Audit Attestation for

CERTIGNA

Reference: LSTI_AAL_23_1625/3

Saint Malo, 2023-10-24

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_1625/3 and consists of 10 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
2023.11.03 14:55:00 +0100

C.E.O

Philippe BOUCHET

C.T.O

This attestation is based on the template version 3.1 as of 2023-04-28, 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 ☐ 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 Contract TECH21014 ☐ 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 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:	2022-09-09 to 2023-08-11
Audit dates:	2023-08-07 to 2023-08-11 (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 V2.4.1 (2021-11) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • Baseline Requirements for TLS Server Certificates, version 2.0.0 Browser Policy Requirements: • Mozilla Root Store Policy v2.8.1 • Chrome Root Program Policy v1.4 • 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 V1.2.4 (2020-11)

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

1. PC - FR - Certigna, version 1.5, as of 2023-08-09
2. DPC - FR - Certigna, version 1.5, as of 2023-08-09
3. CGVU - FR - Certigna, version 2.9, as of 2023-05-22
4. GCSU - EN - Certigna, version 2.9, 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:

6.2 Terms and Conditions

Documentation on complaints and dispute settlement shall be improved. [REQ-6.2-02]

6.2 Terms and Conditions

Somes duplications and typos need to be corrected in the Terms and Conditions (e.g. DVCP). [REQ-6.2]

Findings with regard to ETSI EN 319 411-1:

6.6 Certificate, CRL and OCSP Profiles

Certificates with the OID 1.2.250.1.177.2.5.1.2.1/2 do not correctly identify the expected ETSI OID 0.4.0.2042.1.7. [GEN-6.6.1-02]

6.2 Identification and authentication

Documentation and records of checks carried out on customer's HSM shall be improved. [REQ-6.2.2-04]

6.3.9 Certificate revocation and suspension

Documentation on delays in updating the status information for all the methods and how to interpret the results in case of differences, shall be improved. [CSS-6.3.10-9A]

6.3.12 Key escrow and recovery

Documentation on authorisation and access procedures for escrowed keys shall be improved [SDP-6.3.12-07]

6.6.3 OCSP profile

Implementation of the supervision of OCSP requests concerning non-issued certificates shall be improved. [OVR-6.6.3-03]

7.8 Network security

Implementation of vulnerability scans every quarter shall be improved. [REQ-7.8-13A]

7.2 Human resources

Records of checks carried out on the skills of intrusion test auditors shall be improved. [REQ-7.2-17]

6.4.8 Compromise and disaster recovery

Documentation on the business continuity plan does not describe how frequently backup copies of essential business information and software are taken. [OVR-6.4.8-03]

7.4 Access control

Documentation on hardware management shall be improved to describe the management of failed disks. [REQ-7.4-10]

Findings with regard to ETSI EN 319 411-2:

6.3.5 Key Pair and Certificate Usage

Documentation to inform relying parties that the anchor for the validation of the certificate shall be as identified in a service digital identifier of an appropriate EU Trusted list entry for QTSP, shall be improved. [OVR-6.3.5-12]

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 1774418, Certigna: Certificate issued with validity period greater than 398 days.
https://bugzilla.mozilla.org/show_bug.cgi?id=1774418

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

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN=Certigna, O=Dhimyotis, C=FR	E3B6A2DB2ED7CE48842F7AC53241C7B71D54144BFB40C11F3F1D0B42F5EEA12D	ETSI EN 319 411-1 V1.3.1, LCP, NCP+, OVCP, ETSI EN 319 411-2 V2.4.1, QEVCP-w, QNCP-w, QCP-l, QCP-n, QCP-l-qscd, QCP-n-qscd

Table 1: Root-CA 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 and OID
CN = Certigna Services CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	71E653BFBF5E72515B4099BBD5EC8872812B47C6EC1FA9ADD327E1C92C9EA16D	ETSI EN 319 411-1 V1.3.1, OVCP, ETSI EN 319 411-2 V2.4.1, 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 V1.3.1, OVCP, 1.2.250.1.177.1.0.1.2

