SwissSign

SwissSign CPS S/MIME

Certification Practice Statement for S/MIME 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:	10
Issue date:	28.05.2025
Obsoletes:	v9.0, 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 respectively the TSPS [5] describes the practices implemented by SwissSign AG to comply with for the relevant services as well as the terms and conditions under which this is CA is made available:

- “SwissSign CP NCP - Certificate Policy according to Normalized Certificate Policy” [1]
- “SwissSign CP LCP - Certificate Policy according to Lightweight Certificate Policy” [2]
- “SwissSign CP NCP Extended - Certificate Policy for Normalized Certificate Policy with extended EKU” [3]
- “SwissSign CP Organization Validated (OV) S/MIME - Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy” [13]

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 (https://www.cabforum.org), as well as further applicable specifications:

- Root Store Policies
  - Apple Root Certificate Program: https://www.apple.com/certificateauthority/ca_program.html
  - 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/
- SMIME BR Guidelines: “Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates”
- TLS BR Guidelines: “Baseline Requirements for the Issuance and Management of Publicly-Trusted 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 119 411-6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates
- ETSI TS 119 312: Cryptographic Suites

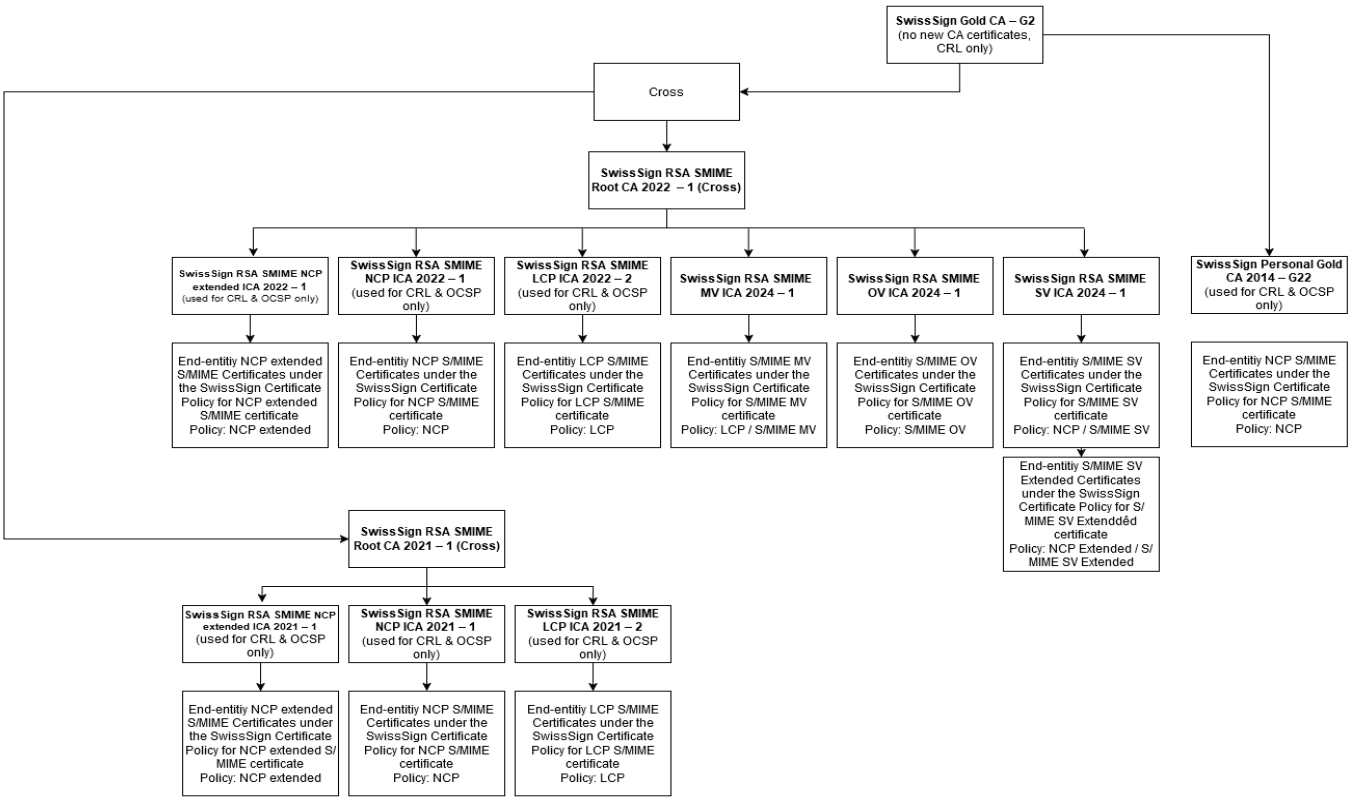

Figure 1: Picture showing SwissSign Gold CA - G2 hierarchy

- IETF RFC 6960: Online Certificate Status Protocol - OCSP
- IETF RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The requirements of root store policies as well as the SMIME BR apply in their latest version, where applicable.

