SwissSign

SwissSign CPS TLS

Certification Practice Statement for TLS certificates

Document Type:	Certificate Practice Statement
OID:	n/a
Author:	Information Security and Compliance
Owner:	CEO
Applicability:	Global
Copyright:	Attribution-NoDerivs (CC-BY-ND) 4.0
Version:	12
Issue date:	07.08.2025
Obsoletes:	v11.0, 13.03.2025

Disclaimer: The electronic version of this document and all its stipulations are considered binding if saved in Adobe PDF Format. Additionally, a version in Markdown may be provided for convenience. In case of discrepancies, the PDF version prevails.

Table of Contents

1. INTRODUCTION

Since 2001 SwissSign AG offers several trust services such as TLS, qualified and non-qualified signature certificates as well as S/MIME certificates to customers all over the world, with a focus on Switzerland and Europe.

SwissSign has divided the description of its processes into four parts:

- Certificate Policy which defines the policy which is followed for each certificate type issued by SwissSign
- Trust Service Practice Statement (TSPS) describes general practices common to all trust services;
- Certification Practice Statements and Time-Stamping Authority Practice Statement describe parts that are specific to each Root CA or Time-Stamping Unit; and
- Technical Certificate Profiles.

The structure of this document corresponds to RFC3647 and is divided into nine parts. To preserve the outline specified by RFC 3647, section headings that do not apply or are not supported by the TSP have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them. Each top-level chapter includes references to the relevant sections the TSPS [5], if the chapter refer to general practices of the TSP independent from the trust service.

The services offered duly comply e.g. regarding the accessibility with the Swiss law. The offered services are non-discriminatory. They respect the applying export regulations. In case partial tasks are outsourced to partners or external providers, the TSP, represented by the management or its agents, remains responsible for compliance with the procedures for the purposes of this document or any legal or certification requirements to the TSP.

The TSP also issues certificates for themselves or their own purposes. The corresponding legal and/or certification requirements are also met.

1.1 Overview

This CPS and respectively the TSPS [5] and Certificate Policies below describe the practices implemented by SwissSign AG to comply with the relevant services as well as the terms and conditions under which this CA is made available:

- "SwissSign CP EV - Certificate Policy for Extended Validation Certificates" [1]
- "SwissSign CP OV - Certificate Policy for Organization Validated Certificates" [2]
- "SwissSign CP DV - Certificate Policy for Domain Validated Certificates" [3]

For the issuance of certificates within this scope, SwissSign fully complies with the rules and regulations published by the Root Store Policies and CA/Browser Forum, using the currently valid versions at https://www.cabforum.org, as well as further applicable specifications:

- Browser Root Store Policies
  - Apple Root Certificate Program: https://www.apple.com/certificateauthority/ca_program.html
  - Google - Chrome Root Program: https://googlechrome.github.io/chromerootprogram/
  - Microsoft Trusted Root Program: https://learn.microsoft.com/en-us/security/trusted-root/program-requirements
  - Mozilla Root Store Policy: https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/
- TLS BR Guidelines: "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates"
- EV Guidelines: „Guidelines for the Issuance and Management of Extended Validation Certificates"
- ETSI EN 319 401: General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI TS 119 312: Cryptographic Suites
- IETF RFC 6960: Online Certificate Status Protocol - OCSP
- IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework

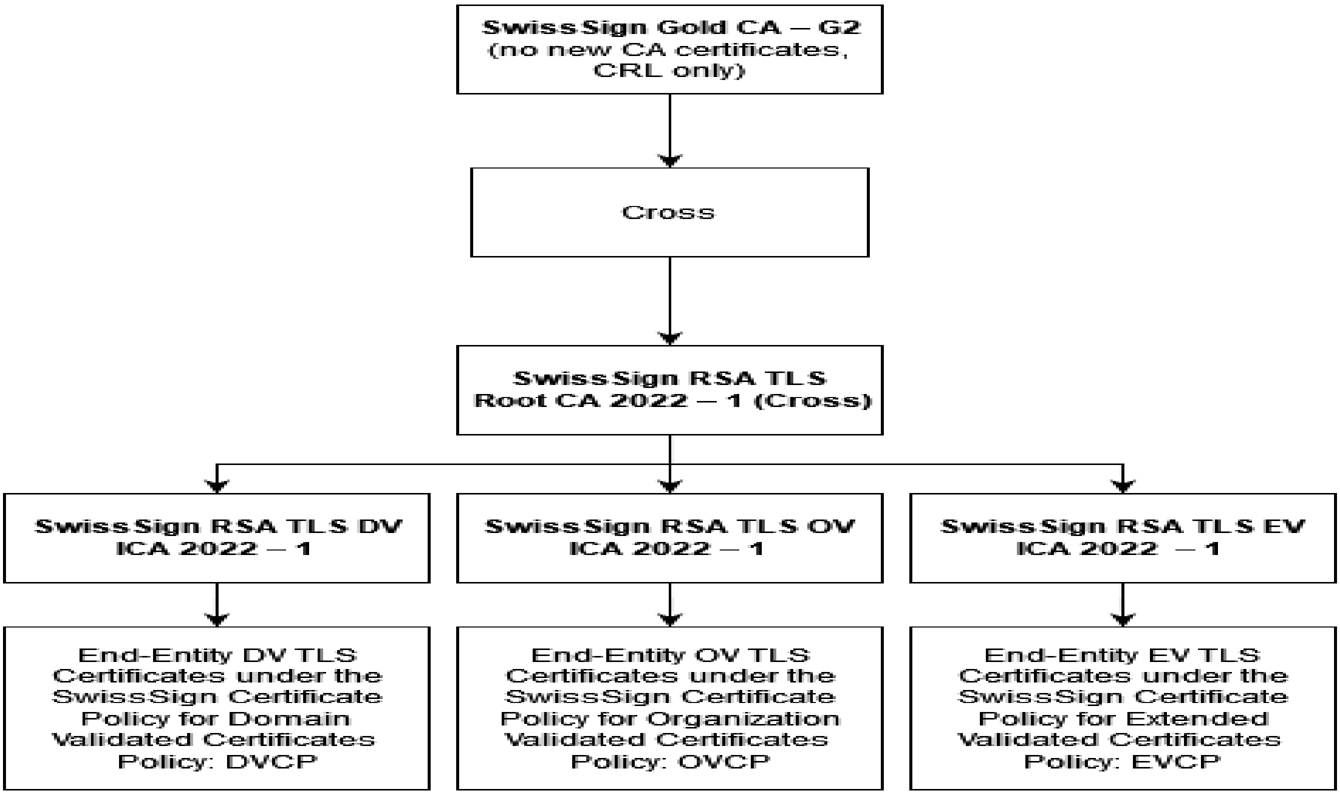
SwissSign Gold CA – G2 (no new CA certificates, CRL only)
Cross
SwissSign RSA TLS Root CA 2022 – 1 (Cross)
SwissSign RSA TLS DV ICA 2022 – 1
SwissSign RSA TLS OV ICA 2022 – 1
SwissSign RSA TLS EV ICA 2022 – 1
End-Entity DV TLS Certificates under the SwissSign Certificate Policy for Domain Validated Certificates Policy: DVCP
End-Entity OV TLS Certificates under the SwissSign Certificate Policy for Organization Validated Certificates Policy: OVCP
End-Entity EV TLS Certificates under the SwissSign Certificate Policy for Extended Validated Certificates Policy: EVCP

Figure 1: Picture showing SwissSign Gold CA - GS hierarchy

- IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The requirements of Browser root store policies as well as the TLS BRs and EV Guidelines apply in their latest version.

