

# Key Ceremony Report for

## SwissSign AG



**Reference: AA20220701**

Cologne, 2026-03-30

To whom it may concern,

This is to confirm that "TÜV Austria GmbH" has audited a key ceremony of "SwissSign AG". The ceremony was followed in its entirety, completed successfully and without non-conformities in accordance with the applicable requirements.

This Key Ceremony Report is registered under the unique identifier number "AA20220701" and consists of 11 pages.

Kindly find here below the details accordingly.

In case of any question, please contact:

Clemens Wanko  
TÜV AUSTRIA 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](mailto:clemens.wanko@tuv-austria.com)  
<https://www.it-tuv.com>

With best regards,

i.A. Clemens Wanko

i.V. Elisabeth Pichler

**TÜV AUSTRIA  
GMBH**

**Office:**  
TÜV AUSTRIA-Platz 1  
2345 Brunn am Gebirge  
T: +43 5 0454-5000  
E: [office@tuv.at](mailto:office@tuv.at)  
W: [www.tuv.at](http://www.tuv.at)

**Business Area**  
Region Austria

**Contact:**  
Clemens Wanko  
T: +49 170 80 20 20 7  
E: [clemens.wanko@tuv-austria.com](mailto:clemens.wanko@tuv-austria.com)  
TÜV®



**Accredited as:**  
Testing Laboratory,  
Inspection Body,  
Certification Body,  
Calibration Laboratory,  
Verification Body

**Notified Body 0408**

**Non-executive  
Board of Directors:**  
DI Dr. Stefan Haas

**Management:**  
Ing. Günter Göttlich  
DI (FH) Hans-Peter  
Weinzettl

**Registered Office:**  
Deutschstrasse 10  
1230 Vienna/Austria

**Branch Offices:**  
[www.tuv.at/standorte](http://www.tuv.at/standorte)

**Company Register  
Court / - Number:**  
Vienna / FN 288476 f

**UID**  
ATU63240488

This key ceremony report is based on the template version 2.0 as of 2026-03-09, that was approved for use by ACAB-c.

# Key Ceremony Report

## Audit Attestation SwissSign AG – AA20220701



### General audit information

Identification of the conformity assessment body (CAB) and assessment organization acting as ETSI auditor

- CAB TÜV AUSTRIA GMBH  
TÜV AUSTRIA-Platz 1, 2345 Brunn am Gebirge,  
registered under: Vienna / Wien / FN 288476 f
- Accredited by Federal Ministry for Economic Affairs, Energy and Tourism, Stubenring 1, 1010 Wien, Austria (mailto: [akkreditierung@bmdw.gv.at](mailto:akkreditierung@bmdw.gv.at), <https://akkreditierung-austria.gv.at/>) under registration 0944<sup>1</sup> for the certification of trust services according to “EN ISO/IEC 17065:2012” and “ETSI EN 319 403-1 V2.3.1 (2020-06)”.
- Insurance Carrier (BRG section 8.2):  
  
Vienna Insurance Group  
Schottenring 30, 1010 Wien
- Third-party affiliate audit firms involved in the audit:  
None.

Identification and qualification of the audit team

- Number of team members: 2
- Academic qualifications of team members:  
All team members have formal academic qualifications or professional training or extensive experience indicating general capability to carry out audits based on the knowledge given below and at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant trust services, public key infrastructure, information security including risk assessment/management, network security and physical security.
- Additional competences of team members:
- All team members have knowledge of
  - 1) audit principles, practices and techniques in the field of CA audits gained in a training course of at least five days;
  - 2) the issues related to various areas of trust services, public key infrastructure, information security including risk assessment/management, network security and physical security;
  - 3) the applicable standards, publicly available specifications and regulatory requirements for CAs and other relevant publicly available specifications including standards for IT product evaluation; and
  - 4) the Conformity Assessment Body's processes.Furthermore, all team members have language skills appropriate for all organizational levels within the CA organization; note-taking, report-writing,

<sup>1</sup> [https://www.tuv.at/wp-content/uploads/2025/05/944\\_Akkreditierungsbestatigung\\_PRODUKTE\\_2025.pdf](https://www.tuv.at/wp-content/uploads/2025/05/944_Akkreditierungsbestatigung_PRODUKTE_2025.pdf)

# Key Ceremony Report

Audit Attestation SwissSign AG – AA20220701



presentation, and interviewing skills; and relevant personal attributes: objective, mature, discerning, analytical, persistent and realistic.

