TLS EV Audit Attestation for

Certigna

Reference: AAL_23-1747/1787-v1-TLS-EV_LSTI

"Saint Malo, 2025-06-03"

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number "AAL_23-1747/1787-v1-TLS-EV_LSTI" covers multiple Root-CAs and consists of 10 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

LSTI
10 Avenue Anita Conti
35400 Saint-Malo, France
E-Mail: julien.bruant@lsti.fr
Phone: +33 (0)2 72 88 12 45

With best regards,

CHRISTOPHE CELISSE
Directeur Technique

Christophe Celisse
Technical Director & Reviewer

Julien Bruant
Julien Bruant ID
2025.06.03 19:33:24 +0200

Julien BRUANT
CEO

This attestation is based on the template version 3.1 as of 2023-08-24, 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 SAS, 10 Avenue Anita Conti, 35400, Saint-Malo - France, registered under n°453867863 • 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: 3 • 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;

[1] https://tools.cofrac.fr/annexes/sect5/5-0546.pdf

d) technical knowledge of the activity to be audited; e) general knowledge of regulatory requirements relevant to TSPs; and 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):	CERTIGNA 20 Allée de la Râperie, 59 650 Villeneuve d'Ascq, France

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:	2024-04-12 to 2025-03-28
Point in time date:	none, as audit was a period of time audit
Audit dates:	2025-03-24 to 2025-03-28 (on site)
Audit location:	Site No1 – CA/RA – CERTIGNA : 20 Allée de la Râperie, 59 650 Villeneuve d'Ascq (FRANCE) Site No2 – RA – PROCHEQUE NORD : 24-26 rue du Carrousel, 59 650 Villeneuve d'Ascq (FRANCE) Site No3 – DR – ETIX ADC1: Parc d'activité du Mélantois, Rue des Saules, 59262 Sainghin-en-Mélantois (FRANCE) Site No4 – DR – ETIX ADC2: 486 Avenue Augusta Ada King, 59400 ANZIN (FRANCE)

Root 1: Certigna

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) 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 TLS Server Certificates, version 2.1.4 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0 • Network and Certificate System Security Requirements, version 2.0.3 Browser Policy Requirements: • Apple Root Certificate Program • Mozilla Root Store Policy, version 3.0 • Microsoft Trusted Root Program • Chrome Root Program Policy, version 1.6 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)

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

- CP-CPS - EN - Certigna TLS CA, version 1.5, as of 2025-03-19
- PC-DPC - FR - Certigna TLS CA, version 1.5, as of 2025-03-19
- CP-CPS - EN - Certigna SMIME CA, version 1.3, as of 2025-03-19
- PC-DPC - FR - Certigna SMIME CA, version 1.3, as of 2025-03-19
- CP-CPS - EN - Certigna Code Signing CA, version 1.2, as of 2025-03-19
- PC-DPC - FR - Certigna Code Signing CA, version 1.2, as of 2025-03-19
- CGVU - EN - Certigna, version 3.4, as of 2025-03-19
- CGVU - FR - Certigna, version 3.4, as of 2025-03-19

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

Findings with regard to ETSI EN 319 401:

5 Risk Assessment

The description of the business risks associated with the possible loss of certification of a cryptographic device shall be improved in the risk assessment [REQ-5-01]

6.1 Trust Service Practice Statement

Typographical errors have been found in the S/MIME CP-CPS (some descriptions have not been translated into French language). [REQ-6.1-01]

Findings with regard to ETSI EN 319 411-1:
6.4.6 Records archival
Event log protection beyond seven years shall be improved. [OVR-6.4.6-01]

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

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

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1883416, Certigna: TLS certificates with Basic constraint non-critical: https://bugzilla.mozilla.org/show_bug.cgi?id=1883416
- Bug 1886442, Certigna: Revocation delay for TLS certificates with basic constraint not marked as critical: https://bugzilla.mozilla.org/show_bug.cgi?id=1886442

