TÜV AUSTRIA CERT GMBH

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

Business Area
Life, Training & Certification Austria

Certification Body

TÜV ®

Audit Attestation for SwissSign AG

Root: SwissSign Silver CA - G2

Reference: AA2019121903

Your ref.:	Your message from:	Our ref.:	Date:
-	-	**TUV TRUST IT/wcl**	**2019-12-19**

To whom it may concern,

This is to confirm that TUV AUSTRIA CERT has successfully audited the CAs of the “SwissSign AG, Silver CA - G2” without critical findings.

This present Audit Attestation letter is registered under the unique identifier number “AA2019121903” and consist of 6 pages. This audit attestation is issued based on the reports TA606182879_SRS and TA606182880_SRS. Predecessor is Audit Attestation letter AA2018122003 as of 2018-12-20 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. i.V.

Certification Body

Managing director:
Rob Bekkers, MSc, BSc
Yiannis Kallias, 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

This template (version 2.0 as of 2018-03-05) was created by TÜViT and LSTI and approved for use by ACAB-c. It may only be used to without modification.

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 and ETSI EN 319 403. 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. Timo Schmitt* *E-Mail: timo.schmitt@swisssign.com* *Company registration: CHE-403.679.996, CHE-109.357.012 (SwissSign Ltd.)*

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

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

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

This template (version 2.0 as of 2018-03-05) was created by TÜViT and LSTI and approved for use by ACAB-c. It may only be used to without modification.

The audit was performed as full annual audit at the TSP's location in *Zurich, Switzerland*. It took place from *2019-09-23* until *2019-10-02* and covered the period from *2018-09-28* until *2019-09-27* 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)" and "Baseline Requirements, version 1.6.6"* considering the requirements of the *"ETSI EN 319 403, V2.2.2 (2015-08) for the Trust Service Provider Conformity Assessment"* as well as "*ETSI TS 119 403-2, V1.2.1 (2019-04), 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: 2.16.756.1.89.1.3.1.12, Version: 3.7.0 as of 2019-11-25
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 2017-07-14
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 Non-Conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

5. Risk Assessment
Documentation of the risk management was required to be improved.
6.3 Information security policy
Documentation and implementation of the access control mechanisms were required to be improved.
7 TSP management and operation
7.3 Asset management
Documentation of the asset register was required to be improved.
7.8 Network security
Documentation and implementation of pentesting was required to be improved.
Documentation and implementation of vulnerability scanning was required to be improved.
7.9 Incident management
Documentation and implementation of info logging was required to be improved.

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

6.2 Identification and authentication
Documentation and implementation of the managed PKI scheme was required to be improved.
Documentation of the CRL policy was required to be improved.
Documentation and implementation of the re-validation procedure was required to be improved.
6.3 Certificate Life-Cycle operational requirements
Documentation and implementation of the certificate profiles was required to be improved.
Documentation of the procedures for renewal and modification was required to be improved.
6.4 Facility, management, and operational controls
Documentation and implementation of the system specific logging was required to be improved.
6.5 Technical security controls
Documentation of specific security modules in use was required to be improved.
Documentation and implementation of the IDS and IPS was required to be improved.
6.6 Certificate, CRL, and OCSP profiles
Documentation and implementation of the MPKI XP profiles was required to be improved.

All Non-Conformities listed above were remediated by the TSP before the issuance of this Audit Attestation.

This template (version 2.0 as of 2018-03-05) was created by TÜViT and LSTI and approved for use by ACAB-c. It may only be used to without modification.

This Audit Attestation also covers the following incident as documented under

- Any policy: Bug 1558552, SwissSign: SwissSign: CP/CPS certificate profile issue: https://bugzilla.mozilla.org/show_bug.cgi?id=1558552.
- Any policy: Bug 1455132, SwissSign: Undisclosed Intermediate Certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1455132.

The remediation measures taken by SwissSign 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 subordinated issuing-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 subordinated issuing-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.

This template (version 2.0 as of 2018-03-05) was created by TÜViT and LSTI and approved for use by ACAB-c. It may only be used to without modification.

Identification of the CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy OID	Service	EKU	Validy
SwissSign Personal Silver CA 2008 - G2	CN = SwissSign Personal Silver CA 2008 - G2 O = SwissSign AG C = CH	FA397DE8DB6F110A7FA34D101BAC8A914750F53B0223A8BD2FB812E757155C20	00E256B753976B7658	*ETSI EN 319 411-1, policy LCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	09 Jul 2008 11:11:09 GMT to 09 Jul 2023 11:11:09 GMT
SwissSign Personal Silver CA 2014 - G22	CN = SwissSign Personal Silver CA 2014 - G22 O = SwissSign AG C = CH	C9E40F4E83396F34A7C861817B4EDAB3DC1F8BAC699FD50CB261FA9123D55EF4	0544D64EAD1ED336D532405D00B936	*ETSI EN 319 411-1, policy LCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	19 Sep 2014 20:36:49 GMT to 15 Sep 2029 20:36:49 GMT
SwissSign Server Silver CA 2008 - G2	CN = SwissSign Silver CA - G2 O = SwissSign AG C = CH	06E5DEC31C91D7D33435201D2E22116C207193A874E0A426532A2F69530C86B5	009D154E306A8BA0CE	*ETSI EN 319 411-1, policy DVCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	07 Jul 2008 17:07:16 GMT to 07 Jul 2023 17:07:16 GMT
SwissSign Server Silver CA 2014 - G22	CN = SwissSign Server Silver CA 2014 - G22 O = SwissSign AG C = CH	67F91F26F5BFBFA48738BE0678DD2F8F75F7B80761D5656783CA8B920AAA5659	6BC318C92ACD1763EB41C86FAF47F7	*ETSI EN 319 411-1, policy DVCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	19 Sep 2014 20:36:43 GMT to 15 Sep 2029 20:36:43 GMT

Table 1: Subordinated issuing-CA issued by the Root-CA

This template (version 2.0 as of 2018-03-05) was created by TÜViT and LSTI and approved for use by ACAB-c. It may only be used to without modification.

Modifications record

Version	Issuing Date	Changes
Version 1	2019-12-19	initial attestation
Version 1.1	2019-12-19	correction audit period

End of the attestation

This template (version 2.0 as of 2018-03-05) was created by TÜViT and LSTI and approved for use by ACAB-c. It may only be used to without modification.