TÜV AUSTRIA GMBH

Office:
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
www.tuv.at

Business Area
Life, Training &
Certification Austria

Certification Body

Contact person:
Clemens Wanko
Phone:
+49 170 80 20 20 7
Mail:
clemens.wanko@tuv.at

TÜV ®

TLS BR Audit Attestation for

SwissSign AG

Reference: AA2024090402_V2

Cologne, 2024-09-09

To whom it may concern,

This is to confirm that TUV AUSTRIA GMBH has audited the CAs listed in this report and operated by SwissSign AG without critical findings.

This present Audit Attestation Letter is registered under the unique identifier number "AA2024090402_V2" covers multiple Root-CAs and consists of 30 pages. This audit attestation is issued based on the report number TA235244866_SR and TA235244867_SR. Predecessor is Audit Attestation letter AA2023091402 as of 2023-09-14.

Kindly find here below the details accordingly.

In case of any question, please contact:

Clemens Wanko
TÜV AUSTRIA GMBH
Cologne office:
51069 Cologne / Germany
Fon: +49 221 96 97 89-0
Mobile: +49 170 80 20 20 7
Fax: +49 221 96 97 89-12
E-Mail: clemens.wanko@tuv-austria.com
https://www.it-tuv.com

With best regards,

i.A. Clemens Wanko

i.V. Andreas Dvorak

Certification Body

Managing director:
Dr. Stefan Haas
Mag. Christoph
Wenninger

Registered office:
Deutschstraße 10
1230 Wien/Österreich

Further offices:
www.tuv.at/standorte

Company register court:
Wien / FN 288476 f

Banking details:
IBAN
AT131200052949001066
BIC BKAUATWW

UID ATU63240488
DVR 3002477

General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor
• CAB *TÜV AUSTRIA GMBH* *TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge,* registered under: Vienna / Wien / FN 288476 f • Accredited by Federal Ministry for Digital and Economic Affairs, Stubenring 1, 1010 Wien, Austria (mailto: akkreditierung@bmdw.gv.at, https://akkreditierung-austria.gv.at/) under registration 0944[1] for the certification of trust services according to "EN ISO/IEC 17065:2012" and "ETSI EN 319 403 V2.2.2 (2015-08)" / "ETSI EN 319 403-1 V2.3.1 (2020-06)". • Insurance Carrier (BRG section 8.2): Vienna Insurance Group Schottenring 30, 1010 Wien • 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;

[1] https://www.tuv.at/wp-content/uploads/2021/09/TA_GmbH_Akkreditierte_Zertifizierungsstelle-fuer-Produkte-17065-2012_2023-ID-0944.pdf

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):	*SwissSign AG* *Sägereistraße 25* *CH-8152 Glattbrugg, Switzerland* *registered under: CHE-109.357.012*

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:	2023-06-17 to 2024-06-14
Point in time date:	none, as audit was a period of time audit
Audit dates:	Stage 1: 2024-02-19 to 2023-04-12 Stage 2: 2024-04-12 to 2024-04-30 and 2024-06-13 to 2024-06-14
Audit location:	Zürich and Glattbrugg, Switzerland

Root 1: SwissSign Gold CA – G2

Standards considered:	European Standards: • 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 2.0.2 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy • Microsoft Trusted Root Program • Google Root Program • Apple Root Store Program Other: 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:

- *SwissSign CP OV - Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign CP DV – Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign TSPS - Trust Services Practice Statement, version 9.0, as of 2024-08-23*
- *SwissSign CPS TLS - Certification Practice Statement for TLS certificates", version 8.0, as of 2024-08-23*
- *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 9.0, as of 2024-08-23*

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

Findings with regard to ETSI EN 319 401:

7.4 Access Control

SwissSign shall develop a way to keep the tokens for the PEM device secure and safe [ETSI EN 319 401, REQ-7.4-04A]

7.2 Human Resources

SwissSign shall perform the training, internally to all relevant employees for the miss-issuance procedure [ETSI EN 319 401, REQ-7.2-02]

7.3.2 Media handling

SwissSign shall implement a rule in order for customer documents after the application has been processed or after a certain period of time. [ETSI EN 319 401, REQ-7.3.2-01]

7.7 Operation security

SwissSign shall implement a process that applies dual control in the DSS. [ETSI EN 319 401, REQ-7.7-03]

Findings with regard to ETSI EN 319 411-1:

