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

Root: SwissSign Gold CA - G2

Reference: AA2019121902

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 TUV AUSTRIA CERT has successfully audited the CAs of the “SwissSign AG, Gold CA - G2” without critical findings.

This present Audit Attestation letter is registered under the unique identifier number “AA2019121902” and consist of 6 pages. This audit attestation is issued based on the reports number TA606182881_SRS, TA606182882_SRS and TA606182918_SRS. Predecessor is Audit Attestation letter AA2018122002 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

With best regards,

i.A. i.V

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 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: 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. Timo Schmitt* *E-Mail: timo.schmitt@swisssign.com* *Company registration: CHE-403.679.996, CHE-109.357.012 (SwissSign Ltd.)*

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

[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 *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)" and "ETSI EN 319 401, V2.2.1 (2018-04)"* as well as CA Browser Forum Requirements "*EV SSL Certificate Guidelines, version 1.7.0" and "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 Gold CA and its subordinated issuing CA",*
   OID: 2.16.756.1.89.1.2.1.12, Version: 2.8.0 as of 2019-11-25
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:

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 and implementation of the certificate profiles was required to be improved.
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.
6.6 Certificate, CRL, and OCSP profiles
Documentation and implementation of the MPKI XP profiles was required to be improved.

Findings with regard to the EV SSL Certificate Guidelines:

11.4. Verification of Applicant's Physical Existence
Documentation and implementation of the application check procedure was required to be improved.

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

This Audit Attestation also covers the following incidents as documented under

- Any Policy: Bug 1558552, SwissSign: CP/CPS certificate profile issue: https://bugzilla.mozilla.org/show_bug.cgi?id=1558552.
- Policy EVCP: Bug 1569651, SwissSign: Misissuance of Leaf Certificates because of incorrect postcode: https://bugzilla.mozilla.org/show_bug.cgi?id=1569651.
- Policy OVCP: Bug 1428877, SwissSign: Invalid DNSName in SAN: https://bugzilla.mozilla.org/show_bug.cgi?id=1428877.
- Policy OVCP: Bug 1551364, SwissSign: Some-State" in stateOrProvinceName: https://bugzilla.mozilla.org/show_bug.cgi?id=1551364.
- Any policy: Bug 1455132, SwissSign: Undisclosed Intermediate Certificates: https://bugzilla.mozilla.org/show_bug.cgi?id=1455132.

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.

Identification of the CA	Distinguished Name	SHA-256 fingerprint	Certificate Serial number	Applied policy OID	Service	EKU	Validy
SwissSign EV Gold CA 2014 - G22	CN = SwissSign EV Gold CA 2014 - G22 O = SwissSign AG C = CH	A434AAE4E15A5519E9B111FD08EC190FD2ADF13BBE30815C6E1606555CB31450	008108383CC00775C40C6D736BE3308B	*ETSI EN 319 411-1, policy EVCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	15 Sep 2014 16:16:37 GMT to 04 Mar 2035 16:16:37 GMT
SwissSign Personal Gold CA 2014 - G22	CN = SwissSign Personal Gold CA 2014 - G22 O = SwissSign AG C = CH	77D6C2AF5A7B86F63D9918C87533779F2AF08D35CFA14DA4938C803F53DE18A1	191795DC22741B121DDB544C5CCBDC	*ETSI EN 319 411-1, policy NCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	19 Sep 2014 14:10:25 GMT to 15 Sep 2029 14:10:25 GMT
SwissSign Personal Gold CA 2008 - G2	CN = SwissSign Personal Gold CA 2008 - G2 O = SwissSign AG C = CH	2B65E45EA181C1CC21B1CC9E9FB1E10F54129432BB78973F608C66A4151FBF0E	392B241D6144C35A	*ETSI EN 319 411-1, policy NCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	07 Jul 2008 17:24:18 GMT to 07 Jul 2023 17:24:18 GMT
SwissSign Server Gold CA 2014 - G22	CN = SwissSign Server Gold CA 2014 - G22 O = SwissSign AG C = CH	561DC78351F5E7EE5A464AC6E58A0D164EF2768F98F02E6EE65501120FCD9C5E	00FA1DAAEAC9B3A5FA57980B9974DA31	*ETSI EN 319 411-1, policy OVCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	19 Sep 2014 14:09:12 GMT to 15 Sep 2029 14:09:12 GMT
SwissSign Server Gold CA 2008 - G2	CN = SwissSign Server Gold CA 2008 - G2 O = SwissSign AG C = CH	FD2991B134CE57BF9CD686878854A5EED5EA64433002452BA40398DA78845CA7	5ECCFA69C03327EF	*ETSI EN 319 411-1, policy OVCP*	*Certificate Signing, Off-line CRL Signing, CRL Signing*	*none*	07 Jul 2008 17:06:03 GMT to 07 Jul 2023 17:06:03 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