Dubai Electronic Security Center

Dubai PKI

Ethaq Plus CA

Certification Practice Statement

Document Title	Ethaq Plus CA, Certification Practice Statement
Classification	PUBLIC
File Name	DubaiPKI-EthaqPlusCA-CertificationPracticeStatement_v1.1
Created on	17 April 2025
Revision	1.1
Modified on	25 April 2026

Document History

Date	Revision	Author(s)	Summary
17 April 2025	1.0	Mohamed Khalifa	First release
25 April 2026	1.1	Mohamed Khalifa	Updates to reflect the adoption of the UAE Trust Services regulatory framework, aligned with applicable ETSI standards and TDRA requirements.

Table of Contents

1. Introduction

This Certification Practice Statement (CPS) describes the certification practices that apply to the digital certificates issued by the Dubai PKI Ethaq Plus Certification Authority (CA). The Ethaq Plus CA is one of the subordinates CAs signed by the Dubai Root CA. This CPS complies with DESC Subordinate CAs Certificate Policy that applies to the provision of certification services offered by DESC through its Subordinate CAs (Issuing CAs).

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 Ethaq Plus CA, such sections state "No stipulation". Additional information is presented in subsections of the standard structure where required.

This CPS aims to comply with the requirements of:

- The UAE legal framework for Trust Services, consists in:
    - The Federal Decree Law (46) of 2021 on Electronic Transactions and Trust Services [Law (46) 2021];
    - The Cabinet Resolution No. (28) of 2023 Regarding the Executive Regulation of the Federal Decree-Law No. (46) of 2021 On Electronic Transactions and Trust Services [Bylaw (28) 2023];
    - The UAE Trust Services Framework Resolutions, issued by TDRA.

  The scope of compliance covers the following Trust Services as specified within the framework:
    - Provision of certificates for electronic signatures;
    - Provision of certificates for electronic seals;
    - Provision of qualified certificates for electronic signatures;
    - Provision of qualified certificates for electronic seals.
- [ETSI 319 411-1]
- [ETSI 319 411-2]

  Note: *References to ETSI standards, including ETSI EN 319 411-1, and ETSI EN 319 411-2, shall be construed in accordance with their profiling and applicability under the UAE legal framework for Trust Services including relevant TDRA resolutions, and do not extend beyond the requirements mandated under UAE law.*

This CPS covers the issuance and controls surrounding the following categories of certificates under the UAE legal framework for Trust Services:

- **Non-Qualified Certificates:** electronic signature and electronic seal certificates conforming with the level of quality defined in [Law (46) 2021] for UAE non-qualified certificates.
- **Qualified Certificates:** electronic signature and electronic seal certificates conforming with the level of quality defined in [Law (46) 2021] for UAE qualified certificates.

Further information about this document and the Ethaq Plus 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. 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, government and private sector 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.

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 the UAE, 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.

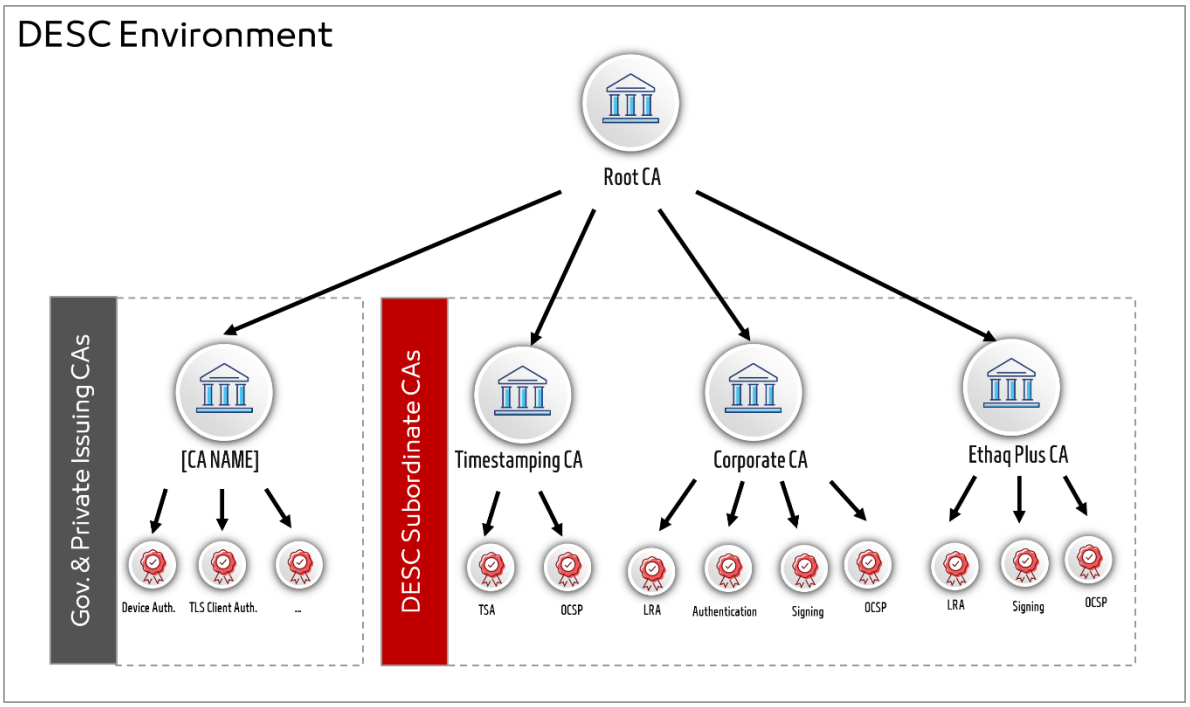

Figure 1: Trust Model for Dubai PKI

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 Ethaq Plus 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, in accordance with the Dubai PKI Key Management and Procedures, the installation, execution of key ceremonies, operation, and full life-cycle management (including deprecation) procedures of the Dubai PKI, as well as the allocation of personnel to key ceremonies in the roles of witnesses, trusted operatives, and key custodians
- Evaluating the proper working of the Dubai PKI environment
- 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 Ethaq Plus 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 Ethaq Plus 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 Ethaq Plus CA as governed by DESC Subordinate CAs CP and related documents which describe the Dubai PKI requirements and use of Certificates.

1.2 Document name and identification

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

The object identifier (OID) of this CPS is 2.16.784.1.2.2.100.1.2.1.5.

Dubai PKI organizes the OID for the certificates that are issued by the Ethaq Plus CA as shown in the following table.

OID	Certificate type	Description
2.16.784.1.2.2.100.1.2.2.1.10	Short-lived, Digital signature certificates (NCP+, formerly “high assurance”)[1]	Certificates used to create **Advanced Electronic Signatures** in accordance with Article (19) of [Law (46) 2021]. The applied identity verification process follows the assurance level defined in the applicable Certificate Policy.
2.16.784.1.2.2.100.1.2.2.1.11	Short-lived, Digital signature certificates (LCP, formerly “moderate assurance”)[2]	Certificates used to create **Advanced Electronic Signatures** in accordance with Article (19) of [Law (46) 2021]. The applied identity verification process follows the assurance level defined in the applicable Certificate Policy.
2.16.784.1.2.2.100.1.2.2.2.3	Long-lived, eSeal certificates (NCP+, formerly “high assurance”)**Error! Bookmark not defined.**	Certificates used to create **Advanced Electronic Seals** for legal persons in accordance with Article (19) of [Law (46) 2021], ensuring the origin and integrity of the sealed data.
2.16.784.1.2.2.100.1.2.2.3.6	Long-lived, LRA certificate (NCP)	Certificate used to authenticate certificate management requests submitted by third-party Local Registration Authorities (LRAs). This certificate is **not a Trust Service certificate** under [Law (46) 2021].
2.16.784.1.2.2.100.1.2.3.1.1.3	Short-lived, Qualified certificates for electronic signatures, requiring UAE-QSCD (UAE-QCP-n-qscd)	**Qualified certificates for electronic signatures** issued by a **Qualified Trust Service Provider (QTSP)** and used to create **Qualified Electronic Signatures** in accordance with Articles (20) and (21) of [Law (46) 2021], with the private key protected by a Qualified Signature Creation Device (UAE-QSCD).
2.16.784.1.2.2.100.1.2.3.1.2.3	Short-lived, Qualified certificates for electronic signatures, doesn’t require UAE-QSCD (UAE-QCP-n)	Qualified certificates for electronic signatures used to create **Advanced Electronic**

[1] Certificates previously categorized as 'high assurance' are now labeled as NCP+ to align with [TDRA Resolution No. (51)]. For consistency, references to 'high assurance' in historical documents or communications correspond to NCP+ in this CPS.
[2] Certificates previously categorized as 'moderate assurance' are now labeled as LCP to align with [TDRA Resolution No. (51)]. For consistency, references to moderate assurance' in historical documents or communications correspond to LCP in this CPS.

		Signatures in accordance with Article (19) of [Law (46) 2021], where a UAE-QSCD is not required.
2.16.784.1.2.2.100.1.2.3.2.1.2	Long-lived, Qualified certificates for eSeal signatures, requiring UAE-QSCD (UAE-QCP-l-qscd)	**Qualified certificates for electronic seals** issued by a **QTSP** and used to create **Qualified Electronic Seals** in accordance with Articles (20) and (21) of [Law (46) 2021].
2.16.784.1.2.2.100.1.2.3.2.2.2	Long-lived, Qualified certificates for eSeal signatures, doesn't require UAE-QSCD (UAE-QCP-l).	Certificates used to create **Advanced Electronic Seals** for legal persons in accordance with Article (19) of [Law (46) 2021].

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 Ethaq Plus CA (also referred to as "CA") is the Certification Authority that issues Certificates in accordance with this CPS. The Ethaq Plus CA issues certificates (see section 1.2) for natural and legal persons, in addition to OCSP certificates. This includes the following tasks:

- **Registration services:** 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 issues end-entity certificates based on the verification conducted by the registration service.
- **Dissemination service:** It disseminates, OCSP certificates, this 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 on certificate suspension or revocation lists, and an OCSP responder service. The status information shall always reflect the current status of the certificates issued by this CA.

The Ethaq Plus CA issues two types of subscriber certificates in terms of the certificate validity period:

- Long-lived certificates with long period of validity, those are issued to legal entities as indicated in section 1.2,
- Short-lived certificates with validity period of 30 minutes, those are issued to natural person and intended to be valid for a single signing transaction.

1.3.2 Registration Authorities

DESC RA

Duly authorized members part of Dubai PKI team act as Registration Authority (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.

Local Registration Authority(LRA)

The Ethaq Plus CA allows UAE-based organizations aiming to manage the certificates life cycle for their own communities to set up and act as a Local Registration Authority (LRA) for the Ethaq Plus CA.