6.3.3 Certificate issuance

SwissSign shall monitor the amount of SHA-1 signed CSRs that are submitted on the FCA platform until the next browser audit and present the results. [ETSI EN 319 411-1, GEN-6.3.3-01]

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.5 Time within which CA Must Process the Revocation Request

SwissSign shall proceed miss-issuance reports only through the miss-issuance mailbox. [BRG 4.9.5]

Findings with regard to Network and Certificate System Security Requirements:

3 Logging, Monitoring, and Alerting

SwissSign shall look into this issue and adopt the system accordingly to have notifications in cases where there are logins in the Online HSMs. [NetSec 3c]

All major non-conformities have been closed before the issuance of this attestation. For all minor 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 described in the following.

- Bug 1849364, SwissSign AG: Missed revocation and opening Bugzilla https://bugzilla.mozilla.org/show_bug.cgi?id=1849364
- Bug 1876771, SwissSign AG: modified fields were not saved into certificates and resulted in miss-issuance https://bugzilla.mozilla.org/show_bug.cgi?id=1876771
- Bug 1874196, SwissSign AG: difference in upper and lower case between CN field and SAN https://bugzilla.mozilla.org/show_bug.cgi?id=1874196

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

All CA's issuing TLS end-entity certificates issued by the Root CA has been either revoked or expired.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = SwissSign Gold CA – G2, O = SwissSign AG, C = CH	62DD0BE9B9F50A163EA0F8E75C053B1ECA57EA55C8688F647C6881F2C8357B95	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP

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 = SwissSign RSA TLS Root CA 2021 - 1, O = SwissSign AG, C = CH	4E5666DAC579161CF00B8D87046D074D6C9C0C0E3994C653BE57998736C55D93	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH	288B4A9F605B09B999B215850825C81F9B537DBAF23664ACA98BF6BA98EDC379	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS Root CA 2021 - 1, O = SwissSign AG, C = CH	7EB8F631AD1C8408E9716AE920BCD677973B059E990AED01DDA5E1C5970B402C	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH	193144F431E0FDDB740717D4DE926A571133884B4360D30E272913CBE660CE41	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA SMIME Root CA 2021 - 1, O = SwissSign AG, C = CH	BC8BBD7D279D2E5F070BCEF6FAF3AAB1BEF30DA3EB2875424295AD147F2AEF07	ETSI EN 319 411-1 V1.3.1, NCP [2] ETSI EN 319 411-1 V1.3.1, LCP [3]
CN = SwissSign RSA SMIME Root CA 2022 - 1, O = SwissSign AG, C = CH	5A84C94054D340D650A29985EF97BB396352E215AED6C0B33CA7FFDD3BD5D2A2	ETSI EN 319 411-1 V1.3.1, NCP [4] ETSI EN 319 411-1 V1.3.1, LCP [5]
CN = SwissSign RSA SMIME Root CA 2021 - 1, O = SwissSign AG, C = CH	B6D56F3DD26AC844E57C8BFE9054F57061350A90894B99CD9811E9A545FC84C5	ETSI EN 319 411-1 V1.3.1, NCP [6] ETSI EN 319 411-1 V1.3.1, LCP [7]
CN = SwissSign RSA SMIME Root CA 2022 - 1, O = SwissSign AG, C = CH	9A12C392BFE57891A0C545309D4D9FD567E480CB613D6342278B195C79A7931F	ETSI EN 319 411-1 V1.3.1, NCP [8] ETSI EN 319 411-1 V1.3.1, LCP [9]

Table 2: Intermediate-CA issued by the Root-CA (includes x-signed and self-signed root CA)

[2] Root CA (cross-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[3] Root CA (cross-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[4] Root CA (cross-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[5] Root CA (cross-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[6] Root CA (self-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[7] Root CA (self-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[8] Root CA (self-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[9] Root CA (self-signed) is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = SwissSign RSA TLS DV ICA 2021 - 1, O = SwissSign AG, C = CH	0E55D0985482BBB7C490EBA147C5A021A2C2A2089D3A8AF57D01EDD540CA5A45	ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS OV ICA 2021 - 1, O = SwissSign AG, C = CH	B3679FDDDC644858B97DBB67DE778DD56C6E5D53A96B70E85AB509D09868186D	ETSI EN 319 411-1 V1.3.1, OVCP
CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1 V1.3.1, OVCP
CN = SwissSign RSA TLS EV ICA 2021 - 1, O = SwissSign AG, C = CH	39CB199F41C6A82AAD83C2810127596D02CC4EC766D0DFE31B01D50D1774749F	ETSI EN 319 411-1 V1.3.1, EVCP
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1 V1.3.1, EVCP

Table 3: CA issuing end entity certificates where the CA was issued by an Intermediate-CA

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = SwissSign Personal Gold CA 2014 - G22, O = SwissSign AG, C = CH	77D6C2AF5A7B86F63D9918C87533779F2AF08D35CFA14DA4938C803F53DE18A1	ETSI EN 319 411-1 V1.3.1, NCP [10]
No Issuing CA under this Root for issuance under DVCP/OVCP.		

