TLS BR Audit Attestation for

certSIGN

Reference: AAL_1612-377-v2-TLS-BR_LSTI

Saint-Malo, 28 Avril 2025

To whom it may concern,

This is to confirm that LSTI has audited the CAs of the certSIGN without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number AAL_1612-377-SA_LSTI covers multiple Root-CAs and consists of 7 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

LSTI Worldwide Limited
Clifton House – Fitzwilliam Street lower
Dublin 2, D02XT91
Ireland
E-Mail: Julien.bruant@lsti.eu
Phone: +353 876 748 511

With best regards,

CHRISTOPHE CELISSE
Directeur Technique

Christophe Celisse
Technical Director & Reviewer

Julien Bruant
Signature numérique de Julien Bruant ID
Date : 2025.05.12 13:18:19 +02'00'

Julien BRUANT
CEO

This attestation is based on the template version 3.3, 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
• LSTI Worldwide Limited, Clifton House – Fitzwilliam Street lower, D02XT91 Dublin 2 - Ireland, registered under LTD - Private Company Limited by Shares - RCS 582309 • Accredited by COFRAC under registration 5-0546 rév. 13[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): HISCOX SA • Third-party affiliate audit firms involved in the audit: None.
Identification and qualification of the audit team
• Number of team members: 2 • 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/sect5/5-0546.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.
- 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: 1.
- 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):	certSIGN - AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29, Bucharest

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:	2024-02-13 to 2025-02-12
Point in time date:	none, as audit was a period of time audit
Audit dates:	2024-01-27 to 2024-01-30 (on site) 2024-02-10 to 2024-02-11 (on site)
Audit location:	Site No1 – CA/RA – AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29, Bucharest Site No2 – DR – Constanta

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

- certSIGN ROOT CA G2, Version 2.25 January 15, 2025
- certSIGN Qualified CA, Version 2.43 15 January 2025
- certSIGN Public CA, Version 2.28, 15 January 2025
- certSIGN WEB CA for QWAC & EV Certificates, Version1.31, 15 January 2025
- certSIGN WEB CA for OV SSL Certificates, Version1.28, 15 January 2025
- certSIGN WEB CA for DV SSL Certificates, Version1.8, 15 January 2025

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

Findings with regard to ETSI EN 319 401:
None.

Findings with regard to ETSI EN 319 411-1:
6.1 Publication and repository responsibilities
[DIS-6.1-05] OID 1.3.6.1.4.1.25017.3.1.4.6 is not listed in OIDs list from certSIGN Web CA - Terms and conditions (https://www.certsign.ro/en/document/certsign-web-ca-terms-and-conditions/).

6.2 Identification and authentication
[RG-6.2.2-03A] In "Certification Practice Statement certSIGN Web CA for DV SSL Certificates" on chapter 3.2.2.1 Identity:
"Verify that the domain mentioned in the certificate is registered by the entity submitting the certificate application or by the one that authorized the use of the domain by the requesting entity according to CA/Browser Forum– cap 3.2.2.4.2 (Email, Fax, SMS, or Postal Mail to Domain Contact), cap. 3.2.2.4.4 (Constructed Email to Domain Contact) or 3.2.2.4.7 (DNS Change)"

6.9 Other provisions
[OVR-6.9.2-01C] On a set of OID (certificate profiles not yet delivered to customers), the certificates are issued for testing purposes in a manner that does not follow the normal registration process, and no reasonable assurance that these certificates cannot be used outside of the testing scope is currently given.

7.1 Certificate policy management
[OVR-7.1-02] On CPS "certSIGN Web CA for QWAC & EV Certificates", no element could be found to unambigously make the correct association of each policy identifier with each specific OID.

Findings with regard to Baseline Requirements v2.1.2:
7.1 Certificate Profile
[7.1.4.1/2] Each RelativeDistinguishedName, if present, is encoded within the RDNSequence in the order that it appears in Section 7.1.4.2.
On the test URL: https://testssl-expired-evcp.certsign.ro/ the certificate: "testssl-expired-evcp.certsign.ro.crt" doesn't respect this order.
Appear in BR Version 2.0.0 (11 April 2023)
- Certificate Profiles Update: “Adopted: 22-Apr-2023 / Effective: 15-Sep-2023 / Compliance: 2023-09-15”, and certificate issued on November 2023.

Root CA 1: certSIGN ROOT CA G2

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 • ETSI EN 319 411-1 V1.4.1 • ETSI EN 319 401 V2.2.1 CA Browser Forum Requirements: • Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.2 For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403 V2.3.1

Distinguished Name	SHA-256 fingerprint	Applied policy
OU=**certSIGN ROOT CA G2**,O=CERTSIGN SA,C=RO	65:7C:FE:2F:A7:3F:AA:38:46:25:71:F3:32:A2:36:3A:46:FC:E7:02:09:51:71:07:02:CD:FB:B6:EE:DA:33:05	ETSI EN 319 411-2 V2.5.1, all policies ETSI EN 319 411-1 V1.4.1, all policies ETSI EN 319 401 V2.2.1

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
ORG_ID=VATRO-18288250,CN=**certSIGN Web CA**,O=CERTSIGN SA,C=RO	F1:14:46:9F:B8:07:78:13:3A:1F:70:E4:D8:33:8E:DA:B9:7D:D4:2C:EB:8E:CC:01:CA:FB:70:D6:B8:7D:F1:1E	ETSI EN 319 411-1 V1.4.1, DVCP, OVCP

Table 2: Sub-CA's issued by the Root-CA 3 or its Sub-CA's in scope of the audit

Modifications record

Version	Issuing Date	Changes
Version 1	2025-04-17	Initial attestation
Version 2	2025-04-28	Corrected version

End of the audit attestation letter.