

Audit Attestation for SwissSign AG

Reference: AA2018070302_V2

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2018-09-18

To whom it may concern,

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

This Audit Attestation is an update of Audit Attestation AA2018070302 as of 2018-07-03 in order to document

- the formal completion of the accreditation of TÜV AUSTRIA CERT (see Accreditation section, page 2 of this document)
- the audit period for the SwissSign Platinum Root CA - G3 as stated on page 3 of this document as well as
- new contact person of the TSP.

No other statements have been edited compared to the Attestation AA2018070302.

This present Audit Attestation letter is registered under the unique identifier number AA2018070302_V2 and consist of 5 pages.

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>

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 BKAUATWWIBAN
AT37310000104093274
BIC RZBAATWWUID ATU63247169
DVR 3002477

With best regards,



i.A.



i.V.

Audit Attestation

Audit Attestation SwissSign - AA2018070302_V2



Identification of the conformity assessment body (CAB):	<p><i>TÜV AUSTRIA CERT GmbH¹</i> <i>TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge,</i> Company registration: Vienna / Wien / FN 288474 b</p> <p>Accreditation Body: Federal Ministry for Digital and Economic Affairs 1010 Wien, Stubenring 1 mailto: akkreditierung@bmdw.gv.at https://www.bmdw.gv.at/</p> <p>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 accreditation²: https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/AA_0943_17065_TUEV_AUSTRIA_CERT_GMBH.pdf</p>								
Identification of the trust service provider (TSP):	<p><i>SwissSign AG</i> <i>Sägereistraße 25</i> <i>CH-8152 Glattbrugg, Switzerland</i> <i>Contact: Mr. Michael Günther</i> <i>Company registration: CHE-403.679.996,</i> <i>CHE-109.357.012 (SwissSign Ltd.)</i></p>								
Identification of the audited Root-CA:	SwissSign Platinum Root CA – G3								
	<table border="1"><tr><td>Distinguished Name</td><td>CN = SwissSign Platinum Root CA - G3 O = SwissSign AG C = CH</td></tr><tr><td>SHA-256 fingerprint</td><td>59 b3 82 9f 1f f4 43 34 49 58 fa e8 bf f6 21 b6 84 c8 48 cf bf 7e ad 6b 63 a6 ca 50 f2 79 4f 89</td></tr><tr><td>Certificate Serial number</td><td>22 3f a9 17 20 de 81 94</td></tr><tr><td>Applied policy</td><td>ETSI EN 319 411-1, policy NCP+, ETSI EN 319 411-2, policies QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd; QCP-w</td></tr></table>	Distinguished Name	CN = SwissSign Platinum Root CA - G3 O = SwissSign AG C = CH	SHA-256 fingerprint	59 b3 82 9f 1f f4 43 34 49 58 fa e8 bf f6 21 b6 84 c8 48 cf bf 7e ad 6b 63 a6 ca 50 f2 79 4f 89	Certificate Serial number	22 3f a9 17 20 de 81 94	Applied policy	ETSI EN 319 411-1, policy NCP+, ETSI EN 319 411-2, policies QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd; QCP-w
Distinguished Name	CN = SwissSign Platinum Root CA - G3 O = SwissSign AG C = CH								
SHA-256 fingerprint	59 b3 82 9f 1f f4 43 34 49 58 fa e8 bf f6 21 b6 84 c8 48 cf bf 7e ad 6b 63 a6 ca 50 f2 79 4f 89								
Certificate Serial number	22 3f a9 17 20 de 81 94								
Applied policy	ETSI EN 319 411-1, policy NCP+, ETSI EN 319 411-2, policies QCP-n, QCP-l, QCP-n-qscd, QCP-l-qscd; QCP-w								

¹ in the following termed shortly „CAB“

² URL to the accreditation certificate hosted by the national accreditation body

Audit Attestation

Audit Attestation SwissSign - AA2018070302_V2



The audit was performed as full annual audit at the TSP's location in Zurich, Switzerland. It took place from May, 14th to May, 17th 2018 and June, 5th to June, 6th 2018 and covered the period from March, 9th 2017 until June, 6th 2018 for all policies. The Root CA and Sub CA addressed do not yet issue certificates to end entities. Despite of that, this audit has been performed as period of time audit at SwissSign covering all other relevant processes and parts of the infrastructure over time for the Root CA and all CA mentioned in the following table. 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, V1.5.8, 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: 2.16.756.1.89.1.1.1.1.7, Version: 3.4.0 as of June, 28st 2018
2. "SwissSign Liechtenstein Platinum CP/CPS, Certificate Policy and Certification Practice Statement of the SwissSign Platinum CA and its subordinated issuing CA", OID: 2.16.756.1.89.1.1.7.1.2, Version: 2.0.0 as of June, 28st 2018
3. "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
4. "SwissSign, Subscriber Agreement Certificate Services", OID: 2.16.756.1.89.1.0.2.0.2, Version: 1.0 as of July, 14th 2017
5. "SwissSign, Relying Party Agreement", OID: 2.16.756.1.89.1.0.5.0.1, Version: 1.0 as of July, 14th 2017

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.