- Professional training of team members:  
See “Additional competences of team members” above. Apart from that are all team members trained to demonstrate adequate competence in:
  - a) knowledge of the CA standards and other relevant publicly available specifications;
  - b) understanding functioning of trust services and information security including network security issues;
  - c) understanding of risk assessment and risk management from the business perspective;
  - d) technical knowledge of the activity to be audited;
  - e) general knowledge of regulatory requirements relevant to TSPs; and
  - f) knowledge of security policies and controls.
- Types of professional experience and practical audit experience:  
The CAB ensures, that its personnel performing audits maintains competence on the basis of appropriate education, training or experience; that all relevant experience is current and prior to assuming responsibility for performing as an auditor, the candidate has gained experience in the entire process of CA auditing. This experience shall have been gained by participating under supervision of lead auditors in a minimum of four TSP audits for a total of at least 20 days, including documentation review, on-site audit and audit reporting.
- Additional qualification and experience Lead Auditor:  
On top of what is required for team members (see above), the Lead Auditor
  - a) has acted as auditor in at least three complete TSP audits;
  - b) has adequate knowledge and attributes to manage the audit process; and
  - c) has the competence to communicate effectively, both orally and in writing.
- Special skills or qualifications employed throughout audit:  
None.
- Special Credentials, Designations, or Certifications:  
All members are qualified and registered assessors within the accredited CAB.
- Auditors code of conduct incl. independence statement:  
Code of Conduct as of Annex A, ETSI EN 319 403 or ETSI EN 319 403-1 respectively.

## Identification and qualification of the reviewer performing audit quality management

- Number of Reviewers/Audit Quality Managers involved independent from the audit team: 1
- The reviewer fulfils the requirements as described for the Audit Team Members above and has acted as an auditor in at least three complete CA audits.

Identification of the CA:

SwissSign AG  
Sägereistrasse 25  
8152 Glattbrugg Switzerland  
registered under CHE-109.357.012

# Key Ceremony Report

## Audit Attestation SwissSign AG – AA20220701



Type of audit:	Point in time audit of a key and certificate generation ceremony
Point in time date generation:	2022-05-19 (Root CA Key pair generation) 2022-06-08 (Root CA certificate issuance) 2022-06-28 (Cross Signed CA issuance) 2022-06-28 (Issuing CA key generation) 2022-06-29 (Issuing CA issuance)
Audit location:	Glattbrugg, Switzerland

A key ceremony script has been prepared in accordance with the normative requirements and with the rules stated in the policy and practice statement documents of the certification service provider. This script has been followed during the whole ceremony.

In particular:

- The key ceremony was performed by [3] individuals of the CA Owner acting in Trusted Roles, each of whom has own credentials to approve technical the key ceremony steps.
- The key ceremony was observed by [2] individuals of the Conformity Assessment Body with independence from the CA Owner.
- Principles of multiparty control and split knowledge were observed.
- The Root CA key pairs were securely generated on the 2022-05-19 within FIPS certified HSMs located in a bank safe. Upon arrival of the auditors on the 2022-06-08, the HSM's were still located offline in the bank safe and private keys were checked to be stored on the same HSM before the Root CA certificate issuance started.
- The Root and Issuing CA key pairs were generated within cryptographic modules meeting the applicable technical and business requirements (FIPS certification) as disclosed in the CA's CPS.
- Effective controls were maintained to provide reasonable assurance that the private key was generated and protected in conformance with the procedures described in its CPS and the Key Generation Script.
- All steps performed regarding the Root and Issuing CA key pair activities were logged.

The key ceremony has been witnessed in person.

No non-conformities have been identified during the key ceremony.