DESC accepts the following LRAs:

- Officer duly authorized by an organization: This officer will be enrolled to DESC Ethaq Plus CA by DESC RA. He will receive credentials that allow to access the Ethaq Plus CA remotely through a dedicated Web RA application and manage the digital certificates of the organization's subscribers community. Multi-factor authentication is implemented whenever RA/LRA officers approve certificate applications for issuance.
- System/application: Operated by an organization and integrated with the Ethaq Plus CA through securely exposed APIs. The system/application is configured with dedicated credentials issued by DESC RA so that it can request certificates from Ethaq Plus CA and manage the subscribers' community certificates.

Before authorizing an entity to operate an LRA, DESC RA validates the organization's identity as specified in section 3.2.2.3 and signs an LRA agreement through which the entity commits to operate their LRA in accordance with DESC Subordinate CA CP and this CPS.

The LRA agreement describes the LRA obligations/responsibilities for:

- Authenticating, approving, or rejecting certificate application requests
- Identify subscribers in accordance with naming conventions defined within the present CP and the applicable CPS to ensure uniqueness and unambiguity
- Submit certification requests to DESC Subordinate CAs only for the applications that have been validated and approved by the LRA
- Creating and maintaining an audit-log that records all significant events related to the RA's operations and fulfilment of the above-mentioned responsibilities
- Providing selective access to audit-log records as specified in this CP
- Implementing other operational controls as specified in this CP
- Ensuring that the information that it stores and processes is handled in a manner that is consistent both with the policies and procedures defined in this document and with the Dubai PKI security's regulations.

1.3.3 Subscribers

Subscribers of the Ethaq Plus CA are Government and private sector entities within UAE, Citizens, Residents, Visitors of the UAE. In addition to the Ethaq Plus CA OCSP responder.

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 Ethaq Plus CA.

Relying Parties are entities that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate issued by the Ethaq Plus CA.

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

Short-lived certificates issued under this CPS are not subject to revocation and do not support revocation status checking. Relying Parties shall rely on the certificate validity period as the sole mechanism for determining certificate validity.

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 three categories of certificates issued by this CA which are:

- Certificates for natural persons :
    - Signature key pair and related certificate
        - Signing documents and digital transactions
- Certificates for legal persons:
    - Signature key pair and related certificate
        - eSeal documents issued by the entity (legal person)
- LRA Certificates:
    - Authentication key pair and related certificate
        - Authenticate Certificate Management requests received from LRAs.
- OCSP certificates for OCSP responder delegated by this CA.

In accordance with its purpose of use, the certificate may be used without limitations.

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 CPS document. Using certificates for other purposes is explicitly prohibited.

Certificates referred to in this CPS document shall not be used for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control. Such certificate usage is expressly prohibited.

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.

Material changes to this CPS shall be approved by the TDRA before it is published.

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

Email 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 review and formal approval of the initial version of this CPS and any subsequent updates.

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.

Under the circumstances outlined in requirement (NTF-2) of section 2.4 of [TDRA Resolution No. (51)], or when deemed necessary by the Dubai PKI PA, TDRA will be notified [60] sixty days prior implementation of changes. Once approved by TDRA, the Dubai PKI PA notifies Subscribers and Relying Parties of the changes through publishing amendments to this document [30] thirty days prior implementation.

Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice.

1.6 Definitions, acronyms and references

1.6.1 Definitions

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

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: (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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Extended Normalized Certificate Policy (NCP+): which offers the same quality as that offered by the NCP for use where a secure cryptographic device (signing or decrypting) is considered necessary. The requirements for this CPS include the policy requirements for the issuance and management of NCP+ certificates.

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 Assurance: Refers to certificates that meet NCP+ requirements as defined in [TDRA Resolution No. (51)]. This terminology was used in earlier versions of this CPS.

ICP Validation Gateway (VG): The ICP Validation Gateway (VG) is an online service provided by ICP that enables approved government entities, organizations, and individuals to securely use the Emirates ID for authentication and related identity functions in online services. It simplifies integration by removing the need for technical or cryptographic expertise and enhances the security, accuracy, and efficiency of digital transactions by relying on the Emirates ID as the single trusted source of user identity.

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. Also referred to as "**Legal Person**" in this document.

Normalized Certificate Policy (NCP): Represents the standard assurance level defined in [ETSI 319 411-1]. Certificates issued under NCP require structured and reliable identity verification based on recognized and verifiable identity evidence.

Lightweight Certificate Policy (LCP): Represents lowest assurance policy defined in [ETSI 319 411-1]. It supports issuance of certificates based on lightweight and less stringent identity verification and reduced security requirements. LCP is intended for low-risk use cases where a basic assurance of subscriber identity and certificate management controls is sufficient.

Moderate Assurance: Refers to certificates that meet LCP requirements as defined in [TDRA Resolution No. (51)]. This terminology was used in earlier versions of this CPS.

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

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

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

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

Primary piece of evidence: as far as this CPS is concerned, a primary piece of evidence is a government-issued photo ID which is issued with robust identity proofing, issuance and management processes.

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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

Qualified Certificates: Certificates that conform to the requirements set out in [TDRA Resolution No. (51)], pursuant to Article 21(4) and 24(6) of [Reg (28) 2023]. This CPS supports two types of Qualified Certificates: Qualified Certificates for Electronic Signatures and Qualified Certificates for Electronic Seals.

Qualified Signature Creation Device (UAE-QSCD): A secure cryptographic device that meets the protection and assurance requirements defined in [TDRA Resolution No. (53)]. A QSCD ensures that private keys are generated, stored, and used in an environment that provides exclusive control to the signer, protects against key extraction, and prevents unauthorized use. The device must be authorized by TDRA according to TDRA decision on the approval of QSCD in the context of the UAE legal framework for Trust Services.

Qualified Timestamping: Timestamping service issuing timestamps conforming with the requirements set out in [TDRA Resolution No. (51)], pursuant to Article 31(1) and 31(4) of the [Reg (28) 2023].

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.

Secondary piece of evidence: evidence types from government or non-government sources that are supported by moderate identity proofing, issuance and management processes. Examples of Secondary evidences are: Human Resource (HR) attestation letters, employee certificate or equivalent information establishing the employment relationship between the employee and the entity.

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.

TDRA Resolutions: The Technical resolutions issued by TDRA to define technical controls applicable to Trust Services Providers (TSPs) and Trust Services (TS) in the UAE as part of the UAE legal framework for Trust Services.

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

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

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

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

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

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

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

1.6.2 Acronyms

CA — Certification Authority

CCTV — Closed circuit TV

CP — Certificate Policy

CPS — Certification Practice Statement

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

FQDN — Fully Qualified Domain Name

HSM — Hardware Security Module

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

ITU — International Telecommunications Union

ICP — Federal Authority For Identity, Citizenship, Customs & Port Security

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.

QC — Qualified Certificate

QcStatement — Qualified Certificate Statement

QESig — Qualified Electronic Signature

QESeal — Qualified Electronic Seal

QSealCD — Qualified electronic Seal Creation Device

QTS — Qualified Trust Service

QTSDS — QTS Disclosure Statement(s)

QTSP — Qualified Trust Service Provider

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

TDRA — Telecommunications and Digital Government Regularity Authority

TRN — Tax Registration Number

TSP — Trust Service Provider

TS — Trust Service

UAE-QSCD — Qualified electronic Signature/Seal Creation Device in the sense of [Law (46) 2021]

UPS — Uninterruptible Power Supply

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

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

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

1.6.3 References

Reference	Title
[Law (46) 2021]	Federal Decree Law No. (46) of 2021 On Electronic Transactions and Trust Services
[Reg (28) 2023]	Federal Executive Regulation No. (28) of 2023
[TDRA Resolution No. (51)]	Resolution No. (51) of 2023 on The technical controls and standards applicable to trust service providers and the trust services they provide (https://tdra.gov.ae/-/media/About/Trust-Services/Resolution/Technical-Controls-Trust-Service-Provider-Resolution.ashx?t=Resolution%20No.%20(51)%20of%202023%20on%20The%20technical%20controls%20and%20standards%20applicable%20to%20trust%20service%20providers%20and%20the%20trust%20services%20they%20provide)
[TDRA Resolution No. (53)]	Resolution No. (53) of 2023 on The rules and conditions regulating the qualified signature/seal creation devices, their certification and approval (https://tdra.gov.ae/-/media/About/Trust-Services/Resolution/Qualified-Signature-Seal-Creation-Devices-Resolution.ashx?t=Resolution%20No.%20(53)%20of%202023%20on%20The%20rules%20and%20conditions%20regulating%20the%20qualified%20signature/seal%20creation%20devices,%20their%20certification%20and%20approval)
[ETSI 319 411-1]	ETSI EN 319 411-1 v1.4.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI 319 411-2]	ETSI EN 319 411-2 v2.5.1 (2023-10): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI 319 421]	ETSI EN 319 421 V1.2.1 (2023-05): Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

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

As part of the public repository, DESC publishes a copy of the Ethaq Plus CA certificates, OCSP certificates as well as this CPS.

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

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

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

2.3 Time or frequency of publication repositories

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

Owing 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 Ethaq Plus CA activities.

2.3.1 Certificates

The Ethaq Plus 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

DESC maintains the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL until minimum 7 years after the expiration date of all certificates, containing the CRL distribution point.

The Ethaq Plus CA publishes CRLs at regular intervals according to the following rules:

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

2.4 Access controls on repositories

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

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

cn = Ethaq Plus Certification Authority , o = UAE Government, c = AE

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

- **Certificates issued for legal persons through DESC RA (eSeal):**

  cn=<entity name>, ou = <optional organizational unit within the entity>, o =<entity meaningful unique name>, l =<entity locality information> , c = AE

- **Certificates issued for individuals:**

  serialnumber=<optional serial number for each subscriber>, cn=<individual end user name>, ou = <optional organizational unit within the entity>, o =< entity meaningful unique name>, l =<entity locality information>, c = AE

- **OCSP responder:**

  cn = Ethaq Plus Certification Authority OCSP "C<n>", o = DESC, l = Dubai, c = AE
  Where "C<n>" is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.

3.1.2 Need for names to be meaningful

For certificates issued to natural persons: names are meaningful since the CN contains the name of the subscriber.

For certificates issued to legal persons: names are meaningful since the CN contains the name of the entity.

For certificate issued to LRAs: name is meaningful since the CN contains the LRA Service name as agreed with during the LRA onboarding process.

For certificates issued to the Ethaq Plus CA OCSP responder: the names are meaningful and indicate the OCSP name (Ethaq Plus Certification Authority OCSP).

