# Dubai Electronic Security Center

# Dubai PKI

## Devices CA

## Certification Practice Statement

| | |
|---|---|
| **Project** | DESC CA Project |
| **Title** | Devices CA Certification Practice Statement |
| **Classification** | PUBLIC |
| **File Name** | Dubai PKI - Devices CA - Certification Practice Statement_v1.2 |
| **Created on** | 18 May 2017 |
| **Revision** | 1.2 |
| **Modified on** | 16 October 2018 |

# Document History

| Date | Revision | Author(s) | Summary |
|---|---|---|---|
| 18 May 2017 | 0.1 | | Initial version |
| 12 September 2017 | 0.2 | | Minor modifications & Incorporation of Dubai government entity Root CA option |
| 3 November 2017 | 0.3 | | Minor modifications to reflect control environment |
| 11 January 2018 | 0.4 | | Updating certificates profiles |
| 18 January 2018 | 0.5 | | Second revision of certificates profiles |
| 30 January 2018 | 1.0 | | Issue final version |
| 25 February 2018 | 1.1 | | Update SSL server certificate profile and add Verification response signing certificate<br>Update publication of certificate information |
| 16 October 2018 | 1.2 | | • Updates based on review of alignment with SSL BRs<br>• Update the profiles of the SSL certificate and the Verification response signing certificate |

# Table of Contents

# 1. Introduction

This Certification Practice Statement (CPS) describes the certification practices that apply to the digital certificates issued by the Dubai Public Key Infrastructure (PKI) Devices Certification Authority (CA). The Devices CA is one of the subordinates CAs signed by the Dubai Root CA. This CPS covers the issuance and controls surrounding the following types of certificates:

- **Device Certificates** — Certificates for device identification and authentication
- **VPN Certificates** — Certificates for device identification and session data encryption for IPSec-based connections. These certificates can be considered as a subset of the devices certificates with the specific purpose of securing VPN connectivity.
- **SSL Certificates** — Certificates for server authentication and session data encryption
- **Certificates Issued for Time stamping Authority (TSA)** — Certificates for signing timestamps issued by the Dubai PKI TSA service.
- **Verification Response Signing Certificates** — Certificates for the Dubai PKI Signature Verification Service to sign verification responses related to certificates issued by the Dubai PKI.
- **OCSP Certificates** — Certificates for the DESC Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by this CA.

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 board is referred to in this CP document as the Dubai PKI PA.

## 1.1 Overview of Dubai PKI

DESC manages a PKI referred to as the “Dubai PKI” that uses standard PKI technologies, policies and operating procedures and application interfaces. The Dubai PKI comprises the Dubai 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 two Subordinate Certification Authorities (CAs), which come at the second level of the PKI hierarchy. Certification services provided by this PKI enable citizens, residents and government entities in the UAE to conduct secure electronic transactions; this includes securing the machine-to-machine communication where devices can transact securely, leveraging the PKI signing and encryption capabilities.

Additionally, the Dubai Root CA also issues subordinate CAs belonging to other Dubai government 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 Dubai government entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai Root CA. There are two options for issuing these CAs: Option 1 is to directly issue a Dubai Government entity issuing CA from the Dubai Root CA, which is a technically constrained subordinate CA[1] owned and operated by a Dubai Government entity. Option 2 is for entities requiring more scalable hierarchy, met by issuing them two hierarchical levels of subordinate CAs – an unconstrained Dubai Government entity Root CA that comes directly under the

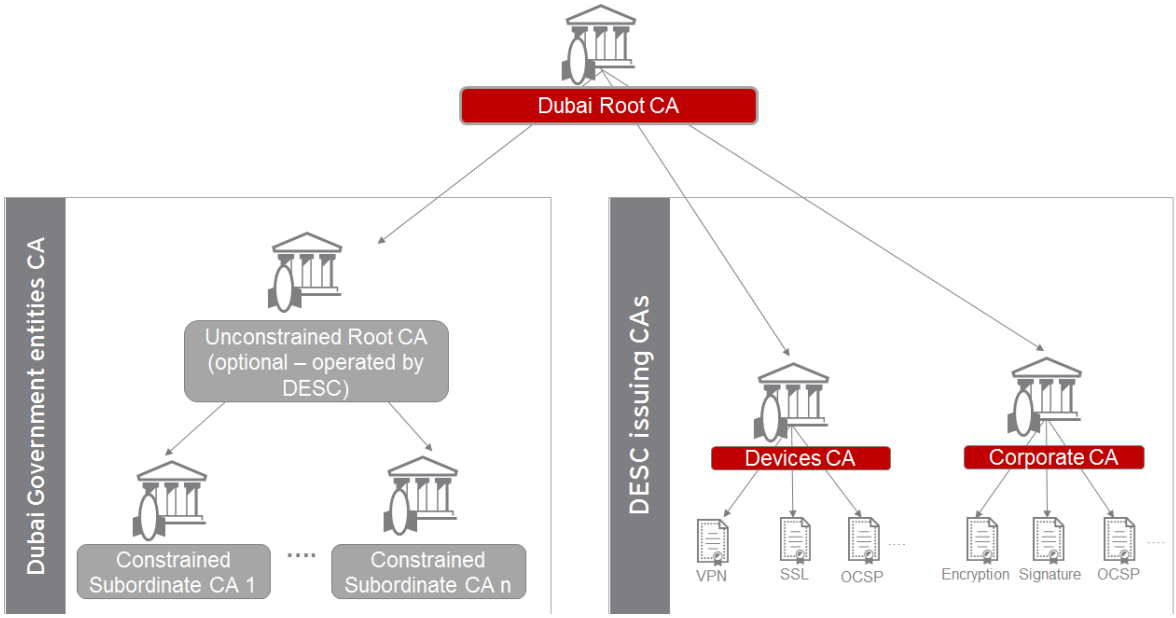
[1] *A Subordinate CA with a certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates*

Dubai Root CA, and a technically constrained Dubai Government entity issuing CA(s) that comes under the Dubai Government entity Root CA.

The Dubai 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 Root CA is the top authority in this PKI with regard to digital certification services offered in Dubai. The Dubai Root CA signs DESC Subordinate Certification Authorities (CAs), which come at the second level of the PKI hierarchy. In addition, the Root CA also signs subordinate CAs belonging to authorized Dubai government entities.




*Trust Model for Dubai PKI*

### 1.1.2 Certification Services

The certification services offered by this CA are outlined as follows:

- **Registration Service** — it verifies the identity and, if applicable, any specific attributes of end-entities applying for certificates. The results of this service are passed to the certificate generation service.
- **Certificate Generation Service** — it creates and signs end-entity certificates based on the verification conducted by the registration service
- **Dissemination Service** — it disseminates TSA, OCSP and Devices CA certificates and makes them available to relying parties. This service also makes available any public policy and practice information to subscribers and relying parties.
- **Revocation Management Service** — it processes requests and reports revocation data for determining the appropriate action to be taken. The results of this service are available through the certificate validity status service.
- **Certificate Validity Status Service** — it provides certificate validity status information to relying parties based upon certificate suspension/revocation lists and an OCSP responder

service. The status information shall always reflect the current status of the certificates issued by this CA.

# 1.2 Document Name and Identification

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

The Object Identifier of this CPS is OID is .2.16.784.1.2.2.100.1.2.1.2 .

