TÜV AUSTRIA CERT GMBH

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

Business Area
Business Assurance

Certification Body

TÜV ®

Audit Attestation for SwissSign AG

Reference: AA2021121501

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2021-12-15

To whom it may concern,

This is to confirm that TUV 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 "AA2021121501" and consist of 10 pages. This audit attestation is issued based on the report number TA235203365_SR. Predecessor is Audit Attestation letter AA2020112501 as of 2020-12-17 which it supersedes.

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

With best regards,

i.A. Clemens Wanko

i.V. Andreas Dvorak

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 BKAUATWW

IBAN
AT373100000104093274
BIC RZBAATWW

UID ATU63247169
DVR 3002477

Auditor:	*TÜV AUSTRIA CERT GmbH*[1] *TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge,* Company registration: Vienna / Wien / FN 288474 b Accreditation Body: Federal Ministry for Digital and Economic Affairs 1010 Wien, Stubenring 1 mailto: akkreditierung@bmdw.gv.at https://akkreditierung-austria.gv.at/ 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. URL to accreditation: https://www.tuv.at/fileadmin/user_upload/docs/certification/Akkreditierungs-Urkunde_und_-Umfang_Produktzertifizierung.pdf 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:

[1] in the following termed shortly „*CAB*“

	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; 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 trust service provider (TSP/CA):	*SwissSign AG* *Sägereistraße 25* *CH-8152 Glattbrugg, Switzerland* *All relevant TSP sites are located in Glattbrugg, Switzerland* *Contact: Mr. Michael Günther* *E-Mail: michael.guenther@swisssign.com* *Company registration:* *CHE-403.679.996, CHE-109.357.012 (SwissSign Ltd.)*

Audit Period covered for all policies:	2020-09-25 to 2021-09-24
Audit dates:	Stage 1: 2021-07-05 to 2021-07-30 Stage 2: 2021-09-06 to 2021-09-24
Audit Location:	Zürich and Glattbrugg, Switzerland
Type of audit	☐ Point in time audit ☐ Period of time, after x month of CA operation ☒ Period of time, full audit

Standards considered	European Standards: ☒ ETSI EN 319 411-2, V2.3.1 (2021-05) ☒ ETSI EN 319 411-1, V1.3.1 (2021-05) ☒ ETSI EN 319 401, V2.3.1 (2021-05) CA Browser Forum Requirements: ☒ EV SSL Certificate Guidelines, version 1.8.0 ☒ Baseline Requirements, version 1.7.8 ☒ ETSI TS 119 403-2 V1.2.4 (2020-11) for the Trust Service Provider Conformity Assessment Browser Policy Requirements: ☒ Mozilla Root Store policy ☒ Microsoft Trusted Root Program ☒ Google Root Program ☒ Apple Root Store Program

Identification of the audited Root-CA:	SwissSign Platinum CA - G2	
	Distinguished Name	CN = SwissSign Platinum CA - G2 O = SwissSign AG C = CH
	SHA-256 fingerprint	3B222E566711E992300DC0B15AB9473DAFDEF8C84D0CEF7D3317B4C1821D1436
	Certificate Serial number	4EB200670C035D4F
	Applied policy	ETSI EN 319 411-1, policies NCP+; ETSI EN 319 411-2, policies QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd

The full annual audit was based on the following policy and practice statement documents of the TSP:

1. *SwissSign Platinum CP/CPS - Certificate Policy and Certification Practice Statement of the SwissSign Platinum CA and its subordinated issuing CA, version 3.10.0 as of 2021-06-14*

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

Findings with regard to ETSI EN 319 401:
5. Risk Assessment
The TSP shall improve its risk assessment.
The TSP shall improve the handling and resolution of singular risk factors.
6.3 Certificate Life-Cycle operational requirements
The TSP shall improve its access and authentication policy.
7.5 Cryptographic controls
The TSP shall improve the handling of its back-up HSMs.
7.8 Network security
The TSP shall perform the planned penetration tests.
7.10 Collection of evidence
The TSP shall improve the archiving of logged events.
The TSP shall improve the archiving and review of paper application.
7.11 Business Continuity Management
The Business Continuity Policy shall be improved.

Findings with regard to ETSI EN 319 411-1:
6.4 Facility, management, and operational controls
The TSP shall improve the processes of PKI key management.

All **major non-conformities** have been closed before the issuance of this attestation.

