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 ®

Standard Audit Attestation for

SwissSign AG

Reference: AA2025091201

Cologne, 2025-09-12

To whom it may concern,

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

This present Audit Attestation Letter is registered under the unique identifier number "AA2025091201" covers multiple Root-CAs and consists of 22 pages. This audit attestation is issued based on the reports TA235255424_SR, TA235255425_SR, TA235255426_SR, TA235255427_SR, TA235255428_SR and TA235255429_SR. Predecessor is Audit Attestation letter AA2024090401 as of 2024-09-04 which it supersedes.

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. Elisabeth Pichler

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 Economic Affairs, Energy and Tourism, 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 319 403-1 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; b) understanding functioning of trust services and information security including network security issues;

[1] https://www.tuv.at/wp-content/uploads/2025/05/944_Akkreditierungsbestatigung_PRODUKTE_2025.pdf

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:	2024-06-15 to 2025-06-13
Point in time date:	none, as audit was a period of time audit
Audit dates:	Stage 1: 2025-03-11 to 2025-04-09 Stage 2: 2025-05-05 to 2025-05-28 and 2025-06-12 to 2025-06-13
Audit location:	Glattbrugg, Switzerland

Root 1: SwissSign Gold CA – G2

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.5 • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 2.0.4 Browser Policy Requirements: • Mozilla Root Store Policy, Version 3.0, 2025-03-15 (except chapter 6.1.3 on Mass Revocation Events) • Microsoft Trusted Root Program, 2024-10-28 • Chrome Root Program Policy, 2025-02-15 • Apple Root Certificate Program, 2023-08-15 Other: For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.4.1 (2023-03)

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

- *SwissSign CP Extended Validation Certificates (EV) TLS - Certificate Policy for Extended Validation Certificates, version 5, as of 2025-08-07*
- *SwissSign CP Organization Validated (OV) TLS - Certificate Policy for Organization Validated Certificates, version 5, as of 2025-08-07*
- *SwissSign CP Domain Validated (DV) TLS – Certificate Policy for Domain Validated Certificates, version 5, as of 2025-08-07*
- *SwissSign CP Sponsor Validated (SV) S/MIME - Certificate Policy according to S/MIME BR Sponsor Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 5, as of 2025-08-07*
- *SwissSign CP Sponsor Validated (SV) S/MIME Extended - Certificate Policy according to S/MIME BR Sponsor Validated with extended EKU and ETSI EN 319 411-1 Normalized Certificate Policy with extended EKU, version 5, as of 2025-08-07*
- *SwissSign CP Mailbox Validated (MV) S/MIME- Certificate Policy according to S/MIME BR Mailbox Validated and ETSI EN 319 411-1 Lightweight Certificate Policy, version 5, as of 2025-08-07*
- *SwissSign CP Organization Validated (OV) S/MIME - Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 2.0 as of 2025-05-15*
- *SwissSign TSPS - Trust Services Practice Statement, version 13.0, as of 2025-09-11*
- *SwissSign CPS TLS - Certification Practice Statement for TLS certificates", version 12.0 as of 2025-08-07*
- *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 12.0 as of 2025-08-07*

- *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates, version 10, as of 2025-05-28*
- *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 13.0 as of 2025-08-07*

No major or minor non-conformities have been identified during the audit.

In the following areas, recommendations have been identified throughout the audit:

Recommendations with regard to ETSI EN 319 401:

Risk Assessment

SwS shall further improve its risk assessment and the tracking of countermeasures. [ETSI EN 319 401, REQ-5-04]

Business Continuity Management

SwissSign shall improve the regular review of the BIA and the BCP to keep them synchronised. [ETSI EN 319 401, REQ-7.11.1-01X]

Business Continuity Management

SwissSign shall improve the test coverage regarding to BIA and BCP. [ETSI EN 319 401, REQ-7.11.1-01X]

Documents Management Process

SwissSign shall improve the dual control for any public document release in the markdown process. [ETSI EN 319 401, REQ-6.1-01]

Firewall

SwissSign shall further improve its firewall review. [ETSI EN 319 401, REQ-7.8-21X]

Backup

SwissSign shall further improve its regular backup testing. [ETSI EN 319 401, REQ-7.11.2-04X]

Setup of CA-environments

SwissSign shall improve the synchronization of its staging- and production-environments. [ETSI EN 319 401, REQ-7.7-03]

Recommendations with regard to ETSI EN 319 411-1:

Publication

SwissSign shall improve its publication process for CA related data (e.g. PKI chain and relevant certificates including issuing CAs) in its public repository. [ETSI EN 319 411-1, DIS-6.1-01A]

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

Security Management

SwissSign shall improve its internal questionnaire to further improve the evaluation of cloud service providers when used. [CA/B-F TLS BR, 8]

Risk Assessment

SwissSign shall further improve its risk assessment process to assess risks specific for certification authority related operations. [CA/B-F TLS BR #5]

Self Assessment

SwissSign shall improve its additional self-developed Self-Assessment Tool to reflect additional SwissSign specific certificate content besides the common linting tools. [CA/B-F TLS BR, 7.1]

Certificate check

SwissSign shall improve the process for updating the linting software used to ensure that the update is always completed within three months of a linter release. [CA/B-F TLS BR, 6.6.1]

CA Operation

SwissSign shall improve the regular review of its implementation with the requirements of the NIST SP 800-89 specification for key pair generation. [TLS BR, 6.1.6]

Recommendations with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates:

Certificate check

SwissSign shall improve the verification algorithm to block non-Latin characters in the CN-fields as already planned. [CA/B-F SMIME BR, 3.2.4]

CA operation

SwissSign shall improve its process for updating their weak key database. [CA/B-F S/MIME BR, 6.1.1.3]

Recommendations with regard to Network and Certificate System Security Requirements

Operational control

SwissSign improve the review process of its logs. [CA/B-F NetSec, 3.1.2]

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

- Bug 1914020 SwissSign AG: S/MIME NCP non ASCII symbols in email and SAN field wrong coding: https://bugzilla.mozilla.org/show_bug.cgi?id=1914020
- Bug 1921424 SwissSign AG: Findings in 2024 Audit: https://bugzilla.mozilla.org/show_bug.cgi?id=1921424
- Bug 1929189 SwissSign: S/MIME certificates deviate from CPR: https://bugzilla.mozilla.org/show_bug.cgi?id=1929189
- Bug 1916489 SwissSign: LDAP URL still in CRL distribution point (CDP): https://bugzilla.mozilla.org/show_bug.cgi?id=1916489
- Bug 1914023 SwissSign: S/MIME LCP not-permitted key usage: https://bugzilla.mozilla.org/show_bug.cgi?id=1914023

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

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = SwissSign Gold CA – G2, O = SwissSign AG, C = CH	62DD0BE9B9F50A163EA0F8E75C053B1ECA57EA55C8688F647C6881F2C8357B95	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, LCP ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, 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 SMIME Root CA 2021 - 1, O = SwissSign AG, C = CH	BC8BBD7D279D2E5F070BCEF6FAF3AAB1BEF30DA3EB2875424295AD147F2AEF07	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME Root CA 2022 - 1, O = SwissSign AG, C = CH	5A84C94054D340D650A29985EF97BB396352E215AED6C0B33CA7FFDD3BD5D2A2	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH	288B4A9F605B09B999B215850825C81F9B537DBAF23664ACA98BF6BA98EDC379	ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP
CN = SwissSign RSA SMIME Root CA 2021 - 1, O = SwissSign AG, C = CH	B6D56F3DD26AC844E57C8BFE9054F57061350A90894B99CD9811E9A545FC84C5	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME Root CA 2022 - 1, O = SwissSign AG, C = CH	9A12C392BFE57891A0C545309D4D9FD567E480CB613D6342278B195C79A7931F	ETSI EN 319 411-1 V1.4.1, NCP ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH	193144F431E0FDDB740717D4DE926A571133884B4360D30E272913CBE660CE41	ETSI EN 319 411-1 V1.4.1, EVCP ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP

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

Distinguished Name	SHA-256 fingerprint	Applied policy
CN = SwissSign RSA SMIME LCP ICA 2021 - 2, O = SwissSign AG, C = CH	5CFFA8DB135F913363ACEB7CE362D098F3C1EBD26C63C560C095381E896504FA	ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME NCP extended ICA 2021 - 1, O = SwissSign AG, C = CH	0A6EEB87C2B4AC4A0DF4A68CA7E5244408E06A0CF3BE973156A52AAD835D7466	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME NCP ICA 2021 - 1, O = SwissSign AG, C = CH	1935AA544A73D755E913357FCE0E44AFC90E0809AC97A89964F0A90A59C376B6	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME LCP ICA 2022 - 1, O = SwissSign AG, C = CH	D7F41FABE5A459BAC6882465C75CCFF2BAA52487AABC34706CAF2A18AC53A5C2	ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME NCP ICA 2022 - 1, O = SwissSign AG, C = CH	99A56DD8DACA399FCA2E3834ED75760E96C133564062F8B530B355BED99A409D	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME NCP extended ICA 2022 - 1, O = SwissSign AG, C = CH	7196E86DCFDB92B0509213D806DCA2465FC41415A0B4069D35F946DE6813CF79	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1 V1.4.1, DVCP
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1 V1.4.1, OVCP
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1 V1.4.1, EVCP
CN = SwissSign RSA SMIME MV ICA 2024 – 1, O = SwissSign AG, C = CH	E3367FE0597156205E947903D226C30329951CEE3E63E01FD414F00F85804667	ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME SV ICA 2024 - 1, O = SwissSign AG, C = CH	7E301988A102A5E93D2249666BB631020BA58FC703DE7B583E91D5449FD0D3AF	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME OV ICA 2024 - 1, O = SwissSign AG, C = CH	1F11D479C62DE8DAA554E28674DC58C00BDC0401C175E23689E8BE95DFD687BF	ETSI EN 319 411-1 V1.4.1, NCP

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 V1.4.1, NCP

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

Root 2: SwissSign RSA TLS Root CA 2022 - 1

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) CA Browser Forum Requirements: • Guidelines for the Issuance and Management of Extended Validation Certificates, version 2.0.1 • Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 2.1.5 • Network and Certificate System Security Requirements, version 2.0.4 Browser Policy Requirements: • Mozilla Root Store Policy, Version 3.0, 2025-03-15 (except chapter 6.1.3 on Mass Revocation Events) • Microsoft Trusted Root Program, 2024-10-28 • Chrome Root Program Policy, 2025-02-15 • Apple Root Certificate Program, 2023-08-15 Other: For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.4.1 (2023-03)

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

- *SwissSign CP Extended Validation Certificates (EV) TLS - Certificate Policy for Extended Validation Certificates, version 5, as of 2025-08-07*
- *SwissSign CP Organization Validated (OV) TLS - Certificate Policy for Organization Validated Certificates, version 5, as of 2025-08-07*
- *SwissSign CP Domain Validated (DV) TLS – Certificate Policy for Domain Validated Certificates, version 5, as of 2025-08-07*
- *SwissSign TSPS - Trust Services Practice Statement, version 13.0, as of 2025-09-11*
- *SwissSign CPS TLS - Certification Practice Statement for TLS certificates", version 12.0 as of 2025-08-07*
- *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 12.0 as of 2025-08-07*

No major or minor non-conformities have been identified during the audit.

In the following areas, recommendations have been identified throughout the audit:

Recommendations with regard to ETSI EN 319 401:

Risk Assessment

SwS shall further improve its risk assessment and the tracking of countermeasures. [ETSI EN 319 401, REQ-5-04]

Business Continuity Management

SwissSign shall improve the regular review of the BIA and the BCP to keep them synchronised. [ETSI EN 319 401, REQ-7.11.1-01X]

Business Continuity Management

SwissSign shall improve the test coverage regarding to BIA and BCP. [ETSI EN 319 401, REQ-7.11.1-01X]

Documents Management Process

SwissSign shall improve the dual control for any public document release in the markdown process. [ETSI EN 319 401, REQ-6.1-01]

Firewall

SwissSign shall further improve its firewall review. [ETSI EN 319 401, REQ-7.8-21X]

Backup

SwissSign shall further improve its regular backup testing. [ETSI EN 319 401, REQ-7.11.2-04X]

Setup of CA-environments

SwissSign shall improve the synchronization of its staging- and production-environments. [ETSI EN 319 401, REQ-7.7-03]

Recommendations with regard to ETSI EN 319 411-1:

Publication

SwissSign shall improve its publication process for CA related data (e.g. PKI chain and relevant certificates including issuing CAs) in its public repository. [ETSI EN 319 411-1, DIS-6.1-01A]

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

Security Management

SwissSign shall improve its internal questionnaire to further improve the evaluation of cloud service providers when used. [CA/B-F TLS BR, 8]

Risk Assessment

SwissSign shall further improve its risk assessment process to assess risks specific for certification authority related operations. [CA/B-F TLS BR #5]

Self Assessment

SwissSign shall improve its additional self-developed Self-Assessment Tool to reflect additional SwissSign specific certificate content besides the common linting tools. [CA/B-F TLS BR, 7.1]

Certificate check

SwissSign shall improve the process for updating the linting software used to ensure that the update is always completed within three months of a linter release. [CA/B-F TLS BR, 6.6.1]