DESC organizes the OID for the certificates that are issued by the Devices CA as depicted in the table below.

| 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 | Certificates for 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 | A 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 Devices CA are as follows:

- Subordinate Certification Authorities
- Registration Authority (RA)
- Subscribers
- Relying Parties

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

## 1.3.1 Subordinate Certification Authorities

The Devices CA (further referred to as “CA”) issues certificates for IT systems and infrastructure devices and other devices belong to Government entities in addition to OCSP response signing certificates and Dubai PKI signature verification service. This includes the following tasks:

- 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 TSA, OCSP and Devices CA certificates to a public repository
- Maintaining and providing certificates status information through publicly available CRL and OCSP mechanisms

### 1.3.2 Registration Authorities

Duly authorized members part of DESC PKI team act as Registration Authority (RA) for this CA. This team is involved in validating and accepting certificate issuance and management operations, in addition to triggering related certification operations by this CA.

### 1.3.3 Subscribers

IT systems, such as OCSP responder, Signature verification service, TSA, web servers and infrastructure devices, such as VPNs, routers, switches and other devices.

Individuals with a formal mandate (authorization) request infrastructure certificates for devices and IT systems. They undergo a dedicated enrollment process through which they provide Certificate Signing Request (CSR) either automatically through the supported device enrollment protocols or manually by submitting CSR files to a designated DESC RA Officer.

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

### 1.3.4 Relying Parties

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

### 1.3.5 Other Participants

There are no other participants for this CA.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Use

There are five categories of certificates issued by this CA. They are:

- **Device Certificates** — Used for device identification and authentication
- **VPN Certificates** — Used for device identification and session data encryption for IPSec-based connections
- **SSL Certificates** — Used for server authentication and session data encryption
- **Signature verification service certificate** — Used by the DESC signature verification service to sign verification responses generated by the service
- **Certificates Issued for Time stamping Authority (TSA)** — Used to sign the time stamps issued by the Dubai Time Stamping Authority service
- **OCSP Certificates** — Used by the DESC Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by this CA

In accordance with its purpose of use, the certificate may be used without limitations in services provided by the Government entities.

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

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

### 1.4.2 Prohibited Certificate Use

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

# 1.5 Policy Administration

### 1.5.1 Organization Administering the Document

DESC, through the Dubai PKI PA, bears responsibility for the drafting, publishing, Object Identifier (OID) registration, maintenance and interpretation of this CP and other policies and practices within the realm of the Dubai PKI.

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

a. Specifying and approving the Dubai PKI infrastructure

b. Approving Dubai government entity applications to have their own Subordinate CA(s) within the Dubai PKI hierarchy

c. Specifying, maintaining and approving the Dubai PKI practices and policies, in particular the Certification Practice Statements (CPS) and the related Certificate Policies (CPs) when applicable

d. Defining the review process for such practices and policies including responsibilities for maintaining the Dubai PKI CP/CPSs and related policies

e. Defining the review process that ensures that the Dubai PKI properly implements the above practices

f. Defining the review process that ensures that the related policies are supported by the Dubai PKI CP and CPSs

g. Publication of CP and CPSs and of its revisions

h. Specifying installation, key ceremonies, operation and life cycle management (including depreciation) procedures of the Dubai PKI

i. Evaluating the proper working of the Dubai PKI environment

j. Allocating members to the key ceremonies as witness, as well as trusted operatives and key custodians

k. Evaluating of changes to the Dubai PKI environment (management, operational, hardware, software and security)

l. Evaluating case-by-case issues where key DESC staff/personnel did not respect the security and/or operational procedures, including ethics

m. Deciding on critical issues in case of incidents, disasters and other severe problems with regard to 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

### 1.5.3 Person Determining CPS Suitability for the Policy

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

### 1.5.4 CP Approval Procedures

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

## 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/ class of application with common security requirements

**Certification Practice Statement (CPS)** — A statement of the practices which 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

**IEC** — International Electro-technical Commission

**IETF** — Internet Engineering Task Force

**IPSEC** — Internet Protocol Security

**ISO** — International Standards Organization

**Issuer** — The name of the CA that signs the certificate

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

**ITU** — International Telecommunications Union

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

**DESC** — Dubai Electronics Security Center

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

**OSCP** — Online Certificate Status Protocol

**OTP** — One Time Password

**PA** — Policy Authority of Dubai PKI

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

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

**PKCS # 7** — Cryptographic Message Syntax

**PKCS #10** — Certification Request Syntax Specification

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

**PKE** — Public Key Encryption

**PKI** — Public Key Infrastructure

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

**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/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

**SCEP** — Simple Certificate Enrolment Protocol

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

**SHA** — Secure Hash Algorithm

**S/MIME** — Secure Multipurpose Internet Mail Extensions

**SSL/TLS** — Secure Sockets Layer/Transport Layer Security

**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** — A subject is the entity named in a certificate

**Subscriber** — A subject who is issued a certificate

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

**UPS** — Uninterruptible Power Supply

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

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

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

### 1.6.2 Acronyms

Please refer to section 1.6.1.

### 1.6.3 References

The Devices CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those requirements, the requirements take precedence over this document.

The Devices CA conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. If there is any inconsistency between this document and those requirements, 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 Devices CA certificates, OCSP certificates and TSA certificates at this location. An updated version of this CPS is published at the least, annually. DESC reserves its rights to publish certificate status information on third-party repositories.

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

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

DESC operates the certificate status repository for the Devices 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

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

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 Devices CA:

- At the minimum, CRLs shall be refreshed every 24 hours, even if no changes have occurred since the last issuance.
- CRLs lifetime shall be set to 26 hours (24 hours update period + 2 hours pre-update period).

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 Devices CA activities.

# 2.4 Access Controls on Repositories

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

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

# 3. Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

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

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

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

- **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 < 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 = <FQDN> or <IP address> of the server, service, or application
  ou = <optional organizational unit within the organization>
  o = <organization meaningful unique name>
  l = <organization's locality information>
  c = AE

  Wildcard SSL Certificates include a wildcard asterisk character as the first character in the Common Name (CN) attribute of the Subject field and or in the SubjectAltName extension.

- **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

Distinguished Names (DN) are used to identify both the subject and the issuer of the certificate in a meaningful way. Hence, this CA issues certificates to subscribers (subjects) that demonstrate legitimately ownership and control on the domain names, IP addresses mentioned in the Subject DN.

### 3.1.3 Anonymity and Pseudonymity of Subscribers

This CPS does not permit anonymous subscribers.

### 3.1.4 Rules for Interpreting Various Name Forms

No stipulation — this section is intentionally left blank.

### 3.1.5 Uniqueness of Names

The usage of Fully Qualified Domain Names (FQDNs), unique device identifier, IP address or unique system common names agreed with DESC, guarantees the uniqueness of DNs. Devices may have several alias names supported by this CA. The usage of internal domain names and reserved IP addresses is prohibited.

For SSL certificates, the Subject Alternative Name extension must be used to define the applicable domain and one or more additional domain names for the certificate.

### 3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation — this section is intentionally left blank.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

Certificate Signing Requests (CSRs) generated by IT systems or devices contain a Proof-of-Possession (POP) of the private key as part of the certificate requests submitted to this CA.

### 3.2.2 Authentication of Government Entity Identity

For all certificates that contain the identity of a Government entity, the applicant is required to provide the Government entity's name, organizational unit (if applicable) and official address. DESC RA will verify this information against a trusted government register listing entities and their representatives.

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

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

### 3.2.3 Authentication of Individual Identity

The Devices CA issues certificates for IT systems and devices belong to Government entities applicants must apply for these certificates through DESC RA.