3.1.3 Anonymity and pseudonymity of subscribers

This CA does not support the issuance of anonymous certificates.

3.1.4 Rules for interpreting various name forms

No stipulation – this section is intentionally left blank.

3.1.5 Uniqueness of names

As per section 3.1.1 of this CPS, DESC enforces uniqueness of subject DNs are enforced as follows:

- **Certificates issued for natural persons:** Uniqueness enforced through the "cn" attribute potentially combined with the "serialnumber" attribute.
- **Certificates issued for legal persons:** A convention for a meaningful name representing uniquely an entity is enforced by DESC.
- **Certificates issued for Ethaq Plus CA OCSP responder:** The OCSP responder unique name is included in the subject DN of issued OCSP certificate.

3.1.6 Recognition, authentication and role of trademarks

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

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

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

This CA always verifies that the certificate applicant possesses the private key corresponding to the public key being certified by performing signature verification on the certificate request received. The CA expects that the certificate request is signed by the private key associated to the public key being certified.

3.2.2 Authentication of Organization identity

3.2.2.1 Identity

For certificates issued for legal persons (for electronic seals), DESC RA performs the validation of the organization and its representative according to the following process:

A. Verification of presence / legal standing

Verify the existence of the Organization using a government authoritative source that is expected to provide detailed information about the entity including its legal name, identifier (TRN) and address, the most common authoritative source used by DESC RA is the UAE Official Gazette.

B. Authority of the applicant

DESC RA verifies the authority of **Authorized Representative** as the signatory of the certificate request form and subscriber agreement as follows:

- Government authoritative source that is expected to provide such details, Or
- A trusted communication of the Organization's HR, or based on a formal letter signed by the Organization's top authority (e.g. Director General).

DESC RA verifies the authority of **Certificate Requester** to manage the certificate lifecycle on behalf of the Organization as follows:

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

(2) DESC RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized representative that attests the ability of the requestor to requests certificates on behalf of the Organization to which the requester belongs to.

C. Association

Certificates for Advanced electronic Seals: The organization name to be inserted in the requested certificate must exactly match the legal name of the Organization requesting the certificate unless there is an authentic proof linking the entity with the name to be included in the certificate.

Certificates for Qualified electronic Seals (UAE-QCP-l, UAE-QCP-l-qscd): DESC RA conducts an in-person interview with the authorized representative for identity verification as natural person representing legal person according to section 3.2.3 of this document.

Once identity verification is done successfully, the following organization's identity details is validated at the presence of authorized representative:

- Full legal name, official address, and phone numbers of the organizational entity consistent with the government authoritative source that is expected to provide such details,
- When applicable, the association between the legal person and the other organizational entity identified in association with this legal person that would appear in the organization attribute of the certificate, consistent with the government authoritative source that is expected to provide such details.

For certificates issued to DESC OCSP responder: the certification process is initiated by an authorized administrator under the supervision of the Dubai PKI PA. A dedicated operational key ceremony is documented by DESC.

3.2.2.2 DBA/Tradename

The use of DBA or Tradename in the Subject Identity Information is not supported by the Ethaq Plus CA.

3.2.2.3 Organizations applying to operate an LRA

When a government or a private sector entity aims to issue and manage natural person certificates for their user base (e.g. employees), they communicate with DESC RA or the Dubai PKI PA to go through the following enrollment process:

(1) verify the presence / legal standing of the organization as specified under point A in section 3.2.2.1,

(2) verify the authority of authorized representative of the Organization as specified under point B in section 3.2.2.1 to signs the LRA agreement,

(3) DESC RA add the required configurations on the Corporate CA RA system to enroll the Organization and its service plan(s). The information received from the Government entity during the enrolment process is used to populate this profile. LRA officers and/or RA systems are enrolled with proper authentication credentials that are used to execute certificate requests and related certificate management operations.

3.2.3 Authentication of individual identity

The DESC RA/LRA relies on primary and secondary evidences in order to verify the identity of applicants. The types of supported evidences are listed below:

The identity verification requirements for the different types of certificates is listed in the table below:

Certificate type	Identity verification requirements

For LCP certificates	**Identity proofing evidences:**
	• A Primary Evidence stating the Applicant name, date of birth, and nationality
	• Secondary Evidence confirming the applicant's address and contact information if required (including phone number and email address)
	Validation of evidences:
	• Validate that presented evidences do not seem forged or counterfeit and do not show signs of falsification
	• Verify that full name of the applicant from the Primary Evidence matches the full name from the Secondary Evidence
	• Validate Government issued IDs using the PRADO register and guidelines available from www.consilium.europa.eu/prado
	• For certificates including email address(es): a Challenge-Response mechanism to verify the applicant ownership of the email to be included in the certificate. The RA/LRA officer sends an email with a random, unique value to the email address. If the applicant replies to the email, and that email includes the original random value as sent by the RA/LRA officer, the validation is passed. The reply should be within 3 days.
	Identity binding:
	The link between the claimed identity and the claimant subscriber is verified through on of the following methods:
	• Using trusted KYC database shall fulfil one of the following requirements:
	  ○ Owned and operated by a licensee of the UAE National Bank or an organization operating under the AML (Anti-Money Laundering) regulations
	  ○ Existence of ID proofing artifacts substantiate the antecedent verification outcome
	  ○ Mechanisms are in place that bind the individual to the asserted identity
	• Using recorded videos or video calls where person's face is visually verified by an officer against a government issued photo ID
	• Using UAE PASS authentication
	• Receive a digitally signed request from by the applicant using a moderate assurance certificate

For NCP+, UAE-QCP-n, and UAE-QCP-n-qscd certificates	**Identity proofing evidences:** • A Primary Evidence stating the Applicant name, date of birth, and nationality • Secondary Evidence confirming the applicant's address and contact information if required (including phone number and email address) **Validation of evidences:** • Validate that presented evidences do not seem forged or counterfeit and do not show signs of falsification • Verify that full name of the applicant from the Primary Evidence matches the full name from the Secondary Evidence • Validate Government issued IDs using the PRADO register and guidelines available from www.consilium.europa.eu/prado • For certificates including email address(es): a Challenge-Response mechanism to verify the applicant ownership of the email to be included in the certificate. The RA/LRA officer sends an email with a random, unique value to the email address. If the applicant replies to the email, and that email includes the original random value as sent by the RA/LRA officer, the validation is passed. The reply should be within 3 days. **Identity binding:** The link between the claimed identity and the claimant subscriber is verified through on of the following methods: • Conduct an in-person meeting with the individual to complete the identity verification against the government-issued photo ID. During the meeting, the applicant presents his government-issued ID to RA/LRA officer that verifies that full name/date of birth of the individual from the attestation letter matches the full name/date of birth from the ID. Where identity binding is performed during an in-person meeting, the RA/LRA Officer shall perform binding to the applicant by manual face verification, including a morphological analysis using a defined feature list as specified in the RA/LRA verification procedures. • Verification of a biometric previously collected

3.2.4 Non-verified subscriber information

All fields constituting the subscriber information written in the certificate are verified by the relevant RA/LRA.

3.2.5 Validation of authority

- **For certificates issued by DESC RA for electronic seal (including LRA certificates):** The authority of both the Authorized Representative and Certificate Requestor are verified as specified in point B under section 3.2.2.1 of this document.
- **For natural persons certificates to be issued through an LRA:** The LRA officer/system (that was previously approved by The Dubai PKI PA) is authorized to submit certification requests on behalf of the LRA's subscribers.

3.2.6 Criteria for interoperation

No stipulation – this section is intentionally left blank.

3.3 Identification and authentication for re-keying requests

3.3.1 Identification and authentication for routine re-keying

Identification and authentication for re-keying is performed as in initial registration. Short-lived certificates are not subject to re-key, such certificates are requested for every signing transaction.

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 request

- **Certificates issued by DESC RA for electronic seal and LRA certificates:** DESC RA verifies that an authorized representative has requested the revocation through one of the following methods:
    - Receiving a revocation request through email from the organization'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 organization's representative by using some of the available information (phone call, email)
    - Receiving a revocation request through DESC WebRA that the organization has been enrolled into as part of the onboarding process for the initial registration.

  Once the revocation request is successfully authenticated, DESC RA revokes the subject certificate through the relevant RA system.
- **Certificates issued to natural persons through the RA\LRA:** The RA/LRA officer authenticates the revocation request through one of the following methods:
    - Receiving a revocation request from the subscriber through channels authorized by the RA\LRA. This may include a face to face, call from the subscriber and the RA/LRA asking relevant questions to identify the subscriber (e.g. employee ID, name, date of birth, ….) or email from the subscribe using an email address that can be verified by the RA/LRA and linked to the subscriber's identity.
    - Communication with the requesting party to provide reasonable assurances that the individual or department requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include telephone and/or email.

  - HR (or team within the entity with similar mandate) if the subscriber is terminated or changed role within the entity which would trigger the revocation request. The RA/LRA would have the internal means to confirm with HR the validity of the revocation request.

- **Certificates issued to natural persons through LRA system\application:** Revocation requests are authenticated through one of the following methods:
  - When a revocation request is triggered by a business process. The LRA system/application interacts with the subscriber and validates the subscriber's identity and confirms that a revocation request is required. The LRA system/application then interacts (through integration) with the Ethaq Plus CA to revoke the certificate.
  - A revocation request is triggered by the Subscriber through the LRA helpdesk. The LRA helpdesk communicates with DESC RA through agreed channels (telephone, email) which results in the revocation request being authenticated by DESC RA which can then process it through their dedicated RA applications.

4. Certificate Life Cycle Management

4.1 Certificate application

4.1.1 Who can submit a certificate application

- **Certificates for legal persons issued through DESC RA (electronic seal certificates and LRA certificates) :** An authorized person from the organization submits the certificate application as part of the certificate issuance process. Whoever is submitting the certificate request (requester) needs to sign the application form and ensure that an organization's authorized representative approves the certificate request by signing and stamping the certificate request form and the appended subscriber agreement.

