority of the applicant to request a certificate on behalf of the Government entity. • Individual certificates to be issued through the LRA (including DESC RA): The RA/LRA officer/system (that is approved by DESC) is authorized to submit certification requests on behalf of the Government Entity subscribers.
Devices CA	The authority of the certificate requestor to request a certificate on behalf of a Government entity shall be performed through a reliable means of communication with the Government entity to establish the authority of the applicant to request a certificate on behalf of the Government entity.

3.2.7 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 Routine Re-Key shall be the same as applied during initial certification.

3.4 Identification and Authentication for Revocation Requests

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

OCSP, TSA and Signature Verification Service certificates' revocation shall be conducted as part of DESC internal processes and the Dubai PKI PA shall approve it.

4. Certificate Life Cycle Management

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

- **Certificates for entities issued through DESC RA:** An authorized person from the Government entity submits the certificate application as part of the certificate issuance process.
- **Certificates for individuals issued through the Government entity LRA (including DESC RA):** The entity LRA or DESC RA submits the certificate application.
- **Certificates for individuals issued through the UAE PASS:** The UAE PASS system is the interface through which certificate applications are triggered to the CA.
- **OCSP responder certificates:** An authorized OCSP administrator can submit a certificate request.

4.1.2 Enrolment Process and Responsibilities

For any certificate issued by the Corporate or Devices CA, the certificate applicant shall agree on the subscriber agreement.

For further details on the enrollment process, please refer to the applicable CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Refer to section 3.2 of this CP.

Certification Authority	Acceptance/rejection of certificate applications
Corporate CA	• **Certificates issued to Government entities through DESC RA:** Any applicant for certificates through the DESC RA shall undergo the following enrolment process: o Identity validation process by the DESC RA o The DESC RA validates the association between the applicant and the Government entity o If all verifications are successful, the DESC RA accepts the certificate application, and issues the required PKI credentials and related certificates

	• **Certificates issued to individuals through the Government entity LRA (including DESC RA):** The RA/LRA shall validate the identity of the applicant and confirm if he/she is authorized to receive PKI credentials by the Government entity. If all verifications by RA/LRA are successful, the RA/LRA accepts the certificate application. The RA/LRA then enroll the individual to the PKI and issue the requested certificate. *Note: DESC RA is responsible of issuing certificates to DESC employees. Government LRAs are only responsible for issuing certificates to their community that is agreed with DESC as per the LRA agreement)*
Devices CA	Certificates issued to system/device/domain, the DESC RA shall validate the identity of the certificate applicant who needs to proof ownership of the subject system/device/domain. Further, for SSL certificate applications, Certificate Authority Authorization (CAA) records shall be checked to identify the CA authorized to issue certificates for the subject domain (if any). If all verifications are successful, DESC RA accepts the certificate application then enroll the subject to the PKI and issue the requested certificate.

For further details, please refer to the applicable CPS.

4.2.2 Approval or Rejection of Certificate Applications

Refer to the applicable CPS.

4.2.3 Time to Process Certificate Applications

No stipulation — this section is intentionally left blank.

4.3 Certificate Issuance

DESC shall process a certificate issuance request as follows:

- Verify that the certificate request originated from a valid (L)RA
- Issue the required digital certificates that contain the information provided in the certificate request
- If applicable, publish the issued certificates on the DESC 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.

OCSP, TSA and Signature Verification Service certificates shall be accepted as part of DESC internal processes and the Dubai PKI PA shall approve it.

4.4.2 Publication of the Certificate by the CA

The CA, TSA and OCSP certificates shall be published on the dissemination page as described in section 2.2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation — this section is intentionally left blank.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

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 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 Corporate and Devices CAs.

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.

Re-key for OCSP, TSA and Signature Verification Service certificates shall happen as part of internal DESC processes and approved by the Dubai PKI PA.

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

Certification Authority	Circumstances for revocation
Corporate CA	• **Circumstances of revocation of government entity certificates through DESC RA:** Certificates shall be revoked under the circumstances mentioned in the applicable CPS. • **Circumstance for revocation of Government entity certificates through an LRA (including DESC RA):** DESC RA or the LRA of the government entity shall revoke digital certificates corresponding to its community when required by the organization internal processes. The RA/LRA shall submit the certificate revocation request to the CA in an authenticated manner. Further, DESC reserves the right to revoke certificates under the circumstances mentioned in the applicable CPS.
Devices CA	Certificates shall be revoked under the circumstances mentioned in the applicable CPS.

