TÜV AUSTRIA

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

Reference: AA2018122003

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2018-12-20

To whom it may concern,

This is to confirm that TUV AUSTRIA CERT has successfully audited the CAs of "SwissSign" without critical findings.

This present Audit Attestation letter is registered under the unique identifier number AA2018122003 and consist of 5 pages. Predecessor is Audit Attestation letter AA2018070303_V2 as of 2018-09-18.

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 Vienna/Austria

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 and ETSI EN 319 403. URL to accreditation[2]: https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/AA_0943_17065_TUEV_AUSTRIA_CERT_GMBH.pdf

Identification of the trust service provider (TSP):	*SwissSign AG* *Sägereistraße 25* *CH-8152 Glattbrugg, Schwitzerland* *Contact: Mr. Michael Günther* *E-Mail: michael.guenther@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	be 6c 4d a2 bb b9 ba 59 b6 f3 93 97 68 37 42 46 c3 c0 05 99 3f a9 8f 02 0d 1d ed be d4 8a 81 d5
	Certificate Serial number	4f 1b d4 2f 54 bb 2f 4b
	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*

The audit was performed as full annual audit at the TSP's location in Zurich, Switzerland. It took place from September, 24th to September, 28th 2018 and covered the period from June, 7th until September 28th, 2018 for all policies. The audit was performed according to the applicable European Standards ETSI EN 319 411-1, V1.2.2 (2018-04), ETSI EN 319 401, V2.2.1 (2018-04), CA/B-Forum Requirements: EV SSL Certificate Guidelines, V1.6.8, Baseline Requirements, V1.6.0, under consideration of ETSI EN 319 403, V2.2.2 (2015-08) as guidelines for general Trust Service Provider Conformity Assessment.

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

1. "SwissSign Silver CP/CPS, Certificate Policy and Certification Practice Statement of the SwissSign Silver CA and its subordinated issuing CA", OID: 2.16.756.1.89.1.3.1.11, Version: 3.6.0 as of December 17th, 2018
2. "SwissSign, PKI Disclosure Statement Certificate Services",
   OID: 2.16.756.1.89.1.0.6.0.1, Version: 1.0 as of July 14th, 2017
3. "SwissSign, Subscriber Agreement Certificate Services",
   OID: 2.16.756.1.89.1.0.2.0.2, Version 1.01 as of November 20th, 2018
4. "SwissSign, Relying Party Agreement",
   OID: 2.16.756.1.89.1.0.5.0.1, Version: 1.0 as of July 14th, 2017

No Major Non-Conformities have been identified throughout the audit.
In the following areas minor Non-Conformities have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7.2 Human resources
Documentation and/or implementation of the training and role concept shall be improved.
7.4 Access control
Documentation and implementation physical system access control measures shall be improved.
7.8 Network security
Documentation and/or implementation of regular pentesting shall be improved.

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

6.2 Identification and authentication
Documentation and/or implementation of certificate application shall be improved.
6.5 Technical security controls
Documentation and/or implementation of user authentication shall be improved.
6.9 Other provisions
Documentation and/or implementation of test certificate provisioning shall be improved.

All Minor Non-Conformities have been scheduled to be remediated within three month after the onsite audit and will be covered by a corresponding audit.

This Audit Attestation also covers the following incident as documented under

- Policy DVCP: Bug 1473971, SwissSign: "*Domain validated certificate but with stateOrProvinceName"* on: https://bugzilla.mozilla.org/show_bug.cgi?id=1473971.
- 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 longterm effectiveness of the measures will be rechecked at the next regular audit.

The Sub-CAs 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 SubCA's 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.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy OID	Service	EKU	Validy
SwissSign Personal Silver CA 2014 - G22	CN = SwissSign Personal Silver CA 2014 - G22 O = SwissSign AG C = CH	c9 e4 0f 4e 83 39 6f 34 a7 c8 61 81 7b 4e da b3 dc 1f 8b ac 69 9f d5 0c b2 61 fa 91 23 d5 5e f4	05 44 d6 4e ad 1e d3 36 d5 32 40 5d 00 b9 36	ETSI EN 319 411-1, policy LCP	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 19/09/2014 20:36:49 GMT to UTCTime 15/09/2029 20:36:49 GMT
SwissSign Server Silver CA 2014 - G22	CN = SwissSign Server Silver CA 2014 - G22 O = SwissSign AG C = CH	67 f9 1f 26 f5 bf bf a4 87 38 be 06 78 dd 2f 8f 75 f7 b8 07 61d5 65 67 83 ca 8b 92 0a aa 56 59	6b c3 18 c9 2a cd 17 63 eb 41 c8 6f af 47 f7	ETSI EN 319 411-1, policy DVCP	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 19/09/2014 20:36:43 GMT to UTCTime 15/09/2029 20:36:43 GMT
SwissSign Personal Silver CA 2008 - G2	CN = SwissSign Personal Silver CA 2008 - G2 O = SwissSign AG C = CH	fa 39 7d e8 db 6f 11 0a 7f a3 4d 10 1b ac 8a 91 47 50 f5 3b 02 23 a8 bd 2f b8 12 e7 57 15 5c 20	00 e2 56 b7 53 97 6b 76 58	ETSI EN 319 411-1, policy LCP	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 09/07/2008 11:11:09 GMT to UTCTime 09/07/2023 11:11:09 GMT
SwissSign Server Silver CA 2008 - G2	CN = SwissSign Server Silver CA 2008 - G2 O = SwissSign AG C = CH	06 e5 de c3 1c 91 d7 d3 34 35 20 1d 2e 22 11 6c 20 71 93 a8 74 e0 a4 26 53 2a 2f 69 53 0c 86 b5	00 9d 15 4e 30 6a 8b a0 ce	ETSI EN 319 411-1, policy DVCP	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 07/07/2008 17:07:16 GMT to UTCTime 07/07/2023 17:07:16 GMT

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

Modifications record

Version	Issuing Date	Changes
Version 1	2018-12-20	initial attestation

End of the audit attestation letter.