Audit Attestation for

CERTIGNA

Reference: LSTI_AAL_23-1713_tlsbr_V1.0

Saint Malo, 2024-07-10

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number 23-1713_tlsbr_V1.0 and consists of 13 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

LSTI Group
10 Avenue Anita Conti
35400 Saint-Malo, France
E-Mails: pbouchet@lsti.fr & cabforum@acab-c.com
Phone: +33 6 33 38 80 78

With best regards,

ARMELLE TROTIN ID Signature numérique de ARMELLE TROTIN ID

Director

LSTI Philippe BOUCHET

Director

This attestation is based on the template version 3.1 as of 2023-08-23, 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, Dublin 2 – Ireland, registered under n°582309 • Accredited by COFRAC under registration number 5-0546 in accordance with EN ISO/IEC 17065:2012 and in accordance with the eIDAS EU Regulation art. 3 (18) and the ETSI EN 319 403 v2.2.2. Detailed scope at https://www.cofrac.fr/ • 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;

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:	2023-08-11 to 2024-04-12
Audit dates:	From 2024-04-08 to 2024-04-12 (on site)
Audit location:	CERTIGNA : 20 Allée de la Râperie, 59 650 Villeneuve d'Ascq (FRANCE) CIV ADC1: Parc d'activité du Melantois, Rue des Saules 59262 Sainghin-en-Mélantois (FRANCE) CIV 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 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.2 Browser Policy Requirements: • Mozilla Root Store Policy, version 2.9 • Chrome Root Program Policy, version 1.5 • Microsoft Trusted Root Program • Apple Root Certificate Program 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:

- PC - FR - Certigna Root CA, version 4.6, as of 2024-04-05
- DPC - FR - Certigna Root CA, version 4.6, as of 2024-04-05
- PC - EN - Certigna Root CA, version 4.6, as of 2024-04-05
- DPC - EN - Certigna Root CA, version 4.6, as of 2024-04-05
- PC - EN - Certigna TLS CA, version 1.0, as of 2024-04-05
- DPC - EN - Certigna TLS CA, version 1.0, as of 2024-04-05
- CGVU - FR - Certigna, version 3.2, as of 2024-04-08
- CGVU - EN - Certigna, version 3.2, as of 2023-05-22

No major non-conformities have been identified during the audit.
In the following areas, non-conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

[2] 7.2 Human resources [REQ-7.2-03]
Training of RA operators shall be improved.

[7] 6.3 Information security policy [REQ-6.3-07]
Planification of the periodic review of the information security policy shall be improved.

[8] 7.1.2 Segregation of duties [REQ-7.1.2-01]
Documentation shall be improved.

[10] 7.9 Incident management [REQ-7.9-10]
The Vulnerability Management Procedure shall be improved.

Findings with regard to ETSI EN 319 411-1:

[4] 7.1 Certificate policy management [OVR-7.1-02]
Documentation of the OIDs in the terms and conditions shall be improved.

[11] 6.3.4 Certificate acceptance [OVR-6.3.4-01
Conditions of certificate acceptance and new Terms and conditions acceptance in the context of the use of ACME shall be improved in the Terms and Conditions.

[12] 6.3.5 Key pair and certificate usage [OVR-6.3.5-01 j]
Obligations that the private key must be no longer in use when the issuing CA has been compromised shall be more precisely described within the CPS.

[13] 6.9.2 Additional testing [OVR-6.9.2-01C]
The scope of testing certificates in the CPS shall be more precisely described.

[18] 6.6.3 OCSP Profile [CSS-6.6.3-01B]
OCSP certificates profiles implementation shall be improved.

[20] 6.3.1 Certificate application [REG-6.3.1-00D]
The persistence of the Identity validation should be more precisely described within the CPS.

[22] 6.6.1 Certificate Profile [GEN-6.6.1-02]
The RA procedure shall be improved regarding the “OrganizationName” field of legal entity certificates.

Findings with regard to Network and Certificate System Security Requirements:

[24] 2. Trusted Roles, Delegated Third Parties, and System Accounts [2.g.4]
Implementation of periodic password change shall be improved.