Table 4: CA issuing end entity certificates issued by the Root-CA

[10] ICA is not technically constraint. Under this ICA, certificates of policy NCP were issued. Certificate issuance has stopped under this ICA. ICA serves OCSP/CRL only.

Root 2: SwissSign Silver CA - G2

Standards considered:	European Standards: • 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 2.0.2 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy • Microsoft Trusted Root Program • Google Root Program • Apple Root Store Program Other: 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:

- *SwissSign CP DV – Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign TSPS - Trust Services Practice Statement, version 9.0, as of 2024-08-23*
- *SwissSign CPS TLS - Certification Practice Statement for TLS certificates", version 8.0, as of 2024-08-23*
- *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 9.0, as of 2024-08-23*

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

Findings with regard to ETSI EN 319 401:

7.4 Access Control

SwissSign shall develop a way to keep the tokens for the PEM device secure and safe [ETSI EN 319 401, REQ-7.4-04A]

7.2 Human Resources

SwissSign shall perform the training, internally to all relevant employees for the miss-issuance procedure [ETSI EN 319 401, REQ-7.2-02]

7.3.2 Media handling

SwissSign shall implement a rule in order for customer documents after the application has been processed or after a certain period of time. [ETSI EN 319 401, REQ-7.3.2-01]

7.7 Operation security

SwissSign shall implement a process that applies dual control in the DSS. [ETSI EN 319 401, REQ-7.7-03]

Findings with regard to ETSI EN 319 411-1:

6.3.3 Certificate issuance

SwissSign shall monitor the amount of SHA-1 signed CSRs that are submitted on the FCA platform until the next browser audit and present the results. [ETSI EN 319 411-1, GEN-6.3.3-01]

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.5 Time within which CA Must Process the Revocation Request

SwissSign shall proceed miss-issuance reports only through the miss-issuance mailbox. [BRG 4.9.5]

Findings with regard to Network and Certificate System Security Requirements:

3 Logging, Monitoring, and Alerting

SwissSign shall look into this issue and adopt the system accordingly to have notifications in cases where there are logins in the Online HSMs. [NetSec 3c]

All major non-conformities have been closed before the issuance of this attestation. For all minor 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 described in the following.

- Bug 1849364, SwissSign AG: Missed revocation and opening Bugzilla https://bugzilla.mozilla.org/show_bug.cgi?id=1849364
- Bug 1876771, SwissSign AG: modified fields were not saved into certificates and resulted in miss-issuance https://bugzilla.mozilla.org/show_bug.cgi?id=1876771
- Bug 1874196, SwissSign AG: difference in upper and lower case between CN field and SAN https://bugzilla.mozilla.org/show_bug.cgi?id=1874196

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

All CA's issuing TLS end-entity certificates issued by the Root CA has been either revoked or expired.

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = SwissSign Silver CA - G2, O = SwissSign AG, C = CH	BE6C4DA2BBB9BA59B6F3939768374246C3C005993FA98F020D1DEDBED48A81D5	ETSI EN 319 411-1 V1.3.1, DVCP [11]

Table 5: 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 = SwissSign Personal Silver CA 2014 - G22, O = SwissSign AG, C = CH	C9E40F4E83396F34A7C861817B4EDAB3DC1F8BAC699FD50CB261FA9123D55EF4	ETSI EN 319 411-1 V1.3.1, LCP [12]
No Issuing CA under this Root for issuance under DVCP/OVCP.		

Table 6: CA issuing end entity certificates issued by the Root-CA

[11] Root CA is not technically constraint. Under this Root CA, certificates of policies LCP, DVCP were issued. Certificate issuance has stopped under this Root. Root/ICA serve OCSP/CRL only.
[12] ICA is not technically constraint. Under this ICA, certificates of policy LCP were issued. Certificate issuance has stopped under this ICA. ICA serves OCSP/CRL only.

