

Audit Attestation for SwissSign AG

Root: SwissSign Platinum CA - G2

Reference: AA2019121901

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 TÜV AUSTRIA CERT has audited the CAs of the "SwissSign AG, Platinum CA - G2" with remaining critical findings.

This present Audit Attestation letter is registered under the unique identifier number "AA2019121901" and consist of 7 pages. This audit attestation is issued based on the report number TA606182885_SRS. Predecessor is Audit Attestation letter AA2018122001 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>

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 BKAUATWWIBAN
AT373100000104093274
BIC RZBAATWWUID ATU63247169
DVR 3002477

With best regards,



i.A.



i.V.

Audit Attestation

Audit Attestation SwissSign - AA2019121901



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 accreditation: https://www.bmdw.gv.at/dam/jcr:ffe6b296-8c4c-4977-80de-d2566942a715/AA_0943_17065_TUEV_AUSTRIA_CERT_GMBH.pdf</p>
---	---

Identification of the trust service provider (TSP/CA):	<p><i>SwissSign AG</i> <i>Sägereistraße 25</i> <i>CH-8152 Glattbrugg, Switzerland</i> <i>All relevant TSP sites are located in</i> <i>Glattbrugg, Switzerland.</i> <i>Contact: Mr. Timo Schmitt</i> <i>E-Mail: timo.schmitt@swissign.com</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 CA - G2	
	Distinguished Name	CN = SwissSign Platinum CA - G2 O = SwissSign AG C = CH
	SHA-256 fingerprint	3B222E566711E992300DC0B15AB9473DAFDEF8C84D0 CEF7D3317B4C1821D1436
	Certificate Serial number	4EB200670C035D4F
	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

Audit Attestation

Audit Attestation SwissSign - AA2019121901



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)*", "*ETSI EN 319 411-2, V2.2.2 (2018-04)*" and "*ETSI EN 319 401, V2.2.1 (2018-04)*" as well as "*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 Platinum CA and its subordinated issuing CA*",
OID: 2.16.756.1.89.1.1.1.1.10, Version: 3.7.1 as of 2019-12-13
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 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.

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

Audit Attestation

Audit Attestation SwissSign - AA2019121901



The following Non-Conformity remained to be open on issuance of this Audit Attestation:

6.3 Certificate Life-Cycle operational requirements

Documentation and implementation of the certificate profiles was required to be improved. Certificates issued based upon the certificate profiles mentioned above are open to be checked by the TSP for a possible revocation. Depending on the result of the checks the TSP performs, an incident needs to be reported on Bugzilla.

This Audit Attestation also covers the following incidents as documented under

- Any policy: Bug 1455132, SwissSign: Undisclosed Intermediate Certificates:
https://bugzilla.mozilla.org/show_bug.cgi?id=1455132
- Any policy: Bug 1506607, SwissSign: Misissuance of Intermediate Certificates because of incorrect organizationIdentifier:
https://bugzilla.mozilla.org/show_bug.cgi?id=1506607
- Any policy: Bug 1541064, SwissSign Error in OrganisationIdentifier in signature/seal certificate:
https://bugzilla.mozilla.org/show_bug.cgi?id=1541064

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.

It has been verified during the audit that subordinated issuing-CA according to policies QCP-n or QCP-I issue person certificates only but no SSL certs.

The subordinated issuing-CA "SwissSign Advanced Platinum CA 2019 - G22" is a new CA under this Root CA. On 2019-12-12 a point-in-time audit (PIT) was performed. Furthermore, during this audit a leaf certificate for SwissSign was issued and revoked together with the auditors. This subordinated issuing-CA shall issue NCP+ certificates for legal persons (electronic seals) only, but no SSL certificates.

Audit Attestation

Audit Attestation SwissSign - AA2019121901



Identification of the CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy OID	Service	EKU	Validy
SwissSign TSA Platinum CA 2016 - G22	CN = SwissSign TSA Platinum CA 2016 - G22 O = SwissSign AG C = CH	B0C2AF82F2C158E87F611 723E624A10836D5AD3E42 4A18DAD2AE24FDE5A9E3 94	00F3C2C311288429C 56FB6FDD5A183F3	ETSI EN 319 411-2, policy QCP-I-qscd (technically constrained)	Certificate Signing, Off-line CRL Signing, CRL Signing	Time Stamping (1.3.6.1.5.5.7.3.8)	19 Dec 2016 12:46:39 GMT to 16 Dec 2031 12:46:39 GMT
SwissSign CH Person Platinum CA 2017 - G22	CN = SwissSign CH Person Platinum CA 2017 - G22 O = SwissSign AG C = CH	3CC9509C0FBF0BBBF2B AB0B4117811E95C58A37 D7F6902DE67524A9FE07 C040	6456CF80F9C7A0335 437F537250705	ETSI EN 319 411-2, policies QCP-I, QCP-I- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	18 Dec 2017 06:25:36 GMT to 18 Dec 2032 06.25:36 GMT
SwissSign CH Qualified Platinum CA 2017 - G22	CN = SwissSign CH Qualified Platinum CA 2017 - G22 O = SwissSign AG C = CH	29CC90779084B25D2142A B1E9F52B6A4463765E86A B321C3293FEE51300E33B 1	00B8DF8370FAA54E7 6C088635A89BDAE	ETSI EN 319 411-2, policies QCP-n, QCP-n- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	18 Dec 2017 06:31:59 GMT to 18 Dec 2032 06:31:59 GMT
SwissSign CH Qualified Platinum CA 2017 - G22 17-1	CN = SwissSign CH Qualified Platinum CA 2017 - G22 17-1 O = SwissSign AG C = CH	78B08B7D449A53DEA551 DBE9BEA5DD60FC7939C 775535C018DFA24A3D9E 9FFD7	00F5889E21886117E 255D645810556F8	ETSI EN 319 411-2, policies QCP-n, QCP-n- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	18 Dec 2017 06:29:55 GMT to 18 Dec 2032 06:29:55 GMT
SwissSign Personal Platinum CA 2010 - G2	CN = SwissSign Personal Platinum CA 2010 - G2 O = SwissSign AG C = CH	275F8A75C02DECAC9DC C945C30C7F370EDF4E73 9B0CEA75652897B16D2B D75D7	00A640439701136756 7BCA96067A54ED	ETSI EN 319 411-2, policies QCP-I, QCP-I- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	05 Jul 2010 12:13:35 GMT to 01 Jul 2025 12:13:35 GMT
SwissSign Personal Platinum CA 2014 - G22	CN = SwissSign Personal Platinum CA 2014 - G22	7C9CCF1733FD36AC3E3A 9B179AB0C755FBB1421E	00C79B9900921A423 AB1D15B5DF721A4	ETSI EN 319 411-2, policies QCP-I, QCP-I- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	15 Sep 2014 16:21:16 GMT to 11