The TSP issues under this CPS certificates that meet the stipulations of the following policies:

- EVCP and CAB-EV (EV certificates)
- OVCP and CAB-OV (OV certificates)
- DVCP and CAB-DV (DV certificates)

The relevant Issuing CAs for these certificates under this CPS are shown in the PKI overview of SwissSign shown in Figure 1.

This Root Certificate Authorities as well as the Issuing CAs are operated by SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Switzerland.

This CPS is applicable to all persons, including, without limitation, all Subjects, Subscribers, Relying Parties, registration authorities and any other persons that have a relationship with SwissSign AG with respect to TLS Server certificates issued by this CA. This CPS also provides statements of the rights and obligations of SwissSign AG, authorized Registration Authorities, Subjects, Subscribers, Relying Parties, resellers, co-marketers and any other person, or organization that may use or rely on certificates issued by this CA.

In this CPS, “this CA” refers to Root CAs “SwissSign Gold CA - G2”, “SwissSign RSA TLS Root CA 2022 - 1” and all their subordinated issuing CAs for TLS certificates as shown in Figure 1 above unless stated differently. “SwissSign RSA TLS Root CA 2022 - 1” has obtained a Cross-certificate by the Root CA “SwissSign Gold CA - G2”.

1.2 Document name and identification

This document is named “SwissSign CPS TLS - Certification Practice Statement for TLS certificates” as indicated on the cover page of this document.

The applicable reference to the CPS for each certificate can be found in the issued certificate (please see chapter 7).

SwissSign has defined a fix Certificate Policy for each certificate type issued.

The TSPS and the service- related Certification Practice Statements do not contain an OID.

1.2.1 Revisions

Version	Date	Author	Comment
1.0	14.06.2021	Michael Günther	Initial CPS
2.0	11.10.2021	Michael Günther	Adding TLS Root
3.0	08.11.2021	Michael Günther	Correction to figure 2 and in chapter 4.9.1
4.0	01.07.2022	Adrian Mueller, Michael Günther	Adding new hierarchy, features (ACME) and requirements on signatures
5.0	26.06.2023	Adrian Mueller, Michael Günther	6.1.2 Archiving
6.0	19.10.2023	Adrian Mueller, Michael Günther	Updating chapters 1.5.4, 3.2.2, 3.2.3, 3.2.5, 4.2.1, 10
7.0	03.04.2024	Raffaela Achermann, Adrian Mueller	Deletion of CA (SwissSign EV Gold CA 2014-G22 and SwissSign Sever Gold CA 2014 -G22)
8.0	23.08.2024	Raffaela Achermann, Adrian, Mueller, Roman Fischer	Changed disclaimer and chapters 1.5.3 and 1.5.4, updated picture
9.0	15.10.2024	Adrian Mueller, Raffaela Achermann	Delete SwissSign RSA TLS Root CA 2021 and 2021 ICAs, update Graphic and remove demo pages under 2021
10.0	29.01.2025	Raffaela Achermann, Roman Fischer	Conversion to Markdown, Deletion of root: SwissSign Silver CA - G2
11.0	13.03.2025	Roman Fischer	Added MPIC
12.0	07.08.2025	Roman Fischer	Changes based on feedback from Mozilla during Root Inclusion and mass revocation in 5.7.1

1.3 PKI participants

1.3.1 Certification authorities

The TSP operates a Public Key Infrastructure, consisting of Root CAs “SwissSign Gold CA - G2”, “SwissSign RSA TLS Root CA 2022 - 1” and all their subordinated issuing CAs for TLS certificates as shown in Figure 1 above. “SwissSign RSA TLS Root CA 2022 - 1” has obtained a Cross-certificate by the Root CA “SwissSign Gold CA - G2”.

The issuing CAs shown in the overview are the only public CAs operated by the TSP that issue TLS certificates under this CPS.

The certification service provided by SwissSign includes by default all the procedures related to the life cycle of the pairs of keys and Certificates, which are described in this CPS.

1.3.2 Registration authorities

The TSP operates a Registration Authority, called “SwissSign RA” (abbreviated as RAO) that registers Subscribers of certificates issued by these CAs.

No external Registration Authorities are operated under this CPS.

1.3.3 Subscribers

In the context of this CPS, the term “Subscriber” refers to the “Requestor” of a certificate and “Subject” refers to the “Certificate Holder”.

Please refer to clause 9.6.3 of the TSPS [5] for Subject’s and Subscriber’s responsibilities.

1.3.4 Relying parties

Relying Parties are individuals or organizations that use certificates of this CA to verify the identity of Subscribers and to validate the secure communication with these Subscribers.

Relying Parties are allowed to use such certificates only in accordance with the terms and conditions set forth in this CPS. It is in the sole responsibility of the Relying Party to verify revocation status, legal validity and applicable policies.

Relying Parties can also be Subscribers within the PKI described by this CPS.

1.3.5 Other participants

Not applicable

1.4 Certificate usage

The certificate usage in relation of the key usage as well extended key usage are defined within the CPR [4].

1.5 Policy administration

1.5.1 Organization administering the document

The CPS is written and updated by SwissSign AG.
SwissSign AG
Sägereistrasse 25
8152 Glattbrugg
Switzerland
Tel.: +41 800 55 77 77
Mail: helpdesk@swisssign.com
Web: https://swisssign.com

1.5.2 Contact person

For all questions or suggestions concerning this document, and to submit Certificate Problem Reports, the following contact options are available:

SwissSign AG
Sägereistrasse 25
8152 Glattbrugg
Switzerland
Tel.: +41 800 55 77 77
Mail: certificatemisuse@swisssign.com
Web: https://swisssign.com

Business hours are business days (excluding public holidays)
from 08:00 to 12:00, 13:00 to 17:00 CET/CEST.

1.5.3 Person determining CPS suitability for the policy

The Management Board of SwissSign AG shall determine the suitability of this document.

Changes or updates to relevant documents shall be made in accordance with the stipulations of technical and legal requirements and the provisions contained in this document.

1.5.4 CPS approval procedures

This document and its related documentation shall be regularly reviewed by Information Security & Compliance and approved by a member of the SwissSign AG management board.

Following the approval, this document and its relevant documentation shall be published and communicated to employees of SwissSign and external parties as relevant.

1.6 Definitions and acronyms

Refer to clause 1.6 of the TSPS [5].

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Refer to clause 2 of SwissSign TSPS [5].

2.1 Repositories

Refer to clause 2.1 of SwissSign TSPS [5].

2.2 Publication of certification information

Refer to clause 2.2 of SwissSign TSPS [5].

2.3 Time or frequency of publication

Refer to clause 2.2 of SwissSign TSPS [5].

The TSP publishes the information on a regular schedule:

- CRLs are published according to the schedule detailed in chapter 4.9.7.
- OCSP Information: Real-time. The OCSP responder immediately reports a certificate that has been revoked. See also chapter 4.9.9.

Even if no updates are required, a new version of this document is published at least once a year.

2.4 Access controls on repositories

Refer to clause 2.4 of SwissSign TSPS [5].

2.5 Additional testing

Demo pages are offered for all web server certificate types.