# Key Ceremony Report

Audit Attestation SwissSign AG – AA20220701



## Root 1: SwissSign RSA TLS Root CA 2022 - 1

Standards considered: (Only with regard to key generation and key protection requirements)	<p>European Standards:</p> <ul style="list-style-type: none"><li>• ETSI EN 319 411-1 V1.3.1 (2021-05)</li><li>• ETSI EN 319 401 V2.3.1 (2021-05)</li></ul> <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"><li>• Guidelines for the Issuance and Management of Extended Validation Certificates, version 1.7.9</li><li>• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.8.4</li><li>•</li></ul> <p>Browser Policy Requirements:</p> <ul style="list-style-type: none"><li>• Mozilla Root Store Policy, Version 3.0, 2025-03-15</li><li>• Microsoft Trusted Root Program, 2025-09-04</li><li>• Chrome Root Program Policy, 2026-02-05</li><li>• Apple Root Certificate Program, 2023-08-15</li></ul> <p>Other:</p> <ul style="list-style-type: none"><li>• State-of-the-art technical and organizational requirements (e.g. interpretations of strength and durability of crypto functions used)</li></ul> <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"><li>• ETSI EN 319 403 V2.2.2 (2015-08)</li><li>• ETSI EN 319 403-1 V2.3.1 (2020-06)</li><li>• ETSI TS 119 403-2 V1.2.4 (2020-11)</li></ul>
---	--

The key ceremony was based on the following policy and practice statement documents of the CA:

- SwissSign CPS TLS

Version	Release Date	Effective from	Effective until
Version 3.0	2021-11-08	2021-11-08	2022-07-01

- SwissSign TSPS

Version	Release Date	Effective from	Effective until
Version 3.0	2021-11-08	2021-11-08	2022-07-18

- SwissSign CPR

Version	Release Date	Effective from	Effective until
Version 3.0	2022-04-25	2022-04-25	2022-07-01

# Key Ceremony Report

## Audit Attestation SwissSign AG – AA20220701



- SwissSign CP OV

Version	Release Date	Effective from	Effective until
Version 1.0	2021-06-14	2021-06-14	2022-08-15

- SwissSign CP EV

Version	Release Date	Effective from	Effective until
Version 1.0	2021-06-14	2021-06-14	2022-08-15

- SwissSign CP DV

Version	Release Date	Effective from	Effective until
Version 1.0	2021-06-14	2021-06-14	2022-08-15

This report covers the generation of the key pairs and certificates of the Root-CA and Sub-CAs referenced in the following tables.

# Key Ceremony Report

Audit Attestation SwissSign AG – AA20220701



Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
CN = SwissSign RSA TLS Root CA 2022 - 1 O = SwissSign AG C = CH	288B4A9F605B09B999B215850825C81F9B537DBAF23664ACA98BF6BA98EDC379	ETSI EN 319 411-1, policies EVCP, OVCP, DVCP
	SHA-256 fingerprint of Subject Public Key Info	
	6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5	

**Table 1: Root-CA 1 generated during the key ceremony**

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this key ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH	B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4	ETSI EN 319 411-1 DVCP
	SHA-256 fingerprint of Subject Public Key Info	
	EBBD7F49938CC9EEECA2BAF71CD267F083B1EADE	
CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH	6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D	ETSI EN 319 411-1 EVCP
	SHA-256 fingerprint of Subject Public Key Info	
	4952DF308692595F349C254824ABC0EBD106F2D6	
CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH	332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23	ETSI EN 319 411-1 OVCP
	SHA-256 fingerprint of Subject Public Key Info	
	7C6F0A6F130FD98C246F2634F35C6B436DB723B6	

