

Audit Attestation for SwissSign AG

Reference: AA2021080502

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2021-08-05

To whom it may concern,

This is to confirm that TÜV AUSTRIA CERT has successfully audited the CA of the SwissSign AG without critical findings.

This present Audit Attestation letter is registered under the unique identifier number "AA2021080502" and consist of 9 pages. This audit attestation is issued based on the report number AA20210805_KC. This Audit Attestation is the initial Audit Attestation for the new Root CA listed below.

Kindly find here below the details accordingly.

In case of any question, please contact:

Clemens Wanko
TÜV AUSTRIA CERT 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>

Certification Body

Managing director:
DI (FH) Andreas Dvorak,
MSc**Registered office:**
Deutschstraße 10
1230 Wien/Österreich**Further offices:**
www.tuv.at/standorte**Company register
court:**
Wien / FN 288474 b**Banking details:**
IBAN
AT141200052949025201
BIC BKAUATWWIBAN
AT373100000104093274
BIC RZBAATWWUID ATU63247169
DVR 3002477

With best regards,



i.A. Clemens Wanko



i.V. Andreas Dvorak

Audit Attestation

Audit Attestation SwissSign AA2021080502



Auditor:	<p>TÜV AUSTRIA CERT GmbH¹ TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge, Company registration: Vienna / Wien / FN 288474 b</p> <p>Accreditation Body: Federal Ministry for Digital and Economic Affairs 1010 Wien, Stubenring 1 mailto: akkreditierung@bmdw.gv.at https://www.bmdw.gv.at/en/Services/Accreditation.html https://akkreditierung-austria.gv.at/overview</p> <p>Accreditation: The CAB is accredited for the certification of trust services according to DIN EN ISO/IEC 17065:2012, ETSI EN 319 403 v2.2.2:2015 and ETSI EN 319 403-1 V2.3.1:2020.</p> <p>URL to accreditation details: https://www.tuv.at/fileadmin/user_upload/docs/certification/Akkreditierungs-Urkunde_und_Umfang_Produktzertifizierung.pdf</p> <p>Third-party affiliate audit firms involved in the audit: none.</p>
Identification and qualification of the audit team:	<ul style="list-style-type: none">• 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<ol style="list-style-type: none">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; and4) 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.

¹ in the following termed shortly „CAB“

Audit Attestation

Audit Attestation SwissSign AA2021080502



	<ul style="list-style-type: none">• 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:<ul style="list-style-type: none">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; andf) 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<ul style="list-style-type: none">a) has acted as auditor in at least three complete TSP audits;b) has adequate knowledge and attributes to manage the audit process; andc) 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:	<ul style="list-style-type: none">• 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.

Audit Attestation

Audit Attestation SwissSign AA2021080502



Identification of the trust service provider (TSP/CA):	<i>SwissSign AG Sägereistraße 25 CH-8152 Glattbrugg, Switzerland All relevant TSP sites are located in Glattbrugg, Switzerland. Contact: Mr. Michael Günther E-Mail: michael.quenther@swissign.com Company registration: CHE-403.679.996, CHE-109.357.012 (SwissSign Ltd.)</i>
--	---

Audit Period covered for all policies:	none, as this was a point in time (PIT) audit
Audit dates:	2021-08-02 to 2021-08-04 (on site)
Audit Locations:	Zürich and Glattbrugg, Switzerland
Type of audit	<input checked="" type="checkbox"/> Point in time audit <input type="checkbox"/> Period of time, after x month of CA operation <input type="checkbox"/> Period of time, full audit

Standards considered	<p>European Standards:</p> <ul style="list-style-type: none"><input type="checkbox"/> ETSI EN 319 411-2, V2.2.2 (2021-05)<input checked="" type="checkbox"/> ETSI EN 319 411-1, V1.2.2 (2021-05)<input checked="" type="checkbox"/> ETSI EN 319 401, V2.2.1 (2021-05) <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> EV SSL Certificate Guidelines, version 1.7.6<input checked="" type="checkbox"/> Baseline Requirements, version 1.7.8 considering the requirements of the ETSI EN 319 403-1 V2.3.1 (2020-06)<input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.2.4 (2020-11) for the Trust Service Provider Conformity Assessment <p>Browser Policy Requirements:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Mozilla Root Store Policy<input checked="" type="checkbox"/> Microsoft Trusted root Program<input checked="" type="checkbox"/> Google Root Program<input checked="" type="checkbox"/> Apple Root Store Program <p>Other:</p> <ul style="list-style-type: none"><input type="checkbox"/> add or delete
----------------------	---