Root 3: SwissSign RSA TLS Root CA 2021 - 1

Standards considered:	European Standards: • 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 2.0.2 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy • Microsoft Trusted Root Program • Google Root Program • Apple Root Store Program Other: 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:

- *SwissSign CP OV - Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign CP DV – Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign TSPS - Trust Services Practice Statement, version 9.0, as of 2024-08-23*
- *SwissSign CPS TLS - Certification Practice Statement for TLS certificates", version 8.0, as of 2024-08-23*
- *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 9.0, as of 2024-08-23*

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

Findings with regard to ETSI EN 319 401:

7.4 Access Control

SwissSign shall develop a way to keep the tokens for the PEM device secure and safe [ETSI EN 319 401, REQ-7.4-04A]

7.2 Human Resources

SwissSign shall perform the training, internally to all relevant employees for the miss-issuance procedure [ETSI EN 319 401, REQ-7.2-02]

7.3.2 Media handling

SwissSign shall implement a rule in order for customer documents after the application has been processed or after a certain period of time. [ETSI EN 319 401, REQ-7.3.2-01]

7.7 Operation security

SwissSign shall implement a process that applies dual control in the DSS. [ETSI EN 319 401, REQ-7.7-03]

Findings with regard to ETSI EN 319 411-1:

6.3.3 Certificate issuance

SwissSign shall monitor the amount of SHA-1 signed CSRs that are submitted on the FCA platform until the next browser audit and present the results. [ETSI EN 319 411-1, GEN-6.3.3-01]

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.5 Time within which CA Must Process the Revocation Request

SwissSign shall proceed miss-issuance reports only through the miss-issuance mailbox. [BRG 4.9.5]

Findings with regard to Network and Certificate System Security Requirements:

3 Logging, Monitoring, and Alerting

SwissSign shall look into this issue and adopt the system accordingly to have notifications in cases where there are logins in the Online HSMs. [NetSec 3c]

All major non-conformities have been closed before the issuance of this attestation. For all minor 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 described in the following.

- Bug 1849364, SwissSign AG: Missed revocation and opening Bugzilla https://bugzilla.mozilla.org/show_bug.cgi?id=1849364
- Bug 1876771, SwissSign AG: modified fields were not saved into certificates and resulted in miss-issuance https://bugzilla.mozilla.org/show_bug.cgi?id=1876771
- Bug 1874196, SwissSign AG: difference in upper and lower case between CN field and SAN https://bugzilla.mozilla.org/show_bug.cgi?id=1874196

The remediation measures taken by SwissSign AG 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
CN = SwissSign RSA TLS Root CA 2021 – 1, O = SwissSign AG, C = CH	7EB8F631AD1C8408E9716AE920BCD677973B059E990AED01DDA5E1C5970B402C	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP

Table 7: 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 = SwissSign RSA TLS DV ICA 2021 - 1, O = SwissSign AG, C = CH	0E55D0985482BBB7C490EBA147C5A021A2C2A2089D3A8AF57D01EDD540CA5A45	ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS OV ICA 2021 - 1, O = SwissSign AG, C = CH	B3679FDDDC644858B97DBB67DE778DD56C6E5D53A96B70E85AB509D09868186D	ETSI EN 319 411-1 V1.3.1, OVCP
CN = SwissSign RSA TLS EV ICA 2021 - 1, O = SwissSign AG, C = CH	39CB199F41C6A82AAD83C2810127596D02CC4EC766D0DFE31B01D50D1774749F	ETSI EN 319 411-1 V1.3.1, EVCP

Table 8: CA issuing end entity certificates issued by the Root-CA

Root 4: SwissSign RSA TLS Root CA 2022 - 1

Standards considered:	European Standards: • 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 2.0.2 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy • Microsoft Trusted Root Program • Google Root Program • Apple Root Store Program Other: 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:

- *SwissSign CP OV - Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign CP DV – Certificate Policy for Organization Validated Certificates, version 4.0, as of 2024-08-08*
- *SwissSign TSPS - Trust Services Practice Statement, version 9.0, as of 2024-08-23*
- *SwissSign CPS TLS - Certification Practice Statement for TLS certificates", version 8.0, as of 2024-08-23*
- *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 9.0, as of 2024-08-23*

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

Findings with regard to ETSI EN 319 401:

