Audit Attestation for

certSIGN

Reference: LSTI_AAL_1612-337_V1.0

Saint Malo, 2024-05-08

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number 1612-300 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
Director

Philippe Bouchet ID
Director

This attestation is based on the template version 3.2 as of 2023-02-20, 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):	certSIGN, AFI Tech Park 1, Bulevardul Tudor Vladimirescu 29A, Bucharest, Romania, registered in Romania under J40/484/2006

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:	2023-02-13 to 2024-02-12
Point in time dates:	none, as audit was a period of time audit
Audit dates:	2024-02-12 to 2024-02-15 (on site)

Root 1: certSIGN ROOT CA G2

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 ☐ Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.2 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. certSIGN-ROOT-CA-G2-Certification-Practice-Statement-v2.23.pdf
2. certSIGN-Public-CA-Certification-Practice-Statement-v2.25.pdf
3. certSIGN-Qualified-CA-Certification-Practice-Statement-v2.41.pdf
4. certSIGN-Web-CA-DV-Certification-Practice-Statement-v1.3.pdf
5. certSIGN-Web-CA-OV-Certification-Practice-Statement-v1.2.pdf
6. certSIGN-Web-CA-QWAC-Certification-Practice-Statement-v1.2.pdf
7. certSIGN-ROOT-CA-G2-PKI-Disclosure-Statement-v2.24.pdf
8. 3.123.13-TC_Seal-NoQSCD-v1.3-RO-EN.pdf
9. 3.13.2-TC_Sign-QSCD-token-v3.3-RO-EN.pdf
10. 3.14-TC_Sign-QSCD-OUG140-token-v1.1-RO-EN.pdf
11. 3.15-TC_SignQSCD-OUG140-Remote-v1.2-RO-EN.pdf
12. 3.2.13.2.2-TC_SignQSCD-Remote-v1.5-RO-EN.pdf
13. 3.4-TC_SealQSCD-v3.3-RO-EN.pdf
14. 3.4.13.10-TC_SealQSCD-Remote-v1.3-RO-EN.pdf
15. 3.5-TC_Seal-TimeStamp-v1.3-RO-EN.pdf
16. 3.9-TC_Sign-NoQSCD-v1.3-RO-EN.pdf
17. TC-SSL-EN_EIDAS_v1.1-Feb2024.pdf
18. TC_remote_simplu_v1.2.pdf
19. TC_sigiliu_simplu_v1.3.pdf
20. TC_simplu_v2.4-1.pdf
21. CONTRACT-QWACPSD2-eIDAS-v1.5.pdf
22. CONTRACT-WEB-SSL-DVOV_v2.4_eIDAS_en.pdf
23. certSIGN-CA-Calificat-Contract.pdf

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

Findings with regard to ETSI EN 319 401:

5 Operational risk assessment

[REQ-5-01] Implementation and documentation shall be improved.

6.1 Trust Service Practice statement

[REQ-6.1-01] Implementation and documentation shall be improved.

7.3 Asset management

[REQ-7.3.1-02] Documentation shall be improved.

Findings with regard to ETSI EN 319 411-1:

None

Findings with regard to ETSI EN 319 411-2:

None.

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

Bug 1859748, certSIGN: “certSIGN: Ransomware attack incident”
https://bugzilla.mozilla.org/show_bug.cgi?id=1859748
The bug was opened on 18-Oct-2023 and was closed on 14-Dec-2023
The remediation measures taken by certSign 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
OU = certSIGN ROOT CA G2 O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: 657CFE2FA73FAA38462571F332A2363A46FCE7020951710702CDFBB6EEDA3305	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, all policies ETSI EN 319 411-2 V2.4.1, all policies

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
2.5.4.97 = VATRO-18288250 CN = certSIGN Public CA O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: 9917BFD853738985E46C920419410E966C316982769E71817E27D0384BBE3679	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1; LCP, NCP	EKU of the CA none

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
2.5.4.97 = VATRO-18288250 CN = certSIGN Qualified CA O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: C670C79BF277AF7E7B34A6AA4FA304441833C6BD01A70A7E9B7A2D94C1C1F926	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1; NCP ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd	EKU of the CA none

Distinguished Name	SHA-256 fingerprint	Applied policy and OID	EKU
2.5.4.97 = VATRO-18288250 CN = certSIGN Web CA O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: F114469FB80778133A1F70E4D8338EDAB97DD42CEB8ECC01CAFB70D6B87DF11E	ETSI EN policy that this S has been assessed against: ETSI EN 319 411-1 V1.3.1; NCP+, DVCP, OVCP ETSI EN 319 411-2 V2.4.1, QEVCP-W	EKU of the CA none

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

Root 2: CERTSIGN ROOT CA G3

Standards considered:	European Standards: ☒ ETSI EN 319 411-2 V2.4.1 (2021-11) ☐ ETSI EN 319 411-1 V1.3.1 (2021-50) ☒ 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 ☐ Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.2 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. certSIGN-ROOT-CA-G3-Certification-Practice-Statement-v1.2.pdf
2. certSIGN-ROOT-CA-G3-PKI-Disclosure-Statement-v1.2
3. certSIGN-CADef-CA-–-Certification-Practice-Statement-v1.21.pdf
4. TC-CADef-CA_en.pdf

In the following areas, non-conformities have been identified throughout the audit:
Findings with regard to ETSI EN 319 401:

5 Operational risk assessment

[REQ-5-01] Implementation and documentation shall be improved.

