Dubai Electronic Security Center

Dubai PKI

PKI Disclosure Statement

Title	PKI Disclosure Statement
Classification	PUBLIC
File Name	DubaiPKI-PKIDisclosureStatement_v1.0
Created on	25 April 2026
Revision	1.0
Modified on	

Document History

Date	Revision	Author(s)	Summary
25 April 2026	1.0	Mohamed Khalifa	First document release

Table of Contents

1. Introduction

1.1 Overview on the Dubai PKI

The "Dubai PKI" uses standard PKI technologies, policies and operating procedures and application interfaces. The Dubai PKI comprises the Dubai PKI Root CA that is the trust anchor of this PKI, which comes at the first level of the PKI hierarchy. The Dubai PKI also comprises multiple Subordinate Certification Authorities (CAs), hereinafter, DESC Subordinate CAs or Issuing 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.

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

CAs belonging to other entities come at the second level of the Dubai PKI hierarchy, being signed by the Dubai PKI Root CA. These issuing CAs will be directly signed by the Dubai PKI Root CA, which makes them subordinate CAs owned by the corresponding government or private sector entity but

operated by DESC. Policies and procedures of these Subordinate CAs must follow and be in full compliance with Dubai PKI Root CA CP/CPS.

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

1.2 Purpose

This PKI Disclosure Statement (PDS) applies to certificates issued by the Dubai PKI in accordance with the UAE legal framework for Trust Services, which consists of the following:

- 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 purpose of this document is to summarize the key points related to the provisioning of the certificates issued in accordance with UAE legal framework for Trust Services for the benefit of Subscribers and Relying Parties.

This document does not replace the applicable agreements and CPS (refer to section 8 “Applicable Agreements, CPS/CP”). Any terms used but not defined herein shall have the meaning ascribed to them in the CPS.

1.3 Definitions, acronyms and references

1.3.1 Definitions

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate is issued, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request. In the context of this CPS, the applicants are Government entities subscribing to the Corporate CA services.

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 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.

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

Intellectual Property Rights: means any and all now known or hereafter existing rights associated with intangible property, including, but not limited to, registered and unregistered, trademarks, trade dress, trade names, corporate names, logos, inventions, patents, patent applications, software, know-how and all other intellectual property and proprietary rights (of every kind and nature throughout the universe and however designated).

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

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.

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.

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.

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.

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.

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.

Services: mean, collectively, the certification service and any collateral product, benefit, or utility that DESC makes available to subscribers and relying parties.

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.

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.

1.3.2 Acronyms

CA — Certification Authority

CP — Certificate Policy

CPS — Certification Practice Statement

CRL — Certificate Revocation List

HSM — Hardware Security Module

HTTP — Hyper Text Transfer Protocol

DESC — Dubai Electronics Security Center

OID — Object Identifier

OCSP — Online Certificate Status Protocol

PA — Policy Authority of Dubai PKI

PKI — Public Key Infrastructure

RA — Registration Authority

TDRA — Telecommunications and Digital Government Regulatory Authority

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

1.3.3 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. Contact information

The Dubai PKI Policy Authority can be contacted at the following address:

Dubai PKI Policy Authority:

Dubai Electronic Security Center

PO Box 36996, Dubai, UAE

Phone +97144150400

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.

3. Certificate Type, Validation Procedures and Usages

The following certificate types are issued by the Dubai PKI to Subscribers in accordance with the conditions and requirements published in the Dubai PKI repository. The tables below are organized by the respective issuing CA.

Corporate CA

OID	Certificate type	Description and Usage
2.16.784.1.2.2.100.1.2.2.1.3	Digital signature certificates (NCP+, formerly “high assurance”)	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.
2.16.784.1.2.2.100.1.2.2.1.4	Digital signature certificates (LCP, formerly “moderate assurance”)	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.
2.16.784.1.2.2.100.1.2.2.1.7	Visitors digital signature certificates (NCP+, formerly “high assurance”)	Certificates issued to UAE visitors and used to create **Advanced Electronic Signatures** in accordance with Article

		(19) of [Law (46) 2021], based on the applicable identity verification procedures.
2.16.784.1.2.2.100.1.2.2.1.8	Visitors digital signature certificates (LCP, formerly "moderate assurance")	Certificates issued to UAE visitors and used to create **Advanced Electronic Signatures** in accordance with Article (19) of [Law (46) 2021], based on the applicable identity verification procedures.
2.16.784.1.2.2.100.1.2.2.2.1	eSeal certificates (NCP+, formerly "high assurance")	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.
2.16.784.1.2.2.100.1.2.3.1.1.1	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).
2.16.784.1.2.2.100.1.2.3.1.1.2	Visitors Qualified certificates for electronic signatures, requiring UAE-QSCD (UAE-QCP-n-qscd)	Qualified certificates issued to UAE visitors 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 UAE-QSCD.
2.16.784.1.2.2.100.1.2.3.1.2.1	Qualified certificates for electronic signatures, doesn't require UAE-QSCD (UAE-QCP-n)	Qualified certificates for electronic signatures used to create **Advanced Electronic Signatures** in accordance with Article (19) of [Law (46) 2021], where a UAE-QSCD is not required[1].
2.16.784.1.2.2.100.1.2.3.1.2.2	Visitors Qualified certificates for electronic signatures, doesn't require UAE-QSCD (UAE-QCP-n)	Qualified certificates issued to UAE visitors and used to create **Advanced Electronic Signatures** in accordance with Article (19) of [Law (46) 2021].
2.16.784.1.2.2.100.1.2.3.2.1.1	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].
2.16.784.1.2.2.100.1.2.3.2.2.1	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].