2.5.1 RSA TLS EV Certificates (EV)

- Valid: https://ev-rsa-tls-2022-valid-cert-demo.swisssign.com
- Expired: https://ev-rsa-tls-2022-expired-cert-demo.swisssign.com
- Revoked: https://ev-rsa-tls-2022-revoked-cert-demo.swisssign.com

2.5.2 RSA TLS OV Certificates (OV)

- Valid: https://ov-rsa-tls-2022-valid-cert-demo.swisssign.com
- Expired: https://ov-rsa-tls-2022-expired-cert-demo.swisssign.com
- Revoked: https://ov-rsa-tls-2022-revoked-cert-demo.swisssign.com

2.5.3 RSA TLS DV Certificates (DV)

- Valid: https://dv-rsa-tls-2022-valid-cert-demo.swisssign.com
- Expired: https://dv-rsa-tls-2022-expired-cert-demo.swisssign.com
- Revoked: https://dv-rsa-tls-2022-revoked-cert-demo.swisssign.com

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

(DVCP) DV TLS certificates contain only the FQDN in the common name field within the distinguished name.

(EVCP & OVCP) EV and OV TLS certificates contain the FQDN in the common name field as well as further attributes of the organization owning the FQDN.

Type of names assigned to the Subscriber is described in detail in the Certificate Profile [4].

For all TLS Certificates: Prohibited IPv4 or IPv6 addresses are these, that the IANA has marked as reserved:

- http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
- http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Underscore characters are not allowed in a any part of the subject information.

For Extended Validation Certificates the following, additional practices is implemented:

- The certificate Subject is conforming to the EV guidelines
- Wildcard certificates are not allowed

An excerpt from the national trademark registry is required when requesting certificates with trademark.

3.1.2 Need for names to be meaningful

The Subject and issuer name contained in a certificate are chosen to be meaningful in the sense that the registration authority has proper evidence of the existing association between these names and the entities to which they belong. The use of a name is authorized by the rightful owner or a legal representative of the rightful owner.

The meaning of names in different fields of the Certificates is described in the Certificate Profile [4].

3.1.3 Anonymity or pseudonymity of subscribers

For all types of TLS certificates, pseudonyms are not supported.

3.1.4 Rules for interpreting various name forms

For all attributes in the distinguished name that are specified as UTF8string, it is permissible to use UTF8 encoding.

Many languages have special characters that are not supported by the ASCII character set used to define the Subject in the certificate. To avoid problems, local substitution rules may be used:

- In general, national characters are represented by their ASCII equivalent, e.g. é, è, à, ç are represented by e, e, a, c.
- The German “Umlaut” characters ä, ö, ü are represented by either ae, oe, ue or a, o, u.
- SwissSign follows RFC 5890/5891 (Internationalized Domain Names) guidelines to internationalize domain names.

3.1.5 Uniqueness of names

All Issuing CAs under this CPS enforce the uniqueness of certificate Subject fields in such a manner that all certificates with identical Subject fields belong to the same individual or organization. The following practices are enforced:

- All actual valid, revoked and expired TLS certificates with identical Subjects belong to the same Subscriber.

Depending on the certificates issued the uniqueness of the Distinguished Name is achieved through different unique identifiers as defined in the CPR [4].

3.1.6 Recognition, authentication, and role of trademarks

The TSP and its RAs reserve the right to reject certificate requests or revoke certificates containing offensive or misleading information or names protected by legislation and possibly infringing rights of others. The TSP is not obliged to verify lawful use of names. It is the sole responsibility of the Subscriber to ensure lawful use of chosen names.

The TSP will comply as quickly as possible with any court orders issued in accordance with Swiss Law that pertain to remedies for any infringements of third party rights by certificates issued under this CPS.

3.2 Initial identity validation

The initial identity validation is part of the Certificate Application process as described in chapter 4.1. Existing evidences can be re-used to validate the identity depending on the validity of the evidence.

(EVCP) The evidences are not used if older than 13 months.

(DVCP & OVCP) The evidences are not used if older than 825 days.

The TSP has implemented procedures that identify certain certificate requests they will require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval. Each certificate request that is categorized as High Risk Certificate Request is reviewed separately by a member of the compliance department of the TSP.

3.2.1 Method to prove possession of private key

The Certificate Signing Request sent to the CA from the Subscriber is signed with the private key. The Subscriber must present a PKCS#10 formatted request. The CA verifies the signature.

3.2.2 Authentication of organization and domain identity

3.2.2.1 Authentication of organization identity

The RA collects and verifies the following evidence about the organization identity as well as the authorization to use the identity attributes before issuing the certificate as follows:

(EVCP & OVCP):

- Prior to using any data source as a Reliable Data Source, the RA evaluates the source for its reliability, accuracy, and resistance to alteration or falsification.
- To validate the name and location of the organization, the Subscriber must provide official documentation about the organization provided by a government agency in the jurisdiction of the organization's legal creation, existence, or recognition or by any other official source that is considered a reliable data source.
- (EVCP) The list of Registers for Private Organizations used to validate organization information for EV TLS certificates can be found in our repository.
- Organizations with an entry in the federal or a nationally recognized commercial register must supply verifiably current excerpt. All other organizations must supply evidence of registration of a nationally recognized register (e.g. FTA or VAT).
- Government entities must supply official documentation to prove the existence and the correct spelling of the entities' name.

- The validation of an organization's name is performed directly with the authoritative source instead of the organization.
- The address information is verified in context of legal identity.

(EVCP) EV Certificates will only be issued in accordance with the EV Guidelines to the following types of organizations:

- Private Organizations
- Government Entities
- Business Entities
- Non-commercial Entities

3.2.2.2 Authentication of domain identity

(all TLS policies):

- The use of a domain name in an FQDN must be authorized. The TSP only accepts the automated SwissSign-check procedure as proof of domain ownership. In this automated procedure, the applicant must prove control of the domain according to the methods for domain validation permitted in chapter 3.2.2.4 of the CA Browser Forum Baseline Requirements (BR). Internal domain names that cannot be accessed through public DNS are not accepted by the TSP, in particular domain names containing a gTLD which is not yet resolvable. The TSP generates random value valid for 30 days. Only after a successful check of the random value is the control of the domain ownership completed. The following three methods for proving domain ownership are in use:
  - BRG 3.2.2.4.4 Constructed Email to Domain Contact (webshop only)
  - BRG 3.2.2.4.7 DNS Change (Managed PKI and webshop)
  - BRG 3.2.2.4.19 Agreed-Upon Change to Website - ACME; according to RFC 8555 plus additional requirements (Managed PKI only)
    BRG 3.2.2.4.19 Agreed-Upon Change to Website - ACME is not allowed for validating wildcard domain names.
- No .onion certificates are issued.

Please note:

- For the issuance of wildcard certificates only BRG 3.2.2.4.4 Constructed Email to Domain Contact and BRG 3.2.2.4.7 DNS Change are applied as validation methods.

3.2.2.3 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration (MPIC) attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the primary network perspective from multiple remote network perspectives before certificate issuance.