DESC RA officers perform verification of the identity of the applicant for a certificate through the following procedures:

1. The applicant appears in person at DESC and present his/her Emirates ID card and proof of employment by a Government entity.
2. DESC RA conducts an identity proofing through face-to-face verification of the applicant against his/her Emirates ID Card.
3. DESC RA uses the proof of employment to validate the association between the applicant and the Government entity.
4. DESC RA identifies the IT system or device for which certificate(s) shall be requested from this CA. These IT systems or devices must be part of the IT infrastructure of a government entity in Dubai.
5. The DESC RA verifies that the applicant is a legitimate sponsor or authorized device or system administrator of the device or system for which certificate(s) shall be requested.

For DESC TSA service, signature verification service and OCSP responder, an authorized administrator under the supervision of the Dubai PKI PA initiates the certification process. DESC documents a dedicated operational key ceremony.

### 3.2.4 Authentication of Domain name

For SSL certificates:

DESC RA validates the domain ownership for the domains to be added in the certificate through the following methods:

- **Email validation:** By sending an e-mail with a random, unique value to an administrative e-mail address associated with the domain (i.e. admin@example.com). If the applicant replies to the e-mail, and that e-mail includes the original random value as sent by DESC, the validation passes. The reply should be within three days.
  This validation may be performed using the following e-mail addresses:
  admin@, administrator@, webmaster@, hostmaster@, postmaster@
- **Website change:** By requesting the applicant to proof ownership over a domain by performing changes to the website provided on the domain.
- **DNS record validation:** By requesting the applicant to proof ownership over a domain by performing changes to the DNS configuration of the domain.

DESC RA validates the ownership for the IPs to be added in the certificate through the following methods:

- Proof control over the IP Address by asking the application to apply an agreed-upon change to information found on an online Web page identified by a URI containing the IP Address;
- Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name
- Requesting documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry

- Email challenge based on email address or via phone information listed in the IANA or similar repository

### 3.2.5 Non-Verified Subscriber Information

The DESC RA verifies all subscriber information contained within certificate issued by the Devices CA.

### 3.2.6 Validation of Authority

The authority of the certificate requestor to request a certificate on behalf of a Government entity will be performed through a reliable means of communication with the Government entity that include the following steps at minimum: (1) DESC RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized signatory that attests the ability of the requestor to requests certificates on behalf of the government entity. (2) DESC RA verifies the existence of the government entity and their authorized signatory against a trusted government register listing entities and their representatives

### 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 for re-keying is performed as in initial registration.

### 3.3.2 Identification and Authentication for Re-Key After Revocation

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

## 3.4 Identification and Authentication for Revocation Requests

DESC RA shall verifies that an authorized representative has requested the revocation through one of the following methods:

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

Once the revocation request is successfully authenticated, DESC RA revokes the subject certificate through the relevant RA system.

TSA, signature verification service and OCSP certificates revocation shall be conducted as part of DESC internal processes and shall be approved by the Dubai PKI PA.

# 4. Certificate Life Cycle Management

## 4.1 Certificate Application

### 4.1.1 Who can Submit a Certificate Application

A Government entity authorized device or system administrator.

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

### 4.1.2 Enrolment Process and Responsibilities

The certificate enrolment process is described below:

- The DESC RA receives a certificate application form. He then identifies the applicant as described in Section 3.2.3
- The DESC RA asks the subscriber to sign the Subscriber Agreement and the certificate application form
- The applicant submits the certificate application form to the DESC RA officer
- Once the application is approved by DESC, the application executes the certification request process either manually or automatically using certificate management protocol such as SCEP:

  **Manual certification request:**

  - The DESC RA officer uses a dedicated RA application to enroll the IT system or device into this CA. The IT system or device's unique name taken from the application form is used to produce a unique distinguished name identifying it within this CA system. As part of the enrolment, DESC RA generates a unique authorization code for this certificate application and submits this code to the applicant email address (as provided in the certification application form)
  - The subscriber generates a key pair on its own IT system or device. He then creates a CSR file using the received authorization code provided by DESC RA, the CSR should include a Proof-of-Possession (POP) of the private key
  - The CSR file is sent to DESC RA through the entity representative email (as provided in the certificate application form)
  - DESC RA submits the CSR along with the authorization code to the CA in order to and retrieve the certificate

    Note: this step can also be conducted by the subscriber himself (or IT system/Device administrator) through the RA application exposed over a private network, in this case

the below step is omitted since the subscriber will be able to download the certificate directly once issued by the CA

- DESC RA send the certificate to the entity representative email address

**Automatic certification request (through SCEP protocol):**

- DESC RA officer provides the administrator of the IT system or Device with the required parameters to established communication with the CA and submit an authorized certificate request
- The administrator configures the system/device with the parameters given by DESC RA officer, then initiate the certification request from the system or device
- DESC RA offices generates an OTP that is used to authorize the system/device while communicating with the CA
- The administrator configures the system/device to pass the OTP along with the certificate request, The system/device communicates with the CA that authorizes the system/device based on the OTP
- The CA validates the certificate request and the prove possession of the private key then issues the certificate and send it back to the system/device
- The system/device validates the certificate and installs it

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

# 4.2 Certificate Application Processing

## 4.2.1 Performing Identification and Authentication Functions

As stated in Section 4.1.

For SSL certificate applications, Certificate Authority Authorization (CAA) records are verified; the CAA records are DNS records that a subscriber can configure on its domain to specify which CA can issue certificates for the respective domain. If the CAA record is undefined or pointing towards DESC CA, DESC will proceed with processing the certificate application.

Whenever the ‘issue’ and ‘issuewild’ tags are present within a CAA record, DESC verifies that those tags contain DESC.GOV.AE as granting authorization for issuance by DESC.

## 4.2.2 Approval or Rejection of Certificate Applications

The DESC RA officer approves or rejects the application for the certificate as part of the overall approval/rejection of the certificate issuance process.

OCSP, Signature verification and TSA certifications are conducted as part of the DESC’s internal processes and shall be approved by the Dubai PKI PA.

## 4.2.3 Time to Process Certificate Applications

No stipulation — this section is intentionally left blank.

# 4.3 Certificate Issuance

### 4.3.1 CA Actions During Certificate Issuance

Following the approval of the certificate application by the DESC RA, the CSR is uploaded and submitted to the CA either manually using a dedicated RA application or automatically through one of the mentioned certificate management protocols.

The CA then signs the certificate in accordance with the specified certificate template. The certificate is activated by the CA and is ready for usage. The certificate then delivered to the subscriber as follows:

- **For Certificates issued to IT systems and Devices** —The certificate is sent by the RA officer to the subscriber's email address or downloaded by the subscriber directly or downloaded by the system/device through one of the mentioned certificate management protocols.
- **For TSA, Signature verification service and OCSP Certificates** —The DESC administrator manually delivers the CSR file including the device's PEM or DER encoded public key to the CA administrator. The CA administrator submits the CSR file directly to the CA who will sign and publish a certificate suitable for verification. The certificate is returned to the DESC administrator thereafter

### 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

In case of a CSR is submitted manually, the RA Officer notifies the subscriber to collect his or her certificate.

In case of using an automated certificate management protocol, the subscriber is notified through its system/device once the certificate is automatically received from the CA.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct Constituting Certificate Acceptance

The user confirms certificate acceptance upon signing a dedicated form.

TSA, Signature verification service and OCSP certificates shall be issued as part of DESC internal processes and the Dubai PKI PA approves it.

