Dubai Electronic Security Center

Dubai PKI

Code Signing CA

Certification Practice Statement

Title	Code Signing CA, Certification Practice Statement
Classification	PUBLIC
File Name	DubaiPKI-CodeSigningCA-CertificationPracticeStatement_v1.8
Created on	15 March 2022
Revision	1.8
Modified on	25 April 2026

Document History

Date	Revision	Author(s)	Summary
15 Mar 2022	0.1	Khawla Hassan	Initial version
1st April 2022	1.0	Khawla Hassan	First Release
1st June 2022	1.1	Khawla Hassan	Update section 4.1.2 to align with the technology in use
7 September 2022	1.2	Khawla Hassan	Correct typographical errors and general enhancements
6 April 2023	1.3	Khawla Hassan	• Annual review • Add more options of identity vetting as per the CS BRs • Add more clarifications on the time limits for re-use of validation information • Align the definitions and log retention with the SSL BRs • Updates to accommodate the CA/B Forum ballots CSCWG-13 and CSCWG-17
2 November 2023	1.4	Khawla Hassan	• Update the certificates supported under the Devices CA in the PKI hierarchy • Updates to accommodate the CA/B Forum ballot CSCWG-19
08 April 2024	1.5	Khawla Hassan	• Annual review • Updates to accommodate the CA/B Forum ballot CSCWG-18
17 April 2025	1.6	Mohamed Khalifa	• Annual review • Specify public key vulnerability assessments before certificate issuance

16 Jan 2026	1.7	Mohamed Khalifa	• Announcement of planned decommissioning of Code Signing Certification Authority
25 April 2025	1.8	Mohamed Khalifa	Updates to reflect the decommissioning of the Code Signing CA. The CPS has been revised to designate all operational sections as **[Deprecated]**, and consistent with the DESC Subordinate CAs Certificate Policy.

Table of Contents

1. Introduction

The Code Signing Certification Authority is a legacy Certification Authority within the Dubai PKI hierarchy. Following decommissioning, the Code Signing CA remains inactive and shall not perform any certification, revocation, validation, or cryptographic operations. This CPS is maintained solely for historical reference and relying party transparency, in accordance with the DESC Subordinate CAs CP. No post-decommissioning certificate status services are required, as no end-entity certificates were ever issued by this CA.

Given that the CA did not issue any end-entity certificates and did not provide subscriber or relying-party services. The sections in this CPS that describe certificate lifecycle, validation, audit, or cryptographic operations are marked as [deprecated] and are superseded by the publicly published Decommissioning Notice.

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

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

1.1 Overview

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

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

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

The Dubai PKI Root CA and DESC Subordinate CAs are established and operated by DESC. The mandate of DESC also includes the responsibility for providing PKI certification services in Dubai, encompassing the issuance and management of subordinate and end-entity certificates.