This CP does not provide provisions for revoking an OCSP, TSA and Signature Verification Service certificates apart from the compromise of the corresponding key pair, which shall be considered by DESC as per its disaster recovery and business continuity procedures.

The following sub-sections focus only on the revocation provisions that apply for individual and device certificates issued by the Corporate or Devices CA.

4.9.2 Who Can Request Revocation

Refer to section 4.9.1.

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 (L)RA.

4.9.5 Revocation Request Response Time

Certificate revocation requests and problem reports shall be processed within 24 hours.

An interface for revocation shall be enabled for registered LRAs to be used for revocation requests and ensure they are processed immediately.

4.9.6 Revocation Checking Requirement for Relying Parties

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

The OCSP responder shall be compliant with RFC 6960. OCSP information shall be available immediately to relying party applications.

The actual OCSP URL to be queried by relying party organizations shall be referenced in the certificates issued by the Corporate or Devices 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

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

4.9.13 Circumstances for Suspension

Certificate suspension is not supported by the Corporate and Devices 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 Corporate and Devices 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 is not supported by the Corporate and Devices 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 of the PKI solution are housed within a highly secure enclave Data Center. Physical access controls are in place to protect the infrastructure, management systems and related operational activities of the PKI solution.

5.1.2 Physical Access

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

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

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

The secure enclave shall be furnished with 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.

5.1.3 Water Exposures

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

5.1.4 Fire Prevention and Protection

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

5.1.5 Media Storage

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

5.1.6 Waste Disposal

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

5.1.7 Offsite Backup

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

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

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

5.2 Procedural Controls

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

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

5.2.1 Trusted Roles

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

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

5.2.2 Number of Persons Required Per Task

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

The most sensitive tasks, such as access to and management of CA cryptographic hardware security module (HSM) shall require the involvement of two or more persons.

5.2.3 Identification and Authentication for Each Role

Before exercising the responsibilities of a trusted role:

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

5.2.4 Roles Requiring Separation of Duties

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

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

5.3 Personnel Controls

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

5.3.1 Qualifications Experience and Clearance Requirements

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

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

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

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

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

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

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

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

For details on the audit logging procedures, refer to the applicable CPSs. The following provisions are made in this CP.

5.4.1 Types of Event Recorded

Following events occurring on the Corporate and Devices CA shall be 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:

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

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

- Start and stop of servers
- Outages and major problems
- Physical access of personnel and other persons to sensitive parts of the DESC site
- Backup and restore
- Report of disaster recovery tests
- Audit inspections
- Upgrades and changes to systems, software and infrastructure
- Security intrusions and attempts at intrusion
- Other documents that are required for audits include:
    - Infrastructure plans and descriptions
    - Physical site plans and descriptions
    - Configuration of hardware and software
    - Personnel access control lists

5.4.2 Frequency of Processing Log

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

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

All log entries include the following elements:

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

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

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the Corporate and Devices CA audit log:

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

5.4.6 Audit Collection System (internal vs. external)

No stipulation — this section is intentionally left blank.

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

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

5.5 Records Archival

DESC keeps records of the following items:

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

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

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

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

Archives are accessible to authorized personnel of DESC.

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

Only the records administrator (member of staff assigned with the records retention duty) may access an archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium

- Protection against deletion of archive
- Protection against deterioration and/or obsolescence of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media

5.5.4 Archive Backup Procedures

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

5.5.5 Requirements for timestamping of Records

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

5.5.6 Archive Collection System (internal or external)

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

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

DESC Subordinate CAs private keys are maintained until such time as all relying certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

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

5.7.2 Computing Resources, Software and/or Data Corruption

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

DESC establishes:

- Disaster recovery resources in a location sufficiently distant from the regular DESC Subordinate CAs operation facility
- Fast communications between the two sites to ensure data integrity

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

5.7.3 Entity Private Key Compromise Procedures

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

In the event of a key compromise of the Corporate or Devices CA, the following actions shall be taken by DESC:

- All active certificates issued by the Subordinate CA shall be revoked.
- Organizations holding Client and Device Certificates shall be notified.
- A new Subordinate CA key pair shall be generated and certificate produced by the Dubai PKI Root CA.
- A Subordinate CA compromise notice shall be published toward relevant relying parties.
- After DESC has identified the compromise scenario and established proper remedies, issuing certificates for existing and new entities may start. This shall happen according to the certificate management procedures listed in this CP document.