### 4.4.2 Publication of the Certificate by the CA

Devices 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

When using a subscriber's private key and corresponding certificate, a subscriber is obligated to:

- Use certificates exclusively for legal activities consistent with this CPS

- Comply with the terms of the subscriber agreement
- Avoid using the private key until after the CA has issued, and the subscriber has accepted the corresponding certificate
- Discontinue the use of a private key following expiration or revocation of the corresponding certificate unless a subsequent unexpired or unrevoked certificate corresponding to that private key has been issued

### 4.5.2 Relying Party Public Key and Certificate Usage

When using a subscriber's public key and corresponding certificate, a relying party is obligated to:

- Validate the certificate path
- Ensure that the key is appropriate for the intended use as set forth in this CPS and that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage, and certificate policies extension fields.
- Check the status of the certificate in accordance with the requirements stated in Section 4.9.6 of this CPS. As part of the validation process, the authenticity of the revocation must be validated as follows:
  - In case of using CRLs, the digital signature of the CRLs is validated
  - In case of using OCSP, the digital signature of the OCSP response is validated
- Ensure that reliance was reasonable and made in good faith in light of all the circumstances that were known or should have been known to the relying party at the time of reliance

If a party relying on the Dubai PKI accepts a certificate that cannot be validated through the Devices CA OCSP or CRL, it decides to do so completely at his or her own risk.

## 4.6 Certificate Renewal

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

This CA does not support certificate Renewal. Only certificate re-key is supported.

## 4.7 Certificate Re-Key

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

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

### 4.7.1 Circumstance for Certificate Re-key

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

### 4.7.2 Who May Request Certification of a New Public Key

As per initial certificate

### 4.7.3 Processing Certificate Re-Keying Requests

As per initial certificate

### 4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per initial certificate

### 4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certificate

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per initial certificate

## 4.8 Certificate Modification

This CPS 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 CPS 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

An individual or an authorized Government entity's representative may request a revocation of his or her certificate if:

- The subscriber discovers or has reasons to believe that there has been a compromise of the private signing key
- The information on the certificate is no longer accurate, for example, a change of DNS name or a system has been decommissioned

This CA will revoke the certificate upon:

- The request of the individual or an authorized Government entities' representative
- Knowing that the information on the certificate is no longer accurate
- Discovering that the certificate was issued in a manner not materially in accordance with the procedures required by the CPS
- Determination that the certificate was issued to an entity other than the one named as the subject of the certificate
- The Government entity or the subscriber has been declared legally incompetent
- A third party provides information that leads the CA to believe that the certificate is compromised or is being used for suspect code

On the other hand, this CPS does not provide provisions for revoking an OCSP/TSA/Signature verification service certificates apart from the compromise of the OCSP/TSA/Signature verification service key pair which is treated by DESC as per its disaster recovery and business continuity procedures. The following sub-sections focus only on the revocation provisions that apply to the other certificates issued by this CA.

### 4.9.2 Who can Request Revocation

- The Subscriber or an authorized representative
- The Government entity to whom certificates were issued, may request revocation
- Any relying party possessing evidence of compromise of the subscriber's certificate may request revocation from DESC
- DESC's RA officers directly initiate revocations in the cases described in Section 4.9.1
- DESC at its own discretion (if for instance, a compromise is known for this CA key)

### 4.9.3 Procedure for Revocation Request

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

1. DESC RA officer looks up DN in the RA application
2. Selects the desired certificate

3. Selects “Revoke this certificate”
4. Enter revocation reason and submit
5. The CA produces a new CRL which is published to its repository

OCSP/TSA/Signature verification service certificates revocation is conducted as part of a PKI process internal to the DESC and approved by the Dubai PKI PA. This process involves communications with relying parties in order to update them on the OCSP/TSA/Signature verification service certificate revocation.

### 4.9.4 Revocation Request Grace Period

There is no revocation grace period. The CA processes revocation requests as per schedule or immediately.

### 4.9.5 Revocation Request Response Time

Certification revocation requests and problem reports must be processed within 24 hours.

### 4.9.6 Revocation Checking Requirement for Relying Parties

This PKI offers revocation information to relying parties through CRLs published on a publicly available web server and through its publicly available OCSP responder.

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

### 4.9.7 CRL Issuance Frequency

CRLs are issued as per Section 2.3 or this document.

### 4.9.8 Maximum Latency for CRLs

No stipulation — this section is intentionally left blank.

### 4.9.9 Online Revocation/Status Checking Availability

OCSP is supported within this PKI solution and is compliant with RFC 6960. OCSP information is available immediately to relying party applications.

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

### 4.9.10 Online Revocation Checking Requirements

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

### 4.9.11 Other Forms of Revocation Advertisements Available

No stipulation — this section is intentionally left blank.

### 4.9.12 Special Requirements — Key Compromise

No stipulation — this section is intentionally left blank.

### 4.9.13 Circumstances for Suspension

Certificate suspension is not supported by this CA.

### 4.9.14 Who Can Request Suspension

Not applicable.

### 4.9.15 Procedure for Suspension Request

Not applicable.

## 4.10 Certificate Status Services

Refer to Section 4.9.6 of this document. In addition, the following provisions are made.

### 4.10.1 Operational Characteristics

CRLs are published by this CA on a public repository which is available to relying parties. Apart from CRLs distributed at distribution points, DESC also publishes combined (uniform) CRLs on its public repository.

The DESC OCSP responder exposes an HTTP interface accessible to relying parties.

### 4.10.2 Service Availability

The repository including the latest CRL should be available 24X7 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

Key escrow and recovery are not supported by this CA.

# 5. Facility, Management and Operational Controls

## 5.1 Physical Controls

### 5.1.1 Site Location and Construction

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

### 5.1.2 Physical Access

Physical security controls include security guard controlled building access, man traps, biometric IRIS access and CCTV monitoring. These physical controls protect the hardware and software from unauthorized access, furthermore these controls are monitored on a 24*7*365 basis.

### 5.1.3 Power and Air Conditioning

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

### 5.1.4 Water Exposures

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

### 5.1.5 Fire Prevention and Protection

The enclave must be protected from fire, heat with a smoke detection equipment monitored on a 24*7*365. Fire suppression equipment must be installed within the enclave.

### 5.1.6 Media Storage

Electronic optical and other media must be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains security audit archive and backup information must be stored in a secure fire-protected safe while within the enclave.

### 5.1.7 Waste Disposal

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

### 5.1.8 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 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.

### 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 a 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:

- Personnel managing operations on certificates
- Administrative personnel who operate the supporting platform

- Security personnel who 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 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 makes the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

## 5.3.3 Training Requirements

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 to avoid dependency on key staff members.

## 5.3.6 Sanctions for Unauthorized Actions

DESC sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the 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

### 5.4.1 Types of Event Recorded

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. DESC ensures that at least the following details are recorded:

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

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

### 5.5.4 Archive Backup Procedures

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

### 5.5.5 Requirements for Time stamping of Records

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

Only authorized and authenticated staff is allowed to handle archived material.

### 5.5.6 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

Devices CA private keys are maintained until such time as all relying certificates have expired.

# 5.7 Compromise and Disaster Recovery

## 5.7.1 Incident and Compromise Handling Procedures

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

## 5.7.2 Computing Resources, Software Data Corruption

DESC and all other PKI Participants (other than Subscribers and Relying Parties), establish the necessary measures to ensure full recovery of Devices CA 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 with 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 Devices CA, the following actions shall be taken by DESC:

- All active certificates issued by the Devices CA shall be revoked
- Organizations holding Client Certificates shall be notified
- A new Devices CA key pair shall be generated and certificate produced by the Dubai Root CA
- A Devices 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 CPS 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. 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 this 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.

