



Certi-Trust – AUDIT ATTESTATION LETTER (AAL)

Dubai Electronic Security Center (DESC)



Confidence in the Digital Era



1. AUDIT ATTESTATION LETTER (AAL)

1.1. ETSI CONFORMITY ASSESSMENT

Conformity Assessment Body (CAB): Certi-Trust France

Accreditation Body: COFRAC

Accreditation Number: 5-0597

Trust Service Provider (TSP): Dubai Electronic Security Center (DESC)

Country: United Arab Emirates

Assessment Type: ETSI Conformity Assessment

Audit Period: 02 February 2026 – 01 May 2026

Audit Report Date: 10 May 2026

2. AUDIT ATTESTATION

Certi-Trust France, acting as an accredited Conformity Assessment Body (CAB), has performed an independent conformity assessment of the trust services and Public Key Infrastructure (PKI) operated by the Dubai Electronic Security Center (DESC).

The assessment was conducted in accordance with ETSI EN 319 403-1 and covered the requirements specified in:

- ETSI EN 319 401: General Policy Requirements for Trust Service Providers;
- ETSI EN 319 411-1: Policy and Security Requirements for Trust Service Providers Issuing Certificates.

3. AUDIT OPINION

Based on the assessment procedures performed and the evidence obtained during the conformity assessment activities, Certi-Trust France concludes that:

Dubai Electronic Security Center (DESC) complies, in all material respects, with the requirements of ETSI EN 319 401 and ETSI EN 319 411-1 for the services and systems included within the scope of the assessment.

Accordingly, Certi-Trust France expresses an:

3.1. UNQUALIFIED OPINION

for the audit period identified above.

4. SCOPE OF ASSESSMENT

The assessment covered the governance, management and operation of the certification services operated by DESC, including:

- ❖ Trust Service governance;
- ❖ Information security management;
- ❖ Certification Authority operations;
- ❖ Certificate lifecycle management;
- ❖ Cryptographic key management;
- ❖ Hardware Security Module (HSM) administration;
- ❖ Trusted role management;
- ❖ Access control mechanisms;
- ❖ Logging and monitoring controls;
- ❖ Business continuity and disaster recovery arrangements;
- ❖ Revocation services and OCSP infrastructure.

The assessment also considered evidence associated with the Root CA Certificate Re-Issuance whose objective was the technical rectification of ASN.1 DER encoding non-conformities to ensure compliance with RFC 5480 and ETSI TS 119 312 while maintaining the existing cryptographic key material.

5. CERTIFICATES INCLUDED IN SCOPE

See appendix A: PKI Hierarchy in scope of the audit.

6. ACCREDITATION STATEMENT

Certi-Trust France is accredited according to ISO/IEC 17065 by the Comité Français d'Accréditation (COFRAC) under accreditation number 5-0597.

The accreditation scope includes conformity assessment activities relating to Trust Service Providers and applicable ETSI standards.

The accreditation was valid throughout the audit period.

7. INTENDED USE

This Audit Attestation Letter is issued for the purpose of:

- ❖ Supervisory Authority review;
- ❖ Regulatory compliance demonstration;
- ❖ Trust Service Provider conformity evidence;
- ❖ Common CA Database (CCADB) reporting;
- ❖ Root Store Program compliance activities;
- ❖ Public disclosure requirements.

8. RESTRICTIONS

This Audit Attestation Letter shall be read in conjunction with the corresponding Conformity Assessment Report issued by Certi-Trust France.

The opinion expressed herein is limited to the scope and period identified in this letter and does not constitute a guarantee of future compliance.