  DESC maintains its own internal blacklist of applicants from which it will not accept certificate requests. DESC RA logs in this database previously rejected certificate requests due to suspected or fraudulent usage and revoked certificate requests. This internal blacklist database is queried by the DESC RA whenever it receives any certificate request.
- **Certificates for natural persons issued by DESC RA and the LRAs:** The LRA or DESC RA submits the certificate application. The RA\LRA maintains its own internal blacklist of applicants from which it will not accept certificate requests.
- **Certificates issued to the OCSP responder certificate:** 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

For certificates issued by DESC RA for electronic seal and LRA certificates:

a) DESC RA shares the list of evidences required along with Subscriber Agreement and the certificate request form with the applicant,

b) the applicant prepares the list of evidences, fills the certificate request form and signs a Subscriber Agreement or ratify a certificate terms of use,

c) DESC RA receives the signed subscriber agreement, certificate application form along with the requests list of evidences (refer to section 3.2.2 for the evidences required),

d) DESC RA verifies that received documents do not seem forged or counterfeit and do not show signs of falsification,

e) One of DESC RA verifies the applicant's authority and the organization's identity as described in section 3.2.2,

f) A second DESC RA officer (who was not involved in the previous steps) reviews the work done the first officer to conclude application's approval,

g) Once the application is approved, DESC RA officer uses a dedicated RA application to enroll the applicant into this CA. The applicant's unique name from the application form is used to produce a unique distinguished name necessary for enrolment into the CA system,

h) The applicant generates a key pair on its own IT system or device as per the requirements set forth in section 6.1.1.2 of this document, then generated the CSR,

i) The CSR file is sent to DESC RA through the requester's email (as provided in the certificate application form). DESC RA processes the CSR and issue the certificate from the CA,

j) DESC RA send the certificate to the entity requester's email address.

Certificates for natural persons issued through the DESC RA and the LRAs via Manual Registration

This method involves physical identity verification by a designated Registration Authority (RA) or Local Registration Authority (LRA) Officer:

1. **Physical Presence:**
   The Subscriber physically presents themselves at an authorized RA/LRA location.

2. **Documentation and Consent:**
   The Subscriber completes and signs the Registration Form and the Certificate Issuance Terms and Conditions.

3. **Identity Verification:**
   The RA/LRA Officer:
   - Validates the Emirates ID visually using the specifications available from https://www.consilium.europa.eu/prado;
   - Manual comparison of the applicant's face against the photograph on the identity document. The RA/LRA Officer performs binding to the individual by manual face verification, including a morphological analysis using a defined feature list as specified in the RA/LRA verification procedure;
   - Matches personal data from the Emirates ID with the registration form.

4. **Recordkeeping:**
   The signed documents are retained by the RA/LRA Officer as part of the certificate issuance record.

5. **Digital Archive Creation:**
   The RA/LRA Officer creates a PDF archive comprising:
   - Scanned Emirates ID,
   - Signed Registration Form,
   - Signed Terms and Conditions.
     This archive is digitally signed using the RA/LRA Officer's DESC-issued certificate via the RA Signing Tool.

6. **Key Generation and Certificate Request:**
   Using the RA Enrollment Platform:
   - A signing key pair is generated on a hardware cryptographic device,
   - A certificate signing request (CSR) is created and submitted to the Ethaq Plus CA.

7. **Certificate Issuance and Deployment:**
   The CA validates the CSR and issues the signing certificate, which is returned to the RA system and linked to the Subscriber's digital identity profile.

Certificates for natural persons issued through the LRA system/application via Digital Onboarding

Remote, unattended registration of natural persons is supported via the LRA Digital Identity Verification Platform (also referred to as the eKYC Platform). The platform supports multiple identity verification channels.

A. UAE PASS

1. **Authentication via UAE PASS:**
   The Subscriber authenticates using UAE PASS credentials.

2. **Verified Identity Data Retrieval:**
   The platform retrieves verified identity attributes via secure integration with UAE PASS.

3. **Trust in Prior Verification:**
   The process relies on prior biometric face verification and liveness detection already conducted by UAE PASS.

4. **Consent and Key Generation:**

   - The Subscriber accepts the Certificate Issuance Terms and Conditions via the eKYC Platform.
   - A signing key pair is generated on a hardware cryptographic device.

5. **Certificate Issuance and Deployment:**

   - A CSR is generated and submitted to the Ethaq Plus CA,
   - The signing certificate is issued and securely deployed on the Subscriber's device.

B. Emirates ID Card

1. **ID Capture and Data Validation:**

   - The Emirates ID card is scanned via camera and user data is read via contact/contactless reader,
   - Data is validated against the issuing authority using trusted APIs.

2. **Biometric Verification:**

   - A live facial image is captured and subjected to liveness detection (ETSI-compliant),
   - The image is matched against the chip-stored photo on the Emirates ID,
   - The process must meet a **False Acceptance Rate (FAR) ≤ 1/1000**.

3. **Consent and Key Generation:**

   - Subscriber accepts the Terms and Conditions;
   - A signing key pair is generated on a hardware cryptographic device;
   - The CSR is submitted to the Ethaq Plus CA.

4. **Certificate Issuance and Deployment:**

   - The signing certificate is issued and deployed to the Subscriber's device.

C. ICAO-Compliant ePassport (eMRTD)

1. **eMRTD Scan and Validation:**

   - The Subscriber's passport is scanned and eMRTD data is read using an NFC-enabled device,
   - Data is validated using CSCA certificates from the **ICAO PKD**.

2. **Biometric and Liveness Verification:**

   - Live image is captured and checked for liveness (FAR ≤ 1/1000),
   - Face verification is performed against the image in the ePassport chip.

3. **Consent and Key Generation:**

- Subscriber accepts the Certificate Issuance Terms and Conditions;
- A signing key pair is generated on a cryptographic device;
- A CSR is created and submitted to the Ethaq Plus CA.

4. **Certificate Issuance and Deployment:**
    - The signing certificate is issued and securely deployed to the Subscriber's device.

For certificates issued to the OCSP responder

The certification process is initiated by an authorized administrator under the supervision of the Dubai PKI PA. A dedicated operational key ceremony is documented by DESC.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Initial identity vetting is performed by DESC RA or the LRA as set forth in Section 3.2. All the activities comprising the certificate application processing (email communication, phone calls, vetting evidence) are stored along with the certificate application.

As described in section 4.1, in addition to the backlist check that done by the RA/LRA according to its own internal blacklist. If the requestor/entity is in the blacklist, the certificate application is rejected.

DESC RA or the LRA may use the documents and data provided in Section 3.2 to verify Certificate information, or may reuse previous validations themselves, provided that:

- The data or documents are obtained from a source specified in Section 3.2, or the validation was completed no more than 90 days prior to issuing the Certificate; or
- Irrespective of the age of the previously validated data, DESC may rely on an earlier verified certificate request to issue a replacement certificate, provided that:
    - The certificate being referenced was not revoked due to fraud or any other illegal activity;
    - The expiration date of the replacement certificate matches the expiration date of the Certificate being replaced; and
    - The Subject information in the replacement Certificate is identical to the Subject information in the Qualified Certificate being replaced.

4.2.2 Approval or rejection of certificate applications

The certificate application based on the results of the identification and authentication specified in section 4.1.

For OCSP certificates: A certificate application is approved/rejected as part of the overall approval/rejection of the corresponding certification process.

Multi-factor authentication is implemented whenever RA/LRA officers approve certificate applications for issuance.

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

- **For certificates issued to legal persons through DESC RA (electronic seal certificates and LRA certificates):** Following the approval of the certificate application by the DESC RA, the CSR file is uploaded and submitted to this CA by the DESC RA officer using a dedicated application. 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 is then downloaded by DESC RA officer sent to the certificate requester email address.
- **For certificates issued to natural persons through the DESC RA and the LRAs:** Following the approval of the certificate application by the RA/LRA, the certificate request is submitted to this CA by the RA/LRA officer using a dedicated application. The CA validates the format of the request then creates the certificate in accordance with the specified certificate template and is made available to the RA/LRA application. The certificate is activated by the CA and is ready for usage. The RA/LRA officer completes the process by installing the certificate on the target cryptographic device.
- **For certificates issued to natural persons through the LRA system/application:** The CA receives the certificate request from the LRA system/application. The CA validates the format of the request then creates the certificate in accordance with the specified certificate template and automatically returns the certificate to the LRA system/application. The certificate is activated by the CA and is ready for usage.
- **For OCSP certificates:** An authorized administrator manually delivers the CSR file including the servers' public key to DESC RA team. DESC RA team submit the CSR file directly to the CA that will issue the certificate and makes it available to be downloaded by the PKI administrator who will then hand it over to the authorized administrator.

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

- **For certificates issued to legal persons through DESC RA (electronic seal certificates and LRA certificates):** the applicant is notified of the certificate issuance once collecting his certificate from DESC RA.
- **For certificates issued to natural persons through the DESC RA and the LRAs:** The subscriber is notified once collecting his certificate from the RA/LRA officer.
- **For certificates issued through the LRA system/application**: The system/application notifies the user on certificate issuance once it receives the certificate from the CA. This is done through the interaction (message displayed) that the user has with the LRA system/application.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

When applicants receive the certificate, they validate the certificate content against the request made earlier. In case of any discrepancies noted by the requester, he/she initiates a communication with the relevant RA\LRA, that may lead to initiation of the certificate revocation request by the applicant.

If no complaints were raised by the applicant within 10 business days from receiving the certificate, the certificate is deemed accepted by the applicant.

For OCSP: A certificate is deployed on the target system as part of the overall DESC internal operational ceremony.

4.4.2 Publication of the certificate by the CA

The Ethaq Plus CA and OCSP certificates shall be published on the dissemination page as described in section 2.2. The Ethaq Plus CA does not publish other end-user certificates apart from sharing it with the requester.

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:

- Comply with the terms of the Subscriber agreement,
- Use certificates exclusively for legal activities consistent with the CP and this CPS,
- Protect the private key (and related secrets) from compromise, loss, disclosure, or otherwise from unauthorized use. For UAE-QCP-n-qscd and UAE-QCP-l-qscd certificates, Subscriber keys must be generated and stored within a UAE-QSCD.
- 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,
- Notify the RA/LRA immediately if any details in the certificate become invalid, or as a result of any compromise, loss, disclosure, or otherwise unauthorized use of their private keys,
- Avoid using the private key until after the CA has issued, and the Subscriber has accepted the corresponding certificate.

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, 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 Ethaq Plus CA OCSP or CRL, it decides to do so completely at his 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.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate Re-key

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

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

Short-lived certificates are not subject to re-key, a new certificate is requested for every signing transaction.

4.7.1 Circumstance for Certificate Re-key

Certificate Re-key may happen while the certificate is still active, after it has expired or after a revocation. The original certificate may be revoked after re-key is complete, however, the original certificate must not be further re-keyed.

4.7.2 Who may request certification of a new public key

As per initial certificate issuance.

4.7.3 Processing Certificate Re-keying requests

As per initial certificate issuance.

4.7.4 Notification of new certificate issuance to subscriber

As per initial certificate issuance.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As per initial certificate issuance.

4.7.6 Publication of the Re-keyed Certificate by the CA

As per initial certificate issuance.

