

Audit Attestation for SwissSign AG

Reference: AA2022070101

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2022-07-01

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 "AA2022070101" and consist of 8 pages. This audit attestation is issued based on the report number AA20220701_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 AA2022070101



<p>Auditor:</p>	<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>
<p>Identification and qualification of the audit team:</p>	<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 AA2022070101



	<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 AA2022070101



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-109.357.012 (SwissSign Ltd.)</i>
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
Audit period covered for all policies:	none, as audit was pit audit
Point in time date:	2022-06-08, 2022-06-28 and 2022-06-29 (on site)
Audit dates:	2022-06-08, 2022-06-28 and 2022-06-29 (on site)
Audit Locations:	Zürich and Glattbrugg, Switzerland

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 1.7.9<input checked="" type="checkbox"/> Baseline Requirements, version 1.8.4<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>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> ETSI EN 319 403-1 V2.3.1 (2020-06)<input checked="" type="checkbox"/> ETSI TS 119 403-2 V1.2.4 (2020-11)
----------------------	--

Audit Attestation

Audit Attestation SwissSign AA2022070101



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 3.0, as of 2021-11-14*
2. *SwissSign CP EV - Certificate Policy for Extended Validation Certificates, version 1.0, as of 2021-06-14*
3. *SwissSign CP OV - Certificate Policy for Organization Validated Certificates, version 1.0, as of 2021-06-14*
4. *SwissSign CP DV - Certificate Policy for Domain Validated Certificates, version 1.0, as of 2021-06-14*
5. *SwissSign CPS TLS - Certification Practice Statement for TLS Certificates“, version 4.0, as of 2022-07-01*
6. *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 4.0, as of 2022-07-01*

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 2 below.

Audit Attestation

Audit Attestation SwissSign AA2022070101



Identification of the audited Root-CA:	SwissSign RSA TLS Root CA 2022 - 1	
	Distinguished Name	CN = SwissSign RSA TLS Root CA 2022 - 1 O = SwissSign AG C = CH
	SHA-256 fingerprint	193144F431E0FDDB740717D4DE926A571133884B4360D30E272913CBE660CE41
	Certificate Serial number	43FA0C5F4E1B801844EFD1B44F351F44F480EDCB
	Applied policy	<i>ETSI EN 319 411-1, policies EVCP, OVCP, DVCP</i>

Table 1: Root-CA in scope of the audit

Audit Attestation

Audit Attestation SwissSign AA2022070101



Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1 DVCP	1.3.6.1.5.5.7.3.1 serverAuth 1.3.6.1.5.5.7.3.2 clientAuth
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1 EVCP	1.3.6.1.5.5.7.3.1 serverAuth 1.3.6.1.5.5.7.3.2 clientAuth
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1 OVCP	1.3.6.1.5.5.7.3.1 serverAuth 1.3.6.1.5.5.7.3.2 clientAuth

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

Audit Attestation

Audit Attestation SwissSign AA2022070101



Modifications record

Version	Issuing Date	Changes
Version 1	2022-07-01	Initial attestation
-	-	-

End of the audit attestation letter.