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

- LCP (Lightweight Certificate policy defined in ETSI EN 319 411-1; for S/MIME certificates according to SwissSign CP LCP)
- Mailbox Validated (defined in SMIME BR (2.23.140.1.5.1.1, 2.23.140.1.5.1.2); for S/MIME certificates according to SwissSign CP LCP)
- NCP (Normalized Certificate policy defined in ETSI EN 319 411-1, for S/MIME certificates according to SwissSign CP NCP)
- NCP extended EKU (Normalized Certificate policy defined in ETSI EN 319 411-1, for S/MIME certificates according to SwissSign CP NCP Extended)
- Sponsor Validated (defined in SMIME BR (2.23.140.1.5.3.1, 2.23.140.1.5.3.2); for S/MIME certificates according to SwissSign CP NCP and NCP Extended)
- Organization Validated (defined in SMIME BR (2.23.140.1.5.2.1, 2.23.140.1.5.2.2); for S/MIME certificates according to SwissSign CP SMIME OV)

In the following, all procedures for NCP S/MIME are valid also for NCP Extended S/MIME, unless stated differently.

The procedures and policies set forth by the latest version of the SMIME BR apply.

The relevant Issuing CAs for these certificates under this CPS are shown in figure 1.

These 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 certificates issued by these CAs. 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 these CAs.

In this CPS, “these CAs” refers to Root CAs “SwissSign Gold CA - G2”, “SwissSign RSA SMIME CA 2021 - 1“, “SwissSign RSA SMIME Root CA 2022 - 1“ and all their subordinated issuing CAs for S/MIME email certificates as shown in Figure 1 and 2 above, unless stated differently. “SwissSign RSA SMIME Root CA 2021 - 1“ and “SwissSign RSA SMIME Root CA 2022 - 1“ have obtained a Cross-certificate by the Root CA “SwissSign Gold CA - G2”.

1.2 Document name and identification

This document is named “SwissSign CPS S/MIME - Certification Practice Statement for S/MIME 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 SMIME Root
3.0	01.07.2022	Adrian Mueller, Michael Günther	Adding new hierarchy, features and requirements on signatures
4.0	07.11.2022	Adrian Mueller, Michael Günther	Clarifications in chapters 4.12.1 & 6.1.2 (PKCS#12)
5.0	24.07.2023	Adrian Muller	Update for SMIME BRG
6.0	04.06.2024	Raffaela Achermann, Adrian Mueller	Update of chapter 1.1 (CA overview and references;); minor updates, regarding validation and certificate application process
7.0	23.08.2024	Raffaela Achermann, Adrian Mueller	Update Disclaimer, graphics and chapters 1.5.2, 1.5.3 and 4.2.1
8.0	29.01.2025	Raffaela Achermann, Roman Fischer	Deletion of root: SwissSign Silver CA - G2, conversion to markdown, various typos fixed
9.0	13.03.2025	Roman Fischer	Added MPIC
10.0	28.05.2025	Roman Fischer, Adrian Mueller	Changes based on feedback from Mozilla during Root Inclusion, update maximum validity periods in 6.3.2, added SMIME OV

1.3 PKI Participants

1.3.1 Certification Authorities

The TSP operates a Public Key Infrastructure, consisting Root CAs “SwissSign Gold CA - G2”, “SwissSign RSA SMIME Root CA 2021 - 1“, “SwissSign RSA SMIME Root CA 2022 - 1“ and all their subordinated issuing CAs for SMIME certificates as shown in Figure 1 and 2 above. “SwissSign RSA SMIME Root CA 2021 - 1“ and “SwissSign RSA SMIME Root CA 2022 - 1“ have 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 S/MIME 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 (RA), called “SwissSign RA” that registers Subscribers of certificates issued by these CAs.

Enterprise RAs (see section 1.3.3) are operated under this CPS. No other external Registration Authorities are operated under this CPS.

