TÜV AUSTRIA CERT GMBH

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

Business Area
Business Assurance

Certification Body

TÜV ®

Audit Attestation for SwissSign AG

Root: SwissSign Platinum CA - G2

Reference: AA2020112501

Your ref.:	Your message from:	Our ref.:	Date:
-	-	TUV TRUST IT/wcl	2020-12-17

To whom it may concern,

This is to confirm that TUV AUSTRIA CERT has audited the CA of the “SwissSign AG, Platinum CA – G2” with remaining critical findings.

This present Audit Attestation letter is registered under the unique identifier number “AA2020112501” and consist of 6 pages. This audit attestation is issued based on the report number TA235203365_SR and TA235203368_SR. Predecessor is Audit Attestation letter AA2019121901_A1 as of 2020-03-11 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. Clemens Wanko

i.V. Andreas Dvorak

Certification Body

Managing director:
DI (FH) Andreas Dvorak, 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

Auditor:	*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 17065:2012, ETSI EN 319 403 v2.2.2:2015 and ETSI EN 319 403-1 V2.3.1:2020. 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. Michael Günther* *E-Mail: michael.guenther@swisssign.com* *Company registration: CHE-403.679.996, CHE-109.357.012 (SwissSign Ltd.)*

Audit Period covered for all policies:	2019-09-28 to 2020-09-25
Audit dates:	2020-05-04 to 2020-05-15 (remote) 2020-08-31 to 2020-09-03 (onsite in Zürich) 2020-09-25 (onsite in Zürich)
Audit Location:	Zürich

[1] Identification of the accredited conformity assessment body (CAB), in the following termed shortly „*CAB*“

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

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	3B222E566711E992300DC0B15AB9473DAFDEF8C84D0CEF7D3317B4C1821D1436
	Certificate Serial number	4EB200670C035D4F
	Applied policy	ETSI EN 319 411-1, policies NCP+; ETSI EN 319 411-2, policies QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd

The audit was performed as full annual audit at the TSP's location in *Zürich (Glattbrugg), Switzerland* as well as remote for parts where remote audit was possible. During the remote session general parts as human resources, information security policy and procedures as well risk management were covered. Furthermore, the certificate application verification processes were audited. During the onsite inspection all aspects regarding physical security of data centre, RA premises, site environment, as well as key management (storage, protection and usage within certified HSM) of the Root and Issuing CA, the network and system security aspects were covered.

The issued certificate and the related records were audited for the whole audit period from 2019-09-28 until 2020-09-25 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)" and "ETSI EN 319 401, V2.2.1 (2018-04)"* as well as CA Browser Forum Requirements *"Baseline Requirements, version 1.7.2"* considering the requirements of the *"ETSI EN 319 403, V2.2.2 (2015-08) and "ETSI EN 319 403-1, V2.3.1 (2020-06) for the Trust Service Provider Conformity Assessment"* as well as "*ETSI TS 119 403-2, V1.2.4 (2020-11), 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: 2.16.756.1.89.1.1.1.1.12, Version: 3.9.0 as of 2020-11-17
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 2020-06-24
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 **minor non-conformities** have been identified throughout the audit:

Findings with regard to ETSI EN 319 401:

7 TSP management and operation

7.2 Human resources

Documentation and implementation of the yearly training plan were required to be improved.

7.4 Access control

Documentation and implementation of access rights for the new M-PKI application were required to be improved.

7.8 Network security

Documentation and implementation of network migration were required to be improved.

Documentation and implementation of penetration tests were required to be improved.

Documentation of vulnerability scans was required to be improved.

7.9 Incident management

Documentation of implementation of incident management was required to be improved.

7.10 Collection of evidence

Documentation and implementation of internal archives were required to be improved.

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

6.4 Facility, management, and operational controls

Documentation of CCTV records review for the data center was required to be improved.

6.5 Technical security controls

Documentation and implementation of IDS/IPS were required to be improved.

6.6 Certificate, CRL, and OCSP profiles

Documentation and implementation of the certificate profiles for the OU field was required to be improved.

The following **major 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.