7.3 Asset management

[REQ-7.3.1-02] Documentation shall be improved.

Findings with regard to ETSI EN 319 411-1:

None.

Findings with regard to ETSI EN 319 411-2:

None.

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.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
OU = CERTSIGN ROOT CA G3 O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: D74C560595F226C1D2DE212F4B2274E6CA33157233EBB206F2E63BA4A3DB9C17	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, all policies ETSI EN 319 411-2 V2.4.1, all policies

Table 3: 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
2.5.4.97 = VATRO-18288250 CN = CADef O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: 47A920FCEEDAD1F874556A3C44F02DEF1DA1B0396D38458BECF3E7B6E8BC0158	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1; NCP ETSI EN 319 411-2 V2.4.1, QCP-n-qscd	EKU of the CA none

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

Root 3: certSIGN ROOT CA SIGN 2023 RSA,

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 ☐ Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.2 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. certSIGN-ROOT-CA-SIGN-2023-RSA-Certification-Practice-Statement-v1.1.pdf
2. certSIGN-ROOT-CA-SIGN-2023-RSA-PKI-Disclosure-Statement-v1.1.pdf
3. certSIGN-Public-2023-RSA-CA-Certification-Practice-Statement-v1.1.pdf
4. certsign-public-2023-rsa-ca-terms-and-conditions-for-remote-signature_v1.0-2023-1.pdf
5. certsign-public-2023-rsa-ca-terms-and-conditions-for-seals_v1.0-2023.pdf
6. certsign-public-2023-rsa-ca-terms-and-conditions_v1.0-2023.pdf
7. certSIGN-Qualified-2023-RSA-CA-Certification-Practice-Statement-v1.1.pdf
8. certsign-qualified-2023-rsa-ca-terms-and-conditions-conform-to-oug140-for-remote-signature_v1.0-RO-EN-2023-1.pdf
9. certsign-qualified-2023-rsa-ca-terms-and-conditions-conform-to-oug140_v1.0-RO-EN-2023.pdf
10. certsign-qualified-2023-rsa-ca-terms-and-conditions-for-remote-sealing_v1.0-RO-EN-2023.pdf
11. certsign-qualified-2023-rsa-ca-terms-and-conditions-for-remote-signature_v1.0-RO-EN-2023.pdf
12. certsign-qualified-2023-rsa-ca-terms-and-conditions-for-seals-without-device_v1.0-RO-EN-2023.pdf
13. certsign-qualified-2023-rsa-ca-terms-and-conditions-for-seals_v1.0-RO-EN-2023.pdf
14. certsign-qualified-2023-rsa-ca-terms-and-conditions-for-signature-without-device_v1.0-RO-EN-2023.pdf
15. certsign-qualified-2023-rsa-ca-terms-and-conditions-for-timestamp-server_v1.0-RO-EN-2023.pdf

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

Findings with regard to ETSI EN 319 401:

5 Operational risk assessment

[REQ-5-01] Implementation and documentation shall be improved.

7.3 Asset management

[REQ-7.3.1-02] Documentation shall be improved.

Findings with regard to ETSI EN 319 411-1:

5.2 Certification Practice Statement requirements

[OVR-5.2-01] Documentation shall be improved.

Findings with regard to ETSI EN 319 411-2:

None.

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.

To the best of our knowledge, no incidents have occurred within this Root-CA's hierarchy during the audited period.

Distinguished Name	SHA-256 fingerprint	Applied policy and OID
CN = certSIGN ROOT CA SIGN 2023 RSA O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: B6A80A71146BC15F8A9CCA6B57A793B0C502DDC334D62482669C345854040BE6	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, all policies ETSI EN 319 411-2 V2.4.1, all policies

Table 5: 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
2.5.4.97 = VATRO-18288250 CN = certSIGN Public 2023 RSA CA O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: A322601EB7EE3EA2CEB6F6814D9DDE2253B8FC3921CA891482495C27138AF94D	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, LCP, NCP	EKU of the CA none
Distinguished Name	**SHA-256 fingerprint**	**Applied policy and OID**	**EKU**
2.5.4.97 = VATRO-18288250 CN = certSIGN Qualified 2023 RSA CA O = CERTSIGN SA C = RO	SHA-256 fingerprint of the certificate: 09E7679F1DD00ECC4592D36A8B42E2465785AAFB9491A20D413648B5A54720DB	ETSI EN policy that this Root has been assessed against: ETSI EN 319 411-1 V1.3.1, NCP ETSI EN 319 411-2 V2.4.1, QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd	EKU of the CA none

Table 6: Sub-CA's issued by the Root-CA or its Sub-CA's in scope of the audit

Modification records

Version	Issuing Date	Changes
Version 1	2024-05-08	Initial Attestation

End of the audit attestation letter.