Starting (latest) March 15, 2025 Multi-Perspective Issuance Corroboration (MPIC) is used for the domain control validation methods as follows:

- BRG 3.2.2.4.4 Constructed Email to Domain Contact: CAA checks use MPIC
- BRG 3.2.2.4.7 DNS Change: CAA checks and check of random value in DNS use MPIC
- BRG 3.2.2.4.19 Agreed-Upon Change to Website - ACME: CAA checks and check of random value on website use MPIC

SwissSign implements MPIC with the following properties:

- At least 2 remote network perspectives are implemented. SwissSign may proceed if the number of the non-corroborations is greater then allowed.
- Results or information obtained from one Network Perspective are not reused or cached
- All communications between a remote Network Perspective and the CA take place over an authenticated and encrypted channel (HTTPS with mutual authentication)
- Adheres to the “Quorum Requirements” table and Phased Implementation Timeline in TLS BR 3.2.2.9

- Remote perspectives are at least 500km apart from each other and use built-in DNS resolvers for minimal dependency on 3rd party providers
- The same set of Network perspectives are used for all CAA and domain validation checks
- MPIC implementation will return the FQDN and the random value as well as the CAA information found for this FQDN to the primary perspective for verification
- MPIC is retried until the quorum is achieved using the same validation method as initiated
- Relies only upon networks implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the network perspective

3.2.3 Authentication of individual identity

Individuals acting as Applicant subjects are identified by one of the following possibilities.

The registration process of any registration authority operating under this CPS contain provisions to determine the identity of such individuals. The identification is performed as follows:

- The Subscriber is present in person or in an equivalent electronic (manual or automated) procedure according to ETSI EN 319 411-1 6.2.2. This step may be conducted by:
  - the registration authority processing the certificate request,
  - an accredited notary,
  - a trained and contracted partner for the identification service.
- The individual presents a valid original of an official identification document as recognized by national law. The identifying agent (human or automated process) is to make a high-quality copy, scan or photograph of the identifying document, to inspect the copy for any indication of alteration or falsification. and to confirm proper execution of the identification in writing or electronically as agreed with the TSP.
- The photo in the identifying document is compared to has to match (facial features, age, gender and size) the person present as described above.

3.2.4 Non-verified subscriber information

All Subject and/or Subscriber information and evidences needed to be verified in accordance with the certificate policy are verified by the RA. Additional information given by the Subscriber, which do not affect the certificate content or relevant authorization, is not verified.

3.2.5 Validation of authority

(EVCP & OVCP):

The Subscriber provides current and valid documentation for the organizational or corporate name that shall be included in the certificate, according to Chapter 3.2.2 The wording of the organizational or corporate name that shall be included in the certificate must be exactly identical to the wording in the documentation provided.

The use of the organizational name must be authorized by legal representatives of this organization.

- The use of the organizational name of an organization with a commercial register entry must be authorized by representatives from the board of directors and/or executive management, who are listed in the excerpt of the commercial registry.
- The use of the organizational name of a sole proprietorship must be authorized by the owner named in the current VAT invoice.
- The use of the organizational name of an organization with a deed of partnership must be authorized by a partner named in the deed of partnership.
- The use of the organizational name of a community must be authorized by the corresponding cantonal agency and a copy of the directive of election.

In addition, the TSP has established the processes for the Subscriber organization to add and remove operators who are authorized to request certificates.

These individuals (representatives and operators) must be identified according to the stipulations given in chapter 3.2.3.

The RA verifies the presented evidence during the registration process before issuance of the certificate.

Upon request, the TPS provides a list of its authorized operators to one of these operators or a representative only.

(all TLS policies): The successful verification of an FQDN following the procedure stated in chapter 3.2.2 requires and thus proves the authority to manage the corresponding DNS entry.

3.2.6 Criteria for interoperation

SwissSign does not support cross-certification for external organizations. Cross-certificates are issued for Root CA and Issuing CA issued for SwissSign itself as an organization and not allowed for CAs issued for external organizations as Subscriber.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The Subscriber is identified by the SwissSign RA using the identity information and the evidences from the original request, in case they haven't change.

(EVCP) The validity period for the data included in an EV certificate as well as provided evidences is limited to 13 months. After this period (determined by the date on the substantiating documentation provided), the data provided in the certificate as well as the provided evidences are validated again by the SwissSign RA.

(OVCP & DVCP) The validity period for the data included in an OVCP and DVCP certificate as well as provided evidences is limited to 27 months (<825 days). After this period, the data provided in the certificate as well as provided evidences are validated again.

3.3.2 Identification and authentication for re-key after revocation

The TSP does not support re-keying of certificates issued by this CA after revocation.

3.4 Identification and authentication for revocation request

Revocation of a certificate that is issued by this CA requires that the Subscriber is authenticated according to one of the following methods:

- successful login to the user profile on the website of the RA,
- providing proof of the possession of the private key on the web site of the registration authority,
- with a personal signature,an advanced electronic signature (according to NCP+ or EU ordinance eIDAS) or a qualified electronic signature (according to the Swiss Digital Law (ZertES) or eIDAS) on a revocation form,
- appearance in person at the registration authority,
- providing a one-time revocation key on the web site of the registration authority.

Not all methods are supported for all types of certificates.

The process how the revocation request can be submitted is described in chapter 4.9.3.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Each certificate issued by the TSP is securely stored in a database and has a unique reference to the certificate application data.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Applications can be submitted by anyone who complies with the provisions specified in the registration form, CPS and relevant End-User Agreement. The applicable legal documents (Terms and Conditions, CPS) are displayed to the Subscriber during the application process.

Certificate request can be made via customer M-PKI or Webshop.

4.1.2 Enrollment process and responsibilities

The RA collects and verifies the following during its enrollment process:

- identity of the Subscriber and of all persons authorizing the certificate request according to chapter 3,
- type of document(s) and evidences presented by the applicant to support registration according to chapter 3,
- record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable,
- method used to validate identification documents,
- any specific obligations in the Subscriber agreement (Including consent to publication of certificate),
- storage location of copies of applications and identification documents, including the Subscriber agreement,
- identity of entity accepting the application,
- method used to validate the FQDN.

Certificate Subscribers have to follow the TSP registration formalities as specified in the relevant documents and provisions provided by the CA. The certificate is issued only after successful completion of the registration process. The main steps for a certificate registration are:

- Valid identification documentation is provided and complete registration forms have been signed (delivery of a scan by email is sufficient), and the CPS and End-User Agreement have been accepted by the Subscriber,
- Registration forms can also be signed electronically with an advanced electronic signature (according to NCP+ or EU ordinance eIDAS) or a qualified electronic signature (according to the Swiss Digital Law (ZertES) or eIDAS). In this case the RAO checks, validates and keeps all necessary records regarding the qualified electronic signature.
- all documents and information are approved by the SwissSign RA.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Evidence of the identity and if necessary of any specific attributes of the corresponding Subject are collected by the TSP directly or by attestation from a third party. Submitted evidence may be in the form of either paper or electronic documentation. The RA identifies the Subscriber on the basis of the identifying documents that the Subscriber presents, as stipulated in chapter 3.2 of this document.

(all TLS policies) Prior to issuance SwissSign validates each server Name FQDN in publicly trusted TLS certificates to be controlled by the Subscriber as defined in chapter 3.2.

Domain CAA records: If a CAA record exists that does not authorize SwissSign, SwissSign will not issue the certificate. If the verification of the CAA entry fails or is not possible for technical reasons, no certificate will be issued.

Starting (latest) March 15, 2025 Multi-Perspective Issuance Corroboration (MPIC) is used for all CAA and domain validation checks as described in chapter 3.2.2.3.

The default Issuer Domain Name for SwissSign is "swisssign.com".

Furthermore SwissSign:

- caches CAA records for reuse for up to 8 hours,
- supports the issue and issuewild CAA tags,

- processes but does not act on iodef property tag (i.e., SwissSign does not dispatch reports of such, issuance requests to the contact(s) stipulated in the CAA iodef record(s)),
- does not support any additional property tags,
- if an unknown property is marked critical or if a CAA check cannot be executed for any reason, no certificate will be issued.

