SwissSign

SwissSign CP/CPS TLS

Combined Certificate Profile and Certification Practice Statement for TLS certificates

Document Type:	Combined Certificate Profile and Certificate Practice Statement
OID:	n/a
Author:	Information Security and Compliance
Owner:	CEO
Applicability:	Global
Copyright:	Attribution-NoDerivs (CC-BY-ND) 4.0
Version:	1
Issue date:	12.06.2026
Obsoletes:	n/a

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

The structure of this document corresponds to RFC 3647 [8] 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”. If the subsections are omitted, a single reference applies to all of them.

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.

The TSP can outsource partial tasks 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 combined CP/CPS describes 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.

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/
- CCADB Policy: https://www.ccadb.org/policy
- CA/B TLS BR Guidelines: “Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates” https://cabforum.org/working-groups/server/baseline-requirements/requirements/
- CA/B EV Guidelines: “Guidelines for the Issuance and Management of Extended Validation Certificates” https://cabforum.org/working-groups/server/extended-validation/guidelines/
- 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
- IETF RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The requirements of the Apple Root store policies, the Chrome root store policies, the Microsoft Root store policies, the Mozilla root store policies and the CCADB policy as well TLS BRs and EV Guidelines apply in their latest published version. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

This combined CP/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 combined CP/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. “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 CP/CPS TLS - Combined Certificate Profile and Certification Practice Statement for TLS certificates” as indicated on the cover page of this document.

The combined CP/CPS does not contain an OID.

The OID for each certificate type issued is composed according to the contents of the following table:

Meaning	Position 1	Position 2	Position 3	Position 4	Position 5	Position 6	Position 7	Position 8
Joint ISO-CCITT Tree	2							
Country		16						
Switzerland			756					
RDN				1				
SwissSign					89			
TSP Tree						2		
Document Type							1	
Product								1, 2 or 3

This results in the following OID for each certificate type issued:

- Certificate Policy for Domain Validated Certificates: 2.16.756.1.89.2.1.1
- Certificate Policy for Organization Validated Certificates: 2.16.756.1.89.2.1.2
- Certificate Policy for Extended Validation Certificates: 2.16.756.1.89.2.1.3

1.2.1 Revisions

Version	Date	Author	Comment
1.0	12.06.2026	Roman Fischer	Initial combined CP/CPS, based on and replaces: CPS TLS v15, CPR TLS v13, TSPS v13 (TLS use-case only), CP DV v5, CP OV v5, CP EV v5, added new 2026 ICAs in chapter 7.1.1.2

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 described in chapter 7.1.1.1. “SwissSign RSA TLS Root CA 2022 - 1” has obtained a Cross-certificate by the Root CA “SwissSign Gold CA - G2”.

The issuing CAs described in chapter 7.1.1.2 are the only public CAs operated by the TSP that issue TLS certificates under this combined CP/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 combined CP/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 combined CP/CPS.

1.3.3 Subscribers

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

Please refer to chapter 9.6.3 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 combined CP/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 combined CP/CPS.

1.3.5 Other participants

Not applicable

1.4 Certificate usage

1.4.1 Appropriate certificate uses

These CAs serve the following trust purposes by setting the relevant EKU(s):

- Server Authentication: id-kp-serverAuth (1.3.6.1.5.5.7.3.1)
- Legacy TLS: id-kp-serverAuth (1.3.6.1.5.5.7.3.1), id-kp-clientAuth (1.3.6.1.5.5.7.3.2)

1.4.2 Prohibited certificate uses

The key usage bit digitalSignature of End-entity certificates does not allow the certificate to be used for qualified digital signatures mentioned in Article 14 para. 2bis OR (Swiss Code of Obligations).

1.5 Policy administration

1.5.1 Organization administering the document

This combined CP/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

In this combined CP/CPS the following terms and acronyms have the following meanings:

Term	Abbreviation	Explanation
ASCII	ASCII	American Standard Code for Information Interchange, is a character encoding standard for representing a particular set of (English language focused) printable and control characters.
Automatic Certificate Management Environment	ACME	The Automatic Certificate Management Environment protocol is a communications protocol for automating interactions between certificate authorities and their users' servers.
Certification Authority	CA	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certification Authority Authorization	CAA	RFC 6844 defines a Certification Authority Authorization DNS Resource Record (CAA). A CAA allows a DNS domain name holder to specify the CAs authorized to issue certificates for that domain. Publication of the CAA gives domain holders additional controls to reduce the risk of unintended certificate mis-issuance.
Certification Authority Revocation List	CARL	Revocation list containing a list of CA-certificates that have been revoked by the certificate issuer (Root CA).
CCADB	CCADB	Common CA Database
Certificate Policy	CP	A set of rules that a CA must comply when providing the trust service.
Certificate Revocation List	CRL	Revocation list containing a list of leaf certificates that have been revoked by the certificate issuer (Issuing CA).

Term	Abbreviation	Explanation
Certificate Signing Request	CSR	A certificate signing request (CSR or certification request) is a message sent from an applicant to a CA in order to apply for a digital certificate.
Certificate Transparency	CT	Certificate Transparency (CT) is an Internet security standard for monitoring and auditing the issuance of digital certificates.
Certification Authority	CA	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certification Practice Statement	CPS	Document that describes the implemented practices of the CA when providing the trust service.
Coordinated Universal Time	UTC	Coordinated Universal Time is the primary time standard globally used to regulate clocks and time.
Cryptographically-secure pseudo-random number generator	CSPRNG	Pseudo-random number generator meeting the quality requirements for the use in cryptology.
DCF77	DCF77	DCF77 is a German longwave time signal and standard-frequency radio station.
DNSSEC	DNSSEC	The Domain Name System Security Extensions is a suite of extension specifications for securing data exchanged in the Domain Name System.
Domain Name System	DNS	The Internet system of holding a distributed register of entity names. For example, the domain is the part of the email address to the right of the “@”, e.g. “anytown.ac.uk”.
Domain Validated Certificate	DV	A digital certificate that contains only information about domain names and that has been validated in accordance with the guidelines.
eIDAS	eIDAS	The eIDAS Regulation (for “electronic IDentification, Authentication and trust Services”) is an EU regulation with the stated purpose of governing “electronic identification and trust services for electronic transactions”.
ETSI	ETSI	European Telecommunications Standards Institute
Extended Validation	EV	Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.
FIPS 140	FIPS 140	FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules.
FQDN	FQDN	Fully Qualified Domain Name
Generic top-level domain	gTLD	gTLDs are one of the categories of top-level domains (TLDs) maintained by the Internet Assigned Numbers Authority (IANA) for use in the Domain Name System of the Internet.
Hardware Security Module	HSM	Hardware Security Module is a device that physically protects key material against unauthorized parties.
IANA	IANA	Internet Assigned Numbers Authority
IETF	IETF	Internet Engineering Task Force
Information Security Management System	ISMS	An information security management system is a set of policies and procedures for systematically managing an organization’s sensitive data.
ISO/IEC JTC1	ISO/IEC	ISO/IEC JTC 1, entitled “Information technology”, is a joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission. Its purpose is to develop, maintain and promote standards in the fields of information and communications technology.

Term	Abbreviation	Explanation
ITIL	ITIL	ITIL is a framework with a set of practices for IT activities such as IT service management and IT asset management that focus on aligning IT services with the needs of the business.
Object identifier	OID	Object identifiers or OIDs are an identifier mechanism standardized by the International Telecommunication Union (ITU) and ISO/IEC for naming any object, concept, or “thing” with a globally unambiguous persistent name.
Online Certificate Status Protocol	OCSP	Method to verify the certificate status of a certificate in real time.
Organization Validated Certificate	OV	A digital certificate that contains information about domain names and organization information and that has been validated in accordance with the guidelines.
Public Key Infrastructure	PKI	Processes and technologies that are used to issue and manage digital identities that may be used by third parties to authenticate individuals or organizations.
Qualified Signature/Seal Creation Device	QSCD/SSCD	Signature-creation device which meets the requirements specified in article 30 of eIDAS.
Registration Authority	RA	A registration authority (RA) verifies the identity of entities requesting their digital certificates and approves the CSR to the Certificate Authority (CA) to issue the leaf-certificate.
RA Operator	RAO	The person responsible for identifying the requester, collecting and verifying the identity substantiating evidence, authorizing the CSR, and forwarding the authorized CSR to the CA.
Relying Party		Relying Parties are individuals or organizations that use certificates of this CA to validate the signatures and verify the identity of Subscribers and/or to secure communication with these Subscribers.
S/MIME	S/MIME	Secure / Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail.
Signed Certificate Timestamps	SCT	SCTs are part of certificate transparency, as defined in RFC 6962.
Subject		Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.
Subscriber		Legal or natural person bound by agreement with a trust service provider to any subscriber obligations.
Subscriber Agreement	SA	Contractual agreement between the CA and the Subscriber.
TLS	TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). A protocol that enables secure transactions via the Internet. URLs that require an TLS connection for HTTP start with https: instead of http:
TSP	TSP	Trust Service Provider is an organization providing trust services, e.g. issuing leaf-certificates for a subscriber.
Uniform Resource Locator	URL	The global address of documents and other resources on the WWW, e.g. https://swisssign.net. The first part indicates the protocol to be used (http) and the second part shows the domain where the document is located.
UTF-8	UTF8	UTF-8 is a character encoding standard used for electronic communication. Defined by the Unicode Standard, the name is derived from Unicode Transformation Format – 8-bit.
X.509	X.509	X.509 is an International Telecommunication Union (ITU) standard defining the format of public key certificates.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The TSP makes its certificates, combined CP/CPS, Subscriber agreement with terms and conditions, CRL, CA certificates and related documents for these CAs publicly available. To document the validity period of the document, a version history is included.

