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: AA2018122001

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 AA2018122001 and consist of 5 pages. Predecessor is Audit Attestation letter AA2018070301_V2 as of 2018-09-18 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 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 Platinum CA - G2	
	Distinguished Name	CN = SwissSign Platinum CA - G2 O = SwissSign AG C = CH
	SHA-256 fingerprint	3b 22 2e 56 67 11 e9 92 30 0d c0 b1 5a b9 47 3d af de f8 c8 4d 0c ef 7d 33 17 b4 c1 82 1d 14 36
	Certificate Serial number	4e b2 00 67 0c 03 5d 4f
	Applied policy	ETSI EN 319 411-1, policy NCP+; ETSI EN 319 411-2, policies QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd

[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 319 411-2, V2.2.2 (2018-04), 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 Platinum CP/CPS, Certificate Policy and Certification Practice Statement of the SwissSign Platinum CA and its subordinated issuing CA", OID: 2.16.756.1.89.1.1.1.1.9, 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 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 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 cryptographic algorithms being used shall be improved.
Documentation and/or implementation of subscriber information 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.

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 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.
It has been verified during the audit that SubCA according to policies QCP-n or QCP-l issue person certificates only but no SSL certs.
It has been verified during the audit that SubCA according to time stamping policies issue TSA certificates only but no time stamps and no SSL certs.

Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy OID	Service	EKU	Validy
SwissSign Qualified Platinum CA 2010 - G2	CN = SwissSign Qualified Platinum CA 2010 - G2 O = SwissSign AG C = CH	b0 b0 5d 71 31 d7 88 1f 78 ba 41 72 b4 42 b7 d7 74 d0 4f f2 7d 38 3b e3 e4 59 a3 72 47 3b 1e 15	00 ab 32 cd bc 59 94 23 04 fa 6d 84 e4 0d bd	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 06/04/2010 14:03:34 GMT to UTCTime 02/04/2025 14:03:34 GMT
SwissSign PSS Qualified Platinum CA 2013 - G2	CN = SwissSign PSS Qualified Platinum CA 2013 - G2 O = SwissSign AG C = CH	a6 36 26 b4 94 ac 3f 6b b5 9c 9a 51 03 30 7a e3 6d 0d 5c a6 e0 cb b6 e3 c4 fb 95 d0 8c fa c5 f2	00 bf 27 4b 8e b1 e4 8a 27 17 86 5d d8 51 09 5d	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 09/12/2013 08:52:36 GMT to UTCTime 05/12/2028 08:52:36 GMT
SwissSign Personal Platinum CA 2014 - G22	CN = SwissSign Personal Platinum CA 2014 - G22 O = SwissSign AG C = CH	7c 9c cf 17 33 fd 36 ac 3e 3a 9b 17 9a b0 c7 55 fb b1 42 1e b8 03 59 63 55 c2 ed 5d 03 cd 27 65	00 c7 9b 99 00 92 1a 42 3a b1 d1 5b 5d f7 21 a4	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 15/09/2014 16:21:16 GMT to UTCTime 11/09/2029 16:21:16 GMT
SwissSign Qualified Platinum CA G22 16-1	CN = SwissSign Qualified Platinum CA G22 16-1 O = SwissSign AG C = CH	0f ac 8b 71 a8 c9 79 b8 61 32 2c 4b 2a f2 1a e1 2a 51 96 52 5a c2 f0 79 bd 92 68 d8 16 d2 b6 fc	5b 24 00 36 4e 9d 95 f3 e8 70 11 8a bd 7d 09	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 13/09/2016 08:51:42 GMT to UTCTime 10/09/2031 08:51:42 GMT
SwissSign CH Qualified Platinum CA 2017 - G22	2.5.4.97 = NTRCH-CHE-109.357.012 CN = SwissSign CH Qualified Platinum CA 2017 - G22 O = SwissSign AG C = CH	29 cc 90 77 90 84 b2 5d 21 42 ab 1e 9f 52 b6 a4 46 37 65 e8 6a b3 21 c3 29 3f ee 51 30 0e 33 b1	00 b8 df 83 70 fa a5 4e 76 c0 88 63 5a 89 bd ae	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 18/12/2017 06:31:59 GMT to UTCTime 18/12/2032 06:31:59 GMT
SwissSign TSA Platinum CA 2016 - G22	CN = SwissSign TSA Platinum CA 2016 - G22 O = SwissSign AG C = CH	b0 c2 af 82 f2 c1 58 e8 7f 61 17 23 e6 24 a1 08 36 d5 ad 3e 42 4a 18 da d2 ae 24 fd e5 a9 e3 94	00 f3 c2 c3 11 28 84 29 c5 6f b6 fd d5 a1 83 f3	ETSI EN 319 411-2, policy QCP-l-qscd (technically constrained)	Certificate Signing, Off-line CRL Signing, CRL Signing, Time Stamping	Zeitstempel (1.3.6.1.5.5.7.3.8)	from UTCTime 19/12/2016 12:46:39 GMT to UTCTime 16/12/2031 12:46:39 GMT