# 6. Technical Security Controls

## 6.1 Key Pair Generation

The requirements for generating and installing the Devices CAs are stated in the following sections.

### 6.1.1 Key Pair Generation

#### 6.1.1.1 CA Key Pair Generation

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

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

#### 6.1.1.2 Subscriber Key Pair Generation

The Devices CA does not perform subscriber key generation.

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

| Certificate Type | Key generation requirements |
|---|---|
| Device certificates | Key pair is generated using a FIPS-approved methods for key generation |
| VPN certificates | Key pair is generated using a FIPS-approved methods for key generation |
| SSL server certificates | Typically the key generation utility provided with the web server software is used to generate keys |
| Time stamping certificates | Key generation is done using a dedicated Timestamping service key management utility. The Timestamping signing key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module |
| Signature Verification Service certificates | Key generation is done using a dedicated verification services key management utility. The verification services key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module |
| OCSP certificates | Key generation is done using a dedicated OCSP key management utility. The OCSP key pair is generated inside the memory of a FIPS 140-1 level 3 hardware security module |

### 6.1.2 Private Key Delivery to Subscriber

Not applicable.

### 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 and 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

This Devices CA key pair is 4096 bit RSA.

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

### 6.1.6 Public Key Parameters Generation and Quality Checking

The 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)

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

#### 6.1.7.1 Devices CA Certificate

| **CA Signing** |
|---|
| CA signing keys are the only keys permitted to be used for signing Certificates and CRLs.<br>The Certificate Key Usage field must be set to: Key Cert Sign and cRL Sign. |

**Table 1**: Devices CA Key Usage

#### 6.1.7.2 Subscribers

| **Device Certificate** | **VPN Certificate** |
|---|---|
| The Certificate Key Usage field will be set to:<br>Key usage: Bit string {digitalSignature, keyEncipherment } | The Certificate Key Usage field will be set to:<br>Key usage: Bit string {digitalSignature} |
| **SSL Certificate** | **Time Stamping Certificates** |
| The Certificate Key Usage field will be set to:<br>Key usage: Bit string {digitalSignature, keyEncipherment} | The Certificate Key Usage field will be set to:<br>Key usage: Bit string {digitalSignature} |

**Table 2**: Subscriber's Key Usage

# 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 HSM that is certified according to the rating specified in 6.2.11.

## 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 Devices CA private keys shall be backed up within backup HSMs 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 HSMs 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

No stipulation — this section is intentionally left blank.

## 6.2.6 Private Key Transfer into or From a HSM

The Devices CA key pairs shall only be transferred to another hardware cryptographic device 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.

## 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

A minimum of two privileged users activate the private keys for the Devices CA 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 Devices CA.

### 6.2.9 Method of Deactivating Private Key

This CA's private Key is deactivated in the following situations:

- The CA software is shut down.
- The CA HSM is manually stopped.
- There is a power failure within the CA room.
- The CA HSM is operated outside the range of supported temperatures.
- The HSM detects a security breach and deletes all key material within its internal memory.

When private keys are deactivated, they are cleared from memory before the memory is de-allocated. Any disk space where keys were stored must be overwritten 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 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 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 shall use an HSM certified to FIPS 140-2 Level 3 or ISO 15408 Common Criteria (CC) EAL 4+ or above.

## 6.3 Other Aspects of Key Pair Management

### 6.3.1 Public Key Archival

Refer to Section 5.5 of this CP.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

- The maximum operational period of the CA's key pair must be set for eight years
- The maximum operational period for a subscriber's key pair must be five years

| Key Certificate Type | Maximum Validity Period |
|---|---|
| Certification Authority Certificate and associated keys | Recommended 96 months, re-key at 37% lifetime, i.e., 36 months |
| Certificates for subscribers and associated keys | Maximum operational period for a subscriber's key pair must be 36 months |

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

#### 6.4.1.1 CA Key Generation

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

During the Key Generation ceremony of a 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 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 an automated process through the secure exchange of activation data between the Devices CA and RA applications.

### 6.4.3 Other Aspects of Activation Data

No stipulation — this section is intentionally left blank.

## 6.5 Computer Security Controls

The 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 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 CA's history and audit data
- Audit of security related events
- Automatic and regular validation of the CA systems' integrity
- Recovery mechanisms for keys and CA systems
- Hardening CA servers operating system according to best practices and PKI vendor requirements
- Network protection, including intrusion detection systems

### 6.5.2 Computer Security Rating

No stipulation — this section 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 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 the NTP.

# 7. Certificate, CRL and OCSP Profiles

## 7.1 Certificate Profile

### 7.1.1 Devices Certificate Profile

This is the complete ASN1 description of the devices certificate.

| Field | CE[2] | O/M[3] | CO[4] | Value | Comment |
|---|---|---|---|---|---|
| Certificate | | M | | | |
| TBSCertificate | | M | S | | See 4.1.2 of RFC 3280 |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| signatureValue | | M | D | Devices CA Signature | CA signature value |
| TBSCertificate | | | | | |
| Version | False | | | | |
| | | M | S | 2 | Version 3 |
| SerialNumber | False | | | | |
| certificateSerialNumber | | M | D | | At least 64 bits of entropy<br>Validated on duplicates. |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| countryName | | M | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| | organizationName | | M | S | UAE Government | UTF8 encoded |
| | commonName | | M | S | Devices Certification Authority | UTF8 encoded |
| Validity | | False | M | | | Implementations MUST specify using UTC time until 2049 from then on using Generalized Time |
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + not more than **[36]** Months | |
| Subject | | False | M | | | |
| | countryName | | M | S | AE | Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| | organizationUnitName | | O | D | Allocated as per certificate request | UTF8 encoded |
| | organizationName | | M | D | Allocated as per certificate request | UTF8 encoded |
| | localityName | | M/O | D | Dubai | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| | stateOrProvinceName | | M/O | D | Dubai | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| | commonName | | M | D | System unique common name, unique device identifier or IP address that are applicable | UTF8 encoded |
| subjectPublicKeyInfo | | False | M | | | |
| | algorithm | | | D | RSA/ECDSA | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | subjectPublicKey | | M | D | Public Key length: 4096 (RSA) | |
| Extensions | | | M | | | |
| Authority Properties | | | | | | |
| authorityKeyIdentifier | | False | M | | | |
| | keyIdentifier | | M | D | SHA-1 Hash of the devices CA public key | |
| authorityInfoAccess | | False | M | | | |
| | accessMethod | | M | S | Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp) | OCSP Responder field |
| | accessLocation | | M | D | http://ca-services.desc.gov.ae/adss/ocsp | OCSP responder URL |
| | accessMethod | | O | S | Id-ad-2 2 id-ad-caIssuers OID i.e.1.3.6.1.5.5.7.48.2 (ca cert) | CA Issuers field |
| | accessLocation | | O | D | http://ca-repository.desc.gov.ae/certificate/devices.p7b | Devices CA Certificate download URL |
| cRLDistributionPoints | | False | O | | | |
| | distributionPoint | | O | D | http://ca-repository.desc.gov.ae/CRL/Devices/devices_certification_authority_uae_government_ae_crlfile<CRLNumber>.crl | CRL download URL |
| Subject Properties | | | | | | |
| subjectKeyIdentifier | | False | M | | | |
| | keyIdentifier | | M | D | SHA-1 Hash | |
| | | | | | | |
| Key Usage Properties | | | | | | |
| keyUsage | | True | M | | | |
| | digitalSignature | | M | S | True | |
| | keyEncipherment | | M | S | True | |
| extendedKeyUsage | | False | M | | | |
| | clientAuth | | M | S | True | |
| Certificate Policy Property | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | certificatePolicies | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | D | URL location of this CPS | |
| | certificatePolicies | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.2.3.1 | |