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 properly addressed the incident

Root 1: Certigna

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
CN = Certigna Wild CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	211F3083B9E77A01D0828565897A1CE945EEAAE04942CCC369087D8080C9E4A6	ETSI EN 319 411-1 V1.4.1, OVCP, 1.2.250.1.177.1.0.1.2
CN = Certigna Server Authentication ACME CA G1, 2.5.4.97 = NTRFR-48146308100036, O = Certigna, C = FR	B1C8E470CA1F4885DDDEE0FE80B805F2CA823770EC6071C1CCEB77F70A0FB6C2	ETSI EN 319 411-1 V1.4.1, OVCP 1.2.250.1.177.1.0.1.2
CN = Certigna Server Authentication ACME FR CA G1, 2.5.4.97 = NTRFR-48146308100036, O = Certigna, C = FR	CA1FF54E031186F9006BB148F8CE6A53F05742A4B6CE8FFE79DFD2AE471EBAA5	ETSI EN 319 411-1 V1.4.1, OVCP 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 V2.3.1 (2021-05) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 1.8.1 • Baseline Requirements for TLS Server Certificates, version 2.0.2 Browser Policy Requirements: • Mozilla Root Store Policy, version 2.9 • Chrome Root Program Policy, version 1.5 • Microsoft Trusted Root Program • Apple Root Certificate Program 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:

- PC - FR - Certigna Root CA, version 4.6, as of 2024-04-05
- DPC - FR - Certigna Root CA, version 4.6, as of 2024-04-05
- PC - EN - Certigna Root CA, version 4.6, as of 2024-04-05
- DPC - EN - Certigna Root CA, version 4.6, as of 2024-04-05
- PC - EN - Certigna TLS CA, version 1.0, as of 2024-04-05
- DPC - EN - Certigna TLS CA, version 1.0, as of 2024-04-05
- CGVU - FR - Certigna, version 3.2, as of 2024-04-08
- CGVU - EN - Certigna, version 3.2, as of 2023-05-22

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

Findings with regard to ETSI EN 319 401:

[2] 7.2 Human resources [REQ-7.2-03]
Training of RA operators shall be improved.

[7] 6.3 Information security policy [REQ-6.3-07]
Planification of the periodic review of the information security policy shall be improved.

[8] 7.1.2 Segregation of duties [REQ-7.1.2-01]
Documentation shall be improved.

[10] 7.9 Incident management [REQ-7.9-10]
The Vulnerability Management Procedure shall be improved.

Findings with regard to ETSI EN 319 411-1:

[4] 7.1 Certificate policy management [OVR-7.1-02]
Documentation of the OIDs in the terms and conditions shall be improved.

[11] 6.3.4 Certificate acceptance [OVR-6.3.4-01
Conditions of certificate acceptance and new Terms and conditions acceptance in the context of the use of ACME shall be improved in the Terms and Conditions.

[12] 6.3.5 Key pair and certificate usage [OVR-6.3.5-01 j]
Obligations that the private key must be no longer in use when the issuing CA has been compromised shall be more precisely described within the CPS.

[13] 6.9.2 Additional testing [OVR-6.9.2-01C]
The scope of testing certificates in the CPS shall be more precisely described.

[18] 6.6.3 OCSP Profile [CSS-6.6.3-01B]
OCSP certificates profiles implementation shall be improved.

[20] 6.3.1 Certificate application [REG-6.3.1-00D]
The persistence of the Identity validation should be more precisely described within the CPS.

[22] 6.6.1 Certificate Profile [GEN-6.6.1-02]
The RA procedure shall be improved regarding the “OrganizationName” field of legal entity certificates.

Findings with regard to Network and Certificate System Security Requirements:

[24] 2. Trusted Roles, Delegated Third Parties, and System Accounts [2.g.4]
Implementation of periodic password change shall be improved.

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 properly addressed the incident

Root 2: Certigna Root CA

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, QEVCP-w, QNCP-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
CN = Certigna Wild CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	B8D5D65C23FF9D8C902FFE6BEC1DD2F20693AF20E98AE47751F1ECB298127B6E	ETSI EN 319 411-1 V1.4.1, OVCP, 1.2.250.1.177.2.0.1.1
CN = Certigna Server Authentication ACME CA G2, 2.5.4.97 = NTRFR-48146308100036, O = Certigna, C = FR	60FD1DF177AB8EDE87472E8E728307F56EC41A60CCAD794C4FDB6D1CB7D40D56	ETSI EN 319 411-1 V1.4.1, OVCP 1.2.250.1.177.2.0.1.1
CN = Certigna Server Authentication ACME FR CA G2, 2.5.4.97=NTRFR-48146308100036, O = Certigna, C = FR	4E42E2D88C4E4DB5919C79004D1C9C0E9C2D6FBB453DA1D642D3D30F78C0572E	ETSI EN 319 411-1 V1.4.1, OVCP 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