For **all minor non-conformities** listed above, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

This Audit Attestation also covers the following incidents as documented under

- Any Policy: Bug *1662137, SwissSign AG: OCSP responder unreachable:* https://bugzilla.mozilla.org/show_bug.cgi?id=1662137
- Any Policy: *Bug 1613406, SwissSign AG : Delayed revocation for mispellings in Location for a number of Certificates:* https://bugzilla.mozilla.org/show_bug.cgi?id=1613406
- Any Policy: Bug *1636141, SwissSign AG: failure to provide a preliminary report within 24 hours:* https://bugzilla.mozilla.org/show_bug.cgi?id=1636141
- Any Policy: Bug *1614450, SwissSign AG: Audit Letter Validation failures on intermediate certificates:* https://bugzilla.mozilla.org/show_bug.cgi?id=1614450
- Any Policy: Bug *1558552, SwissSign AG: CP/CPS certificate profile issue:* https://bugzilla.mozilla.org/show_bug.cgi?id=1558552

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 Sub-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 Sub-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.

Subject Distinguished Name	SHA-256 fingerprint	Applied Policy	EKU
CN = SwissSign Advanced Platinum CA 2019 - G22, O = SwissSign AG, C = CH, NTRCH-CHE-109.357.012	9D7D1ABDDC9F23838B26C56B0A0FE6ADD5F0A6E398D8C0BCE712A438CE33B69B	ETSI EN 319 411-1, policy NCP+	none
CN = SwissSign CH Person Platinum CA 2017 - G22, O = SwissSign AG, C = CH, OI = NTRCH-CHE-109.357.012	3CC9509C0FBF0BBBFE2BAB0B4117811E95C58A37D7F6902DE67524A9FE07C040	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	none
CN = SwissSign CH Qualified Platinum CA 2017 - G22, O = SwissSign AG, C = CH, OI = NTRCH-CHE-109.357.012	29CC90779084B25D2142AB1E9F52B6A4463765E86AB321C3293FEE51300E33B1	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	none
CN = SwissSign CH Qualified Platinum CA 2017 - G22 17-1, O = SwissSign AG, C = CH, OI = NTRCH-CHE-109.357.012	78B08B7D449A53DEA551DBE9BEA5DD60FC7939C775535C018DFA24A3D9E9FFD7	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	none
CN = SwissSign Personal Platinum CA 2010 - G2, O = SwissSign AG, C = CH	275F8A75C02DECAC9DCC945C30C7F370EDF4E739B0CEA75652897B16D2BD75D7	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	none
CN = SwissSign Personal Platinum CA 2014 - G22, O = SwissSign AG, C = CH	7C9CCF1733FD36AC3E3A9B179AB0C755FBB1421EB803596355C2ED5D03CD2765	ETSI EN 319 411-2, policies QCP-l, QCP-l-qscd	none
CN = SwissSign Qualified Platinum CA 2010 - G2, O = SwissSign AG, C = CH	B0B05D7131D7881F78BA4172B442B7D774D04FF27D383BE3E459A372473B1E15	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	none
CN = SwissSign Qualified Platinum CA G22 16-1, O = SwissSign AG, C = CH	0FAC8B71A8C979B861322C4B2AF21AE12A5196525AC2F079BD9268D816D2B6FC	ETSI EN 319 411-2, policies QCP-n, QCP-n-qscd	none
CN = SwissSign SuisseID Platinum CA 2010 - G2, O = SwissSign AG, C = CH	395995EF7D204CD7F7E67480E348766EFD93D5CDADC8DBE7DF5D4B39F5C32410	ETSI EN 319 411-1, policy NCP+	none
CN = SwissSign SuisseID Platinum CA 2014 - G22, O = SwissSign AG, C = CH	122071FD4527C2997A2F8366A6D3CE12E085BD74199AC5133829F68F06E9832A	ETSI EN 319 411-1, policy NCP+	none

CN = SwissSign TSA Platinum CA 2017 - G22, O = SwissSign AG, C = CH, OI = NTRCH-CHE-109.357.012	8E510BD4177C10A22E70C18C7B917A1AF6679342A79CBD1B13129DB482A27444	ETSI EN 319 411-2, policy QCP-l-qscd (technically constrained)	Time Stamping

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

Modifications record

Version	Issuing Date	Changes
Version 1.1	2020-12-17	Re-formated dates and SHA256 to address errors from AVL (no change in content)
Version 1	2020-11-25	Initial attestation

End of the audit attestation letter