CA Operation

SwissSign shall improve the regular review of its implementation with the requirements of the NIST SP 800-89 specification for key pair generation. [TLS BR, 6.1.6]

Recommendations with regard to Network and Certificate System Security Requirements

Operational control

SwissSign improve the review process of its logs. [CA/B-F NetSec, 3.1.2]

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

- Bug 1921424 SwissSign AG: Findings in 2024 Audit: https://bugzilla.mozilla.org/show_bug.cgi?id=1921424
- Bug 1916489 SwissSign: LDAP URL still in CRL distribution point (CDP): https://bugzilla.mozilla.org/show_bug.cgi?id=1916489

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 V1.4.1, EVCP ETSI EN 319 411-1 V1.4.1, OVCP ETSI EN 319 411-1 V1.4.1, DVCP

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 RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1 V1.4.1, DVCP
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1 V1.4.1, OVCP
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1 V1.4.1, EVCP

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

Root 3: SwissSign RSA SMIME Root CA 2021 - 1

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 2.0.4 Browser Policy Requirements: • Mozilla Root Store Policy, Version 3.0, 2025-03-15 (except chapter 6.1.3 on Mass Revocation Events) • Microsoft Trusted Root Program, 2024-10-28 • Chrome Root Program Policy, 2025-02-15 • Apple Root Certificate Program, 2023-08-15 Other: For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.4.1 (2023-03)

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

- *SwissSign CP Sponsor Validated (SV) S/MIME - Certificate Policy according to S/MIME BR Sponsor Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 5, as of 2025-08-07*
- *SwissSign CP Sponsor Validated (SV) S/MIME Extended - Certificate Policy according to S/MIME BR Sponsor Validated with extended EKU and ETSI EN 319 411-1 Normalized Certificate Policy with extended EKU, version 5, as of 2025-08-07*
- *SwissSign CP Mailbox Validated (MV) S/MIME- Certificate Policy according to S/MIME BR Mailbox Validated and ETSI EN 319 411-1 Lightweight Certificate Policy, version 5, as of 2025-08-07*
- *SwissSign CP Organization Validated (OV) S/MIME - Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 2.0 as of 2025-05-15*
- *SwissSign TSPS - Trust Services Practice Statement, version 13.0, as of 2025-09-11*
- *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates, version 10, as of 2025-05-28*
- *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 13.0 as of 2025-08-07*

No major or minor non-conformities have been identified during the audit.

In the following areas, recommendations have been identified throughout the audit:

Recommendations with regard to ETSI EN 319 401:

Risk Assessment

SwS shall further improve its risk assessment and the tracking of countermeasures. [ETSI EN 319 401, REQ-5-04]

Business Continuity Management

SwissSign shall improve the regular review of the BIA and the BCP to keep them synchronised. [ETSI EN 319 401, REQ-7.11.1-01X]

Business Continuity Management

SwissSign shall improve the test coverage regarding to BIA and BCP. [ETSI EN 319 401, REQ-7.11.1-01X]

Documents Management Process

SwissSign shall improve the dual control for any public document release in the markdown process. [ETSI EN 319 401, REQ-6.1-01]

Firewall

SwissSign shall further improve its firewall review. [ETSI EN 319 401, REQ-7.8-21X]

Backup

SwissSign shall further improve its regular backup testing. [ETSI EN 319 401, REQ-7.11.2-04X]

Setup of CA-environments

SwissSign shall improve the synchronization of its staging- and production-environments. [ETSI EN 319 401, REQ-7.7-03]

Recommendations with regard to ETSI EN 319 411-1:

Publication

SwissSign shall improve its publication process for CA related data (e.g. PKI chain and relevant certificates including issuing CAs) in its public repository. [ETSI EN 319 411-1, DIS-6.1-01A]

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

Security Management

SwissSign shall improve its internal questionnaire to further improve the evaluation of cloud service providers when used. [CA/B-F TLS BR, 8]

Risk Assessment

SwissSign shall further improve its risk assessment process to assess risks specific for certification authority related operations. [CA/B-F TLS BR #5]

Self Assessment

SwissSign shall improve its additional self-developed Self-Assessment Tool to reflect additional SwissSign specific certificate content besides the common linting tools. [CA/B-F TLS BR, 7.1]

Certificate check

SwissSign shall improve the process for updating the linting software used to ensure that the update is always completed within three months of a linter release. [CA/B-F TLS BR, 6.6.1]

