Audit Attestation for

CERTIGNA

Reference: No 23-1582-AL-V1.0

Saint-Malo, 2022-12-09

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number n°23-1582-AL_V1.0 and consists of 10 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

LSTI SAS
10 Avenue Anita Conti
35400 Saint-Malo, France
E-Mail: armelle.trotin@lsti.eu
Phone: +33 608675144

With best regards,

Armelle TROTIN
2022.12.09 16:21:00 +0100

Philippe BOUCHET
2022.12.09 16:21:00 +0100

Armelle Trotin
Head of Certification Body

Philippe Bouchet
C.T.O

This attestation is based on the template version 2.9 as of 2021-xx-xx, that was approved for use by ACAB-c.

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor:	• LSTI SAS: 10 Avenue Anita Conti, 35400 Saint-Malo, France • Accredited by COFRAC under registration accreditation_registration[1] for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403 V2.2.2 (2015-08)” and/or “ETSI EN 319 403-1 V2.3.1 (2020-06)” respectively. • Insurance Carrier (BRG section 8.2): HISCOX SA, contract n°TECH21014 • 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;

[1] URL to the accreditation certificate hosted by the national accreditation body

	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:	2021-09-24 to 2022-09-09
Point in time date:	None
Audit dates:	2022-09-05 to 2022-09-09 (on site)
Audit location:	CERTIGNA: 20 Allée de la Râperie, 59 650 Villeneuve d'Ascq (FRANCE) TESSI: 137 Rue du Fontenoy, 59100 Roubaix (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)

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 SSL Certificate Guidelines, version 1.7.9 ☒ Baseline Requirements, version 1.8.4 Browser Policy Requirements: ☒ Mozilla Root Store Policy v2.8 ☒ Chrome Root Program Policy v1.2 ☒ Microsoft Trusted Root Program ☒ Appel Root Certificate Program For the Trust Service Provider Conformity Assessment: ☒ ETSI EN 319 403 V2.2.2 (2015-08) ☒ ETSI TS 119 403-2 V1.2.4 (2020-11)

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

1. PC - FR - Certigna v1.4, as of 2022-09-01
2. DPC - FR - Certigna v1.4, as of 2022-09-01
3. PC - FR - Certigna Root CA v3.6, as of 2022-09-01
4. PC - EN - Certigna Root CA v3.6, as of 2022-09-01
5. DPC - FR - Certigna Root CA v3.6, as of 2022-09-01
6. DPC - EN - Certigna Root CA v3.6, as of 2022-09-01
7. CGVU - FR - Certigna v2.7, as of 2022-09-01
8. CGVU - EN - Certigna v2.7, as of 2022-09-01

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

Findings with regard to ETSI EN 319 401:
7.9 Incident management

Documentation on the notification of the national privacy body within 24 hours shall be improved. [REQ-7.9-07]

Findings with regard to ETSI EN 319 411-1:
6.2 Identification and authentication

Documentation of controls on digital signatures for the requests shall be improved. [REG-6.2.2-01]

6.3 Certificate Life-Cycle operational requirements

Documentation of CA's old name shall be improved. [GEN-6.3.3-12]

Implementation of an online revocation request service for Certificate Agent, shall be improved. [REV-6.3.9-01]

6.4 Facility, management, and operational controls

Implementation of the labelling of logs shall be improved. [OVR-6.4.6-01]

Documentation of destruction practices in case of CA termination shall be improved. [6.4.9-02]

Documentation of information that certificates and revocation status information issued using CA key may no longer be valid, shall be improved. [6.4.8-13]

Findings with regard to ETSI EN 319 411-2:

Implementation in lower case of the country code in QcPDS Extension, shall be improved. [GEN-6.6.1-03]

For all non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as documented under

- 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. The long-term effectiveness of the measures will be rechecked at the next regular audit.

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
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	EKU
CN = Certigna Entity CA,2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	EBBF4DC600C17DA04381DEFDCFC119C3F34EFB4A04D0860910B813C7792D7585	ETSI EN 319 411-1 V1.3.1, LCP, ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, 1.2.250.1.177.1.0.1.2	1.3.6.1.5.5.7.3.4 (emailProtection), 1.3.6.1.5.5.7.3.8 (id-kp-timeStamping)
CN = Certigna Entity CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	1CC358A6DFA0A76BB5470660D78F3B25F23CCD6395667E49CCFC8201DA3D192D	ETSI EN 319 411-1 V1.3.1, LCP, ETSI EN 319 411-2 V2.4.1, QCP-l, QCP-l-qscd, 1.2.250.1.177.2.0.1.1	1.3.6.1.5.5.7.3.4 (emailProtection), 1.3.6.1.5.5.7.3.8 (id-kp-timeStamping)

CN = Certigna Entity Code Signing CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	935061BE52C8EA88C034B39ADFD522BB314CBF5304E5A7064735DDBDA3242AAF	ETSI EN 319 411-1 V1.3.1, LCP, ETSI EN 319 411-2 V2.4.1, QCP-l-qscd, 1.2.250.1.177.1.0.1.2	1.3.6.1.5.5.7.3.3 (id-kp-codeSigning)
CN = Certigna Entity Code Signing CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	781ACD209D3B873F148F5DB31C680ADADCED40238D8C1BF1A2D553391FA5D0F3	ETSI EN 319 411-1 V1.3.1, LCP, ETSI EN 319 411-2 V2.4.1, QCP-l-qscd, 1.2.250.1.177.2.0.1.1	1.3.6.1.5.5.7.3.3 (id-kp-codeSigning)
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	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
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	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
CN = FR03, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	080E7E36B3C7FA96ECC67DB7F4D41CECE1D194401AF196A4A47B79BDC4970574	ETSI EN 319 411-1 V1.3.1, LCP, 1.2.250.1.177.2.0.1.1	None
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	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
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	1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
CN = Certigna Identity CA, 2.5.4.97 = NTRFR-0002 48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	23BCD5D7A96A513A981EAD27936E59A8028A807BD72860418F68B555A2911670	ETSI EN 319 411-1 V1.3.1, LCP, 1.2.250.1.177.1.0.1.2	1.3.6.1.5.5.7.3.4 (emailProtection), 1.3.6.1.4.1.311.10.3.4 (encryptingFileSystem)

CN = Certigna Identity CA, 2.5.4.97 = NTRFR-0002 48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	B5E4491CF1E0A06C19441FAC295B678226429603FCC414C626E210B2EFC95F00	ETSI EN 319 411-1 V1.3.1, LCP, 1.2.250.1.177.2.0.1.1	1.3.6.1.5.5.7.3.4 (emailProtection), 1.3.6.1.4.1.311.10.3.4 (encryptingFileSystem)
CN = Certigna Identity Plus CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	02C4A300A09C1B893B11F9567659AF95BBB9BBE7953893E36C5BAF17B555CEE3	ETSI EN 319 411-1 V1.3.1, NCP+, ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-qscd 1.2.250.1.177.1.0.1.2	1.3.6.1.5.5.7.3.4 (emailProtection), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
CN = Certigna Identity Plus CA, 2.5.4.97 = NTRFR-48146308100036, OU = 0002 48146308100036, O = DHIMYOTIS, C = FR	736B996D339684729C43CB397D1BB2B2F3F4A7816A5E3C5D589203F885C5D47C	ETSI EN 319 411-1 V1.3.1, NCP+, ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-qscd 1.2.250.1.177.2.0.1.1	1.3.6.1.5.5.7.3.4 (emailProtection), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

Table 2: 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	2022-12-09	Initial attestation

End of the audit attestation letter.