2.1 Repositories

The TSP publishes all current and past documentation on https://repository.swisssign.com which is available 24h a day / 7 days a week with a minimum of 99.6% availability overall per year and a maximum unavailability for not longer than 0.4%.

The TSP publishes root certificates and CA certificates as well as Certificate Revocation Lists on https://www.swisssign.com/support/ca-prod.html. Certificate status information is also available via OCSP Responder.

The exact URLs for Certificate Revocation Lists and (if available) OSCP Responders are documented in every certificate that is issued by the CA or the subordinated issuing CAs in the field: “CRL Distribution Point”. For details, please refer to clause 7.

Certificate dissemination services are available 24 hours per day, 7 days per week.

2.2 Publication of certification information

For its CAs, the TSP publishes the current and approved (as described in clause 1.5.4) version of:

- PKI Disclosure Statement (PDS)
- End User Agreement / Subscriber Agreement (EUA)
- Relying Party Agreement (RPA)

This combined CP/CPS is published in case of changes and changes are communicated as described in chapter 9.12.

SwissSign AG reserves the right to publish newer versions of the documentation without prior notice.

Even if no updates are required, new versions of CA/B-relevant documents are published at least once a year.

2.3 Time or frequency of publication

Refer to clause 2.2 above.

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

The CRL and OCSP information is managed in a database system. All public access to the data in this database system is managed through standard protocols and is read-only.

This combined CP/CPS is provided as public information on the swisssign.com web site.

Management access always requires two factor authentication.

2.5 Additional testing

Demo pages are offered for all certificate types under these CAs.

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, see chapter 7.

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 chapter 7.

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.

Every Distinguished Name (DN) described in this document is a sequence of Relative DNs (RDNs) where every RDN contains exactly one naming attribute. All attributes are encoded according to the requirements set forth in:

- X.509,
- RFC 5280 and
- the TLS BR, chapter 7

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 chapter 7.

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 combined CP/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 398 days.

The TSP has implemented procedures that identify certain certificate requests that 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 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.
- Unregistered International Organizations / non-commercial 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

3.2.2.1 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/B TLS BR Guidelines. 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:
  - TLS BR 3.2.2.4.4 Constructed Email to Domain Contact (webshop only)
  - TLS BR 3.2.2.4.7 DNS Change (Managed PKI and webshop)
  - TLS BR 3.2.2.4.19 Agreed-Upon Change to Website - ACME; according to RFC 8555 [11] plus additional requirements (Managed PKI only)
    TLS BR 3.2.2.4.19 Agreed-Upon Change to Website - ACME is not allowed for validating wildcard domain names.
- No .onion certificates are issued.

Domain validation requires successful DNSSEC validation to the IANA DNSSEC root trust anchor, and must follow the requirements specified in TLS BR chapter 3.2.2.4. Specifically:

- DNSSEC validation for methods 3.2.2.4.7 and 3.2.2.4.19 is done on all DNS queries (e.g. CNAME, CAA, TXT queries) associated with the validation of domain authorization or control by the primary network perspective
- DNSSEC validation for method 3.2.4.4.4 is done on CAA DNS queries associated with the validation of domain authorization or control by the primary network perspective
- Any failed DNSSEC validation during domain validation will result in a failed domain validation and no certificate will be issued until DNSSEC validation is successful

- No local policy to disable DNSSEC validation on any DNS query associated with the validation of domain authorization or control is in place

The reuse of Domain Control Validation (DCV) data is limited to:

- 200 days for validations performed on or after 15 March 2026
- 100 days for validations performed on or after 15 March 2027
- 10 days for validations performed on or after 15 March 2029

Reuse beyond these limits is not permitted.

Please note:

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

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.

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
- TLS BR 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:

- Adheres to the “Quorum Requirements” table and Phased Implementation Timeline in TLS BR 3.2.2.9
- Results or information obtained from a remote 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)
- 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 [4] chapter 6.2.2. This step may be conducted by:
  - the registration authority processing the certificate request,
  - 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 identi-

fying 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 TSP 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 changed.

The validity period for the data included in certificates as well as provided evidences is limited to the durations specified in 3.2. 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, combined CP/CPS and relevant End-User Agreement. The applicable legal documents (Terms and Conditions, combined CP/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 full name and date and place of birth as stated in 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 submitted. In case of an EV application it must be signed (delivery of a scan by email is sufficient).

    - and the combined CP/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.

The communication channel to the applicant is confirmed by the previously gathered email or telephone contact.

(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.

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 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,
- DNSEC validation is done for all CAA DNS queries as described in chapter 3.2.2.1.

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),

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.

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 described 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 [10]. Pre-certificates, as described in RFC 6962, are considered to be a “certificate” subject to the requirements of RFC 5280.

For every TLS certificate a pre-certificate is issued, sent to at least two CT-logs and upon receipt of the Signed Certificate Timestamps (SCTs) the corresponding final certificate is issued. A pre-certificate is issued by the same CA that issues the final certificate. A pre-certificate differs as follows from the final certificate:

- It contains a critical extension “Precertificate Poison” (OID 1.3.6.1.4.1.11129.2.4.3).
- It does not contain the SCT list extension (OID 1.3.6.1.4.1.11129.2.4.2) while the SCT list extension is included in every final end-entity certificate

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.

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 combined CP/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 re-key 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 [3] and ETSI EN 319 411-1 [4].

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, combined CP/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 will not request confirmation of revocation requests as long as the revocation request is valid according to 4.9.2 and 4.9.3.

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. 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 combined CP/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 combined CP/CPS or the TLS BR

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 combined CP/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 combined CP/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 combined CP/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.

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 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 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

In the field of security management, SwissSign guides itself by the generally recognized standards, e.g. ISO/IEC 27001, and other standards required by regulations and law.

SwissSign carries out a regular risk assessment to identify, analyze and evaluate trust service risks taking into account business and technical issues as well. Based on the risk assessment results, corresponding appropriate risk treatment measures commensurate to the degree of risk are selected and the necessary procedures are determined and documented regarding the implementation of these risk treatment measures in accordance to SwissSign's Information Security Policy as well as this combined CP/CPS. A residual risk analysis is carried out and documented as well in which the residual risk is identified and, where appropriate, accepted. The risk assessment is carried out annually, based on the requirements of the ISO 27001:2013 standard and released by SwissSign management body.

SwissSign management is responsible to define, implement and maintain the ISMS policies, which forms a basis for consistency and completeness of information security and management support. SwissSign's ISMS documents include the security controls and operating procedures for the SwissSign facilities, systems, and information assets providing the services. In addition, SwissSign management sets out the approach to manage information security objectives for Trust Services, including auditable procedures for internal control.

The Information Security policy is reviewed annually or if significant changes occur, to ensure the continuing suitability, adequacy, and effectiveness. SwissSign's Chief Information Security Officer approves policies and practices related to information security for the overall SwissSign services. SwissSign management communicates information security policies and procedures to employees and relevant external parties who are impacted by them.

SwissSign has defined a detailed inventory of assets and has assigned a classification consistent with the risk assessment, which is reviewed regularly at planned intervals or if significant changes occur to ensure the continuing suitability, adequacy, and effectiveness. The configuration of the TSP's systems are also regularly checked for changes which violate the TSP's security policies to ensure an appropriate level of protection of all assets including information assets. Controls are implemented to avoid loss, damage, or compromise of assets or information and interruption to business activities.