CA Operation

SwissSign shall improve the regular review of its implementation with the requirements of the NIST SP 800-89 specification for key pair generation. [TLS BR, 6.1.6]

Recommendations with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates:

Certificate check

SwissSign shall improve the verification algorithm to block non-Latin characters in the CN-fields as already planned. [CA/B-F SMIME BR, 3.2.4]

CA operation

SwissSign shall improve its process for updating their weak key database. [CA/B-F S/MIME BR, 6.1.1.3]

Recommendations with regard to Network and Certificate System Security Requirements

Operational control

SwissSign improve the review process of its logs. [CA/B-F NetSec, 3.1.2]

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

- Bug 1914020 SwissSign AG: S/MIME NCP non ASCII symbols in email and SAN field wrong coding: https://bugzilla.mozilla.org/show_bug.cgi?id=1914020
- Bug 1921424 SwissSign AG: Findings in 2024 Audit: https://bugzilla.mozilla.org/show_bug.cgi?id=1921424
- Bug 1929189 SwissSign: S/MIME certificates deviate from CPR: https://bugzilla.mozilla.org/show_bug.cgi?id=1929189
- Bug 1914023 SwissSign: S/MIME LCP not-permitted key usage: https://bugzilla.mozilla.org/show_bug.cgi?id=1914023

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 V1.4.1, LCP ETSI EN 319 411-1 V1.4.1, NCP

Table 7: Root-CA n 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 SMIME LCP ICA 2021 - 2, O = SwissSign AG, C = CH	5CFFA8DB135F913363ACEB7CE362D098F3C1EBD26C63C560C095381E896504FA	ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME NCP ICA 2021 - 1, O = SwissSign AG, C = CH	1935AA544A73D755E913357FCE0E44AFC90E0809AC97A89964F0A90A59C376B6	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME NCP extended ICA 2021 - 1, O = SwissSign AG, C = CH	0A6EEB87C2B4AC4A0DF4A68CA7E5244408E06A0CF3BE973156A52AAD835D7466	ETSI EN 319 411-1 V1.4.1, NCP

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

Root 4: SwissSign RSA SMIME Root CA 2022 - 1

Standards considered:	European Standards: • ETSI EN 319 411-1 V1.4.1 (2023-10) • ETSI EN 319 401 V3.1.1 (2024-06) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, version 1.0.8 • Network and Certificate System Security Requirements, version 2.0.4 Browser Policy Requirements: • Mozilla Root Store Policy, Version 3.0, 2025-03-15 (except chapter 6.1.3 on Mass Revocation Events) • Microsoft Trusted Root Program, 2024-10-28 • Chrome Root Program Policy, 2025-02-15 • Apple Root Certificate Program, 2023-08-15 Other: For the Trust Service Provider Conformity Assessment: • ETSI EN 319 403-1 V2.3.1 (2020-06) • ETSI TS 119 403-2 V1.4.1 (2023-03)

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

- *SwissSign CP Sponsor Validated (SV) S/MIME - Certificate Policy according to S/MIME BR Sponsor Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 5, as of 2025-08-07*
- *SwissSign CP Sponsor Validated (SV) S/MIME Extended - Certificate Policy according to S/MIME BR Sponsor Validated with extended EKU and ETSI EN 319 411-1 Normalized Certificate Policy with extended EKU, version 5, as of 2025-08-07*
- *SwissSign CP Mailbox Validated (MV) S/MIME- Certificate Policy according to S/MIME BR Mailbox Validated and ETSI EN 319 411-1 Lightweight Certificate Policy, version 5, as of 2025-08-07*
- *SwissSign CP Organization Validated (OV) S/MIME - Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 2.0 as of 2025-05-15*
- *SwissSign TSPS - Trust Services Practice Statement, version 13.0, as of 2025-09-11*
- *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates, version 10, as of 2025-05-28*
- *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 13.0 as of 2025-08-07*

No major or minor non-conformities have been identified during the audit.

In the following areas, recommendations have been identified throughout the audit:

Recommendations with regard to ETSI EN 319 401:

Risk Assessment

SwS shall further improve its risk assessment and the tracking of countermeasures. [ETSI EN 319 401, REQ-5-04]

This document is based upon ACAB-c template version 3.4.