The TSP has implemented technical controls that determines that the wildcard character does not occur in the first label position to the left of a "registry-controlled" label or "public suffix".

(EVCP) Before issuing an EV certificate, SwissSign ensures that all Subject organization information in the EV certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended accomplish the following:

Verify the organization's existence and identity, including:

- the organization's legal existence and identity (as established with an incorporating agency),
- the organization's physical existence (business presence at a physical address),
- the organization's operational existence (business activity),
- that the organization (or a corporate parent/subsidiary) is a registered holder or has exclusive control of the domain name to be included in the EV certificate.

Verify the Subscriber's authorization for the EV certificate, including:

- the name, title, and authority of the certificate Subscriber,
- that the certificate Subscriber signed the registration form,
- the authority to approve the EV certificate request ("certificate approver" role according to CA Browser Forum),
- the authority to approve the Terms and Conditions ("contract signer" role according to CA Browser Forum),
- the communication channel to the applicant is confirmed by the previously gathered email or telephone contact.

4.2.2 Approval or rejection of certificate applications

The RA approves a certificate request if all of the following criteria are met:

- the Subscriber has presented the identifying documentation according to chapter 3.2.3,
- all documentation has been received and verified successfully,
- all authorizations have been received and verified successfully,
- the information provided in the registration form is deemed adequate and complete,
- the verification of the Uniqueness of Names according to chapter 3.1.5 has not revealed any collisions.

If the Subscriber fails to adhere to any of the above, or in any other way violates the stipulations of this document, the RA rejects the certificate signing request.

The TSP reserves the right to decline certificate requests without giving reasons.

4.2.3 Time to process certificate applications

The RA processes a regular, fully documented certificate request no longer than two business days.

This time may be extended by circumstances not fully under the control of the registration authority:

- Delivery times of postal services,
- Incomplete or incorrect documentation,
- Validation of information with external sources.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon receipt of an approved certificate signing request, the CA will verify

- the integrity of the request,
- the authenticity and authorization of the RAO,
- the contents of the certificate requests for compliance with the technical specification as outlined in chapter 7.1.2.

On successful verification, the CA will then issue the requested certificate.

As a part of the issuing process pre- and post-linting of the certificates is implemented.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA may:

- email the certificate to the Subscriber,
- electronically provide the certificate to the Subscriber within its self service portal (M-PKI),
- email information permitting the Subscriber to download the certificate from a web site or repository.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Subscribers are not required to confirm the acceptance of the certificate separately.

After notification as in chapter 4.3.2 the subscriber has to verify the certificate content immediately. During a time frame of 24 hours the subscriber can reject or complain about the certificate. After this time frame, he has accepted the certificate. This step is considered sufficient and no further confirmation is required.

4.4.2 Publication of the certificate by the CA

The Subscriber agrees that the TSP will publish the certificate and certificate status information in accordance with applicable regulations.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA will not notify other entities about the issuance of certificates.

4.4.4 Certificate Transparency

SwissSign is supporting Certificate Transparency for all TLS certificates according IETF RFC 6962. During the issuing of a TLS certificate SwissSign provides the TLS certificate to at least two different CT log servers. Pre-certificate, as described in RFC 6962 – Certificate Transparency, are considered to be a “certificate” Subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under this CPS.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The use of certificates by Subscribers must adhere to the obligations stipulated in chapter 9.6.3 of the TSPS [5], summarized as follows:

- Certificates issued under this CPS may only be used in accordance with the key usage declaration contained in the certificate.

- Subscribers may only use SwissSign certificates for intended, legal, and authorized purposes.
- Subscribers may only use a SwissSign certificate on behalf of the person or the organization listed as the Subject of such a certificate.
- Subscribers must read and agree to the General Terms and Conditions and the applicable End-User Agreement,

4.5.2 Relying party public key and certificate usage

Relying Parties shall:

- be held responsible for the understanding of:
  - the proper use of public key cryptography and certificates,
  - the related risks,
- read and agree to all terms and conditions of this CPS and the End-User Agreement for Relying Parties,
- verify certificates issued by this CA, including use of revocation information, in accordance with the certification path validation procedure, taking into account any critical certificate extensions and key usage.
- use their best judgment when relying on a certificate issued by this CA and assess if such reliance is reasonable under the circumstances,
- determine whether such reliance is reasonable given the extent of the security and trust provided by a certificate issued by the CA,
- comply with all laws and regulations applicable to a Relying Party's right to export, import, and/or use a certificate issued by the CA and/or related information. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by the CA and/or related information.

4.6 Certificate renewal

Certificate renewal is not supported by the TSP.

4.7 Certificate re-key

Certificate re-keying is a process where a Subscriber requests a certificate, using a new key pair. The resulting certificate contains new validity information and a new public key, but retains the same validated subject information. The validity of subject information and evidences are defined in chapter 3.3.1. In case, subject information has changed, the initial certificate issuance apply.

Subscriber private key and certificate usage is stipulated as stated in clause 4.5.1.

4.7.1 Circumstance for certificate re-key

The Subscriber may choose to renew a certificate if the following conditions are met:

- The Subscriber owns a currently valid certificate from this CA.
- All information in the certificate is still correct.
- The verification of the identity and evidences is still within the time period allowed by legal and regulatory requirements governing this type of certificate.
- The cryptographic material used meets the requirements of the TLS BR, the EV guidelines as well as ETSI EN 119 312 and ETSI EN 319 411-1.

4.7.2 Who may request certification of a new public key

The TSP accepts a certificate re-key request applied by the Subscriber only.

4.7.3 Processing certificate re-keying requests

The Subscriber can apply for the re-key as defined for the initial process.

In case of M-PKI, the Subscriber uses the interface provided by the TSP to request a new certificate.

The applicable legal documents (Terms and Conditions, CPS) are communicated to and agreed by the Subscriber during the re-key process.

4.7.4 Notification of new certificate issuance to subscriber

The same procedures as for initial certificate issuance apply, see clause 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The same procedures as for initial certificate issuance apply, see clause 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

The same procedures as for initial certificate issuance apply, see clause 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

The same procedures as for initial certificate issuance apply, see clause 4.4.3.

4.8 Certificate modification

The TSP does not support certificate modification. In case the certificate includes wrong content, the certificate is revoked and the Subscriber has to apply as initially.

4.9 Certificate revocation and suspension

The procedures of the TSP meet the requirements of Root Store Policies, CA/B Forum Requirements and ETSI EN 319 411-1. Certificate revocation is irreversible. Once a certificate has been revoked, the certificate cannot be valid again, which is technically enforced by the CA.

Subscribers or Relying Parties are requested to apply for certificate revocation immediately if there is a suspicion that private keys have been compromised or the content of the certificate is no longer correct (e.g. the abolition of the certificate holder's membership of an organization).

Requests for revocation require sufficient authentication by using the provided secret during certificate enrollment, using account and password or signed revocation request.

The TSP maintains a comprehensive and actionable plan for mass revocation events, performs annual testing of its procedures, and incorporates lessons learned to improve preparedness over time.

The TSP logs all revocations in the CA Journal Database (5.4). If the request for revocation has been submitted in writing, the request for revocation is archived with all evidence and checklists.

4.9.1 Circumstances for revocation

Subscribers may revoke their certificates at will.