4.7.7 Notification of certificate issuance by the CA to other entities

As per initial certificate issuance.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

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

4.8.2 Who may request certificate modification

Not applicable. Refer to section 4.8.1.

4.8.3 Processing certificate modification requests

Not applicable. Refer to section 4.8.1.

4.8.4 Notification of new certificate issuance to subscriber

As per initial certificate issuance.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable. Refer to section 4.8.1.

4.8.6 Publication of the modified certificate by the CA

As per initial certificate issuance.

4.8.7 Notification of certificate issuance by the CA to other entities

As per initial certificate issuance.

4.9 Certificate revocation and suspension

Suspension of a certificate is not allowed by this CA. Only permanent certificate revocation is allowed.

4.9.1 Circumstances for revocation

The relevant RA/LRA revoke a certificate within 24 hours if one or more of the following occurs:

1. Received a written request from the Subscriber or an authorized representative;
2. The Subscriber discovers that the original certificate request was not authorized and does not retroactively grant authorization; or
3. The RA/LRA/CA discover or has reasons to believe that there has been a compromise of the private signing key,
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys), or
5. The information on the certificate is no longer accurate.

This CA should ensure a certificate revocation is executed within 24 hours and shall revoke a certificate within 5 days if one or more of the following occurs:

1. DESC obtains evidence that the certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
2. DESC obtains evidence that the Certificate was misused,
3. DESC is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use,
4. DESC is made aware of a material change in the information contained in the Certificate,
5. DESC is made aware that the Certificate was not issued in accordance with DESC CP/CPS,
6. Finding that the certificate was issued without the authorization of the individual named as the subject of such certificate,
7. DESC determines or made aware that any of the information appearing in the Certificate is inaccurate or misleading,
8. Revocation is required by DESC's CP and/or CPS,
9. The entity or the individual has been declared legally incompetent,

10. DESC is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, or if there is clear evidence that the specific method used to generate the Private Key was flawed,
11. The Ethaq Plus CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate, or
12. The Ethaq Plus CA's right to issue Certificates under the requirements defined in this CPS expires or is revoked or terminated, unless the Ethaq Plus CA has made arrangements to continue maintaining the CRL/OCSP Repository.

In addition to the above circumstances, certificates issued through DESC RA or the LRA, the RA/LRA shall revoke digital certificates corresponding to its community when required by the entity's internal processes.

On the other hand, this CPS does not provide provisions for revoking the following certificates:

- OCSPs certificate, apart from the compromise of the OCSP key pair that is treated by DESC as per its Disaster Recovery and Business Continuity procedures.
- Short-term certificates due to their limited validity period and operational characteristics, such certificates are not subject to revocation, including on the initiative of the CA itself. Reliance on these certificates is based solely on their short validity period, and they expire naturally at the end of their validity.

The following sub-sections focus only on the revocation provisions that apply for the certificates issued by this CA.

4.9.2 Who can request revocation

- The individual (natural person) to whom certificates were issued.
- The organization (legal person) to whom certificates were issued.
- Any relying party possessing evidence of compromise of the subscriber's certificate.
- Revocations are directly initiated by DESC's RA officers in the cases described in section 4.9.1.
- The RA/LRA shall revoke certificates corresponding to its community when required by applicable business processes.
- 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 setup by this CA for the revocation of certificates:

- **Revocation of certificates through DESC RA:**
    - The subscriber or an authorized representative can request the revocation of their certificate(s) to the DESC RA.
    - The DESC RA officer authenticates the subscriber's identity as described in section 3.4.
    - The DESC RA officer requests the subscriber to fill in and sign a revocation request form.
    - The DESC RA officer revokes the subscriber's certificate(s).
    - The CA generates an updated CRL and publishes it to the DESC public repository.
- **Revocation of certificates through LRA:**
    - The RA/LRA receives a formal revocation request from the subscriber.
    - The RA/LRA validates the identity of the subscriber as done during initial certificate application.
    - The RA/LRA records the revocation request according to the entity's business rules.

- The RA/LRA officer revokes the subscriber's certificates.
- The CA generates an updated CRL and publishes it to the DESC public repository.

- **Revocation of OCSP:**
  - The revocation is conducted as part of a PKI process internal to DESC and is approved by the Dubai PKI PA. For OCSP, the process will also involve communication with relying parties in order to update them with the OCSP certificate revocation.

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 RA processes reports according to the investigation and preliminary reporting timelines defined in Section 4.9.5.

4.9.4 Revocation request grace period

There is no revocation grace period. Revocation requests are processed timely upon reception by the RA\LRA.

4.9.5 Revocation request response time

Certificate revocation requests received from subscribers, their representatives or initiated by DESC RA are processed within 24 hours.

For certificate problem reports, DESC RA begins investigations within 24 hours from receiving the report. DESC RA initiates communication with the Subscriber and where appropriate, with other concerned authorities (e.g. local regulator). A preliminary communication on the certificate problem is sent to the Subscriber and to the reporting entity of the problem report. In the event that a certificate problem report is received but provides insufficient information to confirm the reported issue within 24 hours, the DESC RA shall issue a preliminary report to both the Subscriber and the reporting party. This preliminary report will detail the current findings and specify the additional information required to complete the investigation. Further action on the revocation request will be resumed once the necessary data is provided by the reporting entity.

DESC RA performs further investigations involving the Dubai PKI PA, the subscriber and other relevant authorities (e.g. local regulator) to decide on the action to be taken on the subject certificate.

If the investigations results led to one of the certificate revocation circumstances listed in section 4.9.1, then the certificate will be revoked within the timeframe set forth in the aforementioned section.

If a revocation request or certificate problem cannot be confirmed and processed within 24 hours, DESC RA shall:

- Conduct a Risk Analysis: Complete and record a formal risk analysis to determine the appropriate timeline for revocation. This analysis considers the severity of the alleged problem, potential harm to Subscribers or Relying Parties, and the credibility of the reporting source.
- Preliminary Reporting: Provide an initial response to the Subscriber and the reporting entity within 24 hours of receipt, acknowledging the report and outlining the investigation status.

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

4.9.6 Revocation checking requirement for relying parties

The Ethaq Plus CA provides 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.

4.9.8 Maximum latency for CRLs

The Ethaq Plus CA issues CRLs as per the CRL issuance frequency listed in section 2.3.

4.9.9 Online revocation/status checking availability

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

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

4.9.10 Online revocation checking requirements

The Ethaq Plus CA OCSP responder supports both HTTP GET and HTTP POST methods.

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

If the OCSP responder receives a request for the status of a certificate serial number that is "unused" (i.e. not issued by) the Ethaq Plus CA, then the OCSP responder responds with a "revoked" status as defined by RFC 6960.

4.9.11 Other forms of revocation advertisements available

The Ethaq Plus CA only uses OCSP and CRL as methods for publishing certificate revocation information.

4.9.12 Special requirements – Key compromise

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

Parties may use the following methods to demonstrate key Compromise:

- Submission of a signed CSR, Private Key or other challenge response signed by the Private Key and verifiable by the Public Key, or
- The private key itself

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.

4.9.16 Limits on Suspension Period

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 through HTTP interface (an HTTP URL of the CRL distribution point is included in the certificate's CDP extension).

The Ethaq Plus CA OCSP responder exposes an HTTP interface accessible to relying parties. It provides revocation information as below:

- it supports real-time revocation status i.e. for every revocation performed by this CA, revocation information is available to the OCSP service immediately,
- responses define value in the nextUpdate field which is not more than 8 hours after the thisUpdate field,
- the value in the nextUpdate field always before or equal to the notAfter date of all certificates included within the BasicOCSPResponse.certs field, or if the certs field is omitted, before or equal to the notAfter date of the CA certificate which issued the certificate that the BasicOCSPResponse is for.

4.10.2 Service availability

The repository including the latest CRL should be available 24X7 at least 99% per year.

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

The CA maintains a 24X7 ability to respond internally to high-priority certificate problem report as described in section 4.9.3 of this CPS.

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.

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

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 Dubai PKI Data Center 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, biometric access, and Closed-Circuit TV (CCTV) monitoring. These physicals controls protect the hardware and software from unauthorized access, furthermore these controls are be monitored on a 24x7x365 basis.

The Dubai PKI systems are protected by six tiers of physical security, with access to the lower tier required before gaining access to the higher most restrictive tier. Sensitive CA operational activities related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is enforced through the use of two factor biometric authentication. Further, access to the enclave where the Dubai PKI systems are hosted is enabled only if two trusted employees are present to open the enclave's door.

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

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

The secure enclave 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

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 Off-site backup

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

Facilities used for offsite backup and archives shall have the same level of security as theDubai PKI'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 Ethaq Plus CA activities, maintaining confidentiality and protecting personal data.

5.2.1 Trusted roles

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

- Director of Cybersecurity Systems and Solutions Department
- Operations Manager
- Credentials Owners
- Chief Information Security Officer (CISO)
- Registration Authority (RA) Officers
- PKI Administrators

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

5.2.2 Number of persons required per task

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

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

- physical access to the secure enclave where the CA systems are hosted,
- access to and management of CA cryptographic hardware security module (HSM),
- validate and authorize the issuance of end-entity certificates. This is enforced during the certificate application processing where an RA officer review and verify all the Applicant information and a second RA officer reviews and finally cross sign the application to get it approved.

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

5.2.3 Identification and authentication for each role

Before carrying out the responsibilities of a trusted role:

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

5.2.4 Roles requiring separation of duties

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

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

5.3 Personnel controls

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

5.3.1 Qualifications, experience and clearance requirements

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

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:
    - The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and

- The verification of well-recognized forms of government-issued photo identification (e.g., Emirates ID); and

2. Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:

   A. Criminal convictions for serious crimes,

   B. Misrepresentations by the candidate,

   C. Appropriateness of references,

   D. Any clearances as deemed appropriate.

5.3.2 Background check procedures

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

5.3.3 Training requirements

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

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

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

- Criminal convictions for serious crimes,
- Misrepresentations by the candidate,
- Appropriateness of references,

- Any clearances as deemed appropriate,
- Privacy protection,
- Confidentiality conditions.

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of event recorded

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

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

DESC ensures that at least the following details are recorded:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction,
  - Cryptographic device lifecycle management events.
- CA and subscriber certificate lifecycle management events, including:
  - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles,
  - Certificate requests, 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 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,
- System configuration changes and maintenance, as defined in the CPS,
- CA personnel changes,
- Discrepancy and compromise reports,
- Information concerning the destruction of sensitive information,
- Current and past versions of all Certificate Policies,
- Current and past versions of Certification Practice Statements,
- Vulnerability Assessment Reports,
- Threat and Risk Assessment Reports,
- Compliance Inspection Reports,
- Current and past versions of Agreements,
- Other documents that are required for audits include:
    - Infrastructure plans and descriptions,
    - Physical site plans and descriptions,
    - Configuration of hardware and software,
    - Personnel access control lists.