1.3.3 Enterprise Registration Authorities

An Enterprise Registration Authority (ERA) is an organization (or an employee or an authorized agent) unaffiliated with the CA. Based upon an RA delegation contract the ERA is authorized to issue certificates to that organization and individuals related to that organization (e.g. employees).

1.3.4 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.

1.3.5 Relying Parties

Relying Parties are individuals or organizations that use certificates of these CAs 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 the sole responsibility of the Relying Party to verify revocation status, legal validity and the appropriateness of reliance on applicable certificate policies.

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

1.3.6 Other participants

Not applicable

1.4 Certificate usage

The certificate usage in relation of the key usage as well as 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

SwissSign AG conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [9] published at https://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

Refer also 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 with the PEM version for all certificate types:

https://repository.swisssign.com/reference_certs/

These certificates are issued from the production environment. The private keys of these demo certificates are not published to prevent usage outside of testing.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

(LCP) The common name contains an e-mail address of the Subscriber.

(NCP) The common name contains the name or the pseudonym of the Subscriber.

(SMIME OV) The common name contains the organization name of the subscriber (or alternatively the email address)

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 or pseudonyms 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.

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

3.1.3 Anonymity or pseudonymity of Subscribers

Pseudonyms are specified as /CN='pseudo': 'pseudonym'. An example of a correctly formulated pseudonym is: "/CN=pseudo: John Doe". Other registration authorities may use other identifiers.

The RA decides on the acceptability of a given identifier based on the following requirements:

- Upon Implementation of the SMIME BR: A chosen pseudonym shall not be identical to an already existing pseudonym referring to another certificate holder within an organization acting as Enterprise RA. The Enterprise RA or the TSP must assure that the pseudonym is unique for the certificate holder within his organization and shall not be assigned to two different persons within an organization. However, one person may use several pseudonyms.
- Identifier is a string that clearly indicates the nature of the CN,
- The identifier and the resulting /CN= values are neither incorrect nor misleading,
- The identifier and the remainder of the /CN= attribute must be separated with a <colon> <space> sequence.

Apart from these requirements, a Subscriber can use any string of characters as a pseudonym.

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 infringing rights of others. However, the TSP and its RAs are not obliged to verify lawful use of such names. The TSP and its RAs reserve the right to decline any request for anonymity or pseudonymity. Anonymous or pseudonymous common names are available on a “first come, first served” basis. Chapter 3.1.6 applies.

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 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 certificates for individuals with identical Subjects belong to the same individual.
- All actual valid, revoked and expired organizational certificates with identical Subjects belong to the same organization.

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. The evidences are not used if older than 825 days.

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, if the key pair is generated by the Subscriber. The Subscriber must present a PKCS#10 formatted request. The CA verifies the signature.

If the key pair is generated by the TSP, the private key is delivered securely to the Subscriber. Further details are described in chapter 6.1.2

3.2.2 Authentication of organization identity and MPIC

3.2.2.1 Authentication of organization identity

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

- 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.
- Organizations with an entry in the federal or a nationally recognized commercial register must supply verifiably current excerpt. All other organizations must supply either the certificate of registration with the FTA or a current VAT invoice.
- Government entities must supply official documentation to prove the existence and the correct spelling of the entity's name.
- The validation of an organization's name is performed directly with the authoritative source instead of the organization. evidence of registration of a nationally recognized register (e.g. FTA or VAT)
- The address information is verified in context of legal identity.

The use of the e-mail in the common name and e-mail address field is verified during the registration process as follows:

- (M-PKI) An organization may contractually define that all certificates using e-mail addresses that are in the domain of the organization. Should such a contract exist, the organization takes full responsibility for the proper management of e-mail accounts. Therefore, the requirement to verify individual e-mail addresses during the registration process is optional. The domain is verified using a SMIME BR method as specified below.
  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 of the S/MIME Baseline Requirements. To check access to the domains, the random value generated by the TSP must be stored at one of the following three locations on the domain owner's website. 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 system checks for 30 days whether the random value was stored at one of the three places mentioned below. Only after a successful check is control of the domain ownership completed.
  - SMIME BR 3.2.2.1 Validating authority over mailbox via domain (LCP/NCP Managed PKI), i.e.
    - TLS BR 3.2.2.4.4 Constructed Email to Domain Contact
    - TLS BR 3.2.2.4.7 DNS Change
  - SMIME BR 3.2.2.2 Validating control over mailbox via email (LCP Webshop)
    (If the /Email= field is used, the e-mail address is verified during the registration process, the Subscriber must prove that he has access to the mailbox and that he can use it to receive mail.)