SwissSign retains the overall responsibility for conformance with the procedures described in the ISMS policies even when the TSP's functionality is undertaken by outsourcers. SwissSign defines the outsourcers' liability as described in clauses 5.3.7 and 9.6 and ensures that outsourcers are bound to implement any controls required by SwissSign. SwissSign has documented agreements and contracts with its subcontractors and outsourcing parties provisioning services. SwissSign has defined in these agreements and contracts the liability, relevant requirements, and right to audit subcontracting and outsourcing parties to ensure that they are bound to implement any requirements and controls required by SwissSign.

5.1 Physical controls

Two identical clones for each of the SwissSign Roots keys are stored offline in Swiss bank safe deposit boxes.

The SwissSign CA servers are located in commercial data centers that

- meet the requirements of ETSI EN 319 411-1 and ETSI EN 319 411-2 [5].
- comply with the IT-Security outsourcing requirements (99/2) of the Swiss banking committee.
- are ISO-27001 certified.
- are annually reviewed by a qualified Auditor.

5.1.1 Site location and construction

Swiss bank: The Swiss bank safe deposit boxes have been opened with different Banks at different geo-locations.

Data center: The SwissSign electronic data processing centers are located in data centers in the greater Zurich area in Switzerland.

RA: The SwissSign RA is located in a dedicated building in the greater Zurich area in Switzerland. The requirements of ETSI EN 319 401 are fulfilled.

5.1.2 Physical access

Facilities concerned with certificate generation and revocation management are operated in environments physically protected from compromise through unauthorized access to systems or data since only personnel concerned with these functions have access in such facilities or zones. Every entry and exit to the physically secure areas listed below is logged, are independently overseen, and visitors are accompanied at all times by authorized personnel while in the secure area. Physical protection is achieved through the existence of clearly defined security perimeters with physical barriers around the certification generation and revocation management services. Any parts of the premises shared with other organizations are outside the perimeter of the certificate generation and revocation management services.

Swiss bank: Physical access is only granted to a group of three people by a member of the board of directors or a member of the SwissSign executive management.
Identification documentation (Passport, ID) and the personal signature of every employee are checked by the personnel of the Swiss Bank.
Swiss bank personnel do not have access to the safe deposit box.

Data center: Physical access is restricted to system administrators and authorized data center personnel. Biometric and electronic badge identification is required to enter the facility in which all movements are recorded and logged by video and access control points. Every entry to the facility is logged and subject to a monthly audit review. The logs are subject to a monthly audit review. The TSP has separate cages in the data centers, containing only hardware used by the TSP.

RA: Physical access is restricted to authorized personnel. Electronic badge identification is required to enter the facility.

5.1.3 Power and air conditioning

Swiss Bank: Workspace with power facilities is available whenever needed.

Data center: The data centers are air-conditioned so as to create an optimal environment for the system according to generally accepted best practices. Power relies on two independent local power suppliers as well as on independent emergency diesel generators and on emergency battery power.

5.1.4 Water exposures

Swiss bank: The two Swiss banks are not located in the same zone of exposure.

Data center: The two data centers are not located in the same zone of exposure. The data centers have water sensors in all double floors. Adequate alarming is ensured.

5.1.5 Fire prevention and protection

Swiss bank: Both Swiss banks have fire prevention and protection.

Data center: The fire prevention system is an advanced VESDA (very early smoke detection system) and gas-type system. The data centers have either an Inergen-based fire extinguishing system or a water-based fire extinguishing system.

5.1.6 Media storage

Media used within the TSP systems is securely handled and protected in accordance to internal policies and procedures from damage, theft, unauthorized access, and obsolescence within the period of time that records are required to be retained.

5.1.7 Waste disposal

The disposal of storage media is outsourced to a third party specializing in the destruction of data on storage media. The TSP ensures that no hardware is reused. Hardware that is no longer used is physically destroyed. The disposal process is monitored and documented by the security officer. Application documents that are no longer required will also be physically destroyed.

5.1.8 Off-site backup

The system periodically generates a backup of all digital information (data, code, configuration, etc.). The backup contains all information relevant for the CA service in encrypted form. Regular recovery tests are carried out, the results are recorded and evaluated.

All PKI environment data destined for off-site storage is encrypted.

5.2 Procedural controls

5.2.1 Trusted roles

In order to guarantee a segregation of duties in conflicting areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets, the roles within the SwissSign TSP are operated by four, clearly defined, authorization groups: Security Officer, System Administrators, System Operators and System Auditors. Any person may only be part of one of these authorization groups with the exception of the Security Officer and System Auditors. Within these authorization groups, multiple roles are defined (see table below). A person assigned to one of the groups may have one or more roles within the same authorization group.

5.2.1.1 Security Officer (SecOff)

The Security Officer has the overall responsibility for administering the implementation of the applicable security practices.

5.2.1.2 System Administrator

In general, the System Administrator is responsible for the installation, configuration, and maintenance of the trustworthy systems of SwissSign, including performing the system backup and recovery functions. Within this authorization group in SwissSign, the following sub-roles are defined:

5.2.1.2.1 Infrastructure Engineer (Infra Eng)

Infrastructure Engineers install, configure, and maintain the TSP's trustworthy systems, including recovery of the systems.

Infrastructure Engineers have full control over the network access to all the systems as well as full control of the layers from hardware up to operation systems.

5.2.1.2.2 Application Engineer (App Eng)

Application Engineers have full control of TSP application software (i.e. all application level systems of the TSP above the operation system), but not of cryptographically relevant information such as the private keys of any of the TSP components.

The Application Engineer is authorized to install, configure, and maintain the TSP's trustworthy systems for registration (of all identity data for certificate issuance), certificate generation, subject-device provision and revocation management.

The Application Engineer is responsible for operating the trustworthy systems on a day-to-day basis and supports system backup and recovery.

5.2.1.3 System Operator

In general, the System Operator is responsible for operating the TSP's trustworthy systems on a day-to-day basis. Within this authorization group in SwissSign, the following sub-roles are defined:

5.2.1.3.1 CA Manager (CAM)

The CAM is responsible for the operational life-cycle (create, change, delete) and therefore has full control of TSP PKIs. Additionally, the CAM configures the PKI parameters (e.g. certificate profiles, ct configuration or linters).

5.2.1.3.2 TSP Operator

The TSP Operator manages customer requests and inquiries on all levels and manages the TSP's customer services on a day-to-day basis. This includes read access on customer-related systems. Additionally, the TSP Operator is enabled to revoke certificates.

5.2.1.3.3 Registration Authority Operators (RAO)

The RAO validates authentication and identification information of organizations and individuals according to chapters 3.2 - 3.4 of this combined CP/CPS.

For a subset of certificates the RAO is enabled to revoke certificates.

5.2.1.4 System Auditor

The System Auditor has audit rights to all systems of the Certificate Authority as well as the Identity Provider to provide internal audit capabilities and verify the rules and regulations of this combined CP/CPS. The System Auditor has no direct operative abilities on production environment.

5.2.2 Number of persons required per task

SwissSign has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple persons in Trusted Roles are required to perform sensitive tasks. The operation of all CAs is entirely role-driven and therefore requires at least:

- System Administrator: 2 employees for network access configuration and TSP maintenance and management tasks
- System Operator: 2 employees for system administration and TSP operation
- System Auditor: 1 auditor

The certificate store and all cryptographically relevant aspects of all TSP's signing operations can only be performed under four-eye-principle.

5.2.3 Identification and authentication for each role

Security roles and responsibilities, as specified in the role concept, are documented in job descriptions or in documents available to all concerned personnel (temporary and permanent as necessary). Personnel dedicated to trusted roles are named and accepted by the management and the person to fulfil the role is appointed following the internal documented procedure for appointing individuals to Trusted Roles. The requirements of the information security policy apply.

Access to systems is always limited to authorized individuals (no accounts are shared) following the 'least privilege' principle and based on 2-factor authentication for SwissSign employees or for subcontractors if applicable. Internal procedures are in place to ensure timely removal of access for all employees, especially for persons in trusted roles or with privileged access to Certificate Systems, within 24 hours upon termination of employment or contractual relationship. Moreover, all system accounts are reviewed at least once every three months to ensure that all accounts that are no longer necessary for operation are deactivated. All personnel are identified and authenticated before using critical applications related to the service. Authentication keys and passwords for any privileged ac count on the Certificate System is changed or revoked whenever a person's role is changed or revoked. Access to information and application system functions is restricted in accordance with the access control policy.