Root 3: Certigna Server Authentication Root CA

Standards considered:	European Standards: • ETSI EN 319 411-2 V2.5.1 (2023-10) • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.2 Browser Policy Requirements: • Mozilla Root Store Policy, version 2.9 • Chrome Root Program Policy, version 1.5 • Microsoft Trusted Root Program • Apple Root Certificate Program 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:

- PC - EN - Certigna TLS CA, version 1.0, as of 2024-04-05
- DPC - EN - Certigna TLS CA, version 1.0, as of 2024-04-05
- CGVU - FR - Certigna, version 3.2, as of 2024-04-08
- CGVU - EN - Certigna, version 3.2, as of 2023-05-22

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

Findings with regard to ETSI EN 319 401:

[1] 6.1 Trust Service Practice statement [REQ-6.1-07]
Deployment of new CAS shall be improved

[2] 7.2 Human resources [REQ-7.2-03]
Training of RA operators shall be improved.

[7] 6.3 Information security policy [REQ-6.3-07]
Planification of the periodic review the information security policy shall be improved.

[8] 7.1.2 Segregation of duties [REQ-7.1.2-01]
Documentation shall be improved.

[9] 7.9 Incident management [REQ-7.9-04]
The supervision of the availability of new CAs need to be improved.

[10] 7.9 Incident management [REQ-7.9-10]
The Vulnerability Management Procedure shall be improved.

Findings with regard to ETSI EN 319 411-1:

[4] 7.1 Certificate policy management [OVR-7.1-02]
Documentation of the OIDs in the terms and conditions shall be improved.

[11] 6.3.4 Certificate acceptance [OVR-6.3.4-01
Conditions of certificate acceptance and new terms and conditions acceptance in the context of the use of ACME shall be improved in the Terms and Conditions.

[12] 6.3.5 Key pair and certificate usage [OVR-6.3.5-01 j]

Obligations that the private key must be no longer in use when the issuing CA has been compromised shall be more precisely described within the CPS.

[13] 6.9.2 Additional testing [OVR-6.9.2-01C]
The scope of testing certificates in the CPS shall be more precisely described.

[18] 6.6.3 OCSP Profile [CSS-6.6.3-01B]
OCSP certificates profiles implementation shall be improved.

[20] 6.3.1 Certificate application [REG-6.3.1-00D]
The persistence of the Identity validation should be more precisely described within the CPS.

[22] 6.6.1 Certificate Profile [GEN-6.6.1-02]
The RA procedure shall be improved regarding the "OrganizationName" field of legal entity certificates.

[23] 5.2 Certificate Practice Statement requirements [OVR-5.2-04]
Documentation for new certificates regarding the signature algorithm description shall be improved.

Findings with regard to Network and Certificate System Security Requirements:

[24] 2. Trusted Roles, Delegated Third Parties, and System Accounts [2.g.4]
Implementation of periodic password change shall be improved.

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.

Root 3: Certigna Server Authentication Root CA

Distinguished Name	SHA-256 fingerprint	Applied policy
CN=Certigna Server Authentication Root CA, O=Certigna, C=FR	38E5A7047A3BA80DF9CBA23F96A5E9BD8BBC937D0E5D739DEEDA9A384542D17A	ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-2 V2.5.1, QNCP-w

Table 5: Root-CA 3 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 Server Authentication CA, 2.5.4.97=NTRFR-48146308100036, O=Certigna, C=FR	F5B4F968DB2AE25141F5AB06A8CF521BC0A116FB122B0627FFDD2FB990D8CAD4	ETSI EN 319 411-1 V1.4.1, OVCP,
CN=Certigna Server Authentication Auto CA, 2.5.4.97=NTRFR-48146308100036, O=Certigna, C=FR	5AC4F884B6332F7D128F6695CE46F881922A58FC3D65E9D718EBB2B1CFC658AA	ETSI EN 319 411-1 V1.4.1, OVCP
CN=Certigna Server Authentication Auto FR CA, 2.5.4.97 = NTRFR-48146308100036, O=Certigna, C=FR	8AE04D0DB06176FAD66F95B14903AA0768361AC4F4B21F3D93AF246519BB0AE4	ETSI EN 319 411-1 V1.4.1, OVCP

Table 6: 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	2024-07-10	Initial attestation

End of the audit attestation letter.