1.1.1 Dubai PKI hierarchy

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

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

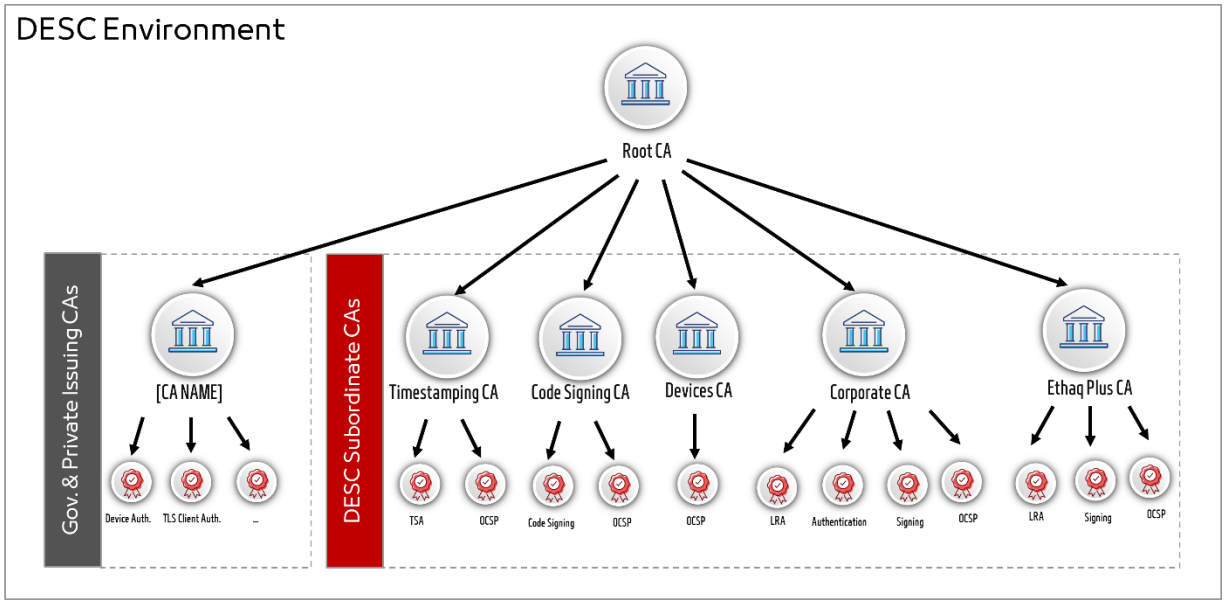

Figure 1: Trust Model for Dubai PKI

1.1.2 Dubai PKI Policy Authority (PA)

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

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

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

1.1.3 Certificate Policy

X.509 certificates issued by the Code Signing CA to subscribers will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a Certificate is trusted for a particular purpose. Subscriber Certificates issued by the Code Signing CA will identify the applicable policy in the certificate Policies extension by including applicable OID(s).

1.1.4 Relationship Between the DESC Subordinate CAs CP and this CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Code Signing CA as governed by DESC Subordinate CAs CP and related documents which describe the Dubai PKI requirements and use of Certificates.

1.1.5 Operational Status of the Devices Certification Authority

The Code Signing CA has been decommissioned and does not perform certificate issuance, renewal, re-key, or revocation operations.

Since no end-entity certificates were issued from this CA, no CRL/OCSP status services are required for relying party validation. The CA certificate (and chain, where applicable) will remain published in the repository for transparency and historical reference.

1.2 Document name and identification

This document is named and referred to as “Dubai PKI – Code Signing CA Certificate Practice Statement”.

The object identifier (OID) of this CPS is 2.16.784.1.2.2.100.1.2.1.4.

No certificate profiles are applicable to this CA. Any certificate types previously referenced in earlier versions of this CPS are **[Deprecated]**.

1.3 PKI participants

Several parties are involved during the lifecycle management of the digital certificates issued by this CA. This include:

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

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

1.3.1 Certification Authorities

The Code Signing CA is decommissioned and no longer performs any Certification Authority functions.

No certificate issuance, revocation, renewal, re-key, or validation services are provided by this CA.

1.3.2 Registration Authorities

The Registration Authority(RA) function described in this section reflect the role of the RA during the operational lifetime of the CA prior to its decommissioning. Following decommissioning, no registration, validation, or certificate request processing activities are performed.

Duly authorized members part of Dubai PKI team act as RA for this CA. DESC RA function falls within the PKI operations structure and, it is responsible for accepting and validating certificate issuance and management operations, in addition to triggering related certification operations by this CA.

1.3.3 Subscribers

Subscribers of the Code Signing CA are Government entities in the UAE.

Before issuing any certificate, the subscriber shall agree to the terms and conditions of DESC subscriber agreement.

1.3.4 Relying Parties

A Relying Party is any entity within UAE that processes a digital certificate issued by the Code Signing CA.

Relying Parties are entities that relay on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber’s certificate issued by the Code Signing CA.

Relying parties shall always verify the validity of a digital certificate issued by the Code Signing CA using the Code Signing CA Certificate Validations Services (e.g. CRL, OCSP), prior to relying on information featured in the certificate.

