Standard Audit Attestation for

DUBAI ELECTRONIC SECURITY CENTER (DESC)

Reference: CT-FR-DESC-2026-AAL-002

Paris, 2026/05/15

To whom it may concern,

This is to confirm that Certi-Trust France has audited the CAs of the DUBAI ELECTRONIC SERVICE CENTER (DESC) without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number CT-FR-DESC-2026-AAL-002 covers multiple Root-CAs and consists of 11 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Certi-Trust France
33 Avenue de Wagram
75017 Paris, France
E-Mail: audit@certi-trust.com
Phone: +33189294444

With best regards,

Tayeb SADIKI
Team Leader

Omar BENAICHA
Reviewer

This attestation is based on the template version 3.5 as of 2026-03-09, that was approved for use by ACAB'c.

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• Certi-Trust France, 33 Avenue WArgram 75017, Paris, France, registered under SIREN 828652974 • Accredited by COFRAC under registration 5-0597 rév. 14 [1] for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403 V2.2.2 (2015-08)” / “ETSI EN 319 403-1 V2.3.1 (2020-06)”. • Insurance Carrier (BRG section 8.2): Liberty Mutual Insurance Europe SE • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: 02 • Academic qualifications of team members: All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security. • Additional competences of team members: • All team members have knowledge of 1) audit principles, practices and techniques in the field of CA/TSP audits gained in a training course of at least five days; 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security; 3) the applicable standards, publicly available specifications and regulatory requirements for CA/TSPs and other relevant publicly available specifications including standards for IT product evaluation; and 4) the Conformity Assessment Body's processes. Furthermore, all team members have language skills appropriate for all organizational levels within the CA/TSP organization; note-taking, report-writing, presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic. • Professional training of team members: See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in: a) knowledge of the CA/TSP standards and other relevant publicly available specifications; b) understanding functioning of trust services and information security including network security issues; c) understanding of risk assessment and risk management from the business perspective; d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and

[1] https://tools.cofrac.fr/annexes/sect5/5-0597.pdf

f) knowledge of security policies and controls.

- Types of professional experience and practical audit experience:
  The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA/TSP auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.
- Additional qualification and experience Lead Auditor:
  On top of what is required for team members (see above), the Lead Auditor
  a) has acted as auditor in at least three complete TSP audits;
  b) has adequate knowledge and attributes to manage the audit process; and
  c) has the competence to communicate effectively, both orally and in writing.
- Special skills or qualifications employed throughout audit:
  None.
- Special Credentials, Designations, or Certifications:
  All members are qualified and registered assessors within the accredited CAB.
  Tayeb SADIKI: PhD in IT, ISO 19011, ISO 27001 Senior Lead Auditor, eIDAS v2, CEN/TS 18170, ISO14641, Prince 2, PMP
  René St-Germain: Msc in IT, MBA, Eidas v2, PSDC, CEN/TS 18170, ISO14641, ISO19011, ISO 27001 LA
- Auditors code of conduct incl. independence statement:
  Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.

Identification and qualification of the reviewer performing audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: 01
- The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA/TSP audits.

Identification of the CA / Trust Service Provider (TSP):	Dubai Electronic Security Center (DESC) 25 8B St – Al Qusais Industrial Area 1, Dubai, United Arab Emirates Dubai Electronic Security Center (DESC) was established and registered under Law No. 11 of 2014 (subsequently updated by Law No. 15 of 2024)

Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2026-04-25 to 2026-05-01
Point in time date:	none
Audit dates:	2026-01-12 to 2026-01-16 (remote) 2026-04-25 to 2026-05-01 (on site)
Audit location:	25 8B St – Al Qusais Industrial Area 1, Dubai, United Arab Emirates

Root 1: UAE Global Root CA G4 E2 (RSA 4096)

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.3.1 (2021-05) • ETSI EN 319 401 V3.3.1 (2024-06) • ETSI EN 319 421 V1.3.1 (2025-07) • ETSI EN 319 422 V1.1.1 (2016-03) CA Browser Forum Requirements: • Network and Certificate System Security Requirements, version 2.0.5 Other : • ETSI TS 119 312 V1.4.3 (2023-08) • UAE TDRA Trust Services Framework (Resolutions n° 51 and n° 53). For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ISO/IEC 17065:2012 – Requirements for accreditation of CABs

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Dubai PKI Root CA – Certification Policy and Certificate Practice Statement

Version	Release Date	Effective from	Effective until
Version 2.4	2026-04-25	2026-04-25	Current

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

6.1 Trust Service Practice Statement

The reviewed UAE PASS Terms of Use define general conditions for service usage but do not specify or reference the formal trust service policies and operational practices applicable to the provided trust services. In particular, no Trust Service Practice Statement (TSPS), Certificate Policy (CP), or Certification Practice Statement (CPS) was identified or made available as part of the reviewed documentation.