7.4 Access Control

SwissSign shall develop a way to keep the tokens for the PEM device secure and safe [ETSI EN 319 401, REQ-7.4-04A]

7.2 Human Resources

SwissSign shall perform the training, internally to all relevant employees for the miss-issuance procedure [ETSI EN 319 401, REQ-7.2-02]

7.3.2 Media handling

SwissSign shall implement a rule in order for customer documents after the application has been processed or after a certain period of time. [ETSI EN 319 401, REQ-7.3.2-01]

7.7 Operation security

SwissSign shall implement a process that applies dual control in the DSS. [ETSI EN 319 401, REQ-7.7-03]

Findings with regard to ETSI EN 319 411-1:

6.3.3 Certificate issuance

SwissSign shall monitor the amount of SHA-1 signed CSRs that are submitted on the FCA platform until the next browser audit and present the results. [ETSI EN 319 411-1, GEN-6.3.3-01]

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.5 Time within which CA Must Process the Revocation Request

SwissSign shall proceed miss-issuance reports only through the miss-issuance mailbox. [BRG 4.9.5]

Findings with regard to Network and Certificate System Security Requirements:

3 Logging, Monitoring, and Alerting

SwissSign shall look into this issue and adopt the system accordingly to have notifications in cases where there are logins in the Online HSMs. [NetSec 3c]

All major non-conformities have been closed before the issuance of this attestation. For all minor 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 described in the following.

- Bug 1849364, SwissSign AG: Missed revocation and opening Bugzilla https://bugzilla.mozilla.org/show_bug.cgi?id=1849364
- Bug 1876771, SwissSign AG: modified fields were not saved into certificates and resulted in miss-issuance https://bugzilla.mozilla.org/show_bug.cgi?id=1876771
- Bug 1874196, SwissSign AG: difference in upper and lower case between CN field and SAN https://bugzilla.mozilla.org/show_bug.cgi?id=1874196

The remediation measures taken by SwissSign AG 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
CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH	193144F431E0FDDB740717D4DE926A571133884B4360D30E272913CBE660CE41	ETSI EN 319 411-1 V1.3.1, OVCP ETSI EN 319 411-1 V1.3.1, DVCP

Table 9: Root-CA 4 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 = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1 V1.3.1, DVCP
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1 V1.3.1, OVCP
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1 V1.3.1, EVCP

Table 10: CA issuing end entity certificates issued by the Root-CA

Root 5: SwissSign RSA SMIME Root CA 2021 - 1

Standards considered:	European Standards: • 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 2.0.2 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy • Microsoft Trusted Root Program • Google Root Program • Apple Root Store Program Other: 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:

- *SwissSign TSPS - Trust Services Practice Statement, version 9.0, as of 2024-08-23*

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

Findings with regard to ETSI EN 319 401:

7.4 Access Control

SwissSign shall develop a way to keep the tokens for the PEM device secure and safe [ETSI EN 319 401, REQ-7.4-04A]

7.2 Human Resources

SwissSign shall perform the training, internally to all relevant employees for the miss-issuance procedure [ETSI EN 319 401, REQ-7.2-02]

7.3.2 Media handling

SwissSign shall implement a rule in order for customer documents after the application has been processed or after a certain period of time. [ETSI EN 319 401, REQ-7.3.2-01]

7.7 Operation security

SwissSign shall implement a process that applies dual control in the DSS. [ETSI EN 319 401, REQ-7.7-03]

Findings with regard to ETSI EN 319 411-1:

6.3.3 Certificate issuance

SwissSign shall monitor the amount of SHA-1 signed CSRs that are submitted on the FCA platform until the next browser audit and present the results. [ETSI EN 319 411-1, GEN-6.3.3-01]

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.5 Time within which CA Must Process the Revocation Request

SwissSign shall proceed miss-issuance reports only through the miss-issuance mailbox. [BRG 4.9.5]

Findings with regard to Network and Certificate System Security Requirements:

3 Logging, Monitoring, and Alerting

SwissSign shall look into this issue and adopt the system accordingly to have notifications in cases where there are logins in the Online HSMs. [NetSec 3c]

All major non-conformities have been closed before the issuance of this attestation. For all minor 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 described in the following.