The CA revokes a Subscriber's certificate within 24 hours of receiving the information that one of the following conditions is met:

- The Subscriber requests in writing that the CA revoke the certificate
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization
- The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise

- The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed.
- The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name in the Certificate should not be relied upon. The private key of the issuing CA or any of its superior CAs has been compromised.

The CA revokes a Subscriber's certificate within 5 days of receiving the information that one of the following conditions is met:

- The certificate issued does not comply with the terms and conditions of this CPS.
- The CA obtains evidence that the Certificate was misused
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use and/or other applicable laws, rules and regulations. In addition, The TSP may investigate any such incidents and take legal action if required.
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name)
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name
- The CA is made aware of a material change in the information contained in the Certificate, e.g.
  - Any part of the certificate Subject has changed.
  - The certificate /O= field is no longer valid. (e.g. bankruptcy of the organization)
  - The certificate /CN= field is no longer valid (e.g. omission of domain registration renewal).
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement
- The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository
- Revocation is required by this CPS or the BRG

The CA revokes an Issuing CA certificate within 7 days of receiving the information that one of the following conditions is met:

- The Issuing CA obtains evidence that the Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the terms and conditions of this CPS.
- The Issuing CA obtains evidence that the Certificate was misused.
- The Issuing CA is made aware that the Certificate was not issued in accordance with this CPS.
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading.
- The Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
- The Issuing CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by this CPS.

4.9.2 Who can request revocation

This CA accepts certificate revocation requests from the following sources:

- Subject or Subscriber of the certificate,
- the owner of the profile used to issue the initial registration request,
- the owner of the private key,
- an authorized representative of the organization that has approved the content of the /O= field in the certificate,
- a properly authorized RAO,

- a properly authorized TSP Operator,
- a Swiss court of law.

Additionally, Subscribers, Relying Parties and everybody else may submit Certificate Problem Reports informing the TSP of reasonable cause to revoke the certificate.

4.9.3 Procedure for revocation request

Any one of these procedures can be used to request a revocation of a certificate:

- (Webshop) The Subscriber can use the online revocation functions in the profile that issued the initial registration request.
- (M-PKI) The Subscriber can use its M-PKI interface.
- (Webshop) By using the provided revocation passphrase at the end of the registration process, the Subscriber can revoke the certificate.
- The Subscriber can personally visit the RA offices and request the revocation of a certificate offline. The Subscriber must present either a valid passport or an identity card issued by an EU or EFTA member state.
- The Subscriber can submit an offline revocation form and send it to the TSP. After checking the validity of the revocation request, the TSP revokes the certificate.
- By submitting a revocation form which can also be signed electronically. See chapter 3.4 for details. In this case RAO check, validates and keeps all necessary records regarding the electronic signature.

Also see the key compromise process explained in chapter 4.9.12.

4.9.3.1 Notification about revocation

The TSP sends the information about certificate revocation to the Subscriber by e-mail using the e-mail address that was given during the certificate application.

4.9.4 Revocation request grace period

The Subscriber is required to request a revocation request immediately if one of the reasons listed in the subscriber agreement occurs. Please see clause 9.6.3 of the TSPS [5].

4.9.5 Time within which CA must process the revocation request

After the verification of the revocation request that details in chapters 4.9.1 and 4.9.2 have been met, the registration authority will process written revocation requests and Certificate Problem Reports within 24 hours. If the Subscriber requires the revocation on an appointed date and the certificate concerned will be revoked at the time required, then the time of the actual revocation is noted as the time of the receipt of the request.

Online revocation is effective on the spot (24x7), offline revocation methods are typically several days slower than online revocations. The Subscriber must take full responsibility for the consequences of any and all delays that result from the chosen revocation method.

Should the online revocation methods be unavailable, the Subscriber must use the offline method. Every registration authority guarantees processing of offline revocation requests without undue delay, if they are supplied according to the procedure described in 4.9.3.

4.9.6 Revocation checking requirement for relying parties

Relying Parties must, when working with certificates issued by this CA, verify these certificates at all times. This includes the use of CRLs, in accordance with the certification path validation procedure specified in RFC 5280. Also, any and all critical extensions, key usage, and approved technical corrigenda as appropriate should be taken into account.

4.9.7 CRL issuance frequency

CA Information Frequency:

- Root CAs
  - CARL: At least once every 365 days and within 24 hours for every revocation. At most 24 hours may pass from the time a certificate is revoked until it is reported on the CARL.
  - OCSP Information: Real-time. The OCSP responder reports a certificate's revocation immediately after the revocation has been completed.
- Subordinated issuing CAs
  - CRL: At least once every 24 hours. At most, one hour may pass from the time a certificate is revoked until the revocation is reported on the CRL.
  - OCSP Information: Real-time. The OCSP responder reports a certificate's revocation immediately respectively 10 minutes after the revocation has been completed.

4.9.8 Maximum latency for CRLs

The CRL of this CA and all its subordinated issuing CAs is issued according to chapter 4.9.7 and published without delay.

4.9.9 On-line revocation/status checking availability

This CA and all its subordinated issuing CAs support the OCSP protocol for online revocation checking. If OCSP is available, the "Authority Information Access" field of the certificate contains the OCSP responder URL. The OCSP response is signed by a dedicated OSCP Responder, whose certificate is signed by the CA which issued the certificate whose revocation status is being checked.

For subordinate CA certificates revocation status is provided over CRLS only and not over OCSP.

4.9.10 On-line revocation checking requirements

Relying parties must, when working with certificates issued by this CA, at all times verify the certificates issued by this CA. This includes the use of CRLs in accordance with the certification path validation procedure specified in RFC 5280 and/or RFC 6960 for OCSP. OCSP is supported over HTTP GET and POST method. While certificate serial numbers are reserved (only a pre certificate is issued) the OCSP responds with the status ‚unknown'. Once the actual certificate is issued, the OCSP starts responding with ‚good'.

4.9.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.9.12 Special requirements regarding key compromise

If a Subscriber knows or suspects that the integrity of his certificate's private key has been compromised, the Subscriber shall:

- immediately cease using the certificate,
- immediately initiate revocation of the certificate,
- delete the certificate from all devices and systems,
- inform all Relying Parties that may depend on this certificate.

The compromise of the private key may have implications on the information protected with this key. The Subscriber must decide how to deal with the affected information before deleting the compromised key.

A party who discovers a key compromise may report it by sending an email to the address keycompromise@swisssign.com. The email must contain:

- Subject: “Key compromise SwissSign certificate”,
- the certificate affected by the key compromise in PEM format.
- a Certificate Signing Request in PEM format
  - signed by the compromised key and
  - containing a Common Name «Key compromise SwissSign certificate”

4.9.13 Circumstances for suspension

The TSP does not provide suspension.

4.9.14 Who can request suspension

The TSP does not provide suspension.

4.9.15 Procedure for suspension request

The TSP does not provide suspension.

4.9.16 Limits on suspension period

The TSP does not provide suspension.

4.10 Certificate status services

The TSP provides CRL and OCSP status service. Access to these services is provided through the web site “swisssign.net” and the online LDAP directory. The certificate status services provide information on the status of certificates until the expiry date of the last end-user certificate issued under the Issuing CA. The integrity and authenticity of the online status information (OCSP) is protected by a digital signature of the dedicated OCSP responder certificate which is signed from the appropriate issuing CA. The CRL is directly signed by the appropriate issuing CA. Integrity and authenticity of the revocation information is guaranteed by a signature of the CRL or the OCSP response.