The remediation measures taken by Certigna as described on Bugzilla (see link above) have been checked by the auditors and Select appropriate addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Certigna, O=Dhimyotis, C=FR	E3B6A2DB2ED7CE48842F7AC53241C7B71D54144BFB40C11F3F1D0B42F5EEA12D	ETSI EN 319 411-1 V1.4.1, LCP, NCP+, OVCP, ETSI EN 319 411-2 V2.5.1, QEVCP-w, QNCP-w, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd

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 = Certigna Services CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	71E653BFBF5E72515B4099BBD5EC8872812B47C6EC1FA9ADD327E1C92C9EA16D	ETSI EN 319 411-1 V1.4.1, OVCP, ETSI EN 319 411-2 V2.5.1, QEVCP-w, QNCP-w, 1.2.250.1.177.1.0.1.2

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

Root 2: Certigna Root CA

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI TS 119 411-6 V1.1.1 (2023-08) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) 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 TLS Server Certificates, version 2.1.4 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, version 3.9.0 • Network and Certificate System Security Requirements, version 2.0.3 Browser Policy Requirements: • Apple Root Certificate Program • Mozilla Root Store Policy, version 3.0 • Microsoft Trusted Root Program • Chrome Root Program Policy, version 1.6 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)

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

- CP-CPS - EN - Certigna TLS CA, version 1.5, as of 2025-03-19
- PC-DPC - FR - Certigna TLS CA, version 1.5, as of 2025-03-19
- CP-CPS - EN - Certigna SMIME CA, version 1.3, as of 2025-03-19
- PC-DPC - FR - Certigna SMIME CA, version 1.3, as of 2025-03-19
- CP-CPS - EN - Certigna Code Signing CA, version 1.2, as of 2025-03-19
- PC-DPC - FR - Certigna Code Signing CA, version 1.2, as of 2025-03-19
- CGVU - EN - Certigna, version 3.4, as of 2025-03-19
- CGVU - FR - Certigna, version 3.4, as of 2025-03-19

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

Findings with regard to ETSI EN 319 401:

5 Risk Assessment

The description of the business risks associated with the possible loss of certification of a cryptographic device shall be improved in the risk assessment [REQ-5-01]

6.1 Trust Service Practice Statement

Typographical errors have been found in the S/MIME CP-CPS (some descriptions have not been translated into French language). [REQ-6.1-01]

Findings with regard to ETSI EN 319 411-1:
6.4.6 Records archival
Event log protection beyond seven years shall be improved. [OVR-6.4.6-01]

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

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

This Audit Attestation also covers the following incidents as described in the following.

- Bug 1883416, Certigna: TLS certificates with Basic constraint non-critical: https://bugzilla.mozilla.org/show_bug.cgi?id=1883416
- Bug 1886442, Certigna: Revocation delay for TLS certificates with basic constraint not marked as critical: https://bugzilla.mozilla.org/show_bug.cgi?id=1886442

The remediation measures taken by Certigna as described on Bugzilla (see link above) have been checked by the auditors and Select appropriate addressed the incident.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = Certigna Root CA, OU=0002 48146308100036, O=Dhimyotis, C=FR	D48D3D23EEDB50A459E55197601C27774B9D7B18C94D5A059511A10250B93168	ETSI EN 319 411-1 V1.4.1, LCP, NCP+, OVCP, ETSI EN 319 411-2 V2.5.1, QNCP-w, QEVCP-w, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd

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 = Certigna Services CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	07F2CE55CA1AA6CB992719B1E423C1D02C1EA759A6E2EAB4E150C88282E22550	ETSI EN 319 411-1 V1.4.1, OVCP, ETSI EN 319 411-2 V2.5.1, QEVCP-w, QNCP-w, 1.2.250.1.177.2.0.1.1

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

Modifications record

Version	Issuing Date	Changes
Version 1	2025-06-03	Initial attestation

End of the audit attestation letter.