On the other hand, DESC offers a Time-stamping Authority (TSA) service in accordance with ETSI EN 319 421, ETSI EN 319 422 and RFC 3161. DESC Time-stamping signing certificate is issued by the Timestamping CA.

DESC Time-stamping Policy Time-stamping Practice Statement specifies the policy requirements relating to the operation of DESC Time-stamping Authority (TSA). It shall be read in conjunction with the Timestamping CA CPS. All documents are published at https://ca-repository.desc.gov.ae/.

All Digital Signatures created by Code Signing certificates issued by the Code Signing CA shall include a trusted timestamp issued from DESC Time-stamping Authority.

1.3.5 Other participants

There are no other participants for this CA.

1.4 Certificate usage

1.4.1 Appropriate certificate use

[Deprecated]

No certificates were issued by this Certification Authority.

1.4.2 Prohibited certificate use

[Deprecated]

1.5 Policy administration

1.5.1 Organization administering the document

DESC, through the Dubai PKI PA, is bearing responsibility for drafting, publishing, OID registration, maintenance and interpretation of this CPS, and other policies and practices within the realm of the Dubai PKI.

1.5.2 Contact Person

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

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

E-mail pa@desc.gov.ae

Certificate Problem Report

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

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

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

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

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

1.6 Definitions, acronyms and references

1.6.1 Definitions

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: 1. who signs and submits, or approves a certificate request on behalf of the Applicant, and/or 2. who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or 3. who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

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

Application Software Supplier: A supplier of software or other relying-party application software that displays or uses Code Signing Certificates, incorporates Root Certificates, and adopts these Requirements as all or part of its requirements for participation in a root store program.

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

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

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

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

and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

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

Business Entity: Any entity that is not a Private Organization, Government Entity, or Non‐Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to:

1. Act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester; and
2. Approve EV Code Signing Certificate Requests submitted by other Certificate Requesters.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant.

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

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

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

Certification Authority: An organization subject to these Requirements that is responsible for a Code Signing Certificate and, under these Requirements, oversees the creation, issuance, revocation, and management of Code Signing Certificates. Where the CA is also the Root CA, references to the CA are synonymous with Root CA.

Certificate Beneficiaries: All Application Software Suppliers with whom the CA or its Root CA has entered into a contract for distribution of its Root Certificate in software distributed by such Application Software Suppliers and all Relying Parties who reasonably rely on such a Certificate while a Code Signature associated with the Certificate is valid.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Government Agency: In the context of a Private Organization, a Government Agency is the authority in the Jurisdiction of Incorporation responsible for establishing the legal existence of such organizations (e.g., the agency that issues the Certificate of Incorporation). For Business Entities, it is the government authority in the jurisdiction of operation that registers business entities. In the case of a Government Entity, it refers to the entity that enacts laws, regulations, or decrees establishing the legal existence of Government Entities.

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

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

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

Independent Confirmation From Applicant: Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.

Individual: A natural person.

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

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

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

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

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

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or a Latin Notary, as described in these Guidelines, and is competent to render an opinion on factual claims of the Applicant.

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

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

Organizational Applicant: An Applicant that requests a Certificate with a name in the Subject field that is for an organization and not the name of an individual.

Non-EV Code Signing Certificate: A term used to signify requirements that are applicable to Code Signing Certificates which do not have to meet the Extended Validation (EV) requirements. This CA issues Non-EV Code Signing certificate.

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

Parent Company: A company that Controls a Subsidiary Company.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

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

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

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

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

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Subsidiary Company: A company that is controlled by a Parent Company.

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

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

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

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

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

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

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

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

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

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

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

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

Verifying Person: A notary, attorney, Latin notary, accountant, individual designated by a government agency as authorized to verify identities, or agent of the CA, who attests to the identity of an individual.