5.4.2 Frequency of processing log

DESC ensures that designated personnel reviews log files at regular intervals in order to validate log integrity and ensure timely identification of anomalous events.

Designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity as per the following audit log review cycle:

- On a monthly basis, the PKI operations management reviews the CA applications and security logs to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly
- On a quarterly basis, the PKI operation management reviews the physical access logs and the user management on the CA systems with an objective to continuously validate the ongoing physical and logical access policies
- Evidence of audit log reviews, outcome of the review process, and executed remediation actions are collected and archived for inspection by authorized DESC personnel.

5.4.3 Retention period for audit log

Audit logs are retained in accordance with the UAE legal framework for Trust Services and for fifteen (15) years from the occurrence of the relevant event, including following decommissioning or termination of the Certification Authority, as applicable.

Specifically:

- CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) are retained for fifteen (15) years from the occurrence of the relevant lifecycle event.
- Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1), where applicable, are retained for fifteen (15) years from the occurrence of the relevant certificate lifecycle event.
- Security event records (as set forth in Section 5.4.1) are retained for fifteen (15) years from the occurrence of the security event, or for a longer period where required by applicable legal or regulatory requirements.

Audit logs are protected against unauthorized modification or deletion and may be made available to competent authorities or auditors upon lawful request.

5.4.4 Protection of audit log

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

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

5.4.5 Audit log backup procedures

The following rules apply for the backup of the Ethaq Plus CA audit log:

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

DESC conducts an annual Risk Assessment that:

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

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

5.5 Records archival

5.5.1 Types of records archived

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

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

5.5.2 Retention period for archive

DESC retains audit logs (as set forth in Section 5.4.1) and records (as set forth in Section 5.5.1) in accordance with the UAE legal framework for Trust Services and for fifteen (15) years from the occurrence of the relevant event, including following decommissioning or termination of the CA, as applicable.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for 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.

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archive Information

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

5.6 Key changeover

To minimize impact of key compromise, Ethaq Plus CA private key is periodically changed over as specified in section 6.3.2.

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

5.7.2 Computing resources, software/data corruption

DESC and all other PKI Participants (other than subscribers and relying parties), establishes the necessary measures to ensure full recovery of the Ethaq Plus CA services in case of a disaster, corrupted servers, software or data.

DESC establishes:

- Disaster recovery resources in a location sufficiently distant from the regular 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 witnessing of more than one member of the Dubai PKI PA.

5.7.3 Entity private key compromise procedures

For subscriber's key compromise, see section 4.9 of the present CPS.

In the event of a key compromise of the Ethaq Plus CA, or of the associated activation data, DESC triggers the Key compromise and CA termination plans detailed as part of DESC Business continuity and disaster recovery plan.

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

5.7.4 Business continuity capabilities after a disaster

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

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

Failover scenarios to the Ethaq Plus CA disaster recovery location are made possible considering the Ethaq Plus CA backup system that enables the continuous replication of critical Ethaq Plus CA data from the primary site to the disaster recovery site.

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. It includes the following:

1. Conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan,
6. Awareness and education requirements,
7. Responsibilities of individuals,
8. Recovery time objective (RTO),
9. Regular testing of contingency plans,
10. Plan to maintain or restore 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. 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, the CA termination plan shall be executed and it shall cover the following actions:

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

6. Technical Security Controls

This section defines the security measures DESC takes to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key access tokens). These measures are intended to complement and be read in conjunction with the Dubai PKI Key Management and Procedures.

6.1 Key pair generation

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

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

The Ethaq Plus 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).

DESC ensures that the implementation and documentation of key generation procedures comply with this CPS, integrating the following requirements:

- The key generation ceremony is subject to the formal authorization of the Dubai PKI PA,
- The key generation ceremony is conducted in presence of a combination of authorized personnel with trusted roles including the Dubai PKI PA representatives,
- The Ethaq Plus CA Key Generation Ceremony is witnessed by DESC internal auditor,
- DESC ensures the distribution of the tokens giving access to the private key(s) to the trusted operatives and key custodians,
- DESC internal auditor issues a report, covering that the Ethaq Plus CA, during its Key Pair and Certificate generation process:
    - Documented its Ethaq Plus CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement,
    - Included appropriate detail in its Ethaq Plus CA Key Generation Script,
    - Maintained effective controls to provide reasonable assurance that the Ethaq Plus CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Ethaq Plus CA Key Generation Script,
    - Performed, during the Ethaq Plus CA key generation process, all the procedures required by its Ethaq Plus CA Key Generation Script,
- A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes.

6.1.1.2 Subscriber key pair generation

The Ethaq Plus 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
LCP, NCP, UAE-QCP-n and UAE-QCP-l Certificates	Key pair shall be generated using a [FIPS 186-4] or [ETSI TS 119 312] approved methods for key generation
NCP+ Certificates	The key pair shall be generated within a hardware-based cryptographic module that is validated to FIPS 140-2 Level 3 or FIPS 140-3 Level 3
UAE-QCP-n-qscd and UAE-QCP-l-qscd Certificates	The key pair shall be generated and remain within a UAE-QSCD. The CA ensures that all key pairs are created and securely stored within a UAE-QSCD. The certification status of each UAE-QSCD is continuously monitored through TDRA, and appropriate actions—including certificate revocation—will be taken if the QSCD's certification status changes
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. The Ethaq Plus CA does not perform Subscriber key generation.

6.1.3 Public key delivery to certificate issuer

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

6.1.4 CA public key delivery to relying parties

The Ethaq Plus CA makes 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 Ethaq Plus 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 Ethaq Plus CA relies on off-the-shelf implementation of key PKI functionality including public key parameters generations. The Ethaq Plus CA HSMs and associated software meet FIPS 186-2 requirements for random generation and primality checks.

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

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

6.1.7.1 Ethaq Plus CA

Ethaq Plus CA key usage.

CA signing
Ethaq Plus CA signing keys are the only keys permitted to be used for signing certificates and CRLs.
The Certificate KeyUsage field must be set to: KeyCertSign and cRLSign

6.1.7.2 Subscriber certificates

Certificates issued to subscribers contain a key usage extension depending on their intended usage in accordance with RFC 5280. Refer to section 7.1 and 7.3 of this CPS.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

DESC generates the CAs' key pairs and store their private keys within a Cryptographic Device that is certified according to the rating specified in 6.2.11.

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

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

DESC implements 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 the CA cryptographic hardware.

DESC keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it keeps track of the renewed tokens and/or password distribution.

6.2.3 Private key escrow

Not applicable.

6.2.4 Private key backup

The Ethaq Plus CA private keys shall be backed up within backup devices that meet the same certification level as the subordinate CA HSM and as described in section 6.2.1. Backup operations are executed as part of the Ethaq Plus CA key generation ceremonies. The Ethaq Plus CA key is backed up under the same dual control and split knowledge as the primary key.

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

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

6.2.5 Private key archival

No stipulation – this section is intentionally left blank.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

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

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

6.2.7 Private key storage on cryptographic module

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

6.2.8 Method of activating private key

6.2.8.1 CA keys

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

6.2.8.2 Subscribers keys

Subscribers are responsible for activating and protecting their private key according to the obligations articulated in the Subscriber Agreement.

6.2.9 Method of deactivating private key

The Ethaq Plus CA's private key is deactivated in the following situations:

- The CA HSM is manually switched off.
- There is a power failure within the CA facility.
- 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 over-written before the space is released to the operating system.

6.2.10 Method of destroying private key

At the end of their lifetime, taking into account business purpose and legal obligations, the Ethaq Plus CA private keys shall be destroyed by multi-person presence including at least one representative of the Dubai PKI PA, in order to ensure that these private keys cannot ever be retrieved and used again.

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

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

6.2.11 Cryptographic module rating

6.2.11.1 Ethaq Plus CA

The Ethaq Plus CA uses a Cryptographic Device certified to FIPS 140-2 Level 3 or above, and approved by TDRA as QSealCD[3].

6.2.11.2 Subscribers

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

Refer to section 5.5 of this CPS.

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 (8) years.
- The maximum operational period for a subscriber's key pair must be five (5) 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
Short-Lived certificates for natural persons and associated keys	Maximum operational period for a subscriber's key pair must be 30 minutes
Long-Lived certificates for legal persons and associated keys	Maximum operational period for a subscriber's key pair must be five years i.e., 60 months

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1.1 Ethaq Plus CA

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

[3] **TDRA approval signifies** that the device is assimilated, as per Art.2 paragraph 4 of Resolution 53 of 2023, as QSealCD only for use by a qualified trust service provider (QTSP) having been duly licensed and qualified in the UAE. QTSPs may only use such device for internal purposes, as part of their trustworthy systems, where they electronically sign or seal, in their name, outputs or evidences as part of the provision of the qualified trust service (QTS) for which they have been granted a license and a qualified status. QTSP may not provide such device to end-users or use them on behalf of end-users.

6.4.1.2 Subscribers keys

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

6.4.2 Activation data protection

6.4.2.1 Ethaq Plus CA

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

6.4.2.2 Subscribers

Refer to section 6.4.1.2 of this CPS.

6.4.3 Other aspects of activation data

No stipulation – this section intentionally left blank.

6.5 Computer security controls

The Ethaq Plus CA performs all CA and RA functions using trustworthy systems that meet DESC security in addition to the present requirements.

6.5.1 Specific computer security technical requirements

The Ethaq Plus CA shall be operated according to the following security controls:

- Physical access control to 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 history and audit data,
- Audit of security-related events,
- Automatic and regular validation of CA systems integrity,
- Recovery mechanisms for keys and CA systems,
- Hardening CA servers operating system according to best practices and PKI vendor requirements,
- Network protection, including intrusion detection systems,
- Proactive patch management for the CA systems,
- Multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

No stipulation – this section is intentionally left blank.

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

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

6.6.2 Security management controls

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

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

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

6.6.3 Life cycle security controls

No stipulation – this section 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 a highly secure network zone .

6.8 Time stamping

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

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

7.1.1 Version number

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

7.1.2 Certificate extensions

X.509 v3 extensions are supported as specified in sections 7.1.10 and 7.1.12 of this CPS for.

7.1.3 Algorithm object identifiers

X.509 v3 standard OIDs are used. The Corporate CA issues certificates indicated by the following OIDs:

- **SHA256WithRSAEncryption** {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
- **ECDSAWithSHA256** {iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2}
- **ECDSAWithSHA384** {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}

7.1.4 Name forms

As per the naming conventions and constraints listed in Section 3.1.1 of this CPS, that is followed while defining the certificate profiles in sections 7.1.10 and 7.1.12 of this CPS.