3.2.2.2 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:

- TLS BR 3.2.2.4.4 Constructed Email to Domain Contact: CAA checks use MPIC
- TLS BR 3.2.2.4.7 DNS Change: CAA checks and check of random value in DNS 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

Various individuals need to authorize the use of names in different parts of the DN.

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

- The Subscriber must be present in person or in an equivalent 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 must present a valid original of an official identification document as recognized by national law. The identifying agent is to make a high-quality copy, scan or photograph of the identifying document 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 and has to match (facial features, age, gender and size) the person present as described above.

The following individuals are identified according to the process defined above:

(LCP) Not applicable as the subject is not a natural person but an e-mail address.

(NCP) The Subject applying for a S/MIME certificate.

(SMIME OV) Not applicable as the subject is not a natural person but an organization.

3.2.4 Non-verified Subscriber information

All 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

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.

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

3.2.6 Criteria for interoperation

SwissSign does not support cross-certification for external organizations. Only SwissSign's own Root and Issuing CA will be cross-signed.

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 changed.

The validity period for the data included in an S/MIME certificate as well as provided evidences is limited to 825 days. 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.

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

Revocation of a certificate that is issued by these CAs requires one of the following authentication 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.

(LCP) Certificate request can be applied via customer M-PKI or Webshop.

(NCP) Certificate request can be applied via customer M-PKI.

(SMIME OV) Certificate request can be applied via customer M-PKI.

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,
- e-mail address and / or FQDN of the requester according to chapter 3,
- record of unique identification data, numbers, or a combination thereof of e-mail address and / or FQDN validation evidence,
- method used to validate e-mail address and / or FQDN,
- type of document(s) 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 choices in the Subscriber agreement (e.g. consent to publication of certificate),
- storage location of copies of applications and identification documents, including the Subscriber agreement,
- identity of entity accepting the application,

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 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 (e.g. name, e-mail address; FQDN) 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 and evidences that the Subscriber presents, as stipulated in chapter 3.2 of this document.

Domain validation / Validation of mailbox authorization or control (upon implementation of the SMIME BR): Completed domain-validation (or validation of the control of a mail server) are obtained no more than 398 days prior to issuing a certificate.

Starting from September 15, 2024, SwissSign MAY retrieve and process CAA records in accordance with Section 4 of RFC 9495 for each mailbox address in a requested certificate. Starting from March 15, 2025, SwissSign WILL retrieve and process CAA records in accordance with Section 4 of RFC 9495 for each mailbox address in a requested certificate.

SwissSign processes the issuemail property tag as specified in RFC 9495.

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 3.2.2.2.

The default Issuer Domain Name for SwissSign is “swisssign.com”.

Furthermore SwissSign:

- caches CAA records for reuse for up to the their respective Time To Live (TTL) or 8 hours, whichever is greater,
- 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.

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 request 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 timeframe 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 certificate status information in accordance with applicable regulations. The Subscriber decides during the registration process whether or not the certificate will be published in a public directory service and is thus available for retrieval. If the Subject is a device or system, the consent of the natural or legal person responsible (Subscriber) for the operating of the device or system needs to be obtained, instead of the Subject's consent.

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

Not applicable 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,

- 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 the certificate,
- comply with all laws and regulations applicable to a Relying Party's right to export, import, and/or use a certificate issued by this 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 this CA and/or related information.

4.6 Certificate renewal

Certificate renewal is not supported by the TSP.

4.6.1 Circumstance for certificate renewal

No Stipulation

4.6.2 Who may request renewal

No Stipulation

4.6.3 Processing certificate renewal requests

No Stipulation

4.6.4 Notification of new certificate issuance to subscriber

No Stipulation

4.6.5 Conduct constituting acceptance of a renewal certificate

No Stipulation

4.6.6 Publication of the renewal certificate by the CA

No Stipulation

4.6.7 Notification of certificate issuance by the CA to other entities

No Stipulation

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 or the used evidence is not valid, the initial certificate issuance applies.

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 re-key a certificate if the following conditions are met:

- The Subscriber owns a currently valid certificate from one of these CAs.
- 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 SMIME BR, 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 initially.