It has been verified during the audit that SubCA according to policies QCP-n or QCP-I 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.

Audit Attestation

Audit Attestation SwissSign - AA2018070302_V2



Identification of the Sub-CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy OID	Service	EKU	Validy
SwissSign CH Platinum Person CA 2017 - G3	2.5.4.97 = NTRCH-CHE-109.357.012 CN = SwissSign CH Platinum Person CA 2017-G3 O = SwissSign AG C = CH	c6 0c 8b 1c 12 43 3c 0a e3 97 ce 70 21 93 52 83 0a 75 11 7e 75 00 e3 98 82 f6 b2 9c ab c1 bd 04	00 E8 27 FC 67 2C C0 D0 F1 DF D4 C5 49 DB AA B2	ETSI EN 319 411-2, policies QCP-I, QCP-I-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 14/12/2017 14:31:36 GMT to UTCTime 14/12/2032 14:31:36 GMT
SwissSign CH Platinum Qualified CA 2017 - G3	2.5.4.97 = NTRCH-CHE-109.357.012 CN = SwissSign CH Platinum Qualified CA 2017 - G3 O = SwissSign AG C = CH	6c e7 36 e6 da f6 bf 05 24 d8 41 71 98 1f 83 f8 74 9d a8 9e 80 df 3b 31 de a0 45 9e d9 01 cb 3a	00 93 33 E9 DB FA E1 69 E8 5B 37 4F 47 87 4B 55	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 22/11/2017 06:37:04 GMT to UTCTime 22/11/2032 06:37:04 GMT
SwissSign LI Platinum Person CA 2017 - G3	2.5.4.97 = NTRL-FL-0002.523.017-8 CN = SwissSign LI Platinum Person CA 2017 - G3 O = SwissSign AG C = LI	d1 b3 e1 66 d4 28 c3 29 21 8a 8f 5b 61 3c 77 57 6c 2a f7 02 e3 d9 9d b4 77 db ac ee 1b fd 1b 3a	00 F6 E3 17 6E 90 FF A8 5F 03 51 02 5D 3A 10 2E	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd, QCP-I, QCP-I-qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 27/06/2017 05:47:24 GMT to UTCTime 27/06/2032 05:47:24 GMT
SwissSign LI Platinum Server CA 2017 - G3	2.5.4.97 = NTRL-FL-0002.523.017-8 CN = SwissSign LI Platinum Server CA 2017 - G3 O = SwissSign AG C = LI	5d cd af 64 fd 22 0b 59 3d 59 05 33 2b 9f 49 f7 6b 45 c9 8d 54 8f e0 21 65 f6 b2 c4 73 94 5e 82	54 2E 82 CA 4B 16 52 1D 6E 14 F8 B2 16 3E DE	ETSI EN 319 411-1, policy NCP, EVCP ETSI EN 319 411-2, policy QCP-w	Certificate Signing, Off-line CRL Signing, CRL Signing	none	from UTCTime 27/06/2017 05:49:28 GMT to UTCTime 27/06/2032 05:49:28 GMT
SwissSign LI Platinum TSA CA 2017 - G3	2.5.4.97 = NTRL-FL-0002.523.017-8 CN = SwissSign LI Platinum TSA CA 2017 - G3 O = SwissSign AG C = LI	fd a6 04 9b 26 61 53 b9 c8 43 66 2a 77 c5 0d 2f 0a 06 b8 cd c8 11 16 66 37 8b b1 18 e7 21 5a ce	00 80 C7 92 8F A7 A6 D0 F4 97 7D 2D 96 3A E8 4C	ETSI EN 319 411-2, policy QCP-I-qscd (technically constrained)	Certificate Signing, Off-line CRL Signing, CRL Signing, Time Stamping	none	from UTCTime 27/06/2017 05:45:18 GMT to UTCTime 27/06/2032 05:45:18 GMT

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

Audit Attestation

Audit Attestation SwissSign - AA2018070302_V2



Modifications record

Version	Issuing Date	Changes
Version 1	2018-07-03	initial attestation
Version 2	2018-09-18	update of initial attestation in order to cover - formal CAB accreditation and - period of time statement for SwissSign Platinum Root CA – G3.

End of the audit attestation letter.