Audit Attestation

Audit Attestation SwissSign - AA2019121901



	O = SwissSign AG C = CH	B803596355C2ED5D03CD 2765					Sep 2029 16:21:16 GMT
SwissSign PSS Qualified Platinum CA 2013 - G2	CN = SwissSign PSS Qualified Platinum CA 2013 - G2 O = SwissSign AG C = CH	A63626B494AC3F6BB59C 9A5103307AE36D0D5CA6 E0CBB6E3C4FB95D08CF AC5F2	00BF274B8EB1E48A2 717865DD851095D	ETSI EN 319 411-2, policies QCP-n, QCP-n- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	09 Dec 2013 08:52:36 GMT to 05 Dec 2028 08:52:36 GMT
SwissSign Qualified Platinum CA 2010 - G2	CN = SwissSign Qualified Platinum CA 2010 - G2 O = SwissSign AG C = CH	B0B05D7131D7881F78BA4 172B442B7D774D04FF27D 383BE3E459A372473B1E1 5	00AB32CDBC9B5994 2304FA6D84E40DBD	ETSI EN 319 411-2, policies QCP-n, QCP-n- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	06 Apr 2010 14:03:34 GMT to 02 Apr 2025 14:03:34 GMT
SwissSign Qualified Platinum CA G22 16-1	CN = SwissSign Qualified Platinum CA G22 16-1 O = SwissSign AG C = CH	0FAC8B71A8C979B861322 C4B2AF21AE12A5196525 AC2F079BD9268D816D2B 6FC	5B2400364E9D95F3E 870118ABD7D09	ETSI EN 319 411-2, policies QCP-n, QCP-n- qscd	Certificate Signing, Off-line CRL Signing, CRL Signing	none	13 Sep 2016 08:51:42 GMT to 10 Sep 2031 08:51:42 GMT
SwissSign SuisseID Platinum CA 2010 - G2	CN = SwissSign SuisseID Platinum CA 2010 - G2 O = SwissSign AG C = CH	395995EF7D204CD7F7E67 480E348766EFD93D5CDA DC8DBE7DF5D4B39F5C3 2410	00D5CB89C293009B EDBD014BDC109602	ETSI EN 319 411-1, policy NCP+	Certificate Signing, Off-line CRL Signing, CRL Signing	none	08 Mar 2010 14:05:04 GMT to 04 Mar 2025 14:05:04 GMT
SwissSign SuisseID Platinum CA 2014 - G22	CN = SwissSign SuisseID Platinum CA 2014 - G22 O = SwissSign AG C = CH	122071FD4527C2997A2F8 366A6D3CE12E085BD741 99AC5133829F68F06E983 2A	00E2A367DDB988194 0A8485E5541A9FD	ETSI EN 319 411-1, policy NCP+	Certificate Signing, Off-line CRL Signing, CRL Signing	none	15 Sep 2014 16:23:36 GMT to 11 Sep 2029 16:23:36 GMT
SwissSign TSA Platinum CA 2017 - G22	CN = SwissSign TSA Platinum CA 2017 - G22 O = SwissSign AG C = CH	8E510BD4177C10A22E70 C18C7B917A1AF6679342A 79CBD1B13129DB482A27 444	644FBE61792DD467B B207976701096	ETSI EN 319 411-2, policy QCP-I-qscd (technically constrained)	Certificate Signing, Off-line CRL Signing, CRL Signing	Time Stamping (1.3.6.1.5.5.7.3.8)	14 Feb 2017 08:29:17 GMT to 15 Feb 2032

Audit Attestation

Audit Attestation SwissSign - AA2019121901



							08:29:17 GMT
SwissSign Advanced Platinum CA 2019 - G22	2.5.4.97 = NTRCH- CHE-109.357.012 CN = SwissSign Advanced Platinum CA 2019 - G22 O = SwissSign AG C = CH	9D7D1ABDDC9F23838B26 C56B0A0FE6ADD5F0A6E3 98D8C0BCE712A438CE33 B69B	CEA6F34A5355EA0B D323F7583ACA18	<i>ETSI EN 319 411-1, policy NCP+</i>	<i>Certificate Signing, Off-line CRL Signing, CRL Signing</i>	<i>none</i>	12 Nov 2019 09:31:35 GMT to 12 Nov 2034, 09:31:35 GMT

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

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