For authentication controls, SwissSign has implemented the following controls:

- In general, multi-factor authentication is implemented to each component of the Certificate System that supports such authentication.
- The password length is based on the user role category. The following categories are defined:
  - non-privileged accounts: must be at least 10 characters long
  - privileged accounts: must be at least 12 characters long
- Password lifetime is 730 days
- After 5 unsuccessful attempts a lockout takes place
- After 10 minutes of inactivity the workstation is automatically locked
- Follow the Clear Desk Policy

5.2.4 Roles requiring separation of duties

To guarantee a strict segregation of duties as described in clause 5.2.1, roles related to access, operations, and audit must be held by separate individuals.

5.3 Personnel controls

The TSP fulfills the requirements for personnel from ETSI EN 319 401 [6], ETSI EN 319 411-1, ETSI EN 319 411-2 and CA/B Forum requirements.

For its eIDAS trust services the TSP fulfills the additional requirements for personnel from SVG and SVV.

If SwissSign as Trust Service provider or its RA applies for a certificate for itself (for its employees), personnel in Trusted Roles are obliged to follow all required procedures without exceptions (including identity validation) as defined in the policies and practice statements.

5.3.1 Qualifications, experience, and clearance requirements

SwissSign ensures to employ staff and subcontractors who possess the necessary expertise, reliability, experience, and qualifications to perform a service/job function and support the trustworthiness of the TSP's operations. Additionally, TSP staff and, if applicable, subcontractors, have received training regarding security and personal data protection rules as appropriate for the offered services and job function. The records documenting personnel qualifications are readily accessible to the Austrian supervisory body for retrieval if required.

Employees who are active in the field of certification and revocation services are independent and free of commercial and financial constraints that could influence their decisions and actions. The organizational structure of the TSP takes into account and supports employees in the independence of their decisions.

Trusted Role	Requirements
System Administrators	proven knowledge of: TCP/IP networking, Unix operating systems, PKI technology and applications that use PKI and PKI concepts
System Operators	proven knowledge of: PKI technology and applications that use PKI good understanding of: PKI processes strong people skills
System Auditors	proven knowledge of: PKI technology and applications that use PKI good understanding of: PKI processes strong people skills
Security Officer	proven knowledge of: TCP/IP networking, Unix operating systems, PKI technology and applications that use PKI, PKI concepts, security in general, PKI processes strong people skills

Before starting work at the TSP, new employees must sign confidentiality (non-disclosure) agreements and independence statements.

The management has acquired the necessary knowledge and experience in relation to the offered trust services by participating in training courses or through several years of professional experience. Knowledge of the risk assessment procedures implied by the TSP and the applicable safety procedures for personnel carrying out safety tasks are ensured by training, sufficient for the performance of management functions.

5.3.2 Background check procedures

The TSP verifies the background of its employees and ensures that employees do not have a criminal record. The background check is repeated at least every 2 years.

The TSP will not appoint any person who is known to have been convicted of a serious crime or other offense which could affect his suitability for the position. Personnel shall not have access to the trusted functions until all necessary checks have been completed. The TSP will ask any candidate to provide such information and refuse an application if access to such information is denied.

5.3.3 Training requirements

The TSP ensures that the persons involved in the certification service have the necessary knowledge, experience, and required skills for their position. The identity, reliability and professional knowledge of the personnel are checked before the start of work. Regular and event-related trainings ensure competence in the areas of activity as well as general information security. Training and performance records are documented.

5.3.4 Retraining frequency and requirements

Retraining of employees is done as necessity arises, depending on the needs of the organization or the needs of the individual, but at least once a year including updates on new threats and current security practices.

5.3.5 Job rotation frequency and sequence

Job rotation of employees is done as necessity arises, depending on the needs of the organization, or by request of an individual employee. Role changes are documented.

5.3.6 Sanctions for unauthorized actions

All TSP personnel are accountable for their activities. The TSP reserves the right to prosecute unauthorized actions to the fullest extent of applicable law. The TSP excludes unreliable employees from the activities in the certification service.

5.3.7 Independent contractor requirements

Above and beyond regular documentation, contractors that are candidates for an Access, Operations, or Audit role must:

- provide proof of their qualifications in the same manner as internal personnel (see clause 5.3.1),
- demonstrate a clean criminal record in a separate confidentiality statement (non-disclosure agreement) in addition to the confidentiality agreement covering the contractual relations with third-party contractors.

5.3.8 Documentation supplied to personnel

On their first day of work, all SwissSign employees receive an introduction and access to the SwissSign security policy, security concept, personal workspace security, and risk management documentation. Every employee is expected to read and understand all of this documentation during the first week of employment with the TSP.

The TSP has an ISMS management system. This ensures that a defined security policy exists and is active. This policy is reviewed at least once a year and released by management. The TSP ensures that all employees and partners are made aware of security relevant requirements and / or behavioral rules in the recurring yearly trainings. The TSP is responsible for adhering to the requirements set out in the policies, even if individual tasks are provided by partners. In case of changes resulting in an update of the information security policy, all employees are informed about the changes.

5.3.9 Transfer and termination

The TSP has established processes to ensure that assets (both physical and electronic) and permissions are revoked or returned upon transfer of role or termination of employment.

5.4 Audit logging procedures

The SwissSign systems are built to log all events that occur. The logs are stored in a centralized manner.

SwissSign records and keeps accessible for an appropriate time as specified in clause 5.4.3, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service taking into consideration the confidentiality and integrity of current logs.

5.4.1 Types of events recorded

The following system audit logs are collected in the logs of the CA relevant systems:

- account violations
- user account logon
- all events relating to the synchronization of the clock to UTC, the detection of loss of synchronization
- Any security events related to Systems, Hardware, Network, and physical security including system start-up and shutdown, administration of the trustworthy systems, system crashes and hardware failures, firewall and router activities, and PKI system access attempts.

The above list is non-conclusive, and it is limited to events that are directly related to certificate management or trust-related functions. In particular, it does not include technical events that are logged elsewhere.

5.4.2 Frequency of processing log

Logs are processed continuously in automatic manner and automated alerts are sent to the responsible team in case of security-relevant events.

Logs are processed in accordance to ETSI EN 319 411-1 and TLS BR to check compliance and take according decisions.

5.4.3 Retention period for audit log

The log information is kept for two years. The log entries can be viewed with the role Auditor.

5.4.4 Protection of audit log

Read access to the log information is granted to personnel requiring this access as part of their duties. The following roles can obtain this access:

- System Auditor – audit logs,
- RAO – logs concerning only the RAO application (user logs),
- TSP Supporter – system logs,
- CAM – system logs

The log information is stored in the database and access to the database is protected against unauthorized access by the CA application and through special security measures on the operating system level.

5.4.5 Audit log backup procedures

The log information is an integral part of the SwissSign CA database and is therefore part of the daily backup. Only employees with the role Infrastructure Engineer have access to the backup media.

5.4.6 Audit collection system (internal vs. external)

The audit log is an integral part of the SwissSign CA system.

5.4.7 Notification to event-causing subject

Depending on the severity of the log entry, the TSP reserves the right to notify the Subscriber and/or the responsible RA of the event, the log entry and/or the results of the event.

5.4.8 Vulnerability assessments

This CA and all its subordinated issuing CAs are constantly (24x7) monitored, and all attempts to gain unauthorized access to any of the services are logged and analyzed. The TSP reserves the right to inform the relevant authorities of such successful or unsuccessful attempts.

5.5 Records archival

The TSP archives all records concerning data issued and received by the TSP, in accordance with the defined processes and procedures, taking into consideration the confidentiality and integrity of the archived records. Records concerning the operation of services are made available if required for the purpose of providing evidence of the correct operation of the services for the purpose of legal proceedings.

Back-up copies of essential information and software is taken on a regularly basis. The back-up facilities guarantee that all essential information and software can be recovered following a disaster or media failure. Back-up arrangements are tested regularly to ensure that they meet the requirements the business continuity plan.

A corresponding request for information can be made via the contact given in this document. The TSP then checks the authorization and provides the required information.

5.5.1 Types of records archived

The following records are archived:

- All events relating to the life-cycle of keys (CA or subject): key generation, backup, storage, recovery, archival and destruction where applicable,
- All events related to the life-cycle of certificates
- certificate requests (also for renewal, rekey)
- acceptance of terms and conditions
- rejected and approved certificate requests
- certificate signing (also for renewal, rekey)
- certificate revocation and the resulting action (CRL and OCSP entries)
- for the signing services, all events related to the signing process
- CRL signing
- CA rollover
- certificate expiration
- certificate downloads/installation
- CAA Check, if applicable
- signature requests (remote signing), if applicable
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
- All verification activities in accordance with this combined CP/CPS and TLS BR requirements
- Multi-Perspective Issuance Corroboration attempts from each Network Perspective are logged with at least the following information:
  - an identifier that uniquely identifies the Network Perspective used
  - the attempted domain name and/or IP address
  - the result of the attempt (e.g., “domain validation pass/fail”, “CAA permission/prohibition”)
- Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request

5.5.2 Retention period for archive

Archived information is kept at least 11 years beyond the end of subscription, as specified in clause 4.11.