1.6.2 Acronyms

CA — Certification Authority

CCTV — Closed circuit TV

CP — Certificate Policy

CPS — Certification Practice Statement

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

FQDN — Fully Qualified Domain Name

HSM — Hardware Security Module

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

ITU — International Telecommunications Union

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

DESC — Dubai Electronics Security Center

OID — Object Identifier

OSCP — Online Certificate Status Protocol

OTP — One Time Password

PA — Policy Authority of Dubai PKI

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

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

PKCS # 7 — Cryptographic Message Syntax

PKCS #10 — Certification Request Syntax Specification

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

PKE — Public Key Encryption

PKI — Public Key Infrastructure

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

RA — Registration Authority

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

SCEP — Simple Certificate Enrolment Protocol

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

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

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

SDG — Dubai Smart Government Establishment

UPS — Uninterruptible Power Supply

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

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

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

2. Publication and repository responsibility

2.1 Repositories

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

2.2 Publication of certificate information

DESC maintains this CPS and the CA certificate in the public repository for historical reference and transparency purposes.

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

2.3 Time or frequency of publication repositories

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

2.3.1 Certificates

The Code Signing CA certificate and OCSP certificates are published to the public repository (https://ca-repository.desc.gov.ae/) as soon as they are issued.

2.3.2 CRLs

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

2.4 Access controls on repositories

Public read-only access to the CPS, certificates, CRLs and documentation 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 name

[Deprecated]

No identification or authentication activities are performed by this CA.

3.1.2 Need for names to be meaningful

[Deprecated]

No identification or authentication activities are performed by this CA.

3.1.3 Anonymity and pseudonymity of subscribers

[Deprecated]

No identification or authentication activities are performed by this CA.

3.1.4 Rules for interpreting various name forms

[Deprecated]

No identification or authentication activities are performed by this CA.

3.1.5 Uniqueness of names

[Deprecated]

- No identification or authentication activities are performed by this CA.

3.1.6 Recognition, authentication and role of trademarks

[Deprecated]

No identification or authentication activities are performed by this CA.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

[Deprecated]

No identification or authentication activities are performed by this CA.

3.2.2 Authentication of Organization identity

[Deprecated]

No identification or authentication activities are performed by this CA.

3.2.3 Authentication of individual identity

[Deprecated]

No identification or authentication activities are performed by this CA.

3.2.4 Non-verified subscriber information

[Deprecated]

No identification or authentication activities are performed by this CA.

3.2.5 Validation of authority

[Deprecated]

No identification or authentication activities are performed by this CA.

3.2.6 Criteria for interoperation

[Deprecated]

No identification or authentication activities are performed by this CA.

3.3 Identification and authentication for re-keying requests

3.3.1 Identification and authentication for routine re-keying

[Deprecated]

No identification or authentication activities are performed by this CA.

3.3.2 Identification and authentication for re-key after revocation

[Deprecated]

No identification or authentication activities are performed by this CA.

3.4 Identification and authentication for revocation request

[Deprecated]

No identification or authentication activities are performed by this CA.

4. Certificate Life Cycle Management

4.1 Certificate application

4.1.1 Who can submit a certificate application

[Deprecated]

This CA does not issue or manage certificates.

4.1.2 Enrolment process and responsibilities

[Deprecated]

This CA does not issue or manage certificates.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

[Deprecated]
This CA does not issue or manage certificates.

4.2.2 Approval or rejection of certificate applications

[Deprecated]

This CA does not issue or manage certificates.

4.2.3 Time to process certificate applications

[Deprecated]

This CA does not issue or manage certificates.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

[Deprecated]

- This CA does not issue or manage certificates.

4.3.2 Notification to the subscriber by the CA of issuance of certificate

[Deprecated]

This CA does not issue or manage certificates.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

[Deprecated]

This CA does not issue or manage certificates.

4.4.2 Publication of the certificate by the CA

[Deprecated]

This CA does not issue or manage certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

[Deprecated]

This CA does not issue or manage certificates.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

[Deprecated]

- This CA does not issue or manage certificates.

4.5.2 Relying party public key and certificate usage

[Deprecated]

This CA does not issue or manage certificates.

