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: AA2022113001

Your ref.:	**Your message from:**	**Our ref.:**	**Date:**
-	**-**	**TUV TRUST IT/wcl**	**2022-11-30**

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 “AA2022113001” and consist of 13 pages.
This audit attestation is issued based on the reports number TA235224002_SR, TA23524003_SR, TA235224004_SR, TA235224005_SR and TA235224006_SR. Predecessor is Audit Attestation letter AA2021112601 as of 2021-11-26 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:

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

	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; 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-109.357.012 (SwissSign AG)*

Audit Period covered for all policies:	2021-09-25 to 2022-09-24
Audit dates:	Stage 1: 2022-08-08 to 2022-08-26 Stage 2: 2022-08-30 to 2022-09-23
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, V2.4.1 (2021-11) ☒ 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 1.7.9 ☒ Baseline Requirements, version 1.8.4 ☒ ETSI TS 119 403-2 V1.2.4 (2020-11) 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 Gold CA – G2	

	Distinguished Name	CN = SwissSign Gold CA – G2
		O = SwissSign AG
		C = CH

	SHA-256 fingerprint	62DD0BE9B9F50A163EA0F8E75C053B1ECA57EA55C8688F647C6881F2C8357B95
	Certificate Serial number	BB401C43F55E4FB0
	Applied policy	*ETSI EN 319 411-1, policies EVCP, OVCP, NCP, DVCP, LCP*

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

1. *SwissSign CP EV - Certificate Policy for Extended Validation Certificates, version 2.0, as of 2022-08-15*
2. *SwissSign CP OV - Certificate Policy for Organization Validated Certificates, version 2.0, as of 2022-08-15*
3. *SwissSign CP DV – Certificate Policy for Organization Validated Certificates, version 2.0, as of 2022-08-15*
4. *SwissSign CP NCP - Certificate Policy according to Normalized Certificate Policy, version 2.0, as of 2022-08-15*
5. *SwissSign CP NCP extended - Certificate Policy according to Normalized Certificate Policy with extended EKU, version 2.0, as of 2022-08-15*
6. *SwissSign CP LCP - Certificate Policy Certificate Policy according to Lightweight Certificate Policy, version 2.0, as of 2022-08-15*
7. *SwissSign TSPS - Trust Services Practice Statement, version 4.0, as of 2022-07-18*
8. *SwissSign CPS TLS - Certification Practice Statement for TLS certificates“, version 4.0, as of 2022-07-01*
9. *SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, version 5.0, as of 2022-09-30*
10. *SwissSign CPS S/MIME - Certification Practice Statement for S/MIME certificates, version 4.0, as of 2022-11-07*
11. *SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME Certificates, version 5.0, as of 2022-11-07*

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.
6.1 Trust Service Practice statement
The TSP shall improve the documented representation of its services.
7.7 Operation security
The TSP shall improve its change management procedures.
7.8 Network security
The TSP shall improve its monitoring of system activities.
The TSP shall improve the regular execution of vulnerability scans for the Kubernetes containers.
7.10 Collection of evidence
The TSP shall improve the archiving of logged events.
The TSP shall improve the process of access rights assignment for the electronic archive.

Findings with regard to ETSI EN 319 411-1:
6.4 Facility, management, and operational controls
The TSP shall improve the oversight of objects to be archived.
The TSP shall improve the processes of PKI key management.
The TSP shall improve the transfer of logs to long-term archives.

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 LCP-SMIME: Bug 1766255, SwissSign: Mis-Issuance of S/MIME certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1766255
- Any Policy: Bug 1784881, SwissSign: Missed deadline of publication of 6 CPs and 1 CP/CPS: https://bugzilla.mozilla.org/show_bug.cgi?id=1784881

The remediation measures taken by SwissSign AG as described on Bugzilla (see links 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
1	CN = SwissSign RSA SMIME Root CA 2021 - 1, O = SwissSign AG, C = CH	BC8BBD7D279D2E5F070BCEF6FAF3AAB1BEF30DA3EB2875424295AD147F2AEF07	ETSI EN 319 411-1, NCP, LCP	Not defined
2	CN = SwissSign RSA TLS Root CA 2021 - 1, O = SwissSign AG, C = CH	4E5666DAC579161CF00B8D87046D074D6C9C0C0E3994C653BE57998736C55D93	ETSI EN 319 411-1, EVCP, OVCP, DVCP	Not defined
3	CN = SwissSign RSA SMIME Root CA 2022 - 1, O = SwissSign AG, C = CH	5A84C94054D340D650A29985EF97BB396352E215AED6C0B33CA7FFDD3BD5D2A2	ETSI EN 319 411-1, NCP, LCP	Not defined
4	CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH	288B4A9F605B09B999B215850825C81F9B537DBAF23664ACA98BF6BA98EDC379	ETSI EN 319 411-1, EVCP, OVCP, DVCP	Not defined