### 7.1.2 SSL Certificate Profile

This is the complete ASN1 description of the SSL certificate.

| Field | CE[5] | O/M[6] | CO[7] | Value | Comment |
|---|---|---|---|---|---|
| Certificate | | M | | | |
| TBSCertificate | | M | S | | |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| signatureValue | | M | D | Devices CA Signature | CA signature value |
| TBSCertificate | | | | | |
| Version | False | | | | |
| | | M | S | 2 | Version 3 |
| SerialNumber | False | | | | |
| certificateSerialNumber | | M | D | | At least 64 bits of entropy<br>Validated on duplicates |
| Signature | False | M | | | |
| Algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| countryName | | M | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| organizationName | | M | S | UAE Government | UTF8 encoded |
| commonName | | M | S | Devices Certification Authority | UTF8 encoded |
| Validity | False | M | | | Implementations MUST specify using UTC time until 2049 from then on using Generalized Time |
| NotBefore | | M | D | Certificate generation | |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + not more than **[27]** Months | |
| Subject | | False | M | | | |
| | countryName | | M | S | AE | Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| | organizationUnitName | | O | D | Allocated as per certificate request | UTF8 encoded |
| | organizationName | | M | D | Allocated as per certificate request | UTF8 encoded |
| | localityName | | M/O | D | Dubai | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| | stateOrProvinceName | | M/O | D | Dubai | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| | commonName | | M | D | Domain name(s) or public IP address that are applicable, potentially linked to the Subject Alternative Name extension | UTF8 encoded |
| subjectPublicKeyInfo | | False | M | | | |
| | algorithm | | M | D | RSA/ECDSA | |
| | subjectPublicKey | | M | D | Public Key length: 2048 or 4096 (RSA)/256 or 384 (ECDSA) | |
| Extensions | | | M | | | |
| Authority Properties | | | | | | |
| authorityKeyIdentifier | | False | O | | | Mandatory in all certificates except for self-signed |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | certificates |
| keyIdentifier | | M | D | SHA-1 Hash of the Devices CA public key | When this extension is used, this field MUST be supported at minimum |
| authorityInfoAccess | False | M | | | |
| accessMethod | | M | S | Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp) | OCSP Responder field |
| accessLocation | | M | D | http://ca-services.desc.gov.ae/adss/ocsp | OCSP responder URL |
| accessMethod | | O | S | Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert) | CA Issuers field |
| accessLocation | | O | D | http://ca-repository.desc.gov.ae/certificate/devices.p7b | Devices CA Certificate download URL |
| cRLDistributionPoints | False | O | | | |
| distributionPoint | | O | D | http://ca-repository.desc.gov.ae/CRL/Devices/devices_certification_authority_uae_government_ae_crlfile<CRLNumber>.crl | CRL download URL |
| Subject Properties | | | | | |
| subjectKeyIdentifier | False | M | | | |
| keyIdentifier | | M | D | SHA-1 Hash | |
| subjectAltName | False | M | D | Allocated as per certificate request | Domain name(s) that are applicable, linked to the subject common name field |
| Key Usage Properties | | | | | |
| keyUsage | True | M | | | |
| digitalSignature | | M | S | True | |
| keyEncipherment | | M | S | True | |
| extendedKeyUsage | False | M | | | |
| serverAuth | | M | S | True | |

| Certificate Policy Property | | | | | |
|---|---|---|---|---|---|
| certificatePolicies | False | O | | | |
| policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.1.2 | |
| policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| policyQualifiers:qualifier:cPSuri | | M | D | URL location of this CPS | |
| certificatePolicies | False | M | | | |
| policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.2.3.2 | |

## 7.1.3 VPN Certificate Profile

This is the complete ASN1 description of the VPN certificate.

| Field | CE[8] | O/M[9] | CO[10] | Value | Comment |
|---|---|---|---|---|---|
| Certificate | | M | | | |
| TBSCertificate | | M | | | |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| signatureValue | | M | D | Devices CA Signature | CA signature value |
| TBSCertificate | | | | | |
| Version | False | | | | |
| | | M | S | 2 | Version 3 |
| SerialNumber | False | | | | |
| certificateSerialNumber | | M | D | | At least 64 bits of entropy<br>Validated on duplicates |
| Signature | False | M | | | |
| Algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| countryName | | M | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. |

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

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | Printable String, size 2 (rfc5280) |
| | organizationName | | M | S | UAE Government | UTF8 encoded |
| | commonName | | M | S | Devices Certification Authority | UTF8 encoded |
| Validity | | False | M | | | Implementations MUST specify using UTC time until 2049 from then on using Generalized Time |
| | NotBefore | | M | D | Certificate generation process date/time. | |
| | NotAfter | | M | D | Certificate generation process date/time + not more than **[27]** Months | |
| Subject | | False | M | | | |
| | countryName | | M | S | AE | Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| | organizationUnitName | | O | D | Allocated as per certificate request | UTF8 encoded |
| | organizationName | | M | D | Allocated as per certificate request | UTF8 encoded |
| | localityName | | M/O | D | Dubai | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |
| | stateOrProvinceName | | M/O | D | Dubai | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| | commonName | | M | D | System unique common name or DNS name or IP address | UTF8 encoded |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | that are applicable, potentially linked to the Subject Alternative Name extension | |
| subjectPublicKeyInfo | | False | M | | | |
| | algorithm | | | D | RSA/ECDSA | |
| | subjectPublicKey | | M | D | Public Key length: 2048 or 4096 (RSA)/256 or 384 (ECDSA) | |
| Extensions | | | M | | | |
| Authority Properties | | | | | | |
| authorityKeyIdentifier | | False | O | | | Mandatory in all certificates except for self-signed CA certificates |
| | keyIdentifier | | M | D | SHA-1 Hash of the Devices CA public key | When this extension is used, this field MUST be supported at minimum |
| authorityInfoAccess | | False | M | | | |
| | accessMethod | | M | S | Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp) | OCSP Responder field |
| | accessLocation | | M | D | http://ca-services.desc.gov.ae/adss/ocsp | OCSP responder URL |
| | accessMethod | | O | S | Id-ad-2 2 id-ad-calssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert) | CA Issuers field |
| | accessLocation | | O | D | http://ca-repository.desc.gov.ae/certificate/devices.p7b | Devices CA Certificate download URL |
| cRLDistributionPoints | | False | O | | | |
| | distributionPoint | | O | D | http://ca-repository.desc.gov.ae/CRL/Devices/devices_certification_authority_uae_government_ae_crlfile<CRLNumber>.crl | CRL download URL |
| Subject Properties | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| subjectKeyIdentifier | | False | M | | | |
| | keyIdentifier | | M | D | SHA-1 Hash | |
| subjectAltName | | False | M | D | Allocated as per certificate request | Domain name(s) that are applicable, linked to the subject common name field |
| Key Usage Properties | | | | | | |
| keyUsage | | True | O | | | |
| | digitalSignature | | M | S | True | |
| extendedKeyUsage | | False | M | | | |
| | serverAuth | | M | S | True | |
| Certificate Policy Property | | | | | | |
| certificatePolicies | | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | D | URL location of this CPS | |
| | certificatePolicies | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.2.3.3 | |