4.6 Certificate renewal

[Deprecated]

This CA does not issue or manage certificates.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate Re-key

[Deprecated]

This CA does not issue or manage certificates.

4.7.1 Circumstance for Certificate Re-key

[Deprecated]

This CA does not issue or manage certificates.

4.7.2 Who may request certification of a new public key

[Deprecated]

This CA does not issue or manage certificates.

4.7.3 Processing Certificate Re-keying requests

[Deprecated]

This CA does not issue or manage certificates.

4.7.4 Notification of new certificate issuance to subscriber

[Deprecated]

This CA does not issue or manage certificates.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

[Deprecated]

This CA does not issue or manage certificates.

4.7.6 Publication of the Re-keyed Certificate by the CA

[Deprecated]

This CA does not issue or manage certificates.

4.7.7 Notification of certificate issuance by the CA to other entities

[Deprecated]

This CA does not issue or manage certificates.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

[Deprecated]

This CA does not issue or manage certificates.

4.8.2 Who may request certificate modification

Not applicable. Refer to section 4.8.1.

4.8.3 Processing certificate modification requests

Not applicable. Refer to section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

As per initial certificate issuance.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable. Refer to section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

[Deprecated]

This CA does not issue or manage certificates.

4.8.7 Notification of certificate issuance by the CA to other entities

[Deprecated]

This CA does not issue or manage certificates.

4.9 Certificate revocation and suspension

[Deprecated]

This CA does not issue or manage certificates.

4.9.1 Circumstances for revocation

[Deprecated]

This CA does not issue or manage certificates.

4.9.2 Who can request revocation

[Deprecated]

- This CA does not issue or manage certificates.

4.9.3 Procedure for revocation request

[Deprecated]

This CA does not issue or manage certificates.

4.9.4 Revocation request grace period

[Deprecated]

This CA does not issue or manage certificates.

4.9.5 Revocation request response time

[Deprecated]

This CA does not issue or manage certificates.

4.9.6 Revocation checking requirement for relying parties

[Deprecated]

This CA does not issue or manage certificates.

4.9.7 CRL issuance frequency

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.9.8 Maximum latency for CRLs

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.9.9 Online revocation/status checking availability

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.9.10 Online revocation checking requirements

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.9.11 Other forms of revocation advertisements available

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.9.12 Special requirements – Key compromise

[Deprecated]

The Code Signing CA has been decommissioned.

4.9.13 Circumstances for suspension

[Deprecated]

This CA does not issue or manage certificates.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.10.1 Operational characteristics

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.10.2 Service availability

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

4.10.3 Optional features

[Deprecated]

No certificate status information (CRL or OCSP) is published or required for this Certification Authority, as no end-entity certificates were issued.

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.

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by this CA.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management and Operational Controls

The Code Signing CA has been decommissioned in accordance with DESC governance decisions and the publicly published Decommissioning Notice.

Following decommissioning, no CA operations are performed. This CPS remains published solely for historical and transparency purposes.

5.1 Physical controls

5.1.1 Site location and construction

[Deprecated]

The Code Signing CA has been decommissioned.

5.1.2 Physical access

[Deprecated]

The Code Signing CA has been decommissioned.

5.1.3 Power and air conditioning

[Deprecated]

The Code Signing CA has been decommissioned..

5.1.4 Water exposures

[Deprecated]

The Code Signing CA has been decommissioned..

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

[Deprecated]

The Code Signing CA has been decommissioned..

5.1.7 Waste disposal

[Deprecated]

The Code Signing CA has been decommissioned.

5.1.8 Off-site backup

[Deprecated]

The Code Signing CA has been decommissioned.

5.2 Procedural controls

[Deprecated]

The Code Signing CA has been decommissioned.

5.2.1 Trusted roles

[Deprecated]

The Code Signing CA has been decommissioned.

5.2.2 Number of persons required per task

[Deprecated]

The Code Signing CA has been decommissioned.

5.2.3 Identification and authentication for each role

[Deprecated]

The Code Signing CA has been decommissioned.