5.7.4 Business Continuity Capabilities after a Disaster

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

DESC establishes 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 has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document. The business continuity plan includes the following:

1. 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 determines that termination of its PKI and Subordinate CA services are deemed necessary, DESC shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

Notification procedures shall exist for informing affected entities and transferring archived CA records to an appropriate custodian. DESC shall arrange for the retention of archived data specified in section 5.5 of this CP, taking into account the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate.

If an LRA decides to terminate operations, the Agreement between Dubai PKI and the LRA shall set forth what actions are to be taken to ensure continued support for certificates previously issued by the Subordinate CAs. Upon termination of the RA Agreement, the RA certificate shall be revoked, and Dubai PKI will be the custodian of LRA archival records in case of termination.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

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

- At least four trusted persons participate in the generation and installation of Corporate CA private key(s); two trusted operatives and two key custodians
- The Corporate CA Key Generation Ceremony will be witnessed by the CA's Qualified Auditor (see section 8 Compliance Audit and Other Assessments)
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians
- The PKI operations team and key custodians act upon authorization by DESC, who is the owner of the Corporate CA private keys, to perform cryptographic operations using the Corporate CA private key(s)
- The Qualified Auditor will then issue a report, covering that the Corporate CA, during its Corporate CA Key Pair and Certificate generation process:
  - Documented its Corporate CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement
  - Included appropriate detail in its Corporate CA Key Generation Script
  - Maintained effective controls to provide reasonable assurance that the Corporate CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Corporate CA Key Generation Script
  - Performed, during the Corporate CA key generation process, all the procedures required by its Corporate CA Key Generation Script

- A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes

6.1.1.2 Subscriber Key Pair Generation

Subscriber key generation is not performed for the Corporate and Devices CA. Subscribers must generate their keys in a manner that is appropriate for the certificate type.

6.1.2 Private Key Delivery to Subscriber

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

The Corporate CA key pair shall be at least 4096-bit RSA.

The Devices 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 Corporate and Devices 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 Corporate and Devices 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

DESC shall generate subordinate key pairs and store their private keys within a Cryptographic Device that is certified according to the rating specified in 6.2.11.

Subscriber and RA key pairs shall be generated in cryptographic modules at least compliant to FIPS 140-2 Level 2 or higher.

6.2.2 Private Key Multi-Role Control

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

6.2.3 Private Key Escrow

Not applicable

6.2.4 Private Key Backup

The Corporate and Devices CA private keys shall be backed up within backup tokens that meet the same certification level as the Subordinate CA HSM and as described in section 6.2.1.

The creation of key backups on backup tokens shall be conducted using the principles of dual controls and split knowledge, involving at least two PKI officers. At least one backup of the Subordinate CAs keys shall be taken. This backup shall be stored in a locked safe at the disaster recovery site.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from an HSM

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

At no time should the CA private key be copied to disk or other media during this operation. LRA and Subscriber private keys shall not be transferred from the module they are generated in.

6.2.7 Private Key Storage on Cryptographic Module

No further stipulation other than those stated in 6.2.1.

6.2.8 Method of Activating Private Key

Private keys for the Corporate and Devices CA are activated by a minimum of two privileged users using the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the CA HSM.

Subscriber's private keys are not generated and managed by the Corporate and Devices CA.

6.2.9 Method of Deactivating Private Key

Private keys for the Corporate and Devices shall be deactivated in situations such as:

- There is a power failure within the CA room.
- The Subordinate 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 Corporate and Devices CA private keys shall be destroyed by multi-person presence, including at least one representative of the Dubai PKI PA, in order to ensure that these private keys cannot ever be retrieved and used again.

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

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

6.2.11 Cryptographic Module Rating

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

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

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

6.4.1.2 Subscribers keys

The Corporate or Devices CA shall register its subscribers prior to issuing digital certificates to the subscribers.

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

6.4.2 Activation Data Protection

Activation data for CA subscribers shall be generated randomly. Any activation data shall be bound to one subscriber only and shall have a limited lifetime. Activation data shall be transmitted via one of the following means:

- For Corporate certificates: automated process through the secure exchange of activation data between the Subordinate CAs and RA applications.
- For Devices and any OCSP certificates: at the discretion of DESC guaranteeing that only the legitimate subscriber organization representative receives the activation data.

