Audit Attestation for

ZETES

Reference: LSTI_AAL_1607-312_V1.0

Saint Malo, 2023-07-11

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number 1607-312 and consists of 9 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,

_____   _____
Director   Director

This attestation is based on the template version 3.0 as of 2023-02-20, 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, 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: 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):	ZETES SA 3 rue de Strasbourg – Haren – 1130 Bruxelles – Belgium Registered number : BE0408425626 Email : Daniel.ocampo@zetes.com ; bart.symons@zetes.com ; sylvain.constancio@zetes.com

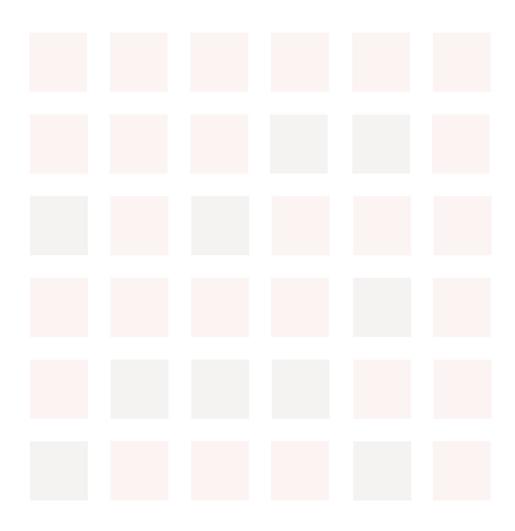| Type of audit:	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit
Audit period covered for all policies:	2022-03-12 to 2023-03-11
Audit dates:	From 2023-03-10 to 2023-03-17

Audit location:	CA/RA Villalaan 13 - 1601 Sint-Pieters-Leeuw – Belgium (AC / OC – main site) RA - Barreaux de Bruxelles, Place Polaert 1, 2000 Bruxelles

Root 1: ZETES TSP Root CA 001

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 1.8.0 ☒ Baseline Requirements, version 1.8.6 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 V1.2.4 (2020-11)

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

1. [CPS] Zetes TSP ROOT CA 001   v1.5   2022-10-14
2. [CPS] Zetes TSP Qualified CA 001   v1.11   2023-03-12
3. [CPS] ZetesConfidens Signature Creation Service issuing CA   v1.9   2023-03-12.
4. [CP] Zetes TSP ROOT CA 001   v1.5   2022-10-14
5. [CP] Zetes TSP Qualified CA 001 for OVB-OBFG-OAC   v1.9   2023-03-12
6. [CP] ZetesConfidens Signature Creation Service issuing CA   v1.9   2023 03 12
7. [CP] Zetes TSP Qualified CA Server Signing Certificates   v1.5   2021 03 08
8. ZetesConfidens E-Seal Certificates for Self-Managed (Q)SCD   v1.2   2023-03-12
9. CTC ZetesConfidens Certificate holders Terms and Conditions   2022-03-05
10. PKI Disclosure Statement OVB-OBFG-OAC -   v1.6   2023-02-28
11. Disclosure Statements for the Certificates for the Zetesconfidens Signature Creation Service Qualified CA 001 -   v1.2   2022-03-07
12. Disclosure Statements for the Certificates for the Zetesconfidens Signature and Seal Creation Service -   v1.2   2022-03-07

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:

    6.1 Trust Service Practice statement

        [REQ-6.1-01] Documentation shall be improved.

        [REQ-6.1-07] Implementation and documentation shall be improved.

    7.11 Business continuity management

        [REQ-7.11-02] Documentation shall be improved.

Findings with regard to ETSI EN 319 411-1:

    6.2 Identification and authentication

        [REG-6.2.2-08] Implementation and documentation shall be improved.

6.4.5 Audit logging procedures

    [REG-6.4.5-04] Documentation shall be improved.

6.4.8 Compromise and disaster recovery

    [OVR-6.4.8-13] Documentation shall be improved.

