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

Root: SwissSign Silver CA - G2

Reference: AA2020112503

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2020-12-17

To whom it may concern,

This is to confirm that TUV AUSTRIA CERT has successfully audited the CA of the "SwissSign AG, Silver CA – G2" without critical findings.

This present Audit Attestation letter is registered under the unique identifier number "AA2020112503" and consist of 5 pages. This audit attestation is issued based on the reports number TA235203363_SR and TA235203364_SR. Predecessor is Audit Attestation letter AA2019121903 as of 2019-12-19 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

Identification of the conformity assessment body (CAB):	*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://www.bmdw.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.bmdw.gv.at/dam/jcr:ffe6b296-8c4c-4977-80de-d2566942a715/AA_0943_17065_TUEV_AUSTRIA_CERT_GMBH.pdf

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:	2019-09-28 to 2020-09-25
Audit dates:	2020-05-04 to 2020-05-15 (remote) 2020-08-31 to 2020-09-03 (onsite in Zürich) 2020-09-25 (onsite in Zürich)
Audit Location:	Zürich

[1] Identification of the accredited conformity assessment body (CAB), in the following termed shortly „*CAB*“

[2] *URL to the accreditation certificate hosted by the national accreditation body*

Identification of the audited Root-CA:	SwissSign Silver CA - G2	
	Distinguished Name	CN = SwissSign Silver CA - G2 O = SwissSign AG C = CH
	SHA-256 fingerprint	BE6C4DA2BBB9BA59B6F3939768374246C3C005993FA98F020D1DEDBED48A81D5
	Certificate Serial number	4F1BD42F54BB2F4B
	Applied policy	ETSI EN 319 411-1, policies LCP, DVCP

The audit was performed as full annual audit at the TSP's location in *Zürich (Glattbrugg), Switzerland* as well as remote for parts where remote audit was possible. During the remote session general parts as human resources, information security policy and procedures as well risk management were covered. Furthermore, the certificate application verification processes were audited. During the onsite inspection, all aspects regarding physical security of data centre, RA premises, site environment, as well as key management (storage, protection and usage within certified HSM) of the Root and Issuing CA, the network and system security aspects were covered.
The certificates issued and the related records were audited for the whole audit period from 2019-09-28 until 2020-09-25 for all policies.

The audit was performed according to the applicable European Standards *"ETSI EN 319 411-1, V1.2.2 (2018-04)" and "ETSI EN 319 401, V2.2.1 (2018-04)"* as well as CA Browser Forum Requirements *"Baseline Requirements, version 1.7.2"* considering the requirements of *"ETSI EN 319 403, V2.2.2 (2015-08) and "ETSI EN 319 403-1, V2.3.1 (2020-06) for the Trust Service Provider Conformity Assessment"* as well as "*ETSI TS 119 403-2, V1.2.4 (2020-11), Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates*".

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

1. *"Certificate Policy and Certification Practice Statement of the SwissSign Silver CA and its subordinated issuing CA",*
   OID: 2.16.756.1.89.1.3.1.13, Version: 3.8.0 as of 2020-11-17
2. *"PKI Disclosure Statement Certificate Services",*
   OID: 2.16.756.1.89.1.0.6.0.1, Version: 1.0 as of 2017-07-14
3. "Subscriber Agreement Certificate Services",
   OID: 2.16.756.1.89.1.0.2.0.2, Version: 2.0 as of 2020-06-24
4. "Relying Party Agreement",
   OID: 2.16.756.1.89.1.0.5.0.1, Version: 1.0 as of 2017-07-14

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

Findings with regard to ETSI EN 319 401:

7 TSP management and operation
7.2 Human resources
Documentation and implementation of the yearly training plan were required to be improved.
7.4 Access control
Documentation and implementation of access rights for the new M-PKI application were required to be improved.
7.8 Network security
Documentation and implementation of network migration were required to be improved.
Documentation and implementation of penetration tests were required to be improved.
Documentation of vulnerability scans was required to be improved.
7.9 Incident management
Documentation of implementation of incident management was required to be improved.
7.10 Collection of evidence
Documentation and implementation of internal archives were required to be improved.

Findings with regard to ETSI EN 319 411-1/2:

6.4 Facility, management, and operational controls
Documentation of CCTV records review for the data center was required to be improved.
6.5 Technical security controls
Documentation and implementation of IDS/IPS were required to be improved.
6.6 Certificate, CRL, and OCSP profiles
Documentation and implementation of the certificate profiles for the OU field was required to be improved.

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, 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

- Any Policy: Bug *1662137, SwissSign AG: OCSP responder unreachable:* https://bugzilla.mozilla.org/show_bug.cgi?id=1662137
- Any Policy: *Bug 1613406, SwissSign AG : Delayed revocation for mispellings in Location for a number of Certificates:* https://bugzilla.mozilla.org/show_bug.cgi?id=1613406
- Any Policy: Bug *1636141, SwissSign AG: failure to provide a preliminary report within 24 hours:* https://bugzilla.mozilla.org/show_bug.cgi?id=1636141
- Policy DVCP: Bug *1636140, SwissSign AG: duplicate serial number:* https://bugzilla.mozilla.org/show_bug.cgi?id=1636140

- Any Policy: Bug *1614450, SwissSign AG: Audit Letter Validation failures on intermediate certificates:* https://bugzilla.mozilla.org/show_bug.cgi?id=1614450
- Any Policy: Bug *1558552, SwissSign AG: CP/CPS certificate profile issue:* https://bugzilla.mozilla.org/show_bug.cgi?id=1558552

The remediation measures taken by SwissSign 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
CN = SwissSign Personal Silver CA 2014 - G22, O = SwissSign AG, C = CH	C9E40F4E83396F34A7C861817B4EDAB3DC1F8BAC699FD50CB261FA9123D55EF4	ETSI EN 319 411-1, policy LCP	none
CN = SwissSign Personal Silver CA 2008 - G2, O = SwissSign AG, C = CH	FA397DE8DB6F110A7FA34D101BAC8A914750F53B0223A8BD2FB812E757155C20	ETSI EN 319 411-1, policy LCP	none
CN = SwissSign Server Silver CA 2014 - G22, O = SwissSign AG, C = CH	67F91F26F5BFBFA48738BE0678DD2F8F75F7B80761D5656783CA8B920AAA5659	ETSI EN 319 411-1, policy DVCP	none
CN = SwissSign Server Silver CA 2008 - G2, O = SwissSign AG, C = CH	06E5DEC31C91D7D33435201D2E22116C207193A874E0A426532A2F69530C86B5	ETSI EN 319 411-1, policy DVCP	none

Table 1: Sub-CA issued by the Root-CA

Modifications record

Version	Issuing Date	Changes
Version 1.1	2020-12-17	Re-formated dates and SHA256 to address errors from AVL (no change in content)
Version 1	2020-11-25	Initial attestation

End of the audit attestation letter