9. CONFORMITY ASSESSMENT BODY

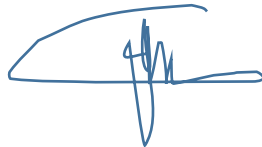
Certi-Trust France

Lead Auditor:

Dr. Tayeb SADIKI

10. SIGNATURE

Dr. Tayeb SADIKI



Lead Auditor

Certi-Trust France

11. DATE OF ISSUE

10 May 2026

12. CAB CONTACT INFORMATION

Certi-Trust France

Address:
33 Avenue de Wagram
75017 Paris
France

Email:
france@certi-trust.com

Website:
<https://www.certi-trust.com>

Appendix A: PKI Hierarchy in scope of the audit

CA#	Subject	Issuer	serialNumber	notBefore	NotAfter	SHA256 Fingerprint
1	CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	1FD880704BC71C38000000005A79686B	Feb 6 08:04:25 2018 GMT	Feb 6 08:34:25 2043 GMT	51A7ECB93ACB55FF0E34CD0ECFD1578978B37E9EDB82FD06F23F6CEC005B986D
1.1	CN=Corporate Certification Authority, O=UAE Government, C=AE	CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	8DF4DE0722E17E710000000005A796A5C	Apr 8 17:34:29 2022 GMT	Apr 8 18:04:29 2030 GMT	2A91EDC852564277BF19D82FB8255F3955A54EA3B87199C933B782152CB9262E

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.2.2.1.1	Certificates issued for encryption purposes (e.g., data and document confidentiality). These certificates are not issued as Trust Services or Qualified Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.2	Deprecated certificates previously issued for authentication purposes. These certificates are not Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.6	Certificates issued to support authentication of individuals. These certificates are not issued as Electronic Signature or Electronic Seal Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.3	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	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
2.16.784.1.2.2.100.1.2.2.1.5	Certificates issued for authentication of individuals on mobile devices (e.g., to establish trust in a personal smart device). These certificates are not issued as Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.7	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	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
2.16.784.1.2.2.100.1.2.2.1.9	Mobile authentication certificates issued to UAE visitors. These certificates are not issued as Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.2.1	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
2.16.784.1.2.2.100.1.2.2.3.4	Certificate used to sign verification responses generated by the signature verification service. This certificate supports a Trust Service as defined under Article (17) of [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.3.5	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]
2.16.784.1.2.2.100.1.2.1.1	OCSP

1.2	CN=Timestamping Certification Authority, O=UAE Government, C=AE	CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	7C463F5861EC2DB70000000005A796A9C	Jun 21 06:42:24 2022 GMT	Jun 21 07:12:24 2030 GMT	085442126B640E9FA4FB52293A3A63B4D969414A9F047C1E4B9B6F3761AC9E9D
-----	---	---	-----------------------------------	--------------------------	--------------------------	--

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.3.1.1	A certificate issued to a Timestamp Authority to use to timestamp data
2.16.784.1.2.2.100.1.2.1.3	OCSP

1.3	CN=Timestamping Certification Authority, O=UAE Government, C=AE	CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	3F7A3C956D73287E55715DCB30A177A6BCE3F954	Feb 27 07:39:34 2025 GMT	Feb 27 07:39:34 2033 GMT	269EE5A6DFA0184EE07F9FCB5AD6BF0C3AD541C1B0800B5B4F547B4E3FFB41C2
-----	---	---	--	--------------------------	--------------------------	--

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.3.1.1	A certificate issued to a Timestamp Authority to use to timestamp data
2.16.784.1.2.2.100.1.2.1.3	OCSP

1.4	CN=Ethaq Plus Certification Authority, O=UAE Government, C=AE	CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	1A238737BA99D0BE803D9D68BC1D79D13C1CCA7A	Apr 16 10:27:03 2025 GMT	Apr 16 10:27:03 2033 GMT	AE008ECF90DD26838078F70CD798806C0594F57921179612AD4512858B4CC47B
-----	---	---	--	--------------------------	--------------------------	--

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.2.2.1.10	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	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	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	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]
2.16.784.1.2.2.100.1.2.1.5	OCSF