5.2.4 Roles requiring separation of duties

[Deprecated]

The Code Signing CA has been decommissioned.

5.3 Personnel controls

[Deprecated]

The Code Signing CA has been decommissioned..

5.3.1 Qualifications, experience and clearance requirements

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.2 Background check procedures

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.3 Training requirements

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.4 Retraining frequency and requirements

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.5 Job rotation frequency and sequence

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.6 Sanctions for unauthorized actions

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.7 Independent contractor requirements

[Deprecated]

The Code Signing CA has been decommissioned.

5.3.8 Documentation supplied to personnel

[Deprecated]

The Code Signing CA has been decommissioned.

5.4 Audit logging procedures

5.4.1 Types of event recorded

[Deprecated]

The Code Signing CA has been decommissioned

5.4.2 Frequency of processing log

[Deprecated]

The Code Signing CA has been decommissioned.

5.4.3 Retention period for audit log

[Deprecated]

The Code Signing CA has been decommissioned.

5.4.4 Protection of audit log

[Deprecated]

The Code Signing CA has been decommissioned.

5.4.5 Audit log backup procedures

[Deprecated]

The Code Signing CA has been decommissioned.

5.4.6 Audit collection system (internal vs. external)

[Deprecated]

The Code Signing CA has been decommissioned.

5.4.7 Notification to event-causing subject

[Deprecated]

The Code Signing CA has been decommissioned.

5.4.8 Vulnerability assessments

[Deprecated]

The Code Signing CA has been decommissioned.

5.5 Records archival

5.5.1 Types of records archived

[Deprecated]

The Code Signing CA has been decommissioned.

5.5.2 Retention period for archive

[Deprecated]

The Code Signing CA has been decommissioned.

5.5.3 Protection of archive

[Deprecated]

The Code Signing CA has been decommissioned.

5.5.4 Archive backup procedures

[Deprecated]

The Code Signing CA has been decommissioned.

5.5.5 Requirements for time-stamping of records

[Deprecated]

The Code Signing CA has been decommissioned.

5.5.6 Archive collection system (internal or external)

[Deprecated]

The Code Signing CA has been decommissioned.

5.5.7 Procedures to obtain and verify archive Information

[Deprecated]

The Code Signing CA has been decommissioned.

5.6 Key changeover

T**[Deprecated]**

The Code Signing CA has been decommissioned.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

[Deprecated]

The Code Signing CA has been decommissioned.

5.7.2 Computing resources, software/data corruption

[Deprecated]

The Code Signing CA has been decommissioned.

5.7.3 Entity private key compromise procedures

[Deprecated]

The Code Signing CA has been decommissioned.

5.7.4 Business continuity capabilities after a disaster

[Deprecated]

The Code Signing CA has been decommissioned.

5.8 CA or RA termination

The Code Signing CA has been designated as a Legacy Certification Authority and is subject to decommissioning in accordance with the publicly published CA Decommissioning Notice.

No end-entity certificates were ever issued by this CA. As such, no subscriber, revocation, or certificate status information services (including CRLs or OCSP) are required to be maintained for relying party validation purposes.

Upon decommissioning, the CA shall cease all CA operations. The CA certificate and associated certification path information shall remain published in the CA repository for transparency and historical reference, as described in the applicable Decommissioning Notice.

No further Certification Authority services shall be performed following decommissioning.

6. Technical Security Controls

6.1 Key pair generation

[Deprecated]

The Code Signing CA has been decommissioned.

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

[Deprecated]

The Code Signing CA has been decommissioned.

6.1.1.2 Subscriber key pair generation

[Deprecated]

The Code Signing CA has been decommissioned.

6.1.2 Private key delivery to subscriber

[Deprecated]

The Code Signing CA has been decommissioned.

6.1.3 Public key delivery to certificate issuer

[Deprecated]

The Code Signing CA has been decommissioned.

6.1.4 CA public key delivery to relying parties

The certificates of the Code Signing CA remains archived and publicly available for historical reference purposes.