**Table 2: Sub-CAs issued by the Root-CA 1 or its Sub-CAs generated during the key ceremony**

# Key Ceremony Report

Audit Attestation SwissSign AG – AA20220701



## Root 2: SwissSign RSA SMIME Root CA 2022 - 1

Standards considered:	<p>European Standards:</p> <ul style="list-style-type: none"><li>• ETSI EN 319 411-1 V1.3.1 (2021-05)</li><li>• ETSI EN 319 401 V2.3.1 (2021-05)</li></ul> <p>CA Browser Forum Requirements:</p> <ul style="list-style-type: none"><li>• Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.8.4</li></ul> <p>Browser Policy Requirements:</p> <ul style="list-style-type: none"><li>• Mozilla Root Store Policy, Version 3.0, 2025-03-15</li><li>• Microsoft Trusted Root Program, 2025-09-04</li><li>• Chrome Root Program Policy, 2026-02-05</li><li>• Apple Root Certificate Program, 2023-08-15</li></ul> <p>Other:</p> <ul style="list-style-type: none"><li>• State-of-the-art technical and organizational requirements (e.g. interpretations of strength and durability of crypto functions used)</li></ul> <p>For the Trust Service Provider Conformity Assessment:</p> <ul style="list-style-type: none"><li>• ETSI EN 319 403 V2.2.2 (2015-08)</li><li>• ETSI EN 319 403-1 V2.3.1 (2020-06)</li><li>• ETSI TS 119 403-2 V1.2.4 (2020-11)</li></ul>
-----------------------	--

The key ceremony was based on the following policy and practice statement documents of the CA:

- SwissSign CPS S/MIME

Version	Release Date	Effective from	Effective until
Version 2.0	2021-10-11	2021-11-08	2022-07-01

- SwissSign TSPS

Version	Release Date	Effective from	Effective until
Version 3.0	2021-11-08	2021-11-08	2022-07-18

- SwissSign CPR

Version	Release Date	Effective from	Effective until
Version 3.0	2022-04-25	2022-04-25	2022-07-01

# Key Ceremony Report

## Audit Attestation SwissSign AG – AA20220701



- SwissSign CP LCP

Version	Release Date	Effective from	Effective until
Version 1.0	2021-06-14	2021-06-14	2022-08-15

- SwissSign CP NCP+

Version	Release Date	Effective from	Effective until
Version 1.0	2021-10-11	2022-12-12	2022-12-12

- SwissSign CP NCP

Version	Release Date	Effective from	Effective until
Version 1.0	2021-06-14	2021-06-14	2022-08-15

This report covers the generation of the key pairs and certificates of the Root-CA and Sub-CAs referenced in the following tables.

# Key Ceremony Report

Audit Attestation SwissSign AG – AA20220701



Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
CN = SwissSign RSA SMIME Root CA 2022 - 1 O = SwissSign AG C = CH	5A84C94054D340D650A29985EF97BB396352E215AED6C0B33CA7FFDD3BD5D2A2	ETSI EN 319 411-1, policies LCP, NCP
	SHA-256 fingerprint of Subject Public Key Info	
	CC2EAD898C83E340A32569A5EA927DD2373AC7C6	

**Table 3: Root-CA 2 generated during the key ceremony**

The TSP named the Sub-CAs that have been issued by the aforementioned Root-CA, that are listed in the following table and that have been covered in this key ceremony.

Distinguished Name	SHA-256 fingerprint of the certificate	Applied policy
CN = SwissSign RSA SMIME LCP ICA 2022 - 1, O = SwissSign AG, C = CH	D7F41FABE5A459BAC6882465C75CCFF2BAA52487AABC34706CAF2A18AC53A5C2	ETSI EN 319 411-1, LCP
	SHA-256 fingerprint of Subject Public Key Info	
	0B83D4722086CCE13AEF99B677CD51A6A3728F5C	
CN = SwissSign RSA SMIME NCP extended ICA 2022 - 1, O = SwissSign AG, C = CH	7196E86DCFD9B92B0509213D806DCA2465FC41415A0B4069D35F946DE6813CF79	ETSI EN 319 411-1, NCP
	SHA-256 fingerprint of Subject Public Key Info	
	E4BEC760A782A318E864FCE216530587D46AE98E	
CN = SwissSign RSA SMIME NCP ICA 2022 - 1, O = SwissSign AG, C = CH	99A56DD8DACA399FCA2E3834ED75760E96C133564062F8B530B355BED99A409D	ETSI EN 319 411-1, NCP
	SHA-256 fingerprint of Subject Public Key Info	
	56A2DFF3E1841D1BA0FF7F3FF071188528F83DCD	

**Table 4: Sub-CAs issued by the Root-CA 2 generated during the key ceremony**

# Key Ceremony Report

Audit Attestation SwissSign AG – AA20220701



## Modifications record

Version	Issuing Date	Changes
Version 1	2022-07-01	Initial attestation
Version 1.1	2026-03-25	Minor corrections

**End of the key ceremony report.**