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 ®

SMIME BR Audit Attestation for

SwissSign AG

Reference: AA2024060501

Cologne, 2024-06-05

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, covers multiple Root-CA and consists of 10 pages. This audit attestation is issued based upon the performed Key Ceremony and the related report AA20240531_KC.

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: 1 • 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 (Key Ceremony) ☐ Period of time, after x month of CA operation ☐ Period of time, full audit
Audit period covered for all policies:	none, as audit was a point in time audit (Key Ceremony)
Point in time date:	2024-05-27 to 2024-05-28
Audit dates:	Stage 1: not applicable Stage 2: 2024-05-27 to 2024-05-28
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) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • S/MIME Baseline Requirements, version 1.0.3 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 NCP - Certificate Policy according to Normalized Certificate Policy, version 3.0, as of 2023-08-11*
- *SwissSign CP NCP extended - Certificate Policy according to Normalized Certificate Policy with extended EKU, version 3.0, as of 2023-08-11*
- *SwissSign CP LCP - Certificate Policy Certificate Policy according to Lightweight Certificate Policy, version 3.0, as of 2023-08-11*
- *SwissSign CP OV – Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 1.0, as of 2024-05-27*
- *SwissSign TSPS - Trust Services Practice Statement, version 6.0, as of 2023-08-31*
- *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates, version 6.0, as of 2024-06-04*
- *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 7.0, as of 2024-06-04*

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

No incidents were reported as this is a point-in-time audit.

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, NCP ETSI EN 319 411-1 V1.3.1, LCP

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 2022 - 1, O = SwissSign AG, C = CH	5A84C94054D340D650A29985EF97BB396352E215AED6C0B33CA7FFDD3BD5D2A2	ETSI EN 319 411-1 V1.3.1, NCP ETSI EN 319 411-1 V1.3.1, LCP
CN = SwissSign RSA SMIME Root CA 2022 - 1, O = SwissSign AG, C = CH	9A12C392BFE57891A0C545309D4D9FD567E480CB613D6342278B195C79A7931F	ETSI EN 319 411-1 V1.3.1, NCP ETSI EN 319 411-1 V1.3.1, LCP

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 MV ICA 2024 - 1, O = SwissSign AG, C = CH	E3367FE0597156205E947903D226C30329951CEE3E63E01FD414F00F85804667	ETSI EN 319 411-1 V1.3.1, LCP ETSI TS 319 411-6 V1.1.1 mailbox-validated – legacy ETSI TS 319 411-6 V1.1.1 mailbox-validated – multipurpose ETSI TS 319 411-6 V1.1.1 mailbox-validated – strict
CN = SwissSign RSA SMIME OV ICA 2024 - 1, O = SwissSign AG, C = CH	1F11D479C62DE8DAA554E28674DC58C00BDC0401C175E23689E8BE95DFD687BF	ETSI EN 319 411-1 V1.3.1, NCP ETSI TS 319 411-6 V1.1.1 organization-validated – legacy ETSI TS 319 411-6 V1.1.1 organization - validated – multipurpose ETSI TS 319 411-6 V1.1.1 organization - validated – strict
CN = SwissSign RSA SMIME SV ICA 2024 - 1, O = SwissSign AG, C = CH	7E301988A102A5E93D2249666BB631020BA58FC703DE7B583E91D5449FD0D3AF	ETSI EN 319 411-1 V1.3.1, NCP ETSI TS 319 411-6 V1.1.1 sponsor-validated – legacy ETSI TS 319 411-6 V1.1.1 sponsor - validated – multipurpose ETSI TS 319 411-6 V1.1.1 sponsor - validated – strict

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

Root 2: 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) • ETSI TS 119 411-6 V1.1.1 (2023-08) CA Browser Forum Requirements: • S/MIME Baseline Requirements, version 1.0.3 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 NCP - Certificate Policy according to Normalized Certificate Policy, version 3.0, as of 2023-08-11*
- *SwissSign CP NCP extended - Certificate Policy according to Normalized Certificate Policy with extended EKU, version 3.0, as of 2023-08-11*
- *SwissSign CP LCP - Certificate Policy Certificate Policy according to Lightweight Certificate Policy, version 3.0, as of 2023-08-11*
- *SwissSign CP OV – Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy, version 1.0, as of 2024-05-27*
- *SwissSign TSPS - Trust Services Practice Statement, version 6.0, as of 2023-08-31*
- *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates, version 6.0, as of 2024-06-04*
- *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 7.0, as of 2024-06-04*

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

No incidents were reported as this is a point-in-time audit.

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 ETSI EN 319 411-1 V1.3.1, NCP

Table 7: 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 SMIME MV ICA 2024 - 1, O = SwissSign AG, C = CH	E3367FE0597156205E947903D226C30329951CEE3E63E01FD414F00F85804667	ETSI EN 319 411-1 V1.3.1, LCP ETSI TS 319 411-6 V1.1.1 mailbox-validated – legacy ETSI TS 319 411-6 V1.1.1 mailbox-validated – multipurpose ETSI TS 319 411-6 V1.1.1 mailbox-validated – strict
CN = SwissSign RSA SMIME OV ICA 2024 - 1, O = SwissSign AG, C = CH	1F11D479C62DE8DAA554E28674DC58C00BDC0401C175E23689E8BE95DFD687BF	ETSI EN 319 411-1 V1.3.1, NCP ETSI TS 319 411-6 V1.1.1 organization-validated – legacy ETSI TS 319 411-6 V1.1.1 organization - validated – multipurpose ETSI TS 319 411-6 V1.1.1 organization - validated – strict
CN = SwissSign RSA SMIME SV ICA 2024 - 1, O = SwissSign AG, C = CH	7E301988A102A5E93D2249666BB631020BA58FC703DE7B583E91D5449FD0D3AF	ETSI EN 319 411-1 V1.3.1, NCP ETSI TS 319 411-6 V1.1.1 sponsor-validated – legacy ETSI TS 319 411-6 V1.1.1 sponsor - validated – multipurpose ETSI TS 319 411-6 V1.1.1 sponsor - validated – strict

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

Modifications record

Version	Issuing Date	Changes
Version 1	2024-06-05	Initial attestation

End of the audit attestation letter.