The certificate subject attributes shall not contain values as meta data of period, hyphen, empty space, etc (Eg: '.' OR '-' OR ' ') indicating the attribute as blank or not applicable.

7.1.5 Name constraints

Name constraints extension is not supported.

7.1.6 Certificate policy object identifier

The Ethaq Plus CA uses certificate policy object identifiers that are defined as part of OID scheme for the Dubai PKI. Refer to sections 7.1.10 and 7.1.12 of this CPS for the profiles of the certificates issued by the Ethaq Plus CA including the values of the OID identifiers.

7.1.7 Usage of policy constraints extension

Policy constraints extension is not supported.

7.1.8 Policy qualifiers syntax and semantics

The use of policy qualifiers as per the RFC 5280 is supported. Refer to sections 7.1.10 and 7.1.12 of this CPS for the profiles of the certificates issued by the Ethaq Plus CA including the used policy qualifiers.

7.1.9 Processing semantics for critical certificate extensions

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

7.1.10 Certificates for natural persons

7.1.10.1 Subscriber's signing certificate (NCP+) ASN1 description

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE[4]	O/M[5]	CO[6]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
signatureValue		M	D	Ethaq Plus CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
issuer	False	M			
CountryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	UAE Government	PrintableString
OrganizationUnit		M	S	Dubai Electronic Security Center (DESC)	PrintableString
CommonName		M	S	DESC Ethaq Plus Certification Authority	PrintableString
OrganizationIdentifier		M	S	VATAE-100027627700003	PrintableString
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime

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

	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[30]** Minutes	
subject		False	M			
	countryName		M	S	AE	PrintableString
	organizationUnitName		O	D	<optional organizational unit name> or as agreed during onboarding process	PrintableString
	organizationName		M	D	<entity meaningful name> or as agreed during onboarding process	PrintableString
	localityName		M/O	D	<Subject Locality>	PrintableString
	stateOrProvinceName		M/O	D	<Subject State or Province>	PrintableString
	commonName		M	D	<Individual end user name>	PrintableString
	surName		M	D	<Individual end user Surname>	PrintableString
	givenName		M	D	<Individual end user Given Name>	PrintableString
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key 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 Ethaq Plus CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	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		M	S	http://ca-repository.desc.gov.ae/certificate/EthaqPlusCA“C<n>”.crt	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
cRLDistributionPoints		False	O			

	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/EthaqPlus/EthaqPlusCA“C<n>”.crl	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
keyUsage		True	M			
	nonRepudiation		M	S	True	
ext-etsi-valassured-ST-certs		False	M	S	05 00	Exists only in short-lived certificates
Certificate Policy Properties						
QCStatements		False				
id-pe-pkiDisclosureStatements			M	S	en: https://ca-repository.desc.gov.ae/pds/DubaiPKI-PDS.pdf	
id-etsi-qcs-QcType			M	S		
	id-etsi-qct-esign		M	S		
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<For digital signature certificates (NCP+, formerly “high assurance”)[7], OID value will be 2.16.784.1.2.2.100.1.2.2.1.10> <For digital signature certificates (LCP, formerly “moderate assurance”)[8], OID value will be 2.16.784.1.2.2.100.1.2.2.1.11>	

7.1.10.2 Subscriber's signing certificate (UAE-QCP-n, UAE-QCP-n-qscd) ASN1 description

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE[9]	O/M[10]	CO[11]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA

[7] Certificates previously categorized as 'high assurance' are now labeled as NCP+ to align with [TDRA Resolution No. (51)]. For consistency, references to 'high assurance' in historical documents or communications correspond to NCP+ in this CPS.
[8] Certificates previously categorized as 'moderate assurance' are now labeled as LCP to align with [TDRA Resolution No. (51)]. For consistency, references to moderate assurance' in historical documents or communications correspond to LCP in this CPS.
[9] CE = Critical Extension.
[10] O/M: O = Optional, M = Mandatory.
[11] CO = Content: S = Static, D = Dynamic

	signatureValue		M	D	Ethaq Plus CA Signature.	CA signature value
TBSCertificate						
Version		False				
			M	S	2	Version 3
SerialNumber		False				
	CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature		False	M			
	algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
issuer		False	M			
	CountryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	OrganizationName		M	S	UAE Government	PrintableString
	OrganizationUnit		M	S	Dubai Electronic Security Center (DESC)	PrintableString
	CommonName		M	S	DESC Ethaq Plus Certification Authority	PrintableString
	OrganizationIdentifier		M	S	VATAE-100027627700003	PrintableString
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[30]** Minutes	
subject		False	M			
	countryName		M	S	AE	PrintableString
	organizationUnitName		O	D	<optional organizational unit name> or as agreed during onboarding process	PrintableString
	organizationName		M	D	<entity meaningful name> or as agreed during onboarding process	PrintableString
	localityName		M/O	D	Subject Locality	PrintableString
	stateOrProvinceName		M/O	D	Subject State or Province	PrintableString
	commonName		M	D	<Individual end user name>	PrintableString
	surName		M	D	<Individual end user Surname>	PrintableString
	givenName		M	D	<Individual end user Given Name>	PrintableString
	SERIALNUMBER		O	D	<Identifier for each individual>	PrintableString
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key 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 Ethaq Plus CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess	False	M			
AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
AccessMethod		M	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		M	S	http://ca-repository.desc.gov.ae/certificate/EthaqPlusCA“C<n>”.crt	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
cRLDistributionPoints	False	O			
distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/EthaqPlus/EthaqPlusCA“C<n>”.crl	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
Subject Properties					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties					
keyUsage	True	M			
nonRepudiation		M	S	True	
ext-etsi-valassured-ST-certs	False	M	S	05 00	Exists only in short-lived certificates
Certificate Policy Properties					
QCStatements	False				
id-etsi-qcs-QcCompliance		M	S		
id-pe-pkiDisclosureStatements		M	S	en: https://ca-repository.desc.gov.ae/pds/DubaiPKI-PDS.pdf	
id-etsi-qcs-QcType		M	S		
id-etsi-qct-esign		M	S		
id-etsi-qcs-QcSSCD		M	S		Present only for UAE-QCP-n-qscd certificates
id-etsi-qcs-QcCClegislation		M	S		

	CountryName		M	S	AE	PrintableString
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<For Qualified certificates for electronic signatures, requiring UAE-QSCD (UAE-QCP-n-qscd), OID value will be 2.16.784.1.2.2.100.1.2.3.1.1.3> <For Qualified certificates for electronic signatures, doesn't require UAE-QSCD (UAE-QCP-n), OID value will be 2.16.784.1.2.2.100.1.2.3.1.2.3>	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<For UAEQCP-n: OID value will be 2.16.784.1.1.8.1.1> <For UAE-QCP-n-qscd: OID value will be 2.16.784.1.1.8.1.3>	

7.1.11 Certificates for legal persons

7.1.11.1 Subscriber's signing certificate (eSeal - NCP+) ASN1 description

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE[12]	O/M[13]	CO[14]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
signatureValue		M	D	Ethaq Plus CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	(1) OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M			
CountryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	UAE Government	PrintableString
OrganizationUnit		M	S	Dubai Electronic Security Center (DESC)	PrintableString
CommonName		M	S	DESC Ethaq Plus Certification Authority	PrintableString
OrganizationIdentifier		M	S	VATAE-100027627700003	PrintableString
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + not more than **[60]** Months	
subject	False	M			
countryName		M	S	AE	Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

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

	organizationUnitName		O	D	<optional organizational unit name within the entity>	PrintableString
	organizationName		M	D	<entity meaningful name>	PrintableString
	organizationIdentifier		O	D	<entity Tax Registration Number (TRN) in the below format : VATAE-[TRN] >	PrintableString
	localityName		M/O	D	<Subject Locality>	PrintableString
	stateOrProvinceName		M/O	D	<Subject State or Province>	PrintableString
	commonName		M	D	<Entity Service Name as agreed during subscriber registration process >	PrintableString
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key 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 Ethaq Plus CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	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		M	S	http://ca-repository.desc.gov.ae/certificate/EthaqPlusCA“C<n>”.crt	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/ EthaqPlus/ EthaqPlusCA“C<n>”.crl	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
Subject Properties						

subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
Certificate Policy Properties					
QCStatements	False				
id-pe-pkiDisclosureStatements		M	S	en: https://ca-repository.desc.gov.ae/pds/DubaiPKI-PDS.pdf	
id-etsi-qcs-QcType		M	S		
id-etsi-qct-eseal		M	S		
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.5	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.2.3	

7.1.11.2 Subscriber's signing certificate (eSeal - UAE-QCP-l, UAE-QCP-l-qscd) ASN1 description

This is the complete ASN1 description of the certificate associated to the signing key of the subscriber.

Field	CE[15]	O/M[16]	CO[17]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
signatureValue		M	D	Ethaq Plus CA Signature.	CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
issuer	False	M			
CountryName		M	S	AE	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	UAE Government	PrintableString
OrganizationUnit		M	S	Dubai Electronic Security Center (DESC)	PrintableString
CommonName		M	S	DESC Ethaq Plus Certification Authority	PrintableString

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

	OrganizationIdentifier		M	S	VATAE-100027627700003	PrintableString
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[60]** Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	<optional organizational unit name within the entity>	PrintableString
	organizationName		M	D	<entity meaningful name>	PrintableString
	organizationIdentifier		O	D	<entity Tax Registration Number (TRN) in the below format : VATAE-[TRN] >	PrintableString
	localityName		M/O	D	<Subject Locality>	PrintableString
	stateOrProvinceName		M/O	D	<Subject State or Province>	PrintableString
	commonName		M	D	<Entity Service Name as agreed during subscriber registration process >	PrintableString
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key 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 Ethaq Plus CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	S	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	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		M	S	http://ca-repository.desc.gov.ae/cer	“C<n>” is added upon the CA key change over (as

					tificate/EthaqPlusCA“C<n>”.crt	specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/ EthaqPlus/ EthaqPlusCA”C<n>”.crl	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
Certificate Policy Properties						
QCStatements		False				
id-etsi-qcs-QcCompliance			M	S		
id-pe-pkiDisclosureStatements			M	S	en: https://ca-repository.desc.gov.ae/pds/DubaiPKI-PDS.pdf	
id-etsi-qcs-QcType			M	S		
	id-etsi-qct-eseal		M	S		
id-etsi-qcs-QcSSCD			M	S		Present only for UAE-QCP-l-qscd certificates
id-etsi-qcs-QcCClegislation			M	S		
	CountryName		M	S	AE	PrintableString
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<For Qualified certificates for eSeal signatures, requiring UAE-QSCD (UAE-QCP-l-qscd): OID value will be 2.16.784.1.2.2.100.1.2.3.2.1.2><For Qualified certificates for eSeal signatures, doesn’t require UAE-QSCD (UAE-QCP-l): OID value will be 2.16.784.1.2.2.100.1.2.3.2.2.2>	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	<For UAEQCP-l: OID value will be 2.16.784.1.1.8.1.2>	

					<For UAE-QCP-l-qscd: OID value will be 2.16.784.1.1.8.1.4>	

7.1.12 LRA certificate ASN1 description

This is the complete ASN1 description of the certificate associated to the authentication key of the subscriber.