6.4.3 Other Aspects of Activation Data

No stipulation — this section is intentionally left blank.

6.5 Computer Security Controls

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

6.5.1 Specific Computer Security Technical Requirements

The Corporate and Devices 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

6.5.2 Computer Security Rating

No stipulation — this section is intentionally left blank.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

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

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

6.6.2 Security Management Controls

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

The Corporate and Devices CA and RAs functionality shall be scanned for malicious code on first use and periodically afterward.

Upon installation, and at least once a week, the integrity of the DESC Subordinate CAs databases shall be validated.

6.6.3 Life Cycle Security Controls

No stipulation — this section is intentionally left blank.

6.7 Network Security Controls

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

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

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

6.8 Time-stamping

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

7. Certificate, CRL profiles

7.1 Certificate Profile

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

For further details, please refer to the applicable CPS.

7.1.1 Version Number

The Corporate and Devices CA shall issue X.509 version 3 certificates as defined in RFC 5280.

7.1.2 Certificate Extensions

End-entity certificates require at least the use of the following extensions. For the complete profile, refer to the applicable CPS.

- Certificate Policies (not critical)
  - Policy Identifier
  - Policy Qualifiers
    - Policy Qualifier Id
- cRL Distribution Points (not critical)
- Authority Information Access (not critical)
  - URL of the Issuing CA's OCSP responder
  - URL of the Issuing CA's certificate
- Key usage (critical): Extended key usage (not critical except for the TSA signing certificate). This extension is not required for the verification service certificate
- Authority key identifier (not critical)

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

Refer to the ASN1 definitions described in the below subsections.

7.1.7 Usage of Policy Constraints Extension

No stipulation — this section is intentionally left blank.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation — this section is intentionally left blank.

7.1.9 Processing Semantics for Critical Certificate Extensions

Critical extensions, when marked, shall be interpreted by relying parties correctly.

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

For further details, please refer to the applicable CPS.

8. Compliance Audit and Other Assessments

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

8.1 Frequency or Circumstances of Assessments

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

8.2 Identity and Qualifications of the Assessor

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

The Devices and Corporate CA are audited for compliance to one or more of the following standards:-

- AICPA/CICA Trust Service Principles and Criteria for Certification Authorities
- AICPA/CICA WebTrust for Certification Authorities — SSL Baseline with Network Security
- AICPA/CICA WebTrust for Certification Authorities — Publicly Trusted Code Signing Certificates
- These audits will be performed by qualified auditors who fulfill the following requirements:
- Independence from the subject of the audit
- The ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities v2.0

- 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

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

8.3 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 CA PKI operations environment is in compliance with the Corporate CA CP/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 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

An 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 no later than three months after the end of the audit period.

9. Other Business and Legal Matters

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

9.1 Fees

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

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

DESC guarantees the confidentiality of any data not published in the certificates issued by the CAs implementing this CP, according to the applicable laws on privacy.

9.4 Privacy of Personal Information

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

- Any personal identifiable information of citizens, other than that contained in a certificate

- Exact reason for the revocation of a certificate
- Audit trails
- Logging information for reporting purposes, such as logs of requests by the RA
- Correspondence regarding services

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

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

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

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

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

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

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

Disclosure Conditions

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

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

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

- Themselves
- Persons in their custody

Only the RA is permitted to access confidential information.

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

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

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

All communications of confidential information are encrypted, including:

- The communications link between the DESC and the (L)RA.
- Sessions to deliver certificates and certificate status information

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

9.6.3 RA Representations and Warranties

Subscribers shall represent to DESC that the Subscriber will:

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

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

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

9.8 Limitations of Liability

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

9.9 Indemnities

Not applicable.

9.10 Term and Termination

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

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

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

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The present CP is compliant to relevant, and applicable laws of Dubai.

9.16 Miscellaneous Provisions

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

- Terms and conditions in this CP
- The mandatory elements of applicable standards
- Any non-mandatory, but customized elements of applicable standards
- Content of extensions and enhanced naming not addressed elsewhere
- Any other information that is indicated to be so in a field of a certificate

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

9.17 Other Provisions

Not applicable.