Before revoking an Issuing CA certificate, the TSP makes sure that all leaf-certificates in the scope of the CRL are either expired or revoked.

4.10.1 Operational characteristics

Consent to the publication is a condition for the application for certificates. CA and OCSP responder certificates are published after they are issued and are available at least until the end of the year in which they become invalid. CRLs are issued regularly and until the end of the validity of the issuing CA.

4.10.2 Service availability

The TSP has ensured through technical measures that the certificate status services are available 24 hours per day, 7 days per week. The availability of this service is indicated in the form of a URL in the certificates.

The TSP operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.10.3 Optional features

The SwissSign certificate status services do not include or require any additional features.

4.11 End of subscription

End of subscription occurs after:

- successful revocation of the last certificate of a Subscriber,
- expiration of the last certificate of a Subscriber.

For reasons of legal compliance, the SwissSign CA and all registration authorities must keep all Subscriber data and documentation for a minimum period of 11 years after termination of a subscription.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Key escrow and key recovery are not supported by the TSP.

4.12.2 Session key encapsulation and recovery policy and practices

This CA does not support session key encapsulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Refer to clause 5.1 of SwissSign TSPS [5].

5.2 Procedural controls

Refer to clause 5.2 of SwissSign TSPS [5].

5.3 Personnel controls

Refer to clause 5.3 of SwissSign TSPS [5].

5.4 Audit logging procedures

Refer to clause 5.4 of SwissSign TSPS [5].

5.5 Records archival

Refer to clause 5.5 of SwissSign TSPS [5].

5.6 Key changeover

Refer to clause 5.6 of SwissSign TSPS [5].

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Refer to clause 5.7.1 of SwissSign TSPS [5] regarding incident and compromise handling procedures in general.

In addition SwissSign maintains a comprehensive and actionable plan for mass revocation events of TLS certificates.

SwissSign performs annual testing of the mass revocation plan, and the lessons learned are incorporated into the mass revocation plan in order to continually improve the preparedness for mass revocation events over time.

5.7.2 Computing resources, software, and/or data are corrupted

Refer to clause 5.7.2 of SwissSign TSPS [5].

5.7.3 Entity private key compromise procedures

Refer to clause 5.7.3 of SwissSign TSPS [5].

5.7.4 Business continuity capabilities after a disaster

Refer to clause 5.7.4 of SwissSign TSPS [5].

5.8 CA or RA termination

Refer to clause 5.8 of SwissSign TSPS [5].

6. TECHNICAL SECURITY CONTROLS

Refer to clause 6 of SwissSign TSPS [5].

6.1 Key pair generation and installation

Refer to clause 6.1 of SwissSign TSPS [5].

6.1.1 Key pair generation

For Root and Issuing CAs, refer to clause 6.1.1 of SwissSign TSPS [5] and clause 6.1.1 of the TLS BR [8].

The key pairs are produced under the responsibility of the Subscriber, they must not use weak Debian keys and shall use secure keys.

6.1.2 Private key delivery to subscriber

Private keys for TLS certificates must be generated by the Subscriber. No certificate requests including Private keys are accepted for TLS certificates.

6.1.3 Public key delivery to certificate issuer

The Subscriber presents the public key as a PKCS#10-formatted certificate signing request to the signing CA using a secure TLS-encrypted communication channel. By transmitting a PKCS # 10 request to the TSP, the Subscriber proves the possession of the private key.

6.1.4 CA public key delivery to relying parties

Refer to clause 6.1.4 of SwissSign TSPS [5].

6.1.5 Key sizes

The TSP follows the recommendations on algorithms and key sizes as they are made available by the following institutions:

- ETSI: ETSI TS 119 312 : http://www.etsi.org/standards-search
- NIST: SP 800-89

The Root CA uses a 4096-bit RSA key.

Issuing CAs issued before 2021 use a 2048-bit RSA key. Issuing CAs issued in 2021 and later use a 4096-bit RSA key.

All Issuing CAs allow Subscribers to use RSA key length with a modulus size of at least 2048 bits and divisible by 8.

6.1.6 Public key parameters generation and quality checking

Parameters can be selected by Subscribers, but are verified by the RA and the CA. The TSP rejects certificate requests when the submitted Public Key does not meet the requirements of Sections 6.1.1.3, 6.1.5 and 6.1.6 of the CA Browser Forum Baseline Requirements or when the submitted Public Key has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage purposes are described in clause 7.1 of this CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The following list shows how the requirements for the different users of cryptographic modules are implemented:

- Root CA keys: Refer to clause 6.2.1 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.1 of SwissSign TSPS [5].
- Subscriber keys: The Subscriber is fully responsible for the evaluation, implementation and protection of the cryptographic module, where the Subscriber keys are generated and stored.

6.2.2 Private key (n out of m) multi-person control

The following list shows how multi-person controls are implemented:

- Root CA keys: Refer to clause 6.2.2 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.2 of SwissSign TSPS [5].

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

- Root CA keys: Refer to clause 6.2.3 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.3 of SwissSign TSPS [5].
- Subscriber keys: Private keys are not escrowed by the TSP

6.2.4 Private key backup

The following list shows how private key backup is implemented:

- Root CA keys: Refer to clause 6.2.4 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.4 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for the backup of Subscriber keys.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

- Root CA keys: Refer to clause 6.2.5 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.5 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for the archival of Subscriber keys.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

- Root CA keys: Refer to clause 6.2.6 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.6 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for the transfer of Subscriber keys into or from a cryptographic module.

6.2.7 Private key storage on cryptographic module

The following list shows how private keys are stored on cryptographic modules:

- Root CA keys: Refer to clause 6.2.7 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.7 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for the transfer of Subscriber keys into or from a cryptographic module.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

- Root CA keys: Refer to clause 6.2.8 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.8 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for the method of activating private keys.

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

- Root CA keys: Refer to clause 6.2.9 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.9 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for the deactivation of private key.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

- Root CA keys: Refer to clause 6.2.10 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.2.10 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are solely responsible for destroying the private key.

If an HSM that was used within the TSP is no longer in use or replaced, the HSM will be physically destroyed.

6.2.11 Cryptographic Module Rating

Refer to clause 6.2.11 of SwissSign TSPS [5].

6.3 Other aspects of key pair management

6.3.1 Public key archival

Refer to clause 6.3.1 of SwissSign TSPS [5].

6.3.2 Certificate operational periods and key pair usage periods

Refer to clause 6.3.2 of SwissSign TSPS [5].

TLS certificates are issued with a validity period not greater than 398 days.

6.4 Activation data

6.4.1 Activation data generation and installation

Refer to clause 6.4.1 of SwissSign TSPS [5].

6.4.2 Activation data protection

- Root CA keys: Refer to clause 6.4.2 of SwissSign TSPS [5].
- Issuing CA keys: Refer to clause 6.4.2 of SwissSign TSPS [5].
- Subscriber keys: Subscribers are obliged to keep the activation data secret at all times.

6.4.3 Other aspects of activation data

Refer to clause 6.4.3 of SwissSign TSPS [5].

6.5 Computer security controls

Refer to clause 6.5 of SwissSign TSPS [5].

6.5.1 Specific computer security technical requirements

Refer to clause 6.5.1 of SwissSign TSPS [5].

6.5.2 Computer security rating

Refer to clause 6.5.2 of SwissSign TSPS [5].

6.6 Life cycle technical controls

6.6.1 System development controls

Refer to clause 6.6.1 of SwissSign TSPS [5].