### 7.1.4 TSA Signing Certificate Profile

This is the complete ASN1 description of the certificate associated to TSA signing private keys. DESC will replace its TSA certificate on an annual base.

| Field | CE[11] | O/M[12] | CO[13] | Value | Comment |
|---|---|---|---|---|---|
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 of RFC 3280 |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| signatureValue | | M | D | Devices CA Signature | CA signature value |
| TBSCertificate | | | | | |
| Version | False | | | | |
| | | M | S | 2 | Version 3 |
| SerialNumber | False | | | | |
| certificateSerialNumber | | M | D | | At least 64 bits of entropy<br>Validated on duplicates |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| countryName | | M | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| organizationName | | M | S | UAE Government | UTF8 encoded |
| commonName | | M | S | Devices Certification Authority | UTF8 encoded |
| Validity | False | M | | | Implementations MUST specify using UTC time until 2049 from then on using |

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

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Generalized Time |
| NotBefore | | M | D | Certificate generation process date/time. | |
| NotAfter | | M | D | Certificate generation process date/time + not more than **[36]** Months | |
| Subject | False | M | | | |
| countryName | | M | S | AE | Will be encoded according to "ISO 3166-1-alpha-2 code elements". Printable String, size 2 (rfc5280) |
| organizationName | | M | D | DESC | UTF8 encoded |
| localityName | | M | D | Dubai | UTF8 encoded |
| commonName | | M | D | Dubai Timestamping Authority | UTF8 encoded |
| Subject Public Key Info | False | M | | | |
| algorithm | | | S | RSA | |
| subjectPublicKey | | M | S | Key length: 2048 or 4096 bits (RSA) | |
| Extensions | | M | | | |
| Authority Properties | | | | | |
| authorityKeyIdentifier | False | O | | | Mandatory in all certificates except for self-signed CA certificates |
| keyIdentifier | | M | D | SHA-1 Hash of the Devices CA public key | When this extension is used, this field MUST be supported at minimum |
| authorityInfoAccess | False | M | | | |
| accessMethod | | M | S | Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp) | OCSP Responder field |
| accessLocation | | M | D | http://ca-services.desc.gov.ae/adss/ocsp | OCSP responder URL |
| accessMethod | | O | S | Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert) | CA Issuers field |

| | | | | | | |
|---|---|---|---|---|---|---|
| | accessLocation | | O | D | http://ca-repository.<br>desc.gov.ae/<br>certificate/devices.p7b | Devices CA Certificate download URL |
| cRLDistributionPoints | | False | O | | | |
| | distributionPoint | | O | D | http://ca-repository.desc.gov.ae/<br>CRL/Devices/devices_<br>certification_authority_<br>uae_government_ae_crlfile<br><CRLNumber>.crl | CRL download URL |
| Subject Properties | | | | | | |
| subjectKeyIdentifier | | False | M | | | |
| | keyIdentifier | | M | S | SHA-1 Hash | |
| | | | | | | |
| Key Usage Properties | | | | | | |
| keyUsage | | True | O | | | |
| | digitalSignature | | M | S | True | |
| extendedKeyUsage | | True | M | | | |
| | timeStamping | | M | S | True | |
| Certificate Policy Property | | | | | | |
| certificatePolicies | | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | D | URL location of this CPS | |
| | certificatePolicies | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.3.1.1 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | D | URL location of the TSA practice disclosure statement | |

### 7.1.5 Verification Response Signing Certificate ASN1 Description

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

| Field | CE[14] | O/M [15] | C O | Value | Comment |
|---|---|---|---|---|---|

[14] CE = Critical Extension.
[15] O/M: O = Optional, M = Mandatory.

| | | | [16] | | |
|---|---|---|---|---|---|
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| signatureValue | | M | D | Devices CA Signature | CA signature value |
| TBS Certificate | | | | | |
| Version | False | | | | |
| | | M | S | 2 | Version 3 |
| Serial Number | False | | | | |
| certificateSerialNumber | | M | D | | At least 64 bits of entropy<br>Validated on duplicates |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| countryName | | M | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| organizationName | | M | S | UAE Government | UTF8 encoded |
| CommonName | | O | S | Devices Certification Authority | UTF8 encoded |
| Validity | False | M | | | Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime |
| NotBefore | | | D | Certificate generation process date/time | |
| NotAfter | | | D | Certificate generation process date/time + not more than **[36]** Months | |
| Subject | False | M | | | |

[16] CO = Content: S = Static, D = Dynamic

| | | | | | | |
|---|---|---|---|---|---|---|
| | countryName | | M | S | AE | Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| | commonName | | M | S | DESC Signature Verification Service | |
| | organizationName | | M | S | DESC | |
| | localityName | | M | S | Dubai | |
| subjectPublicKeyInfo | | False | M | | | |
| | algorithm | | | S | RSA | |
| | subjectPublicKey | | M | D | Public key length: 2048 or 4096 (RSA) | |
| Extensions | | | M | | | |
| Authority Properties | | | | | | |
| authorityKeyIdentifier | | False | O | | | Mandatory in all certificates except for self-signed CA certificates |
| | keyIdentifier | | M | S | SHA-1 Hash of the Devices CA public key | When this extension is used, this field MUST be supported at minimum |
| cRLDistributionPoints | | False | O | | | |
| | distributionPoint | | O | D | http://ca-repository.desc.gov.ae/<br>CRL/Devices/devices_<br>certification_authority_<br>uae_government_ae_crlfile<br><CRLNumber>.crl | CRL download URL |
| Subject Properties | | | | | | |
| subjectKeyIdentifier | | False | M | | | |
| | KeyIdentifier | | M | S | SHA-1 Hash | |
| Key Usage Properties | | | | | | |
| keyUsage | | True | M | | | |
| | digitalSignature | | M | S | True | |
| | nonrepudiation | | M | S | True | |

| Certificate Policy Property | | | | | | |
|---|---|---|---|---|---|---|
| certificatePolicies | | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.1.2 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | D | URL location of this CPS | |
| certificatePolicies | | False | M | | | |
| | policyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.2.3.4 | |

### 7.1.6 Version Number

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

### 7.1.7 Certificate Extensions

Devices CA subscriber certificates require the use of the following extensions:

- 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)

### 7.1.8 Algorithm Object Identifiers

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

### 7.1.9 Name Forms

As per the naming conventions and constraints listed in Section 3.1 of this CPS.

### 7.1.10 Name Constraints

As per the naming conventions and constraints listed in Section 3.1 of this CPS.

### 7.1.11 Certificate Policy Object Identifier

Refer to the ASN1 definitions described in this chapter.

### 7.1.12 Usage of Policy Constraints Extension

No stipulation — this section is intentionally left blank.

### 7.1.13 Policy Qualifiers Syntax and Semantics

No stipulation — this section is intentionally left blank.

### 7.1.14 Processing Semantics for Critical Certificate Extensions

Critical extensions, when marked, is interpreted by relying parties accordingly.