6.1.5 Key sizes

[Deprecated]

The Code Signing CA has been decommissioned.

6.1.6 Public key parameters generation and quality checking

[Deprecated]

The Code Signing CA has been decommissioned.

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

[Deprecated]

The Code Signing CA has been decommissioned.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.2 Private key (n out of m) multi-person control

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.3 Private key escrow

Not applicable.

6.2.4 Private key backup

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.5 Private key archival

No stipulation – this section is intentionally left blank.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.7 Private key storage on cryptographic module

6.2.7.1 Private key storage for CA keys

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.7.2 Subscriber Private Key protection and verification

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.8 Method of activating private key

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.9 Method of deactivating private key

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.10 Method of destroying private key

[Deprecated]

The Code Signing CA has been decommissioned.

6.2.11 Cryptographic module rating

[Deprecated]

The Code Signing CA has been decommissioned.

6.3 Other aspects of key pair management

6.3.1 Public key archival

[Deprecated]

The Code Signing CA has been decommissioned.

6.3.2 Certificate operational periods and key pair usage periods

[Deprecated]

The Code Signing CA has been decommissioned.

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1.1 Code Signing CA

[Deprecated]

The Code Signing CA has been decommissioned.

6.4.1.2 Subscribers keys

[Deprecated]

The Code Signing CA has been decommissioned.

6.4.2 Activation data protection

6.4.2.1 Code Signing CA

[Deprecated]

The Code Signing CA has been decommissioned.

6.4.3 Other aspects of activation data

No stipulation – this section intentionally left blank.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

[Deprecated]

The Code Signing CA has been decommissioned.

6.5.2 Computer security rating

No stipulation – this section is intentionally left blank.

6.6 Life cycle technical controls

6.6.1 System development controls

[Deprecated]

The Code Signing CA has been decommissioned.

6.6.2 Security management controls

[Deprecated]

The Code Signing CA has been decommissioned.

6.6.3 Life cycle security controls

No stipulation – this section intentionally left blank.

6.7 Network security controls

[Deprecated]

The Code Signing CA has been decommissioned.

6.8 Time stamping

[Deprecated]
The Code Signing CA has been decommissioned.

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

7.1.1 Version number

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.2 Certificate extensions

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.3 Algorithm object identifiers

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.4 Name forms

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.5 Name constraints

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.6 Certificate policy object identifier

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.7 Usage of policy constraints extension

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.8 Policy qualifiers syntax and semantics

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.9 Processing semantics for critical certificate extensions

[Deprecated]

The Code Signing CA has been decommissioned.

7.1.10 Code signing certificate ASN1 description

[Deprecated]

The Code Signing CA has been decommissioned.

7.2 CRL profile

7.2.1 Version number(s)

[Deprecated]

The Code Signing CA has been decommissioned.

7.2.2 CRL and CRL entry extensions

[Deprecated]

The Code Signing CA has been decommissioned.

7.2.3 CRL ASN1 description

[Deprecated]

The Code Signing CA has been decommissioned.

7.3 OCSP profile

7.3.1 Version number(s)

[Deprecated]

The Code Signing CA has been decommissioned.

7.3.2 OCSP extensions

[Deprecated]

The Code Signing CA has been decommissioned.

7.3.3 OCSP Response Signing Certificate ASN1 Description

[Deprecated]

The Code Signing CA has been decommissioned.

8. Compliance Audit and Other Assessments

The Code Signing CA has been decommissioned and does not perform Certification Authority issuance, validation, or certificate lifecycle management operations.

No end-entity certificates were issued by this Certification Authority. Accordingly, no Certification Authority–specific compliance audits or assessments are conducted following decommissioning.

Audits and assessments applicable during the period in which this Certification Authority was established and maintained were conducted in accordance with the assurance frameworks in force at that time. Relevant audit records are retained in accordance with the records archival provisions of this CPS.

This section is retained solely for historical reference and does not constitute a commitment to ongoing or future audits for the decommissioned Certification Authority.

9. Other Business and Legal Matters

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

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

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

9.1.2 Certificate Access Fees

Not Applicable.