6.6.2 Security management controls

Refer to clause 6.6.2 of SwissSign TSPS [5].

6.6.3 Life cycle security controls

Refer to clause 6.6.3 of SwissSign TSPS [5].

6.7 Network security controls

Refer to clause 6.7 of SwissSign TSPS [5].

6.8 Time-stamping

Refer to clause 6.8 of SwissSign TSPS [5].

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The Certificate profile is described in the Certificate Profile [4].

7.2 CRL profile

The CRL profile is described in the Certificate Profile [4].

7.3 OCSP profile

The OCSP profile is described in the Certificate Profile [4].

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The present CPS fulfills the requirements for certificates and services according to Root Store Policies, CA/B Forum Requirements as well as EN 319 401, EN 319 411-1. The terms and conditions of this CPS, Swiss Digital Signature Law and all dependent rules and regulations are used to conduct compliance audits for:

- The SwissSign CA and its subsidiaries
- All registration authorities that process requests for issuance by the subordinate CA, if applicable.

8.1 Frequency or circumstances of assessment

Refer to clause 8.1 of SwissSign TSPS [5].

8.2 Identity/qualifications of assessor

Refer to clause 8.2 of SwissSign TSPS [5].

8.3 Assessor’s relationship to assessed entity

Refer to clause 8.3 of SwissSign TSPS [5].

8.4 Topics covered by assessment

Refer to clause 8.4 of SwissSign TSPS [5].

8.5 Actions taken as a result of deficiency

Refer to clause 8.5 of SwissSign TSPS [5].

8.6 Communication of results

Refer to clause 8.6 of SwissSign TSPS [5].

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Refer to clause 9.1 of SwissSign TSPS [5].

9.1.1 Certificate issuance or renewal fees

Refer to clause 9.1.1 of SwissSign TSPS [5].

9.1.2 Certificate access fees

Refer to clause 9.1.2 of SwissSign TSPS [5].

9.1.3 Revocation or status information access fees

Refer to clause 9.1.3 of SwissSign TSPS [5].

9.1.4 Fees for other services

Refer to clause 9.1.4 of SwissSign TSPS [5].

9.1.5 Refund policy

Refer to clause 9.1.5 of SwissSign TSPS [5].

9.2 Financial responsibility

9.2.1 Insurance coverage

Refer to clause 9.2.1 of SwissSign TSPS [5].

9.2.2 Other assets

Refer to clause 9.2.2 of SwissSign TSPS [5].

9.2.3 Insurance or warranty coverage for end-entities

Refer to clause 9.2.3 of SwissSign TSPS [5].

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Refer to clause 9.3.1 of SwissSign TSPS [5].

9.3.2 Information not within the scope of confidential information

Refer to clause 9.3.2 of SwissSign TSPS [5].

9.3.3 Responsibility to protect confidential information

Refer to clause 9.3.3 of SwissSign TSPS [5].

9.4 Privacy of personal information

Refer to clause 9.4 of SwissSign TSPS [5].

9.4.1 Privacy plan

Refer to clause 9.4.1 of SwissSign TSPS [5].

9.4.2 Information treated as private

Refer to clause 9.4.2 of SwissSign TSPS [5].

9.4.3 Information not deemed private

Refer to clause 9.4.3 of SwissSign TSPS [5].

9.4.4 Responsibility to protect private information

Refer to clause 9.4.4 of SwissSign TSPS [5].

9.4.5 Notice and consent to use private information

Refer to clause 9.4.5 of SwissSign TSPS [5].

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to clause 9.4.6 of SwissSign TSPS [5].

9.4.7 Other information disclosure circumstances

Refer to clause 9.4.7 of SwissSign TSPS [5].

9.5 Intellectual property rights

Refer to clause 9.5 of SwissSign TSPS [5].

9.6 Representations and warranties

9.6.1 CA representations and warranties

Refer to clause 9.6.1 of SwissSign TSPS [5].

9.6.2 RA representations and warranties

Refer to clause 9.6.2 of SwissSign TSPS [5].

9.6.3 Subscriber representations and warranties

Refer to clause 9.6.3 of SwissSign TSPS [5].

9.6.4 Relying party representations and warranties

Refer to clause 9.6.4 of SwissSign TSPS [5].

9.6.5 Representations and warranties of other participants

Refer to clause 9.6.5 of SwissSign TSPS [5].

9.7 Disclaimers of warranties

Refer to clause 9.7 of SwissSign TSPS [5].

9.8 Limitations of liability

9.8.1 Liability of the TSP

Refer to clause 9.8.1 of SwissSign TSPS [5].

9.8.2 Liability of the Certificate Holder

Refer to clause 9.8.2 of SwissSign TSPS [5].

9.9 Indemnities

Refer to clause 9.9 of SwissSign TSPS [5].

9.10 Term and termination

9.10.1 Term

Refer to clause 9.10.1 of SwissSign TSPS [5].

9.10.2 Termination

Refer to clause 9.10.2 of SwissSign TSPS [5].

9.10.3 Effect of termination and survival

Refer to clause 9.10.3 of SwissSign TSPS [5].

9.11 Individual notices and communications with participants

Refer to clause 9.11 of SwissSign TSPS [5].

9.12 Amendments

9.12.1 Procedure for amendment

Refer to clause 9.12.1 of SwissSign TSPS [5].

9.12.2 Notification mechanism and period

Refer to clause 9.12.2 of SwissSign TSPS [5].

All changes to the CPS are published according to clause 2 of this CPS.

9.12.3 Circumstances under which OID must be changed

This CPS is used without an OID. In case of change, the version and the date of validity are changed.

In case the scope of the relevant CP changes, the OID will be changed.

9.13 Dispute resolution provisions

Refer to clause 9.13 of SwissSign TSPS [5].

9.14 Governing law

Refer to clause 9.14 of SwissSign TSPS [5].

9.15 Compliance with applicable law

Refer to clause 9.15 of SwissSign TSPS [5].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Refer to clause 9.16.1 of SwissSign TSPS [5].

9.16.2 Assignment

Refer to clause 9.16.2 of SwissSign TSPS [5].

9.16.3 Severability

Refer to clause 9.16.3 of SwissSign TSPS [5].

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

Refer to clause 9.16.5 of SwissSign TSPS [5].

9.17 Other provisions

9.17.1 Language

Refer to clause 9.17.1 of SwissSign TSPS [5].

9.17.2 Delegated or outsourced Services

Refer to clause 9.17.2 of SwissSign TSPS [5].

10. References

[1] SwissSign CP EV - Certificate Policy for Extended Validation Certificates, published under: https://repository.swisssign.com

[2] SwissSign CP OV - Certificate Policy for Organization Validated Certificates, published under: https://repository.swisssign.com

[3] SwissSign CP DV - Certificate Policy for Domain Validated Certificates, published under: https://repository.swisssign.com

[4] SwissSign CPR TLS - Certificate, CRL and OCSP Profiles for TLS Certificates, published under: https://repository.swisssign.com

[5] SwissSign TSPS - Trust Services Practice Statement, published under: https://repository.swisssign.com

[6] ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

[7] ETSI EN 319.401 V3.1.1 (2024-06) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

[8] TLS BR: current version of Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates;

[9] EVCG: current version of the Guidelines For The Issuance And Management Of Extended Validation Certificates;

[10] RFC 3647 – Request For Comments 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework;

[11] RFC 6962 – Certificate Transparency;

[12] RFC 8555 - Automatic Certificate Management Environment (ACME)