## 7.2 CRL Profile

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

### 7.2.1 Version Number(s)

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

### 7.2.2 CRL and CRL Entry Extensions

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

### 7.2.3 CRL ASN1 Description

This is the complete ASN1 description of the CRL certificate.

| Field | | CE[17] | CO[18] | Value | Comment |
|---|---|---|---|---|---|
| Certificate List | | | | | |
| TBSCertificate | | | | | |
| Signature | | False | | | |
| | algorithm | | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| | signatureValue | | D | Devices CA Signature | CA signature value |
| TBSCertList | | | | | |
| Version | | False | | | |
| | | | S | 2 | Version 3 |
| SerialNumber | | False | | | |
| | certificateSerialNumber | | F | | At least 64 bits of entropy<br>Validated on duplicates |

[17] CE = Critical Extension.
[18] CO = Content: S = Static, D = Dynamic

| | | | | | |
|---|---|---|---|---|---|
| Signature | | False | | | |
| | algorithm | | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | | False | S | | |
| | countryName | | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| | organizationName | | S | UAE Government | UTF8 encoded |
| | commonName | | S | Devices Certification Authority | UTF8 encoded |
| Validity | | False | | | Implementations MUST specify using UTC time until 2049 from then on using Generalized Time |
| | ThisUpdate | | D | CRL generation date/time | |
| | NextUpdate | | D | CRL generation date/time + 1 day + 2 hours | |
| Revoked Certificates | | | | | |
| certificate | | | | | |
| | certificateSerial | | D | Serial of the revoked certificate | |
| | revocationDate | | D | UTC Time of revocation (Optional) | |
| crlExtensions | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| authorityKeyIdentifier | | False | D | This MUST be the same value as thez subject Key Identifier field in the CRL Issuer's certificate.<br>Non-critical <subject key identifier CA> | SHA-1 Hash of the Devices CA public key |
| crlNumber | | False | D | < Sequential CRL number > | |
| IssuingDistributionPoint | | True | | | Mandatory for Partitioned RLs |
| | DistributionPoint | | D | CN=CRL1<br>CN=UAE Global Root CA G4 E2<br>O=UAE Government<br>C=AE | Partitioned CRL directory address |
| | DistributionPoint | | *D* | *http://ca-repository.desc.gov.ae/CRL/Root/uae_global_root_ca_g4_e2_uae_government_ae_crlfilea<CRLNumber>.crl* | *CRL hosting URL, where <CRL Number> a dedicated sequence number that the CA uses for CRL file naming* |
| | onlyContainsCACerts | | S | No | |
| | onlyContainsUserCerts | | S | Yes | |
| | IndirectCRL | | S | No | |
| expiredCertsOnCRL (2.5.29.60) | | False | D | < a date-time value specifies the date on or after which revoked certificates are retained on the CRL> | |

# 7.3 OCSP Profile

## 7.3.1 Version Number(s)

The OCSP responder issues OCSP responses of version 1.

## 7.3.2 OCSP Extensions

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

### 7.3.3 OCSP Response Signing Certificate ASN1 Description

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

| Field | CE[19] | O/M[20] | CO[21] | Value | Comment |
|---|---|---|---|---|---|
| Certificate | | M | | | |
| TBSCertificate | | M | | | See 4.1.2 |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| signatureValue | | M | D | Devices CA Signature | CA signature value |
| TBS Certificate | | | | | |
| Version | False | | | | |
| | | M | S | 2 | Version 3 |
| Serial Number | False | | | | |
| certificateSerialNumber | | M | D | | At least 64 bits of entropy<br>Validated on duplicates |
| Signature | False | M | | | |
| algorithm | | M | S | OID = 1.2.840.113549.1.1.11 | SHA256 with RSA Encryption |
| Issuer | False | M | S | | |
| countryName | | M | S | AE | Encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| organizationName | | M | S | UAE Government | UTF8 encoded |
| CommonName | | O | S | Devices Certification Authority | UTF8 encoded |
| Validity | False | M | | | Implementations MUST specify using UTC time until 2049 from then on using |

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

| | | | | | |
|---|---|---|---|---|---|
| | | | | | GeneralisedTime |
| NotBefore | | | D | Certificate generation process date/time | |
| NotAfter | | | D | Certificate generation process date/time + not more than **[36]** Months | |
| Subject | False | M | | | |
| countryName | | M | S | AE | Will be encoded according to “ISO 3166-1-alpha-2 code elements”. Printable String, size 2 (rfc5280) |
| commonName | | M | S | Devices Certification Authority OCSP | |
| organizationName | | M | S | DESC | |
| localityName | | M | S | Dubai | |
| subjectPublicKeyInfo | False | M | | | |
| algorithm | | | S | RSA | |
| subjectPublicKey | | M | D | Public key length: 2048 or 4096 (RSA) | |
| Extensions | | M | | | |
| Authority Properties | | | | | |
| authorityKeyIdentifier | False | O | | | Mandatory in all certificates except for self-signed CA certificates |
| keyIdentifier | | M | S | SHA-1 Hash of the Devices CA public key | When this extension is used, this field MUST be supported at minimum |
| Subject Properties | | | | | |
| subjectKeyIdentifier | False | M | | | |
| KeyIdentifier | | M | S | SHA-1 Hash | |
| Key Usage Properties | | | | | |
| keyUsage | True | M | | | |
| digitalSignature | | M | S | True | |
| nonrepudiation | | M | S | True | |
| extendedKeyUsage | False | M | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | oCSPSigning | | M | S | True | |
| id-pkix-ocsp-nocheck | | False | M | S | 05 00 | |
| Certificate Policy Property | | | | | | |
| certificatePolicies | | False | M | | | |
| | PolicyIdentifier | | M | S | 2.16.784.1.2.2.100.1.2.1.2 | |
| | policyQualifiers:policyQualifierId | | O | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | O | D | URL location of this 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.

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 any person having any conflicting interests thereof.

The Devices CA is 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.

# 9. Other Business and Legal Matters

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

## 9.1 Fees

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

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

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

### 9.2.2 Other Assets

Not applicable.

### 9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

## 9.3 Confidentiality of Business Information

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

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

# 9.4 Privacy of Personal Information

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

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

The following items are not confidential information:

- Certificates and their content
- Status of a certificate

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

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

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

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

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

Disclosure Conditions

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

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

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

- Themselves
- Persons in their custody

Only the RA is permitted to access confidential information.

DESC properly manages the disclosure of information to the Devices CA personnel.

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

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

All communications of confidential information are encrypted, including:

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

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

# 9.5 Intellectual Property Rights

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

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

# 9.6 Representations and Warranties

## 9.6.1 CA Representations and Warranties

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

## 9.6.2 RA Representations and Warranties

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

## 9.6.3 RA Representations and Warranties

Subscribers shall represent to DESC that the Subscriber will:

- Securely generate its Private Keys and protect its Private Keys from compromise (including protecting any tokens or corresponding activation data that provides access to PrivateKeys),
- Provide accurate and complete information and communication to this CA and RA/LRA,
- Confirm the accuracy of certificate data prior to using the certificate,
- Promptly cease using a certificate and notify DESC if (i) any information that was submitted to the CA or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate, and
- Use the certificate only for authorized and legal purposes, consistent with this CPS and 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, the Devices CA, or any person receiving or relying on the certificate
- Any liability incurred as a result of the applicant breaking any laws applicable in Dubai, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- Other damage

# 9.8 Limitations of Liability

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

# 9.9 Indemnities

Not applicable.

# 9.10 Term and Termination

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

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

# 9.11 Individual Notices and Communications with Participants

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

# 9.12 Amendments

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

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

# 9.13 Dispute Resolution Procedures

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

# 9.14 Governing Law

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

# 9.15 Compliance with Applicable Law

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

# 9.16 Miscellaneous Provisions

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

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

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

# 9.17 Other Provisions

Not applicable.