For its eIDAS services archived information is kept at least 30 years beyond the end of subscription according to SVV.

5.5.3 Protection of archive

Protection of the archive is as follows:

- Archived information is only accessible to authorized employees according to the role model as presented in clause 5.2.

- Protection against modification: Archives of digital data are protected according to Swiss law to prevent unknown modification.
- Protection against data loss: The RA must ensure that at least two copies of the archived data is available at all times. The storage locations must be suitable for this purpose and must provide physical protection and access controls.
- Protection against the deterioration of the media on which the archive is stored: Digital data is to be migrated periodically to fresh media.
- Protection against obsolescence of hardware, operating systems, and other software: As part of the archive, the hardware (if necessary), operating systems, and/or other software is archived in order to permit access to and use of archived records over time.

5.5.4 Archive backup procedures

Archived information is stored off-site in a secure location suitable for archiving purposes.

5.5.5 Requirements for time-stamping of records

All records in the database and in log files are time-stamped using the system time of the system where the event is recorded.

The system time of all servers is synchronized (at least once a day) with the time source of the SwissSign Time-Stamping Authority (TSA) or another official time source. The TSP uses three independent time sources. If one of the servers or clients no longer meets the requirements of Stratum 3 an alarm is triggered. When the TSA service is affected the TSP stops to issue timestamps in such a case.

5.5.6 Archive collection system (internal or external)

This CA and all its subordinated issuing CAs use an internal archiving system.

5.5.7 Procedures to obtain and verify archive information

In the event of a court order, a high-quality copy is made of the archived information and the original is temporarily made available to the court. When the original information is returned, the high-quality copy is destroyed. This process is logged and audited. For its eIDAS services, the TSP will make available the certificate database to courts of law and civil services specifically for use in legal proceedings.

5.6 Key changeover

The TSP changes over all keys of subordinated issuing CAs on a regular basis. All certificates of such subordinated issuing CA are available for download on the swisssign.net website and in the public directory directory.swisssign.net. These CA certificates are directly signed by the long-living trust anchors (Root CA) of the SwissSign PKI.

Early enough before expiration of its Trust Service certificate, SwissSign generates a new Trust Service certificate for signing subject's public key and apply all necessary actions to avoid disruptions of any operations that rely on the certificate and to allow all relying parties to become aware of key changeover.

For the existing Root CA certificates issued in the past, key changeover is performed every 15 years or based on a current risk assessment.

For new Root CAs issued after the publication of this combined CP/CPS, key changeover shall be performed based on a current risk assessment taking into consideration the latest risks.

The new Trust Service certificate is generated and distributed according to this combined CP/CPS.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

To manage all operational processes, the TSP has adopted the ITIL best practices framework:

- A service desk receives all incoming service calls and assesses them according to severity.
- Incident management has the goal to restore normal operation as quickly as possible.
- Recurring incidents or incidents with major impact are entered into the problem management process. The goal here is to find the ultimate cause of the problem and to prevent further issues.

To manage a crisis or catastrophe, the TSP has a Business Continuity Management plan. This plan addresses all topics (conditions, procedures, responsibilities etc.) listed in chapter 5.7.1 of the TLS BRG and the SMIME BRG respectively. Once this plan goes into action, the Emergency Management Team assumes managerial duties of the TSP until the crisis is dealt with.

The Emergency Management Team has a charted course of action for the following events:

- Loss of one computing facility,
- System or server compromise,
- CA key compromise,
- Algorithm compromise,
- Compromise of HSM,
- Compromise of QSCD/SSCD.

If a crisis or catastrophe situation is declared, the TSP will communicate this state to the Board of Directors of SwissSign AG, the Swiss authorities, the Swiss Recognition Body, and the relevant Root Store maintainers.

The TSP has an emergency plan in case of HSM or QSCD/SSCD corruption.

In the process of handling crisis or catastrophe situation, the Business Continuity Management might be invoked.

The TSP annually tests, reviews and updates the procedures specified in the Business Continuity Management plan and the according security plans.

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.

The TSP has a process for managing and making use of information received from National CSIRT or, where applicable, competent authorities useful for crisis management.

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

This CA and its subordinated issuing CA are implemented on fully redundant server systems. Any hardware defect will only affect one such system and allow a redundant system to take over and provide full functionality.

The master server of this CA and its subordinated issuing CA are part of a daily backup process.

5.7.3 Entity private key compromise procedures

In the case that any algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP will inform all subscribers and relying parties with whom the TSP has an agreement or established relations. In addition, the TSP will make this information available to the relying parties. Furthermore, the TSP will schedule the revocation of the affected certificates.

If the private key of this CA or one of its subordinates issuing CAs is suspected to be compromised, executive management of the TSP must be informed immediately. The following steps will be taken:

- The TSP will inform the relevant governmental authorities, the corresponding auditor and the relevant Root Store maintainers of any trust-anchor compromise.
- The TSP informs the relying parties about the incident by means of information on the SwissSign homepage.
- All Subscriber certificates will be revoked.
- The OCSP responder certificate(s) will be revoked
- A last CRL will be issued
- The CA certificate will be revoked.
- A new CARL, i.e. the CRL of the Root CA will be issued and published.
- All Subscribers with certificates issued by either the revoked CA or one of its subordinated issuing CA will be informed by e-mail as soon as possible.
- The cause of the key compromise will be determined and the situation rectified.
- The TSP will generate a new key pair for the new CA and the resulting key certificate will be signed by the superior CA.
- The new CA certificate will be published on the swisssign.com or the swisssign.net web site.

5.7.4 Business continuity capabilities after a disaster

The TSP has an emergency concept and a disaster recovery plan, which are known to the roles involved and can be implemented by them if necessary. The responsibilities are clearly allocated and known. Whenever possible, measures are derived from the analysis of the reasons for the occurrence of an emergency and taken in order to avoid such events in the future.

5.8 CA or RA termination

The TSP has an up-to-date termination plan to minimize potential disruption to subscribers and relying parties as a result of the cessation of SwissSign Services, and in particular for continuing the maintenance of information required to verify the correctness of trust services.

Before the TSP terminates its services, the following actions will be executed:

- Before the TSP terminates its services, it will inform of the termination all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, RAs and relevant authorities such as supervisory bodies. The TSP endeavors to give at least 30 days advance notice before revoking any certificates. This explicitly includes the Swiss SAS, the Swiss Recognition Body and any other governmental control agency or legal quality control organization.
- Before the TSP terminates its services, it will make the information of the termination available to other relying parties.
- The TSP will terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.
- The TSP will report, without delay, any threat of bankruptcy to the relevant national accreditation body, the relevant supervisory body, the Swiss Recognition Body and any other governmental control agency or legal quality control organization.
- The TSP will immediately stop all registration services and if applicable will enforce this cessation of services for all other registration authorities.
- The TSP will immediately cancel all current and valid contracts. The cancellation is to be effective after the entire business termination process has been concluded. The TSP will also immediately revoke all rights of contracted parties to act on behalf of the TSP.

After a waiting period of at least 30 days, the following actions will be executed:

- The TSP will revoke all Subscriber certificates and will issue for each issuing CA a last CRL.
- The TSP will revoke all issuing CA certificates and issue for each Root CA a last CARL.
- The TSP will transfer obligations for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period such as registration information, certificate status information, and event log archives that cover the respective time to the appropriate organization.

- The TSP will destroy all private keys, including backup copies of the private signing keys of the SwissSign Root CAs and Subordinated Issuing CAs such that the private keys cannot be retrieved, retained, or put back into use.
- All copies of documents which are required to be saved according to the stipulations of any applicable law will be stored under the conditions and for the duration as stipulated in this combined CP/CPS.
- The TSP will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period such as to make available the public keys or the trust service tokens to relying parties if applicable.

RA termination is subject to negotiations with other equivalent RAs. Another RA may offer to assume the RA function for the Subscribers of the terminating RA. Regardless of whether or not an RA assumes the role of a terminating RA, the TSP will guarantee the safekeeping of any RA documents as stipulated in this document.

To ensure that these activities can be carried out, the TSP has entered into an insurance policy to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

6. TECHNICAL SECURITY CONTROLS

Applied devices are operated according to the manufacturer's instructions. Before commissioning, they are thoroughly tested. They are not used if it is suspected that they have been tampered with. If a component is suspected to have been tampered with, a planned action on the component is not executed and the incident is reported to the CISO. The TSP defines clear escalation guidelines for the individual roles, in order to be able to respond quickly and in a coordinated manner to possible security-relevant incidents.