SwissSign TSA Platinum CA 2017 - G22	2.5.4.97 = NTRCH-CHE-109.357.012 CN = SwissSign TSA Platinum CA 2017 - G22 O = SwissSign AG C = CH	8e 51 0b d4 17 7c 10 a2 2e 70 c1 8c 7b 91 7a 1a f6 67 93 42 a7 9c bd 1b 13 12 9d b4 82 a2 74 44	64 4f be 61 79 2d d4 67 bb 20 79 76 70 10 96	ETSI EN 319 411-2, policy QCP-l-qscd (technically constrained)	Certificate Signing, Off-line CRL Signing, CRL Signing, Time Stamping	Zeitstempel (1.3.6.1.5.5.7.3.8)	from UTCTime 14/02/2017 08:29:17 GMT to UTCTime 15/02/2032 08:29:17 GMT
SwissSign CH Person Platinum CA 2017 - G22	2.5.4.97 = NTRCH-CHE-109.357.012 CN = SwissSign CH Person Platinum CA 2017 - G22 O = SwissSign AG C = CH	3c c9 50 9c 0f bf 0b bb fe 2b ab 0b 41 17 81 1e 95 c5 8a 37 d7 f6 90 2d e6 75 24 a9 fe 07 c0 40	64 56 cf 80 f9 c7 a0 33 54 37 f5 37 25 07 05	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 18/12/2017 06:25:36 GMT to UTCTime 18/12/2032 06:25:36 GMT
SwissSign CH Qualified Platinum CA 2017 - G22 17-1	2.5.4.97 = NTRCH-CHE-109.357.012 CN = SwissSign CH Qualified Platinum CA 2017 - G22 17-1 O = SwissSign AG C = CH	78 b0 8b 7d 44 9a 53 de a5 51 db e9 be a5 dd 60 fc 79 39 c7 75 53 5c 01 8d fa 24 a3 d9 e9 ff d7	00 f5 88 9e 21 88 61 17 e2 55 d6 45 81 05 56 f8	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 18/12/2017 06:29:55 GMT to UTCTime 18/12/2032 06:29:55 GMT
SwissSign SuisseID Platinum CA 2010 - G2	CN = SwissSign SuisseID Platinum CA 2010 - G2 O = SwissSign AG C = CH	39 59 95 ef 7d 20 4c d7 f7 e6 74 80 e3 48 76 6e fd 93 d5 cd ad c8 db e7 df 5d 4b 39 f5 c3 24 10	00 d5 cb 89 c2 93 00 9b ed bd 01 4b dc 10 96 02	ETSI EN 319 411-1, policy NCP+	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 08/03/2010 14:05:04 GMT to UTCTime 04/03/2025 14:05:04 GMT
SwissSign SuisseID Platinum CA 2014 - G22	CN = SwissSign SuisseID Platinum CA 2014 - G22 O = SwissSign AG C = CH	12 20 71 fd 45 27 c2 99 7a 2f 83 66 a6 d3 ce 12 e0 85 bd 74 19 9a c5 13 38 29 f6 8f 06 e9 83 2a	00 e2 a3 67 dd b9 88 19 40 a8 48 5e 55 41 a9 fd	ETSI EN 319 411-1, policy NCP+	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 15/09/2014 16:23:36 GMT to UTCTime 11/09/2029 16:23:36 GMT
SwissSign Personal Platinum CA 2008 - G2	CN = SwissSign Personal Platinum CA 2008 - G2 O = SwissSign AG C = CH	19 bc ac 81 38 c5 dd b8 aa 87 2d 7e 1f 10 27 d0 84 6a ef c4 51 ea d2 2e 30 78 3e cf cd e8 9f b7	00 91 c4 ec 3c 7c 7d 60 55	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 07/07/2008 16:51:19 GMT to UTCTime 07/07/2023 16:51:19 GMT
SwissSign Personal Platinum CA 2010 - G2	CN = SwissSign Personal Platinum CA 2010 - G2 O = SwissSign AG C = CH	27 5f 8a 75 c0 2d ec ac 9d cc 94 5c 30 c7 f3 70 ed f4 e7 39 b0 ce a7 56 52 89 7b 16 d2 bd 75 d7	00 a6 40 43 97 01 13 67 56 7b ca 96 06 7a 54 ed	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 05/07/2010 12:13:35 GMT to UTCTime 01/07/2025 12:13:35 GMT

SwissSign Qualified Platinum CA 2008 – G2	CN = SwissSign Qualified Platinum CA 2008 – G2 O = SwissSign AG C = CH	a4 93 c5 87 f7 1e 88 6a 03 ad 1d 5d 61 36 71 df da 07 db d8 90 8e 29 1e 19 51 4e 55 22 24 9b 49	00 24 3e 11 3b 43 a8 96 8b	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	UTCTime 07/07/2008 16:59:30 GMT to UTCTime 07/07/2023 16:59:30 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.