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

Root 2: Certigna Root CA

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.4.1 (2021-11) ☒ ETSI EN 319 411-1 V1.3.1 (2021-05) ☒ ETSI EN 319 401 V2.3.1 (2021-05) CA Browser Forum Requirements: • EV Guidelines for TLS Server Certificates, version 1.8.0 • Baseline Requirements for TLS Server Certificates, version 2.0.0 • Code Signing Baseline Requirements, version 3.3.0 Browser Policy Requirements: • Mozilla Root Store Policy v2.8.1 • Chrome Root Program Policy v1.4 • 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 V1.2.4 (2020-11)

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

1. PC - FR - Certigna Root CA, version 3.8, as of 2023-05-22
2. CP - EN - Certigna Root CA, version 3.8, as of 2023-05-22
3. DPC - FR - Certigna Root CA, version 3.8, as of 2023-05-22
4. CPS - EN - Certigna Root CA, version 3.8, as of 2023-05-22
5. CGVU - FR - Certigna, version 2.9, as of 2023-05-22
6. GCSU - EN - Certigna, version 2.9, 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:

6.2 Terms and Conditions

Documentation on complaints and dispute settlement shall be improved. [REQ-6.2-02]

6.2 Terms and Conditions

Somes duplications and typos need to be corrected in the Terms and Conditions (e.g. DVCP). [REQ-6.2]Findings with regard to ETSI EN 319 411-2:

None.

Findings with regard to ETSI EN 319 411-1:

6.6 Certificate, CRL and OCSP Profiles

Certificates with the OID 1.2.250.1.177.2.5.1.2.1/2 do not correctly identify the expected ETSI OID 0.4.0.2042.1.7. [GEN-6.6.1-02]

6.2 Identification and authentication
Documentation and records of checks carried out on customer's HSM shall be improved. [REQ-6.2.2-04]
6.3.9 Certificate revocation and suspension
Documentation on delays in updating the status information for all the methods and how to interpret the results in case of differences, shall be improved. [CSS-6.3.10-9A]
6.3.12 Key escrow and recovery
Documentation on authorisation and access procedures for escrowed keys shall be improved [SDP-6.3.12-07]
6.6.3 OCSP profile
Implementation of the supervision of OCSP requests concerning non-issued certificates shall be improved. [OVR-6.6.3-03]
7.8 Network security
Implementation of vulnerability scans every quarter shall be improved. [REQ-7.8-13A]
7.2 Human resources
Records of checks carried out on the skills of intrusion test auditors shall be improved. [REQ-7.2-17]
6.4.8 Compromise and disaster recovery
Documentation on the business continuity plan does not describe how frequently backup copies of essential business information and software are taken. [OVR-6.4.8-03]
7.4 Access control
Documentation on hardware management shall be improved to describe the management of failed disks. [REQ-7.4-10]
Findings with regard to ETSI EN 319 411-2:
6.3.5 Key Pair and Certificate Usage
Documentation to inform relying parties that the anchor for the validation of the certificate shall be as identified in a service digital identifier of an appropriate EU Trusted list entry for QTSP, shall be improved. [OVR-6.3.5-12]

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 1774418, Certigna: Certificate issued with validity period greater than 398-days
  https://bugzilla.mozilla.org/show_bug.cgi?id=1774418

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

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN = Certigna Root CA, OU=0002 48146308100036, O=Dhimyotis, C=FR	D48D3D23EEDB50A459E55197601C27774B9D7B18C94D5A059511A10250B93168	ETSI EN 319 411-1 V1.3.1, LCP, NCP+, OVCP, ETSI EN 319 411-2 V2.4.1, 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 and OID
CN = Certigna Services CA 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	07F2CE55CA1AA6CB992719B1E423C1D02C1EA759A6E2EAB4E150C88282E22550	ETSI EN 319 411-1 V1.3.1, OVCP, ETSI EN 319 411-2 V2.4.1, 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 V1.3.1, OVCP, 1.2.250.1.177.2.0.1.1

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

Modifications record

Version	Issuing Date	Changes
Version 1	2023-10-24	Initial attestation

End of the audit attestation letter.