2	OrganizationIdentifier = VATAE-10002762770000, CN = UAE Global Root CA G4 E2, OU = Dubai Electronic Security Center (DESC), O = UAE Government, C = AE	OrganizationIdentifier = VATAE-10002762770000, CN = UAE Global Root CA G4 E2, OU = Dubai Electronic Security Center (DESC), O = UAE Government, C = AE	401a6e75b2d9b7c05dcd47a44f5121cd	Jan 31 12:20:25 2026 GMT	Jan 31 12:20:25 2051 GMT	66ED1EF9A8248E8B137FC8F5F00E51E6443ED6E366D0FE52FF6702A91ED2B371
2.1	CN = DESC Corporate Certification Authority, OU = Dubai Electronic Security Center (DESC), O = UAE Government, OrganizationIdentifier = VATAE-100027627700003, C = AE	OrganizationIdentifier = VATAE-10002762770000, CN = UAE Global Root CA G4 E2, OU = Dubai Electronic Security Center (DESC), O = UAE Government, C = AE	5668ad01ea16c3c5d497c152497f4638	Apr 21 08:32:18 2026 GMT	Apr 21 08:32:18 2034 GMT	3512C66C89583D3D59C2DB70772A6110AD923F68CCD889ADA1AE52015BABBCDD

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.2.2.1.1	Certificates issued for encryption purposes (e.g., data and document confidentiality). These certificates are not issued as Trust Services or Qualified Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.2	Deprecated certificates previously issued for authentication purposes. These certificates are not Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.6	Certificates issued to support authentication of individuals. These certificates are not issued as Electronic Signature or Electronic Seal Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.1.3	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	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
2.16.784.1.2.2.100.1.2.2.1.5	Certificates issued for authentication of individuals on mobile devices (e.g., to establish trust in a personal smart device). These certificates are not issued as Trust Services under [Law (46) 2021]

2.16.784.1.2.2.100.1.2.2.1.7	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	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
2.16.784.1.2.2.100.1.2.2.1.9	Mobile authentication certificates issued to UAE visitors. These certificates are not issued as Trust Services under [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.2.1	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
2.16.784.1.2.2.100.1.2.2.3.4	Certificate used to sign verification responses generated by the signature verification service. This certificate supports a Trust Service as defined under Article (17) of [Law (46) 2021]
2.16.784.1.2.2.100.1.2.2.3.5	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]
2.16.784.1.2.2.100.1.2.3.1.1.1	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	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 used to create Advanced Electronic Signatures in accordance with Article (19) of [Law (46) 2021], where a UAE-QSCD is not required
2.16.784.1.2.2.100.1.2.3.1.2.2	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 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	Certificates used to create Advanced Electronic Seals for legal persons in accordance with Article (19) of [Law (46) 2021]
2.16.784.1.2.2.100.1.2.1.1	OCSF

2	CN = DESC Timestamping Certification Authority, OU = Dubai Electronic Security Center (DESC), O = UAE Government, OrganizationIdentifier = VATAE-100027627700003, C = AE	OrganizationIdentifier = VATAE-10002762770000, CN = UAE Global Root CA G4 E2, OU = Dubai Electronic Security Center (DESC), O = UAE Government, C = AE	2c6849ed64749868721916145b2e dda8	Apr 21 08:49:03 2026 GMT	Apr 21 08:49:03 2034 GMT	DB3849F963CE5B31CEFD06DBD D40AA553C9A19199CEB2891CD 22914D18F884B0
---	--	--	-----------------------------------	--------------------------	--------------------------	--

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.3.1.1	A certificate issued to a Timestamp Authority to use to timestamp data
2.16.784.1.2.2.100.1.2.1.3	OCSF

2.3	CN = DESC Ethaq Plus Certification Authority, OU = Dubai Electronic Security Center (DESC), O = UAE Government, OrganizationIdentifier = VATAE-100027627700003, C = AE	OrganizationIdentifier = VATAE-10002762770000, CN = UAE Global Root CA G4 E2, OU = Dubai Electronic Security Center (DESC), O = UAE Government, C = AE	25cf61c57f1fd4ec5630d0000fda9200	Apr 21 08:41:18 2026 GMT	Apr 21 08:41:18 2034 GMT	563CE5C1C8E4CE5A555F66935CA3BA499B29BE76E48F821100CFF2B0B 265F9BB
-----	--	--	----------------------------------	--------------------------	--------------------------	---

End-entity: PolicyIdentifier	Name and type
2.16.784.1.2.2.100.1.2.2.1.10	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	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	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	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	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	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	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	Certificates used to create Advanced Electronic Seals for legal persons in accordance with Article (19) of [Law (46) 2021]
2.16.784.1.2.2.100.1.2.1.5	OCSF