For business continuity management purposes capacity requirements, capacity utilization and suitability of the systems involved are monitored and adapted as required.

Exchanged devices or obsolete data carriers which are no longer required, are taken out of service and disposed of in such a way that functionality or data misuse is excluded.

Changes to systems, software or processes go through a documented change management process. Security-critical changes are checked and released by the Change Advisory Board. After expiration of the validity of CAs the private keys are destroyed.

6.1 Key pair generation and installation

SwissSign uses cryptographic keys for its Trust Services and follows industry best practices for key lifecycle management, key length and algorithms. Appropriate security controls are put in place in accordance to the internal TSP policies for the management of any cryptographic keys and cryptographic devices throughout their lifecycle, as detailed later in this clause of the combined CP/CPS.

The HSMs/QSCD/SSCD used by the TSP are checked for authenticity after delivery before commissioning. The TSP shall check the integrity of the equipment and the conformity of the manufacturer's seal numbers with which the equipment is secured. This process is carried out and documented following the four-eyes principle. The log of the check is archived.

After the so called unpacking procedure the HSM/QSCD/SSCD can be put into operation. During commissioning, the firmware and software version of the HSM is checked and the policy settings are made. This procedure is carried out and documented following the four-eyes principle. The log of the check is archived.

The QSCD is operated in its configuration by the TSP as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

6.1.1 Key pair generation

The signing keys of SwissSign Trust Services are created in an HSM in accordance with internal procedures where the followings are indicated:

- Persons participating in the ceremony and their roles (internal or external);
- Functions to be performed by every role and in which phases;
- Responsibilities during and after the key ceremony; and
- Evidences to be collected for the ceremony.

The HSMs are located in a high-security area and operated in FIPS mode, which guarantees that the private keys can never leave the HSM unencrypted. Following the TSP's documented procedures, the key pairs for the Root or subordinated issuing CA of SwissSign have been generated in HSMs that meet at least FIPS 140-2 level 3 requirements. Subsequently, the Issuing CA keys have been cloned into an online HSM meeting at least FIPS 140-2 level 3 requirements. In the case of key generation, the implementation of the role concept and the principle of double control are enforced.

The creation of SwissSign Trust Service keys for Root CAs is performed in the physically secured environment under at least dual control by authorized, trusted personnel in such a way that one person is not able to sign subordinate certificates on his/her own. Moreover, the key ceremony is observed by external auditor(s), who after the creation of the keys draw up an appropriate deed containing the details of the certificate including public key of the created pair of keys and the hash thereof.

The Ceremony Master creates a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. The report is signed by the Ceremony Master, Key Access Operators, and external auditors if applicable. The more detailed procedures for key ceremony, roles, and responsibilities of participants during and after procedure, requirements for report, and collected evidence are defined in internal key ceremony procedures.

For Root and Issuing CAs, also refer to clause 6.1.1 of the TLS BR [1].

Key pairs for TLS certificates 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

Relying Parties can download the issuing CA certificate from the SwissSign website by using the PKCS#7 format.

When a Subscriber receives the certificate, the issuing CA public key is included. Also included is the complete chain of certificates of the hierarchical SwissSign PKI containing all public keys that are part of the trust chain.

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 [3]

- NIST: SP 800-89 [7]

Root CAs and Issuing CAs issued before 2021 use a 2048-bit RSA key.

Root CAs and 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.

All Root CA, Issuing CA and Subscriber RSA keys must be divisible by 8.

6.1.5.1 Algorithm object identifiers

The algorithms with OIDs supported by this CA and its subsidiaries are:

Algorithm	Object Identifier
SHA1withRSAEncryption	1.2.840.113549.1.1.5 (phase out)
SHA256withRSAEncryption	1.2.840.113549.1.1.11
RSASSA-PSS	1.2.840.113549.1.1.10
rsaEncryption	1.2.840.113549.1.1.4

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 TLS BR 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 combined CP/CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

SwissSign verifies that the HSM has not been tampered when received. Appropriate documentation is kept in accordance with the internal procedures for the HSM life-cycle.

6.2.1 Cryptographic module standards and controls

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

- Root CA keys: The HSM used for CA keys is kept offline at all times and meets at least FIPS 140-2 level 3 requirements.
- Issuing CA keys: The HSM used for CA keys meets at least FIPS 140-2 level 3 requirements. These keys are online and access is strictly controlled by using the ‘4-eye’ principle.
- 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: Root CA keys can only be accessed on the physical and on the logical level by adhering to ‘3 out of 6’ control, meaning that 3 of the 6 persons are present.
- Issuing CA keys: Management access to these keys is only possible using ‘4-eye’ principle (2 out of m). Once the issuing CA is operable, signing operations can be authorized by a single RA operator.

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

- Root CA keys: Root CA keys are not in escrow.
- Issuing CA keys: The issuing CA keys are not in escrow.
- 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: Root CA keys have been backed up onto an HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access.
- Issuing CA keys: The Issuing CA keys have been put into backup HSM, so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 2 persons are present in order to gain physical and logical access.
- TSA keys: The TSA keys are not backed up.
- 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: The Root CA keys are not archived.
- Issuing CA keys: The Issuing CA keys are not archived.
- Subscriber keys: Subscribers are solely responsible for the archival of Subscriber keys.

6.2.6 Private key transfer into or from a cryptographic module

Private key transfer is used to create redundancy and geo-independent backups. The following list shows how private key transfers are implemented:

- Root CA keys: The Root CA keys are cloned only into other HSMs providing the same cryptographic security using the functionality provided by the HSM.
- Issuing CA keys: The Issuing CA keys are cloned in the same manner as Root keys.
- 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: The Root CA keys are stored on cryptographic modules so that they can be used only if properly activated.
- Issuing CA keys: The Issuing CA keys are stored on cryptographic modules so that they can be used only if properly activated.
- Subscriber keys: Subscribers are solely responsible for the transfer of Subscriber keys into or from a cryptographic module.

The controls on these processes are explained in clause 6.2.4.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

- Root CA keys: The Root CA keys are activated with a user key (physical), a user pin (knowledge) and 3 authentication keys (physical).
- Issuing CA keys: The Issuing CA keys are activated with role-based access control requiring at least two persons.
- 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: The Root CA keys are deactivated at least under dual control either by logging out of the HSM, by terminating the session with the HSM, by removing the CA token from the computer or by powering down the system.
- Issuing CA keys: The Issuing CA keys are deactivated at least under dual control by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.
- 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: The Root CA keys are destroyed at least under dual control by initializing the partition on the HSM.
- Issuing CA keys: The Issuing CA keys are destroyed at least under dual control by initializing the partition on the HSM.
- Subscriber keys: Subscribers are solely responsible for destroying the private key.

All copies of SwissSign private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible. 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

Minimum standards for cryptographic modules have been specified in clause 6.1.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All certificates, and therefore the public keys of all Subscribers and all CAs, are stored on line in a database. This database is replicated to all servers in the CA cluster. This database is also part of the daily backup. To protect the data in the database, the database is encrypted with a special backup key before it is put into the backup.

The daily backup is copied onto a backup server and kept available online for 4 weeks.

A weekly full dump is copied onto a backup media and stored offsite. Archived media are never destroyed.

6.3.2 Certificate operational periods and key pair usage periods

The usage periods for certificates issued by this CA are as follows:

- The Root CAs as well as all trust-anchor certificates and cross-certificates are valid up to 30 years.
- Issuing CA certificates are issued for a maximum lifetime of 15 years.
- End user certificates can have a lifetime of up to the maximum remaining lifetime of the issuing CA certificate minus 10 days.
- TLS certificates are issued with a validity period not greater than (replacing all previous validity periods, e.g., 398 days):
  - 200 days for certificates issued on or after 15 March 2026
  - 100 days for certificates issued on or after 15 March 2027

  - 47 days for certificates issued on or after 15 March 2029

Serial Numbers for certificates generated by the TSP are non-sequential and greater than zero containing at least 64 bits of output from a CSPRNG.

SwissSign uses appropriately the CA private signing keys and not beyond the end of their life-cycle.

Key changeover will be performed as described in clause 5.6.

6.4 Activation data

6.4.1 Activation data generation and installation

The activation data of the Root CA keys and the issuing CA keys are generated during the Trust Anchor Key Ceremony.

6.4.2 Activation data protection

- Root CA keys: The activation data is distributed over multiple physical keys. The owners of a part are required to store this part in a private safe deposit of a Swiss bank.
- Issuing CA keys: The activation data is known to trusted individuals at the TSP. An escrow copy is stored in a safe deposit with dual controls access.
- Subscriber keys: Subscribers are obliged to keep the activation data secret at all times.