For all **minor non-conformities** listed above, 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 documented under

- Policy NCP-SMIME: Bug 1731586, SwissSign AG: Certificate with key length 16258: https://bugzilla.mozilla.org/show_bug.cgi?id=1731586
- Policy EVCP: Bug 1734131, SwissSign AG: wrong address in EV certificate: https://bugzilla.mozilla.org/show_bug.cgi?id=1734131
- Any Policy: Bug 1613334, SwissSign AG: Misissuance with mispellings in Location for a number of Certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1613334
- Any Policy: Bug 1551364, SwissSign AG: "Some-State" in stateOrProvinceName: https://bugzilla.mozilla.org/show_bug.cgi?id=1551364
- Any Policy: Bug 1670894, SwissSign AG: Invalid stateOrProvinceName field: https://bugzilla.mozilla.org/show_bug.cgi?id=1670894
- Any Policy: Bug 1671113, SwissSign AG: Failure to provide a preliminary report within 24 hours: https://bugzilla.mozilla.org/show_bug.cgi?id=1671113
- Any Policy: Bug 1691704, SwissSign AG: Certificate with key length 4098 bit: https://bugzilla.mozilla.org/show_bug.cgi?id=1691704
- Any Policy: Bug 1677737, SwissSign AG: duplicate serial number: https://bugzilla.mozilla.org/show_bug.cgi?id=1677737

The remediation measures taken by SwissSign AG as described on Bugzilla (see link above) have been accompanied by the auditors and showed to properly address the incident. The long-term effectiveness of the measures will be rechecked at the next regular 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. The TSP assured that all non-revoked Sub-CA that are technically capable of issuing server or email certificates and that have been issued by this Root-CA are in the scope of regular audits

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign Personal Platinum CA 2010 - G2, O = SwissSign AG, C = CH	275F8A75C02DECAC9DCC945C30C7F370EDF4E739B0CEA75652897B16D2BD75D7	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	Not defined
CN = SwissSign Personal Platinum CA 2014 - G22, O = SwissSign AG, C = CH	7C9CCF1733FD36AC3E3A9B179AB0C755FBB1421EB803596355C2ED5D03CD2765	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	Not defined
CN = SwissSign CH Person Platinum CA 2017 - G22, O = SwissSign AG, C = CH	3CC9509C0FBF0BBBFE2BAB0B4117811E95C58A37D7F6902DE67524A9FE07C040	ETSI EN 319 411-2, policies NCP+, QCP-l-qscd	Not defined
CN = SwissSign Qualified Platinum CA 2010 - G2, O = SwissSign AG, C = CH	B0B05D7131D7881F78BA4172B442B7D774D04FF27D383BE3E459A372473B1E15	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Not defined
CN = SwissSign Qualified Platinum CA G22 16-1, O = SwissSign AG, C = CH	0FAC8B71A8C979B861322C4B2AF21AE12A5196525AC2F079BD9268D816D2B6FC	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Not defined
CN = SwissSign CH Qualified Platinum CA 2017 - G22, O = SwissSign AG, C = CH	29CC90779084B25D2142AB1E9F52B6A4463765E86AB321C3293FEE51300E33B1	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Not defined
CN = SwissSign CH Qualified Platinum CA 2017 - G22 17-1, O = SwissSign AG, C = CH	78B08B7D449A53DEA551DBE9BEA5DD60FC7939C775535C018DFA24A3D9E9FFD7	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Not defined

CN = SwissSign TSA Platinum CA 2017 - G22, O = SwissSign AG, C = CH	8E510BD4177C10A22E70C18C7B917A1AF6679342A79CBD1B13129DB482A27444	ETSI EN 319 411-2, policy QCP-l-qscd (technically constrained)	Not defined
CN = SwissSign Advanced Platinum CA 2019 - G22, O = SwissSign AG, C = CH	9D7D1ABDDC9F23838B26C56B0A0FE6ADD5F0A6E398D8C0BCE712A438CE33B69B	ETSI EN 319 411-1, policy NCP+	Not defined
CN = SwissSign SuisseID Platinum CA 2010 - G2, O = SwissSign AG, C = CH	395995EF7D204CD7F7E67480E348766EFD93D5CDADC8DBE7DF5D4B39F5C32410	ETSI EN 319 411-1, policy NCP+	Not defined
CN = SwissSign SuisseID Platinum CA 2014 - G22, O = SwissSign AG, C = CH	122071FD4527C2997A2F8366A6D3CE12E085BD74199AC5133829F68F06E9832A	ETSI EN 319 411-1, policy NCP+	Not defined

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

Modifications record

Version	Issuing Date	Changes
Version 1	2021-12-15	initial attestation

End of the audit attestation letter.