Business Continuity Management
SwissSign shall improve the regular review of the BIA and the BCP to keep them synchronised. [ETSI EN 319 401, REQ-7.11.1-01X]
Business Continuity Management
SwissSign shall improve the test coverage regarding to BIA and BCP. [ETSI EN 319 401, REQ-7.11.1-01X]
Documents Management Process
SwissSign shall improve the dual control for any public document release in the markdown process. [ETSI EN 319 401, REQ-6.1-01]
Firewall
SwissSign shall further improve its firewall review. [ETSI EN 319 401, REQ-7.8-21X]
Backup
SwissSign shall further improve its regular backup testing. [ETSI EN 319 401, REQ-7.11.2-04X]
Setup of CA-environments
SwissSign shall improve the synchronization of its staging- and production-environments. [ETSI EN 319 401, REQ-7.7-03]

Recommendations with regard to ETSI EN 319 411-1:
Publication
SwissSign shall improve its publication process for CA related data (e.g. PKI chain and relevant certificates including issuing CAs) in its public repository. [ETSI EN 319 411-1, DIS-6.1-01A]

Recommendations with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates:
Security Management
SwissSign shall improve its internal questionnaire to further improve the evaluation of cloud service providers when used. [CA/B-F TLS BR, 8]
Risk Assessment
SwissSign shall further improve its risk assessment process to assess risks specific for certification authority related operations. [CA/B-F TLS BR #5]

Self Assessment
SwissSign shall improve its additional self-developed Self-Assessment Tool to reflect additional SwissSign specific certificate content besides the common linting tools. [CA/B-F TLS BR, 7.1]
Certificate check
SwissSign shall improve the process for updating the linting software used to ensure that the update is always completed within three months of a linter release. [CA/B-F TLS BR, 6.6.1]
CA Operation
SwissSign shall improve the regular review of its implementation with the requirements of the NIST SP 800-89 specification for key pair generation. [TLS BR, 6.1.6]

Recommendations with regard to Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates:
Certificate check
SwissSign shall improve the verification algorithm to block non-Latin characters in the CN-fields as already planned. [CA/B-F SMIME BR, 3.2.4]

CA operation

SwissSign shall improve its process for updating their weak key database. [CA/B-F S/MIME BR, 6.1.1.3]

Recommendations with regard to Network and Certificate System Security Requirements

Operational control

SwissSign improve the review process of its logs. [CA/B-F NetSec, 3.1.2]

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

- Bug 1914020 SwissSign AG: S/MIME NCP non ASCII symbols in email and SAN field wrong coding: https://bugzilla.mozilla.org/show_bug.cgi?id=1914020
- Bug 1921424 SwissSign AG: Findings in 2024 Audit: https://bugzilla.mozilla.org/show_bug.cgi?id=1921424
- Bug 1929189 SwissSign: S/MIME certificates deviate from CPR: https://bugzilla.mozilla.org/show_bug.cgi?id=1929189
- Bug 1914023 SwissSign: S/MIME LCP not-permitted key usage: https://bugzilla.mozilla.org/show_bug.cgi?id=1914023

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 V1.4.1, LCP ETSI EN 319 411-1 V1.4.1, NCP

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 SMIME LCP ICA 2022 - 1, O = SwissSign AG, C = CH	D7F41FABE5A459BAC6882465C75CCFF2BAA52487AABC34706CAF2A18AC53A5C2	ETSI EN 319 411-1 V1.4.1, LCP
CN = SwissSign RSA SMIME NCP ICA 2022 - 1, O = SwissSign AG, C = CH	99A56DD8DACA399FCA2E3834ED75760E96C133564062F8B530B355BED99A409D	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME NCP extended ICA 2022 - 1, O = SwissSign AG, C = CH	7196E86DCFDB92B0509213D806DCA2465FC41415A0B4069D35F946DE6813CF79	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME MV ICA 2024 – 1, O = SwissSign AG, C = CH	E3367FE0597156205E947903D226C30329951CEE3E63E01FD414F00F85804667	ETSI EN 319 411-1 V1.4.1, LCP
SwissSign RSA SMIME SV ICA 2024 - 1, O = SwissSign AG, C = CH	7E301988A102A5E93D2249666BB631020BA58FC703DE7B583E91D5449FD0D3AF	ETSI EN 319 411-1 V1.4.1, NCP
CN = SwissSign RSA SMIME OV ICA 2024 - 1, O = SwissSign AG, C = CH	1F11D479C62DE8DAA554E28674DC58C00BDC0401C175E23689E8BE95DFD687BF	ETSI EN 319 411-1 V1.4.1, NCP

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

Key pairs without a corresponding certificate ("parked keys")

- Not applicable -

Modifications record

Version	Issuing Date	Changes
Version 1	2025-09-12	Initial attestation

End of the audit attestation letter.