6.4.3 Other aspects of activation data

SwissSign-approved crypto devices and their product fulfill the requirements of ETSI EN 119 312 [3].

6.5 Computer security controls

The CA servers are protected by internal and external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. CA access to the system is granted only over secure and restricted protocols using strong public-key authentication. This way, the TSP systems are protected against modification and ensure the technical security and reliability of the processes supported by them.

The performance of SwissSign services and IT systems and their capacity is monitored and changes are done when necessary according to internal change management procedure.

6.5.1 Specific computer security technical requirements

SwissSign uses a layered security approach to ensure the security and integrity of the computers used to run the SwissSign CA software in accordance with the information classification scheme. The integrity of the systems and information is protected against viruses, malicious and unauthorized software. The following controls ensure the security of SwissSign-operated computer systems:

- Hardened operating system
- Software packages are only installed from a trusted software repository
- Minimal network connectivity
- Authentication and authorization for all functions
- Strong (multi-factor) authentication and role-based access control for all vital functions
- Proactive patch management
- Monitoring and auditing of all activities

6.5.2 Computer security rating

The TSP has applied procedures which ensure that security patches are applied within a reasonable time after they are available and no later than 6 months from when the security patches are made available. In the case that security

patches will be not applied, because they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them, the reasons for not applying the security patches is documented.

The TSP has established a security framework which covers and governs the technical aspects of its computer security.

The systems themselves and the services running on these systems are subject to thorough reviews and testing (including penetration testing).

In order to make its environment more secure and to keep it on a state-of-the-art security level, the TSP operates a vulnerability management process which includes monitoring of supplier security alerts.

The technical aspects of computer security are subject to periodic audits under supervision of the Chief Information Security Officer (CISO).

The CISO is also responsible for network and Information Security and reporting to top management.

6.6 Life cycle technical controls

6.6.1 System development controls

To ensure quality and availability of the TSP software, SwissSign implements the ITIL model to ensure that security requirements are carried out at the design. The development team adheres to the following principles:

- All software is stored in the Source Code Control System to keep track of software versions.
- The software archive is put onto backup regularly, and a copy is stored externally.
- A Software Life Cycle Control based on separate environments for Development, Test and Production is in place. This software life cycle control ensures adherence to controls and checkpoints within the organization.
- Internal software development policies specify standards and principles for software engineering and related tasks.
- Changes to the systems are accordingly documented.

6.6.2 Security management controls

Continuous monitoring is used to ensure that systems and networks are operated in compliance with the specified security policy and taking into account the sensitivity of any information collected or analyzed. Abnormal system activities that might indicate a potential security violation, including intrusion into the TSP's network are detected and reported as alarms.

All processes are logged and audited according to applicable law and normative requirements. In particular, the TSP monitors the start-up and shutdown of the logging functions, the availability and utilization of needed services within the TSP network. The TSP has implemented automatic mechanisms to process the audit logs and alert personnel of possible critical security events and possible audit log compromise. Persons in trusted roles are appointed to follow up on alerts of potentially critical security events and ensure that relevant response is undertaken and that incidents are reported as defined in SwissSign procedures in order to minimize the damage.

Each vulnerability identified by the TSP is examined and treated within 48 hours according to the vulnerability correction process as defined in the ISMS guidelines for the treatment of security events. For any vulnerability, given the potential impact, SwissSign either creates and implements a plan to mitigate the vulnerability and documents accordingly the identification, review, response and remediation process, or documents the factual basis for the determination that the vulnerability does not require remediation.

In case of incidents, the TSP has defined internal policies and procedures to be followed in order to act in a timely and coordinated manner to respond quickly to the incident and limit the impact of breaches of security.

Procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity with impact on the trust services provided and on the personal data maintained therein within 24 hours of the breach being identified. Where the breach of security or loss of integrity is verified to affect natural or legal persons, the TSP will notify them as well without undue delay.

The TSP monitors OCSP requests and the request for unknown certificates on the OCSP responder as part of the business continuity and security controls.

The TSP monitors the certification status of cryptographic devices.

6.6.3 Life cycle security controls

Development of software systems adheres to principles specified in the internal software development policies. These policies are part of a security management process covering life cycle aspects of security controls.

6.7 Network security controls

The TSP fulfills the CA/B Forum's Network Security Requirements by implementing a network concept based on its risk assessment considering functional, logical, and physical relationships between trustworthy systems and services. This ensures that the sensitive CA systems are operated in dedicated secure network zones to protect SwissSign's internal network domains from unauthorized access, including access from subscribers and third parties, or from attacks. For the network concept, a separate documentation is available, which can be viewed on the premises of the TSP in the relevant parts if there is justified interest. To protect the processes of the TSP, among others, firewalls and intrusion detection/prevention mechanisms are used, which only allow explicitly permitted connections. The TSP operates network segments in differentiated severity levels, thereby separating workstation networks from server networks. Same security controls are applied to all systems co-located in the same zone. Access and communication between zones is restricted to those necessary for the operation of the TSP and communication is established only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure. All other connections, accounts, applications, services, protocols and ports that are not needed are explicitly forbidden or deactivated. Communication channels to external third parties are TLS encrypted.

The TSP uses dedicated systems used for administration of the security policy implementation.

Development and test environments are isolated from production and have different networks.

The TSP has policies governing remote work and storage of information accessed, processed or stored outside of its premises.

The systems are subject to regular revisions and the responsible persons are subject to reporting requirements. Abnormalities are reported by technical systems and organizational processes and are dealt within a defined incident process and consequent processes.

Sensitive data is protected by cryptographic mechanisms. The physical security of the networks operated and used by the TSP is ensured and furthermore adapted to the structural conditions and their changes.

If a high level of availability of external access to an offered service is required, the external network connection is redundant to ensure availability in case of a single failure.

6.7.1 Vulnerability management and penetration tests

The TSP performs:

- Monthly vulnerability scans and annual penetration tests (including application servers as well as network devices) on public and private IP addresses identified by the TSP,
- A vulnerability scan within a week of receiving a request from the CA/Browser Forum,
- Vulnerability scan and penetration test after any systems at set up and after infrastructure/application upgrades or modifications that the TSP determines as significant.

The TSP records evidence for each vulnerability scan and penetration test that was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

All identified vulnerabilities are triaged within 48 hours. Based on the criticality of the affected asset/s, the severity of the vulnerability, availability of patches and other relevant factors the mitigation measures are defined. For critical vulnerabilities on critical assets emergency measures are implemented within 7 days. For all other cases vulnerabilities are mitigated in the next regular monthly update and patching cycle.

6.8 Time-stamping

The TSP operates an internal time service using various sources from the Internet, a GPS receiver and a DCF77 receiver. Time used for all Trust Service operations (including revocation services, time-stamping service, audit log events recording etc.) is synchronized with UTC at least once per day.

Based on this internal time service, the TSP offers a Time -Stamping Authority (TSA) that can be used to create a timestamp for arbitrary documents. This service is implemented in accordance with ETSI EN 319 421.

SwissSign may charge a fee for this service. If not stated otherwise Time-Stamping Authority (TSA) keys are handled the same way as Issuing CA keys with the exception that they are not cloned (6.2.4 and backed up (6.2.4).

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The following certificate profiles are compiled in accordance with ITU-T X.509 version 3, IETF RFC 5280, clause 6.6 of ETSI EN 319 411-1, clause 7 of TLS BR and clause 9 of EVCG [2].