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

4.8.1 Circumstance for certificate modification

No Stipulation

4.8.2 Who may request certificate modification

No Stipulation

4.8.3 Processing certificate modification requests

No Stipulation

4.8.4 Notification of new certificate issuance to subscriber

No Stipulation

4.8.5 Conduct constituting acceptance of modified certificate

No Stipulation

4.8.6 Publication of the modified certificate by the CA

No Stipulation

4.8.7 Notification of certificate issuance by the CA to other entities

No Stipulation

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 as set forth in chapter 3.4.

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 if the conditions described in chapter 4.9.1.1 of the SMIME BR are met (and if the SMIME BR apply), i.e. after receiving the information that one of the following conditions is met:

1. The Subscriber requests in writing that the CA revoke the certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5. The CA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate should not be relied upon.

The CA revokes a Subscriber's certificate within 5 days if the conditions described in chapter 4.9.1.1 of the SMIME BR are met, i.e. after receiving the information that one of the following conditions is met:

1. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of the SMIME BR;
2. The CA obtains evidence that the Certificate was misused;
3. 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;
4. The CA is made aware of any circumstance indicating that use of an email address or 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 an email address or the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);

5. The CA is made aware of a material change in the information contained in the Certificate, e.g.
    1. Any part of the certificate Subject has changed.
    2. The certificate /O= field is no longer valid. (e.g. the organization is completely and finally legally dissolved)
    3. certificate /CN= field is no longer valid (e.g. legal name officially and permanently changed or omission of domain registration renewal).
6. The CA is made aware that the Certificate was not issued in accordance with the SMIME BR or the CA's Certificate Policy or this Certification Practice Statement;
7. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate
8. The CA's legal right to issue Certificates expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the CP, this CPS or the SMIME BR
10. 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 revokes a CA certificate within 7 days if the conditions described in chapter 4.9.1.2 of the SMIME BR, i.e. after receiving the information that one of the following conditions is met:
(Please note: The numeration points 1. and 2. In section 4.9.1.2 of the SMIME BR are not applicable as no CA certificates are issued to other Trust Service Providers.)

1. N/A
2. N/A
3. The Issuing CA obtains evidence that the Private Key corresponding to the Public Key in the CA Certificate suffered a Key Compromise or no longer complies with the terms and conditions of this CPS or Section 6.1.5 and Section 6.1.6 of the SMIME BR;
4. The Issuing CA obtains evidence that the CA Certificate was misused;
5. The Issuing CA is made aware that the CA Certificate was not issued in accordance with this CPS;
6. The Issuing CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading;
7. The Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the CA Certificate;
8. The Issuing CA's legal right to issue Certificates expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the CP or this CPS.

4.9.2 Who can request revocation

These CAs accept 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,
- someone in possession 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 CAO,
- 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 Procedures 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 Identification and authentication for revocation request for details.

Revocation requests must properly authenticated and authorized in order to be executed. Still, electronic requests are logged and paper requests are archived.

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 reasons listed in the subscriber agreement occur. 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 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 these CAs, verify these certificates at all times. This includes the use of CRLs or OCSP, 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 CRLs of these CAs are issued according to chapter 4.9.7 and published without delay.

4.9.9 On-line revocation/status checking availability

These CAs support the OCSP protocol for online revocation checking. The OCSP responder URL is stored in every certificate issued by one of the subordinated issuing CAs of the "SwissSign Gold CA" (field "Authority Information Access"). 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. While certificate serial numbers are not allocated the OCSP responds with the status ‚unknown'. Within at most 15 minutes after the actual certificate is issued, the OCSP starts responding with ‚good'.

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 these CAs, at all times verify the certificates issued by these CAs. This includes the use of CRLs in accordance with the certification path validation procedure specified in RFC 5280 and/or RFC 6960 for OCSP.

4.9.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.9.12 Special requirements re 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 certificate and 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 “directory.swisssign.net”. The certificate status services provide information on the status of certificates for at least 11 years after the certificate has expired or was revoked. 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. Afterwards, a last CRL will be issued and will be available for download at least 11 years after the expiry date of the last leaf-certificate in scope, not only until the end of the Issuing CA validity.

4.10.1 Operational characteristics

S/MIME certificates are only published if the Subscriber approves such publication. 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

Private key escrow is done only for S/MIME Certificate key pairs generated by the TSP under the same conditions as key generation. In these cases, the unique PKCS#12 file containing the key pair and protected with a Subscriber-chosen password is available for download at least for 90 days and maximum for the validity period of the requested certificate.