Audit Attestation

Audit Attestation SwissSign AA2021080502



Identification of the audited Root-CA:	SwissSign RSA SMIME Root CA 2021 - 1	
	Distinguished Name	CN = SwissSign RSA SMIME Root CA 2021 - 1 O = SwissSign AG C = CH
	SHA-256 fingerprint	B6D56F3DD26AC844E57C8BFE9054F57061350A90894B99CD9811E9A545FC84C5
	Certificate Serial number	746CD5D1943C167DAEBE03EDE56E07
	Applied policy	<i>ETSI EN 319 411-1, policies LCP, NCP</i>

Audit Attestation

Audit Attestation SwissSign AA2021080502



The point in time audit comprised the key ceremony and relevant aspects for protection of the keys based on the following policy and practice statement documents of the TSP:

1. *SwissSign TSPS - Trust Services Practice Statement, version 1.0, as of 2021-06-14*
2. *SwissSign CP LCP - Certificate Policy Certificate Policy according to Lightweight Certificate Policy, version 1.0, as of 2021-06-14*
3. *SwissSign CP NCP - Certificate Policy according to Normalized Certificate Policy, version 1.0, as of 2021-06-14*
4. *SwissSign CP NCP extended - Certificate Policy according to Normalized Certificate Policy with extended ECU, version 1.0, as of 2021-06-14*
5. *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates “, version 1.0, as of 2021-06-14*
6. *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 1.0, as of 2021-06-14*

The TSP has followed the defined internal key ceremony protocols and has documented the key generation as well as the certificate issuance as required.

No **non-conformities** have been identified throughout the audit.

The Sub-CA that have been issued by the aforementioned Root-CA and that have been covered by this audit are listed in table 1 below. During the key ceremony one additional ICA (listed in table 2) was issued mistakenly with mistyped CN. It was revoked after the mistake was detected. A corresponding CARL was issued.

Audit Attestation

Audit Attestation SwissSign AA2021080502



Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign RSA SMIME LCP ICA 2021 - 2, O = SwissSign AG, C = CH	5CFFA8DB135F913363ACEB7CE362D098F3C1EBD26C63C560C095381E896504FA	ETSI EN 319 411-1, LCP	1.3.6.1.5.5.7.3.4 emailProtection
CN = SwissSign RSA SMIME NCP extended ICA 2021 - 1, O = SwissSign AG, C = CH	0A6EEB87C2B4AC4A0DF4A68CA7E5244408E06A0CF3BE973156A52AAD835D7466	ETSI EN 319 411-1, NCP	1.3.6.1.5.5.7.3.2 clientAuth 1.3.6.1.5.5.7.3.4 emailProtection 1.3.6.1.4.1.311.10.3.4 encryptedFileSystem 1.3.6.1.4.1.311.20.2.2 smartcardLogon
CN = SwissSign RSA SMIME NCP ICA 2021 - 1, O = SwissSign AG, C = CH	1935AA544A73D755E913357FCE0E44AFC90E0809AC97A89964F0A90A59C376B6	ETSI EN 319 411-1, NCP	1.3.6.1.5.5.7.3.2 clientAuth 1.3.6.1.5.5.7.3.4 emailProtection

Table 1: CA issuing end-entity certificates issued by the Root-CA

Audit Attestation

Audit Attestation SwissSign AA2021080502



Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign RSA SMIME LCP 2021 - 1, O = SwissSign AG, C = CH	8F5DB76CBEE38EAADF8D74BFC179E304821A54826EDFB8EDBD08FC680A4BCFCC	ETSI EN 319 411-1, LCP	1.3.6.1.5.5.7.3.4 emailProtection

Table 2: revoked CA issuing end-entity certificates issued by the Root-CA

Audit Attestation

Audit Attestation SwissSign AA2021080502



Modifications record

Version	Issuing Date	Changes
Version 1	2020-08-05	initial attestation
-	-	-

End of the audit attestation letter.