Timestamping CA

[1] The qualification status of a certificate under UAE law is determined by the applicable Trust Services Framework requirements and does not necessarily mandate the use of a QSCD in all cases

OID	Certificate Type	Description and Usage
2.16.784.1.2.2.100.1.3.1.1	Time stamping certificates	Certificates intended for the Dubai PKI TSA (Time Stamping Authority)

Ethaq Plus CA

OID	Certificate type	Description and Usage
2.16.784.1.2.2.100.1.2.2.1.10	Short-lived, Digital signature certificates (NCP+, formerly “high assurance”)	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”)	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”)	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.
2.16.784.1.2.2.100.1.2.3.1.1.3	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 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].

The issuing CAs' certificates are published at the Dubai PKI repository: https://ca-repository.desc.gov.ae/.

The validity of the above mentioned certificates can be checked through OCSP (Online Certificate Status Protocol) services, and the CRL (Certificate Revocation List) specified in the AIA and CDP extensions respectively.

4. Reliance limits

The usage of issued certificates must comply to that described in the Certificate Policies (CP) and Practice Statements (CPS) published in the Dubai PKI repository: https://ca-repository.desc.gov.ae/.

The Dubai PKI issues both qualified and non-qualified certificates in accordance with the UAE legal framework for Trust Services, and such certificates may only be used as specified in the applicable CPS.

Certificate subscribers are properly identified by the unique name (distinguished name) of the certificate.

For further information on the limitations of liability, refer to section 9.8 of the applicable CPS.

5. Subscriber's obligations

The usage of the private key associated to the certificate public key is only allowed when the subscriber agrees and accepts the subscriber agreement.

The certificate and keys must be used according to the subscriber agreement.

Subscribers use their private key only for appropriate purposes that are not prohibited, or otherwise restricted by the applicable CPS and always for lawful purposes.

Subscribers must protect their private key from unauthorized use and shall discontinue use of the private key following expiration or revocation of the certificate.

Subscriber must request the revocation of a particular certificate, as soon as there is knowledge or suspicion of the private key compromise or any other act that recommends this action.

6. Certificate Status Checking Obligations of Relying Parties

Before any act of trust, relying parties should verify:

- The appropriateness of the use of the certificate for any purpose, and determine that the certificate is in fact used for appropriate purposes that are not prohibited, or otherwise restricted by the applicable CPS. DESC is not responsible for assessing the proper adequacy of the certificate.
- If the certificate is being used as specified in the "KeyUsage" (eg.: if the digital signature nor non-repudiation is enabled, then the certificate cannot be trusted to validate the signature of the subscriber).
- The status of the certificate and all the CA certification chain that issued the certificate. If any of the certificates in the certification chain is revoked, the relying party is solely responsible for assessing whether it is reasonable the trust in a digital signature, performed in prior to the revocation date. Any reliance on a signature created prior to revocation is solely the responsibility of the relying party.
- Be aware and understand the use and functionality provided by public key cryptography and certificates.
- Read and understand the terms and conditions outlined in the applicable CP and CPS.

7. Limitation of liability

DESC is not responsible for the improper use of certificates.

DESC is not responsible for any use of certificates not listed in the applicable CPS.

The use of issued certificates and the protection of private/public key is the sole responsibility of its owner.

See Sections 9.6 and 9.8 of the applicable CPS.

8. Applicable agreements, CPS/CP

Applicable agreements, Certification Policies and Certification Practice Statements and are published at the Dubai PKI repository: https://ca-repository.desc.gov.ae/.

9. Privacy policy

Subscriber information included in their certificates is not published and is processed according to the applicable CP and CPS.

10. Refund policy

No refunds are applicable for any fees charged by DESC.

11. Applicable law

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

All disputes associated with the provisions of this document and the Dubai PKI services, shall be first addressed by the Dubai PKI PA. If mediation by the Dubai PKI PA is not successful, then the dispute will be escalated to the relevant courts of Dubai.

12. Audits and security normative

The Dubai PKI services are subject to conformity assessment against the following applicable requirements:

- The UAE legal framework for Trust Services, consists of:
    - 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;
    - Provision of qualified time stamps.
- [ETSI 319 411-1]
- [ETSI 319 411-2]
- [ETSI 319 421]

Note: *References to ETSI standards, including ETSI EN 319 411-1, ETSI EN 319 411-2, and ETSI EN 319 421, 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.

The conformity assessment is performed by an independent, qualified, and accredited auditor, in accordance with the applicable audit scheme.