Field		CE[18]	O/M[19]	CO[20]	Value	Comment
Certificate			M			
TBSCertificate			M			
Signature		False	M			
	algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
	signatureValue		M	D	Ethaq Plus CA Signature.	CA signature value
TBSCertificate						
Version		False				
			M	S	2	Version 3
SerialNumber		False				
	CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature		False	M			
	algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
issuer		False	M			
	CountryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	OrganizationName		M	S	UAE Government	PrintableString
	OrganizationUnit		M	S	Dubai Electronic Security Center (DESC)	PrintableString
	CommonName		M	S	DESC Ethaq Plus Certification Authority	PrintableString
	OrganizationIdentifier		M	S	VATAE-100027627700003	PrintableString
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[48]** Months	
subject		False	M			
	countryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”.

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

						PrintableString, size 2 (rfc5280)
	organizationUnitName		O	D	<optional organizational unit name within the RA entity>	PrintableString
	organizationName		M	D	<LRA meaningful name>	PrintableString
	localityName		M/O	D	<LRA locality>	PrintableString
	stateOrProvinceName		M/O	D	<LRA State or Province>	PrintableString
	commonName		M	D	<LRA Service Name as agreed during LRA onboarding process >	PrintableString
subjectPublicKeyInfo		False	M			
	algorithm		M	D	RSA/ECDSA	
	subjectPublicKey		M	D	Public Key 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 Ethaq Plus CA public key	When this extension is used this field MUST be supported as a minimum
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	D	http://ca-services.desc.gov.ae/adss/ocsp	OCSP responder URL
	AccessMethod		M	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		M	S	http://ca-repository.desc.gov.ae/certificate/EthaqPlusCA“C<n>”.crt	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
cRLDistributionPoints		False	O			
	distributionPoint		M	D	http://ca-repository.desc.gov.ae/CRL/EthaqPlus/EthaqPlusCA”C<n>”.crl	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	

Key Usage Properties						
keyUsage		True	M			
	digitalSignature		M	S	True	
Extended Key Usage Properties						
extKeyUsage		False	M			
	clientAuth		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.2.3.6	

7.2 CRL profile

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 CRLNumber (a sequential number incremented with each new CRL produced). Please refer to section 7.2.3 below for the other supported extension in the CRLs issued by the Ethaq Plus CA.

7.2.3 CRL ASN1 description

This is the complete ASN1 description of the CRL certificate.

Field	CE[21]	CO[22]	Value	Comment
CertificateList				
TBSCertificate				
Signature	False			
algorithm		S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
signatureValue		D	Ethaq Plus CA Signature.	CA signature value
TbsCertList				
Version	False			
		S	2	V2
SerialNumber	False			
CertificateSerialNumber		F		At least 64 bits of entropy Validated on duplicates.
signature	False			
algorithm		S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
issuer	False	S		
CountryName		S	AE	PrintableString
OrganizationName		S	UAE Government	PrintableString
OrganizationUnit		S	Dubai Electronic Security Center (DESC)	PrintableString
CommonName		S	DESC Corporate Certification Authority	PrintableString
OrganizationIdentifier		S	VATAE-100027627700003	PrintableString
Validity	False			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		D	CRL generation date/time	
nextUpdate		D	CRL generation date/time + 3 days	
revokedCertificates				
Certificate				

[21] CE = Critical Extension.
[22] CO = Content: S = Static, D = Dynamic

	CertificateSerial		D	Serial of the revoked certificate	
	revocationDate		D	UTC Time of revocation (Optional)	
crlExtensions					
authorityKeyIdentifier		False		This MUST be the same value as the subject Key Identifier field in the CRL Issuer's certificate. Non-critical <subject key identifier CA>	SHA-1 Hash of the Ethaq Plus CA public key
crlNumber		False			Sequential CRL number
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>	
authorityInfoAccess		False	S		
	AccessMethod		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		S	http://ca-repository.desc.gov.ae/certificate/EthaqPlusCA"C<n>".crt	"C<n>" is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over.

7.3 OCSP profile

7.3.1 Version number(s)

The OCSP responder issues OCSP responses of version 1.

7.3.2 OCSP extensions

No stipulation – this section intentionally left blank.

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[23]	O/M[24]	CO[25]	Value	Comment
Certificate		M			
TBSCertificate		M			
Signature	False	M			
algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
signatureValue		M	D	Ethaq Plus CA Signature.	CA signature value
TBSCertificate					

[23] CE = Critical Extension.
[24] O/M: O = Optional, M = Mandatory.
[25] CO = Content: S = Static, D = Dynamic

Version		False				
			M	S	2	Version 3
SerialNumber		False				
	CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature		False	M			
	algorithm		M	S	OID = 1.2.840.10045.4.3.3	SHA-384 with ECDSA
issuer		False	M	S		
	CountryName		M	S	AE	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	OrganizationName		M	S	UAE Government	PrintableString
	OrganizationUnit		M	S	Dubai Electronic Security Center (DESC)	PrintableString
	CommonName		M	S	DESC Ethaq Plus Certification Authority	PrintableString
	OrganizationIdentifier		M	S	VATAE-100027627700003	PrintableString
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + not more than **[3]** Months	
subject		False	M			
	countryName		M	S	AE	Will be encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
	commonName		M	S	Ethaq Plus Certification Authority OCSP “C<n>”	“C<n>” is added upon the CA key change over (as specified in section 6.3.2) where <n> is an incremental number starting from 2 and increasing after each CA key change over
	organizationName		M	S	DESC	
	localityName		M	S	Dubai	
subjectPublicKeyInfo		False	M			
	algorithm		M	S	RSA	
	subjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	M			
	KeyIdentifier		M	S	SHA-1 Hash of the Ethaq Plus CA public key	When this extension is used, this field MUST be supported at minimum
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
Key Usage		True	M			

	digitalSignature		M	S	True	
	nonRepudiation		M	S	True	
extKeyUsage		False	M			
	id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck		False	M	S	05 00	
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	2.16.784.1.2.2.100.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	D	URL location of this CPS	

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessments

DESC undergoes an external Surveillance Audit on an annual basis to ensure continuous conformity with ETSI EN 319 411-1 and ETSI EN 319 411-2. Furthermore, a full Conformity Assessment is conducted on a biennial basis to ensure compliance with the UAE Trust Services Framework ([Law (46) 2021], its Executive Regulations, and applicable TDRA resolutions).

DESC accepts these auditing requirements and commits to making the relevant audit attestation letters publicly available no later than three months after the conclusion of the audit period. The Dubai PKI PA evaluates the audit results prior to formal acceptance and continued implementation.

8.2 Identity and Qualifications of the Assessor

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

These audits will be performed by qualified auditors that fulfil the following requirements:

- Independence from the subject of the audit
- Ability to conduct an audit that addresses criteria specified in an eligible Audit as stipulated in section 8 of this document
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Qualified ETSI auditor, and approved by TDRA
- 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 one million US dollars in coverage.

8.3 Assessor’s Relationship to Assessed Party

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

8.4 Topics Covered by Assessment

The audit is conducted in conformity with the audit schemes specified in Section 1.0 that establish the requirements for this assessment..

8.5 Actions Taken as a Result of Deficiency

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

8.6 Communication of Results

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

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

9. Other Business and Legal Matters

Certain Legal conditions apply to the issuance of certificates issued by the Ethaq Plus 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 Ethaq Plus CA,
- Correspondence between the subscribers and DESC RA during the certificate management processing (including the collected subscribers data),
- Contractual agreements between DESC and its suppliers,
- The Dubai PKI internal documentation (technical documentation, operational processes, ….).

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

9.4 Privacy of Personal Information

9.4.1 Privacy plan

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

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

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

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

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

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

- The communications link between the Ethaq Plus CA and the RA/LRA.
- 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 Ethaq Plus CA digital certificates and any other publication whatsoever originating from the Ethaq Plus 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 Ethaq Plus CA has complied with its CPS in issuing and managing the Certificate.
The Certificate Warranties specifically include, but are not limited to, the following:

- **Authorization for Certificate:** That, at the time of issuance, the Ethaq Plus 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 Ethaq Plus CA

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

II. followed the procedure when issuing the Certificate, and

III. accurately described the procedure in this CPS.

- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the Ethaq Plus CA

  I. implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2,

  II. followed the procedure when issuing the Certificate,

  III. accurately described the procedure in this CPS.

- **Subscriber Agreement:** That, if the Ethaq Plus 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 Ethaq Plus 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 Ethaq Plus 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 Ethaq Plus 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 Ethaq Plus CA,

- **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token),
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy,
- **Use of Certificate:** When TLS server certificates are requested, an obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use,
- **Reporting and Revocation:** An obligation and warranty to:
    - promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
    - promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness:** An obligation to respond to DESC's instructions concerning Key Compromise or Certificate misuse within a specified time period**.**
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that DESC is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CPS.

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under the Ethaq Plus 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,
- For a Certificates to be relied upon as a Qualified Certificates (UAE-QCP-l-qscd, UAE-QCP-n-qscd, UAE-QCP-l and UAE-QCP-n), Relying Parties are explicitly informed that the Trust Anchor (this CA certificate or its superior Root) must be validated against the UAE Trusted List. Relying Parties must verify that the Trust Anchor is included in the UAE Trusted List and that its status is marked as 'Accredited' or 'Granted' for the specific service type relevant to the Certificate being relied upon,
- 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 Ethaq Plus 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 Ethaq Plus 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 Ethaq Plus CA repository, the newer version becomes effective. The older versions of this document are also archived on the Ethaq Plus CA repository.

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances Under Which OID Must be Changed

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

9.13 Dispute Resolution Procedures

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

The present CPS and provision of Ethaq Plus 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

If any provision of this CPS is determined to be invalid or unenforceable, the other sections shall remain in effect until this CPS is updated.

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.