4.12.2 Session key encapsulation and recovery policy and practices

These CAs do 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

Refer to clause 5.7 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 CA, refer to clause 6.1.1 of SwissSign TSPS [5].

The Subscriber key pairs are generated either by the Subscriber or by the TSP.

If the key pairs are produced under the responsibility of the Subscriber, they must not use weak keys.

If the TSP generates the Subject Keys, it uses a key length and a public key algorithm as specified in ETSI TS 119 312. The Subject Keys generated by the TSP are generated and stored securely while held by the TSP.

6.1.2 Private key delivery to Subscriber

Private keys generated by the Subscriber do not need to be delivered.

The delivery of private keys generated by the TSP will be through a passphrase-protected download mechanism (PKCS#12):

- The PKCS#12-file is encrypted with an AES (Advanced Encryption Standard) cipher with the length of 128 bit or higher.
- The Subscriber Private Keys are not stored in clear text.
- Upon implementation of the SMIME BR: The PKCS#12-file is encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers and symbols/special characters. The password is delivered to the Subscriber securely and separately from the container (PKCS#12) holding the Private Key.

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.

If keys are generated by the TSP, no public key delivery method is required.

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 keys with a size of at least 2048 bits RSA keys 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.

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 by the Subscriber. The TSP recommends that the Subscriber uses a cryptographic module.
  Subscriber keys generated by the TSP are generated securely meeting the cryptographic requirements.

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 key escrow is done only for key pairs generated by the TSP. In these cases, the PKCS#12 file containing the key pair and protected with a Subscriber-chosen password is available for download for the validity period of the requested certificate.

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: Refer to clause 6.2.3 of this document for keys generated by the TSP. Subscribers are solely responsible for the backup of Subscriber-generated 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: Archival is not provided for keys generated by the TSP. Subscribers are solely responsible for the archival of Subscriber-generated 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: Transfer is not provided for keys generated by the TSP. Subscribers are solely responsible for the transfer of Subscriber-generated keys.

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: Storage on cryptographic module is not provided for keys generated by the TSP. 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 they generated the key pair. For certificates where keys were generated by the TSP, keys are securely deleted following the internal process.

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].

End user certificates can have according to PKI “best practices” a lifetime of up to the maximum remaining lifetime of the issuing CA certificate minus 10 days.

In addition, the lifetime of end user certificates is restricted to a maximum validity period according to the SMIME BR chapter 6.3.2:

- For the Legacy generation (allowed until 15 July 2025) it is 1185 days.
- For the Strict and Multipurpose generation it is 825 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].

7.1.1 Version number(s)

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.2 Certificate extensions

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.3 Algorithm object identifiers

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.4 Name forms

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.5 Name constraints

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.6 Certificate policy object identifier

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.7 Usage of Policy Constraints extension

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.8 Policy qualifiers syntax and semantics

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.1.9 Processing semantics for the critical Certificate Policies extension

The Certificate shall comply with the profile described in the Certificate Profile [4].

7.2 CRL profile

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

7.2.1 Version number(s)

The CRL shall comply with the profile described in the Certificate Profile [4].

7.2.2 CRL and CRL entry extensions

The CRL shall comply with the profile described in the Certificate Profile [4].

7.3 OCSP profile

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

7.3.1 Version number(s)

The OCSP response shall comply with the profile described in the Certificate Profile [4].

7.3.2 OCSP extensions

The OCSP response shall comply with the profile 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].

8.7 Review of delegated parties / Enterprise RAs

Enterprise RAs that issue Sponsor Validated / E-Mail Gold certificates are monitored on an annual basis concerning their practice to only issue certificates to persons known to them and affiliated with them.

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 LCP - Certificate Policy according to Lightweight Certificate Policy, published under: https://repository.swisssign.com

[2] SwissSign CP NCP - Certificate Policy for according to Normalized Certificate Policy, published under: https://repository.swisssign.com

[3] SwissSign CP NCP Extended - Certificate Policy for Normalized Certificate Policy with extended EKU, published under: https://repository.swisssign.com

[4] SwissSign CPR S/MIME - Certificate, CRL and OCSP Profiles for S/MIME 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 TS 119 411-6 (2023-08): Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates

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

[9] SMIME BR: current version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"

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

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

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

[13] SwissSign CP SwissSign CP Organization Validated (OV) S/MIME - Certificate Policy according to S/MIME BR Organization Validated and ETSI EN 319 411-1 Normalized Certificate Policy