The documentation does not sufficiently define:

- the formal policies governing trust service operations,
- the operational practices applicable to certificate lifecycle management,
- the procedures for certificate issuance, validation, suspension, and revocation,
- nor the organizational roles and responsibilities related to trust service delivery.

Consequently, the TSP has not demonstrated that a complete and appropriate set of policies and practices has been formally specified in accordance with ETSI EN 319 401 REQ-6.1-01.

6.1 Trust Service Practice Statement

Based on the reviewed documentation, the UAE PASS Terms of Use provide only high-level user-facing conditions and do not constitute a formal statement of practices and procedures addressing the requirements of the applicable trust service policies.

In particular, the assessment identified the absence of:

a formalized and publicly available Trust Service Practice Statement (TSPS), CPS, or equivalent document,
documented procedures describing operational controls and trust service practices,
detailed procedures covering certificate lifecycle activities,
clearly defined responsibilities and governance arrangements,
and traceability between applicable trust service policy requirements and implemented operational practices.

As a result, the TSP has not demonstrated the existence of documented practices and procedures addressing all applicable trust service policy requirements, as required by ETSI EN 319 401 REQ-6.1-03.

7.2 Human Resources

On the organigram, the auditors and the system operators are the same persons. There are no statement in the documentation on the necessity to separate the 4 trusted roles to ensure conflict of interest. NC not major because we could observed that in reality, the roles are segregated even if not documented.

7.10 Collection of evidence

The document describes technical mechanisms for log storage and archival (e.g., centralized logging via VMware Aria and archival to Data Domain). However, a formalized and comprehensive archival process aligned with the applicable Certificate Practice Statements (CPS) and business practices is not clearly established.
Specifically, the procedure lacks:

- a clearly defined end-to-end archival workflow,
- controls ensuring completeness and integrity of archived records,
- defined roles and responsibilities for archival activities,
- and documented procedures for retrieval and verification of archived

Findings with regard to ETSI EN 319 411-1: None.

Findings with regard to ETSI EN 319 411-2: None.

All non-conformities have been closed before the issuance of this attestation.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=UAE Global Root CA G4 E2, O=UAE Government, C=AE	51A7ECB93ACB55FF0E34CD0ECFD1578978B37E9EDB82FD06F23F6CEC005B986D	ETSI EN 319 411-1 V1.5.1, NCP; ETSI EN 319 401 V3.1.1

Table 1: Root-CA 1 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Corporate Certification Authority, O=UAE Government, C=AE	2A91EDC852564277BF19D82FB8255F3955A54EA3B87199C933B782152CB9262E	ETSI EN 319 411-1 V1.5.1, NCP
CN=Timestamping Certification Authority, O=UAE Government, C=AE	085442126B640E9FA4FB52293A3A63B4D969414A9F047C1E4B9B6F3761AC9E9D	ETSI EN 319 411-1 V1.5.1, NCP
CN=Timestamping Certification Authority, O=UAE Government, C=AE	269EE5A6DFA0184EE07F9FCB5AD6BF0C3AD541C1B0800B5B4F547B4E3FFB41C2	ETSI EN 319 411-1 V1.5.1, NCP
CN=Ethaq Plus Certification Authority, O=UAE Government, C=AE	AE008ECF90DD26838078F70CD798806C0594F57921179612AD4512858B4CC47B	ETSI EN 319 411-1 V1.5.1, NCP

Table 2: Sub-CA’s issued by the Root-CA 1 or its Sub-CA’s in scope of the audit

Root 2: UAE Global Root CA G4 E2 (DESC-ECDSA P-384)

Standards considered:	European Standards: • ETSI EN 319 412-5 V2.5.1 (2025-06) • ETSI EN 319 411-2 V2.4.1 (2021-11) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Network and Certificate System Security Requirements, version 2.0.5 Other: • UAE TDRA Trust Services Framework (Resolutions n° 51 and n° 53). For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.2.2 (2015-08) • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.3.1 (2023-03) • ISO/IEC 17065:2012 – Requirements for accreditation of CABs

The audit was based on the following policy and practice statement documents of the CA / TSP:

- Dubai PKI Root CA – Certification Policy and Certificate Practice Statement

Version	Release Date	Effective from	Effective until
Version 2.4	2026-04-25	2026-04-25	Current

In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

6.1 Trust Service Practice Statement

The reviewed UAE PASS Terms of Use define general conditions for service usage but do not specify or reference the formal trust service policies and operational practices applicable to the provided trust services. In particular, no Trust Service Practice Statement (TSPS), Certificate Policy (CP), or Certification Practice Statement (CPS) was identified or made available as part of the reviewed documentation.