Table 1: Intermediate-CA issued by the Root-CA (includes x-signed root CA)

Distinguished Name	Issuing intermediate CA as of Table 1	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign RSA SMIME LCP ICA 2021 - 2, O = SwissSign AG, C = CH	1	5CFFA8DB135F913363ACEB7CE362D098F3C1EBD26C63C560C095381E896504FA	ETSI EN 319 411-1, LCP	E-mail Protection
CN = SwissSign RSA SMIME NCP extended ICA 2021 - 1, O = SwissSign AG, C = CH	1	0A6EEB87C2B4AC4A0DF4A68CA7E5244408E06A0CF3BE973156A52AAD835D7466	ETSI EN 319 411-1, NCP	TLS Web Client Authentication, E-mail Protection, Microsoft Encrypted File System, Microsoft Smartcard Login
CN = SwissSign RSA SMIME NCP ICA 2021 - 1, O = SwissSign AG, C = CH	1	1935AA544A73D755E913357FCE0E44AFC90E0809AC97A89964F0A90A59C376B6	ETSI EN 319 411-1, NCP	TLS Web Client Authentication, E-mail Protection
CN = SwissSign RSA TLS DV ICA 2021 - 1, O = SwissSign AG, C = CH	2	0E55D0985482BBB7C490EBA147C5A021A2C2A2089D3A8AF57D01EDD540CA5A45	ETSI EN 319 411-1, DVCP	TLS Web Server Authentication, TLS Web Client Authentication

CN = SwissSign RSA TLS OV ICA 2021 - 1, O = SwissSign AG, C = CH	2	B3679FDDDC644858B97DBB67DE778DD56C6E5D53A96B70E85AB509D09868186D	ETSI EN 319 411-1, OVCP	TLS Web Server Authentication, TLS Web Client Authentication
CN = SwissSign RSA TLS EV ICA 2021 - 1, O = SwissSign AG, C = CH	2	39CB199F41C6A82AAD83C2810127596D02CC4EC766D0DFE31B01D50D1774749F	ETSI EN 319 411-1, EVCP	TLS Web Server Authentication, TLS Web Client Authentication
CN = SwissSign RSA SMIME LCP ICA 2022 - 1, O = SwissSign AG, C = CH	3	D7F41FABE5A459BAC6882465C75CCFF2BAA52487AABC34706CAF2A18AC53A5C2	ETSI EN 319 411-1, LCP	E-mail Protection
CN = SwissSign RSA SMIME NCP ICA 2022 - 1, O = SwissSign AG, C = CH	3	99A56DD8DACA399FCA2E3834ED75760E96C133564062F8B530B355BED99A409D	ETSI EN 319 411-1, NCP	TLS Web Client Authentication, E-mail Protection
CN = SwissSign RSA SMIME NCP extended ICA 2022 - 1, O = SwissSign AG, C = CH	3	7196E86DCFDB92B0509213D806DCA2465FC41415A0B4069D35F946DE6813CF79	ETSI EN 319 411-1, NCP	TLS Web Client Authentication, E-mail Protection, Microsoft Encrypted File System, Microsoft Smartcard Login

CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	4	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1, DVCP	TLS Web Server Authentication, TLS Web Client Authentication
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	4	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1, OVCP	TLS Web Server Authentication, TLS Web Client Authentication
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	4	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1, EVCP	TLS Web Server Authentication, TLS Web Client Authentication

Table 2: CA issuing end entity certificates where the CA was issued by an Intermediate-CA

Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign EV Gold CA 2014 - G22, O = SwissSign AG, C = CH	A434AAE4E15A5519E9B111FD08EC190FD2ADF13BBE30815C6E1606555CB31450	ETSI EN 319 411, EVCP	Not defined
CN = SwissSign Personal Gold CA 2014 - G22, O = SwissSign AG, C = CH	77D6C2AF5A7B86F63D9918C87533779F2AF08D35CFA14DA4938C803F53DE18A1	ETSI EN 319 411, NCP	Not defined

CN = SwissSign Server Gold CA 2014 - G22
O = SwissSign AG
C = CH
	561DC78351F5E7EE5A464AC6E58A0D164EF2768F98F02E6EE65501120FCD9C5E	ETSI EN 319 411, OVCP	Not defined

CN = SwissSign Server Gold CA 2008 - G2
O = SwissSign AG
C = CH
	FD2991B134CE57BF9CD686878854A5EED5EA64433002452BA40398DA78845CA7	ETSI EN 319 411-1, OVCP	Not defined

CN = SwissSign Personal Gold CA 2008 - G2
O = SwissSign AG
C = CH
	2B65E45EA181C1CC21B1CC9E9FB1E10F54129432BB78973F608C66A4151FBF0E	ETSI EN 319 411-1, NCP	Not defined

Table 3: CA issuing end entity certificates issued by the Root-CA

Modifications record

Version	Issuing Date	Changes
Version 1	2022-11-30	initial attestation

End of the audit attestation letter.