9.1.3 Revocation or Status Information Access Fees

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

9.1.4 Fees for Other Service

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

9.1.5 Refund Policy

Charged fees cannot be refunded.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

DESC considers the following as confidential information:

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

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of Personal Information

9.4.1 Privacy plan

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

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

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

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

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

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

- The communications link between the Code Signing CA and DESC RA,
- Sessions to deliver certificates and certificate status information.

9.4.2 Information treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to protect private information

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

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

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

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

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

- **Authorization for Certificate:** That, at the time of issuance, the Code Signing CA

  I. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject,

  II. followed the procedure when issuing the Certificate, and

  III. accurately described the procedure in this CPS.

- **Accuracy of Information:** That, at the time of issuance, the Code Signing CA

  I. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate,

  I. followed the procedure when issuing the Certificate, and

  II. accurately described the procedure in this CPS.

- **Key Protection:** The Code Signing CA represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates;

- **Subscriber Agreement:** That, if the Code Signing CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use.

- **Status:** That the Code Signing CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.

- **Revocation:** That the Code Signing CA will revoke the Certificate for any of the reasons specified in these Requirements.

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.

The LRAs warrant (through signing an LRA agreement with DESC) that they perform RA functions as per the stipulations specified in this CPS.

9.6.3 Subscriber Representations and Warranties

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

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

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

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

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

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to DESC, both in the certificate request and as otherwise requested by DESC in connection with the issuance of the Certificate(s) to be supplied by the Code Signing CA,
- **Protection of Private Key:** Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g., password or token; Subscriber shall maintain sole control of, keep confidential, and properly protect, at all times in accordance with Section 6.2.7.2.1 of this CPS, the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token). Subscriber represents that it will generate and operate any device storing private keys in a secure manner. Subscriber shall use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
- **Private Key Reuse:** To not apply for a Code Signing Certificate if the Public Key in the Certificate is or will be used with a non-Code Signing Certificate,
- **Use:** To use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use,
- **Compliance with Industry Standards:** An acknowledgment and acceptance that the CA may modify the Subscriber Agreement or Terms of Use when necessary to comply with any changes in these Requirements or the Baseline Requirements,
- **Prevention of Misuse:** To provide adequate network and other security controls to protect against misuse of the Private Key and that the CA will revoke the Certificate without requiring prior notification if there is unauthorized access to the Private Keys,
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy,
- **Reporting and Revocation:** To promptly cease using a Certificate and its associated Private Key and promptly request that the CA revoke the Certificate if the Subscriber believes that (a) any information in the Certificate is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code.
- **Sharing of Information:** An acknowledgment and acceptance that, if: (a) the Certificate or the Applicant is identified as a source of Suspect Code, (b) the authority to request the Certificate cannot be verified, or (c) the Certificate is revoked for reasons other than Subscriber request (e.g. as a result of private key compromise, discovery of malware, etc.), then the CA is authorized to share information about the Applicant, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.
- **Termination of Use of Certificate:** To promptly cease using the Private Key corresponding to the Public Key listed in a Certificate upon expiration or revocation of the Certificate,
- **Responsiveness:** An obligation to respond to DESC's instructions concerning Key Compromise or Certificate misuse within a specified time period**,**

- **Acknowledgment and Acceptance:** An acknowledgement and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the Terms of Use or the Subscriber Agreement.

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under the Code Signing CA shall:

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

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

9.9 Indemnities

Not applicable.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

Termination or decommissioning of the Code Signing CA shall not affect provisions of this CPS that by their nature are intended to survive termination, including but not limited to provisions relating to records archival and retention, confidentiality, privacy, disclaimers of warranties, limitation of liability, indemnities, and dispute resolution. Following decommissioning, the Code Signing CA shall remain inactive and shall not resume any certification, revocation, validation, or cryptographic operations. No post-decommissioning certificate status services are required, as no end-entity certificates were ever issued by this Certification Authority.

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other Provisions

Not applicable.