The documentation does not sufficiently define:

- the formal policies governing trust service operations,
- the operational practices applicable to certificate lifecycle management,
- the procedures for certificate issuance, validation, suspension, and revocation,
- nor the organizational roles and responsibilities related to trust service delivery.

Consequently, the TSP has not demonstrated that a complete and appropriate set of policies and practices has been formally specified in accordance with ETSI EN 319 401 REQ-6.1-01.

6.1 Trust Service Practice Statement

Based on the reviewed documentation, the UAE PASS Terms of Use provide only high-level user-facing conditions and do not constitute a formal statement of practices and procedures addressing the requirements of the applicable trust service policies.

In particular, the assessment identified the absence of a formalized and publicly available Trust Service Practice Statement (TSPS), CPS, or equivalent document, documented procedures describing operational controls and trust service practices, detailed procedures covering certificate lifecycle activities, clearly defined responsibilities and governance arrangements, and traceability between applicable trust service policy requirements and implemented operational practices.

As a result, the TSP has not demonstrated the existence of documented practices and procedures addressing all applicable trust service policy requirements, as required by ETSI EN 319 401 REQ-6.1-03.

7.2 Human Resources

On the organigram, the auditors and the system operators are the same persons. While we could observe that in practice, the roles are segregated, there are no statement in the documentation on the necessity to separate the 4 trusted roles to avoid conflict of interest as required by ETSI EN 319 401 REQ-7.2-14.

7.10 Collection of evidence

The document describes technical mechanisms for log storage and archival (e.g., centralized logging via VMware Aria and archival to Data Domain). However, a formalized and comprehensive archival process aligned with the applicable Certificate Practice Statements (CPS) and business practices is not clearly established as required by ETSI EN 319 401 clause 7.10.

Findings with regard to ETSI EN 319 411-1: None.

Findings with regard to ETSI EN 319 411-2: None.

All non-conformities have been closed before the issuance of this attestation.

To the best of our knowledge, no incidents have occurred within this Root-CA’s hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy
organizationIdentifier=VATAE-10002762770000, CN=UAE Global Root CA G4 E2, OU=Dubai Electronic Security Center (DESC), O=UAE Government, C=AE	66ED1EF9A8248E8B137FC8F5F00E51E6443ED6E366D0FE52FF6702A91ED2B371	ETSI EN 319 411-1 V1.5.1, NCP; ETSI EN 319 401 V3.1.1

Table 3: Root-CA 2 in scope of the audit

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this audit.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=DESC Corporate Certification Authority, OU=Dubai Electronic Security Center (DESC), O=UAE Government, organizationIdentifier=VATAE-100027627700003, C=AE	3512C66C89583D3D59C2DB70772A6110AD923F68CCD889ADA1AE52015BABBCDD	ETSI EN 319 411-1 V1.5.1, NCP
CN=DESC Timestamping Certification Authority, OU=Dubai Electronic Security Center (DESC), O=UAE Government, organizationIdentifier=VATAE-100027627700003, C=AE	DB3849F963CE5B31CEFD06DBDD40AA553C9A19199CEB2891CD22914D18F884B0	ETSI EN 319 411-1 V1.5.1, NCP
CN=DESC Ethaq Plus Certification Authority, OU=Dubai Electronic Security Center (DESC), O=UAE Government, organizationIdentifier=VATAE-100027627700003, C=AE	563CE5C1C8E4CE5A555F66935CA3BA499B29BE76E48F821100CFF2B0B265F9BB	ETSI EN 319 411-1 V1.5.1, NCP

Table 4: Sub-CA’s issued by the Root-CA 2 in scope of the audit

Key pairs without a corresponding certificate (“parked keys”)

Not applicable, this report doesn’t cover any private key for which no certificate were generated at the time of the audit.

Modifications record

Version	Issuing Date	Changes
Version 1	2026-05-15	Initial attestation

End of the audit attestation letter.