    [OVR-6.4.8-14A] Documentation shall be improved.
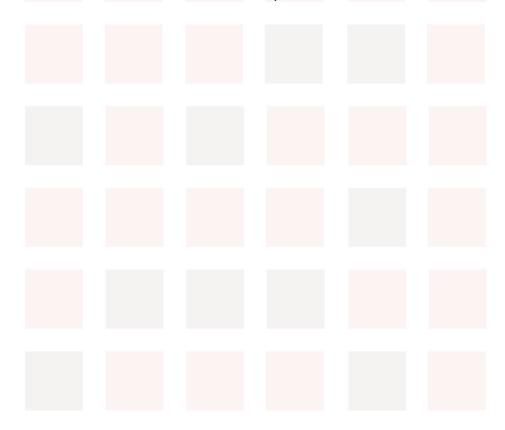
6.6 Certificate, CRL, and OCSP profiles

    [GEN-6.6.1-01] Implementation shall be improved.

Findings with regard to ETSI EN 319 411-2:

    None.

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

    No incident declared within the covered period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN=ZETES TSP ROOT CA 001 O=ZETES SA (VATBE-0408425626) C=BE serialNumber=001	3753D295FC6D8BC39B375650BFFC821A ED504E1A	ETSI EN 319 411-1 V1.2.2, LCP, NCP+ ETSI EN 319 411-2 V2.2.2, QCP-n-qscd, QCP-l

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.
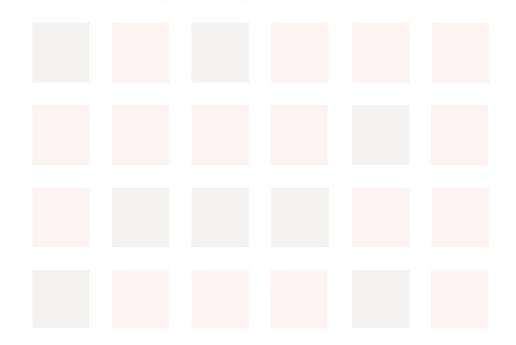
Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
CN=ZETES TSP QUALIFIED CA 001 C=BE O=ZETES SA (VATBE-0408425626) serialNumber=001	1698DC47F4F5FF956C560324E1965AA7ED38E29D	1.3.6.1.4.1.47718.2.1.2.2.1.10 (NCP+) 1.3.6.1.4.1.47718.2.1.2.2.3.10 (QCP-n-qscd) 1.3.6.1.4.1.47718.2.1.2.2.4.1 (LCP) 1.3.6.1.4.1.47718.2.1.2.2.4.2 (NCP+) 1.3.6.1.4.1.47718.2.1.2.2.4.3 (QCP-n-qscd) 1.3.6.1.4.1.47718.2.32.2021.1.3.20.1112.3.2 1.3.6.1.4.1.47718.2.32.2022.1.7.20.1112.3.2 1.3.6.1.4.1.47718.2.32.2022.1.6.21.1112.3.2	1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) None None 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) None None None None

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
CN=ZetesConfidens – Signature Creation Service – Issuing CA 001 C=BE O=ZETES SA (VATBE-0408425626) serialNumber=001	369B535613C8902727507B926D3F57F5423128E0	1.3.6.1.4.1.47718.2.1.2.5.1 (LCP) 1.3.6.1.4.1.47718.2.1.2.5.2 (NCP) 1.3.6.1.4.1.47718.2.1.2.5.3 (QCP-n-qscd) 1.3.6.1.4.1.47718.2.12.2021.2.5.10.1112.4.3 (QCP-n-qscd)	None None 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) None

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
CN=ZETES TSP CA FOR TSA 001 C=BE O=ZETES SA (VATBE-0408425626) serialNumber=001	3702B9F177AFAA8D077C06C3E49482C5A175D32C	1.3.6.1.4.1.47718.2.1.2.50 (QCP-l)	1.3.6.1.5.5.7.3.8 (timeStamping)

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	2023-07-11	Initial attestation

End of the audit attestation letter.