- Bug 1849364, SwissSign AG: Missed revocation and opening Bugzilla https://bugzilla.mozilla.org/show_bug.cgi?id=1849364
- Bug 1876771, SwissSign AG: modified fields were not saved into certificates and resulted in miss-issuance https://bugzilla.mozilla.org/show_bug.cgi?id=1876771
- Bug 1874196, SwissSign AG: difference in upper and lower case between CN field and SAN https://bugzilla.mozilla.org/show_bug.cgi?id=1874196

The remediation measures taken by SwissSign AG 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
CN = SwissSign RSA SMIME Root CA 2021 – 1, O = SwissSign AG, C = CH	B6D56F3DD26AC844E57C8BFE9054F57061350A90894B99CD9811E9A545FC84C5	ETSI EN 319 411-1 V1.3.1, LCP [13] ETSI EN 319 411-1 V1.3.1, NCP [14]

Table 11: Root-CA 5 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
No Issuing CA under this Root for issuance under DVCP/OVCP/EVCP.		

Table 12: CA issuing end entity certificates issued by the Root-CA

[13] Root CA is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued. Certificate issuance has stopped under this Root. Root/ICA serve OCSP/CRL only.
[14] Root CA is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued. Certificate issuance has stopped under this Root. Root/ICA serve OCSP/CRL only.

Root 6: SwissSign RSA SMIME Root CA 2022 - 1

Standards considered:	European Standards: • 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 2.0.2 • Network and Certificate System Security Requirements, version 1.7 Browser Policy Requirements: • Mozilla Root Store Policy • Microsoft Trusted Root Program • Google Root Program • Apple Root Store Program Other: 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:

- *SwissSign TSPS - Trust Services Practice Statement, version 9.0, as of 2024-08-23*

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

Findings with regard to ETSI EN 319 401:

7.4 Access Control

SwissSign shall develop a way to keep the tokens for the PEM device secure and safe [ETSI EN 319 401, REQ-7.4-04A]

7.2 Human Resources

SwissSign shall perform the training, internally to all relevant employees for the miss-issuance procedure [ETSI EN 319 401, REQ-7.2-02]

7.3.2 Media handling

SwissSign shall implement a rule in order for customer documents after the application has been processed or after a certain period of time. [ETSI EN 319 401, REQ-7.3.2-01]

7.7 Operation security

SwissSign shall implement a process that applies dual control in the DSS. [ETSI EN 319 401, REQ-7.7-03]

Findings with regard to ETSI EN 319 411-1:

6.3.3 Certificate issuance

SwissSign shall monitor the amount of SHA-1 signed CSRs that are submitted on the FCA platform until the next browser audit and present the results. [ETSI EN 319 411-1, GEN-6.3.3-01]

Findings with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates:

4.9.5 Time within which CA Must Process the Revocation Request

SwissSign shall proceed miss-issuance reports only through the miss-issuance mailbox. [BRG 4.9.5]

Findings with regard to Network and Certificate System Security Requirements:

3 Logging, Monitoring, and Alerting

SwissSign shall look into this issue and adopt the system accordingly to have notifications in cases where there are logins in the Online HSMs. [NetSec 3c]

All major non-conformities have been closed before the issuance of this attestation. For all minor 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 described in the following.

- Bug 1849364, SwissSign AG: Missed revocation and opening Bugzilla https://bugzilla.mozilla.org/show_bug.cgi?id=1849364
- Bug 1876771, SwissSign AG: modified fields were not saved into certificates and resulted in miss-issuance https://bugzilla.mozilla.org/show_bug.cgi?id=1876771
- Bug 1874196, SwissSign AG: difference in upper and lower case between CN field and SAN https://bugzilla.mozilla.org/show_bug.cgi?id=1874196

The remediation measures taken by SwissSign AG 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
CN = SwissSign RSA SMIME Root CA 2022 – 1, O = SwissSign AG, C = CH	9A12C392BFE57891A0C545309D4D9FD567E480CB613D6342278B195C79A7931F	ETSI EN 319 411-1 V1.3.1, LCP [15] ETSI EN 319 411-1 V1.3.1, NCP [16]

Table 13: Root-CA 6 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
No Issuing CA under this Root for issuance under DVCP/OVCP/EVCP.		

Table 14: CA issuing end entity certificates issued by the Root-CA

[15] Root CA is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.
[16] Root CA is not technically constraint. Under this Root CA, certificates of policies LCP, NCP were issued.

Modifications record

Version	Issuing Date	Changes
Version 1	2024-09-04	Initial attestation
Version 2	2024-09-09	Update of the Cross/Self-Signed ICAs list.

End of the audit attestation letter.