

Audit Attestation for SwissSign AG

Root: SwissSign Gold CA - G2

Reference: AA2020112502

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 TÜV AUSTRIA CERT has successfully audited the CA of the "SwissSign AG, Gold CA – G2" without critical findings.

This present Audit Attestation letter is registered under the unique identifier number "AA2020112502" and consist of 5 pages. This audit attestation is issued based on the report number TA235203360_SR, TA235203361_SR, and TA235203362_SR. Predecessor is Audit Attestation letter AA2019121902 as of 2019-12-19 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:
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 BKAUATWWIBAN
AT373100000104093274
BIC RZBAATWWUID ATU63247169
DVR 3002477

With best regards,



i.A. Clemens Wanko



i.V. Andreas Dvorak

Audit Attestation

Audit Attestation SwissSign AA2020112502



Auditor:	<p>TÜV AUSTRIA CERT GmbH¹ TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge, 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 17065:2012, ETSI EN 319 403 v2.2.2:2015 and ETSI EN 319 403-1 V2.3.1:2020.</p> <p>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>SwissSign AG Sägereistraße 25 CH-8152 Glattbrugg, Switzerland All relevant TSP sites are located in Glattbrugg, Switzerland. Contact: Mr. Michael Günther E-Mail: michael.quenther@swisssign.com Company registration: CHE-403.679.996, CHE-109.357.012 (SwissSign Ltd.)</p>
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

Audit Attestation

Audit Attestation SwissSign AA2020112502



Identification of the audited Root-CA:	SwissSign Gold CA - G2	
	Distinguished Name	CN = SwissSign Gold CA - G2 O = SwissSign AG C = CH
	SHA-256 fingerprint	62DD0BE9B9F50A163EA0F8E75C053B1ECA57EA55C8688F647C6881F2C8357B95
	Certificate Serial number	00BB401C43F55E4FB0
	Applied policy	ETSI EN 319 411-1, policies NCP, OVCP, EVCP

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 319 411-1, V1.2.2 (2018-04)*" and "*ETSI EN 319 401, V2.2.1 (2018-04)*" as well as CA Browser Forum Requirements "*EV SSL Certificate Guidelines, version 1.7.3*" and "*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*".

Audit Attestation

Audit Attestation SwissSign AA2020112502



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 Gold CA and its subordinated issuing CA",
OID: 2.16.756.1.89.1.2.1.14 , Version: 2.10.0 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.

Findings with regard to the EV SSL Certificate Guidelines:

No further findings.

All major non-conformities have been closed before the issuance of this attestation. For all minor non-conformities, remediation has been scheduled within three months after the onsite audit at latest and will be covered by a corresponding audit.

Audit Attestation

Audit Attestation SwissSign AA2020112502



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 misspellings 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
- Policy EVCP, OVCP, NCP: Bug 1613334, SwissSign AG: Misissuance with misspellings in Location for a number of Certificates:
https://bugzilla.mozilla.org/show_bug.cgi?id=1613334
- 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.

Audit Attestation

Audit Attestation SwissSign AA2020112502



Distinguished Name	SHA-256 fingerprint	Applied policy OID	EKU
CN = SwissSign EV Gold CA 2014 - G22, O = SwissSign AG, C = CH	A434AAE4E15A5519E9B111FD08EC190FD2ADF13BBE30815C6E1606555CB31450	ETSI EN 319 411-1, policy EVCP	none
CN = SwissSign Server Gold CA 2014 - G22, O = SwissSign AG, C = CH	561DC78351F5E7EE5A464AC6E58A0D164EF2768F98F02E6EE65501120FCD9C5E	ETSI EN 319 411-1, policy OVCP	none
CN = SwissSign Server Gold CA 2008 - G2, O = SwissSign AG, C = CH	FD2991B134CE57BF9CD686878854A5EED5EA64433002452BA40398DA78845CA7	ETSI EN 319 411-1, policy OVCP	none
CN = SwissSign Personal Gold CA 2014 - G22, O = SwissSign AG, C = CH	77D6C2AF5A7B86F63D9918C87533779F2AF08D35CFA14DA4938C803F53DE18A1	ETSI EN 319 411-1, policy NCP	none
CN = SwissSign Personal Gold CA 2008 - G2, O = SwissSign AG, C = CH	2B65E45EA181C1CC21B1CC9E9FB1E10F54129432BB78973F608C66A4151FBF0E	ETSI EN 319 411-1, policy NCP	none

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