7.1.1 Certificate hierarchy

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

7.1.1.1 Root certificates

The Root CA profile is the following:

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number		Unique serial number of the certificate
SignatureAlgorithm		
Issuer Distinguished name		Unique issuer distinguished name of the certificate
Subject Distinguished name		Unique subject distinguished name of the certificate
Valid from		Start of certificate validity
Valid to		End of certificate validity
SubjectPublicKeyInfo	rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit or higher)	
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier		(mandatory)
Authority Key Identifier		(optional)
Extended Key Usage		Not allowed in the Root CA
Name Constraints		Not allowed in the Root CA

Field/Extension	Value(s)	Comment
Certificate Policies		Not allowed in the Root CA
CRL Distribution Points		Not allowed in the Root CA
Authority Information Access		Not allowed in the Root CA

The Root CA certificates governed by this combined CP/CPS are:

7.1.1.1.1 SwissSign Gold CA - G2

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: BB401C43F55E4FB0 (Unique serial number of the certificate)
- SignatureAlgorithm: sha1WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign Gold CA - G2, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign Gold CA - G2, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 25 Oct 2006 08:30:35 UTC (Start of certificate validity)
- Valid to: 25 Oct 2036 08:30:35 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 5B257B96A465517EB839F3C078665EE83AE7F0EE
- Authority Key Identifier: 5B257B96A465517EB839F3C078665EE83AE7F0EE
- Extended Key Usage: (not included in this Root CA certificate)
- Name Constraints: (not included in this Root CA certificate)
- Certificate Policies:
  - 2.16.756.1.89.1.2.1.1 (SwissSign CP/CPS document OID), CPSURI: http://repository.swisssign.com/
- CRL Distribution Points:
  - (not included in this Root CA certificate)
- Authority Information Access:
  - (not included in this Root CA certificate)

The Root CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: D8C5388AB7301B1B6ED47AE645253A6F9F1A2761
- SHA256 Fingerprint: 62DD0BE9B9F50A163EA0F8E75C053B1ECA57EA55C8688F647C6881F2C8357B95

7.1.1.1.2 SwissSign RSA TLS Root CA 2022 - 1 (Self-signed)

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 43FA0C5F4E1B801844EFD1B44F351F44F480EDCB (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 08 Jun 2022 11:08:22 UTC (Start of certificate validity)
- Valid to: 08 Jun 2047 11:08:22 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True (Critical)

- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: (not included in this Root CA certificate)
- Name Constraints: (not included in this Root CA certificate)
- Certificate Policies:
  - (not included in this Root CA certificate)
- CRL Distribution Points:
  - (not included in this Root CA certificate)
- Authority Information Access:
  - (not included in this Root CA certificate)

The Root CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 81340ABE4CCDCECCE77DCC8AD457E245A0775DCE
- SHA256 Fingerprint: 193144F431E0FDDB740717D4DE926A571133884B4360D30E272913CBE660CE41

7.1.1.1.3 SwissSign RSA TLS Root CA 2022 - 1 (Cross)

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 686F43B4DC404C067E230E3FAFC32B (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign Gold CA - G2, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 28 Jun 2022 11:27:11 UTC (Start of certificate validity)
- Valid to: 22 Sep 2036 11:27:11 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Authority Key Identifier: 5B257B96A465517EB839F3C078665EE83AE7F0EE
- Extended Key Usage: (not included in this Cross certificate)
- Name Constraints: (not included in this Cross certificate)
- Certificate Policies:
  - 2.5.29.32.0 (anyPolicy)
- CRL Distribution Points:
  - http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE
- Authority Information Access:
  - (not included in this Cross certificate)

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 972B0E2FDBAA76A21DF4F4390B714F64F1D78686
- SHA256 Fingerprint: 288B4A9F605B09B999B215850825C81F9B537DBAF23664ACA98BF6BA98EDC379

7.1.1.2 Issuing CAs

The Issuing CA profile is the following:

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version

Field/Extension	Value(s)	Comment
Serial Number		Unique serial number of the certificate
SignatureAlgorithm		
Issuer Distinguished name		Unique issuer distinguished name of the certificate
Subject Distinguished name		Unique subject distinguished name of the certificate
Valid from		Start of certificate validity
Valid to		End of certificate validity
SubjectPublicKeyInfo	rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit or higher)	
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier		(mandatory)
Authority Key Identifier		(mandatory)
Extended Key Usage	id-kp-serverAuth (mandatory), id-kp-clientAuth (optional)	
Name Constraints		(optional)
Certificate Policies		(mandatory)
CRL Distribution Points		(mandatory)
Authority Information Access		(mandatory)

The Issuing CA certificates governed by this combined CP/CPS are:

7.1.1.2.1 SwissSign RSA TLS DV ICA 2022 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 75F85DDB06B0FA815891EA83C5CCFCE5578C190F (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS DV ICA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 29 Jun 2022 09:27:46 UTC (Start of certificate validity)
- Valid to: 29 Jun 2036 09:27:46 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: EBBD7F49938CC9EEECA2BAF71CD267F083B1EADE
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth, id-kp-clientAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.2.1 (CABF DV)
  - 0.4.0.2042.1.6 (ETSI DVCP)
  - 2.16.756.1.89.2.1.1 (SwissSign DVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160

- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 333150010FA78F700BC061323C679938CFC64BCB
- SHA256 Fingerprint: B400250EF2B09B30E9AAA3E2C20017B8911BD039DF8AF54949C60AED5BF697D4

7.1.1.2.2 SwissSign RSA TLS OV ICA 2022 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 6AEC7C44417B9B441FB97634CBC6A780B0041E01 (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS OV ICA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 29 Jun 2022 09:34:30 UTC (Start of certificate validity)
- Valid to: 29 Jun 2036 09:34:30 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 7C6F0A6F130FD98C246F2634F35C6B436DB723B6
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth, id-kp-clientAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.2.2 (CABF OV)
  - 0.4.0.2042.1.7 (ETSI OVCP)
  - 2.16.756.1.89.2.1.2 (SwissSign OVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 37271FFBC6EECF840CEB32B8A7AEED6DCBD6A7F0
- SHA256 Fingerprint: 332F9EAE3650C77454AF14FE1A621A2498FD128773662890A0D12835B3436E23

7.1.1.2.3 SwissSign RSA TLS EV ICA 2022 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 2DAE0FA23A0C385FFBF395C0D903642D14184D2E (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS EV ICA 2022 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 29 Jun 2022 09:30:47 UTC (Start of certificate validity)
- Valid to: 29 Jun 2036 09:30:47 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)

- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 4952DF308692595F349C254824ABC0EBD106F2D6
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth, id-kp-clientAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.1 (CABF EV)
  - 0.4.0.2042.1.4 (ETSI EVCP)
  - 2.16.756.1.89.2.1.3 (SwissSign EVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: CD3D43200F279CC95EA6BD955ACB06ED28090B77
- SHA256 Fingerprint: 6AE61943BF4B4FCC8F08ED5044D1C97AA0AD40E1BCFE1BF1B530BD3B151B364D

7.1.1.2.4 SwissSign RSA TLS DV ICA 2026 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 5CEA8ED36492958D4F57D3CE50D9FC74326ABB0D (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS DV ICA 2026 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 10 Jun 2026 08:15:52 UTC (Start of certificate validity)
- Valid to: 10 Jun 2029 08:15:52 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: C362C4A3374601838953826878 0F7D731DBF7F95
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.2.1 (CABF DV)
  - 0.4.0.2042.1.6 (ETSI DVCP)
  - 2.16.756.1.89.2.1.1 (SwissSign DVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 79318135F1DB6E0E7587F04432FB90576DB7F47C
- SHA256 Fingerprint: D6073FEF5D143DA3CBCCA52F686E3542093F5E5F1A6A8F3A6BEBF65DCC9888F4

7.1.1.2.5 SwissSign RSA TLS OV ICA 2026 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 44026BA335B36A02B1536C5558D9FDFFB9904D91 (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS OV ICA 2026 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 10 Jun 2026 08:29:21 UTC (Start of certificate validity)
- Valid to: 10 Jun 2029 08:29:21 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 3237018DBC7A48AD8335D06248911AF96EDBA609
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.2.2 (CABF OV)
  - 0.4.0.2042.1.7 (ETSI OVCP)
  - 2.16.756.1.89.2.1.2 (SwissSign OVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 67E9351DD3C3314AEE6D89C8550BDF4CF6A5F4DC
- SHA256 Fingerprint: CFD692D83CB455C1E068355D7AABBD5EBD631A42389228822926432D2FB8B1C3

7.1.1.2.6 SwissSign RSA TLS EV ICA 2026 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: 57742DB070DE71D48251BB44BD16A3C46F5C67D5 (Unique serial number of the certificate)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: CN = SwissSign RSA TLS Root CA 2022 - 1, O = SwissSign AG, C = CH (Unique issuer distinguished name of the certificate)
- Subject Distinguished name: CN = SwissSign RSA TLS EV ICA 2026 - 1, O = SwissSign AG, C = CH (Unique subject distinguished name of the certificate)
- Valid from: 10 Jun 2026 08:25:07 UTC (Start of certificate validity)
- Valid to: 10 Jun 2029 08:25:07 UTC (End of certificate validity)
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 4096 bit)
- Basic Constraints: CA:True, pathlen:0 (Critical)
- Key Usage: Certificate Sign, CRL Sign (Critical)
- Subject Key Identifier: 8077B8DBCC1C4DEB3F9DB3E20DFD26F5A66757AB
- Authority Key Identifier: 6F8E628B9343B0E140F6A7C3FDF10FB80F1538A5
- Extended Key Usage: id-kp-serverAuth
- Name Constraints: (not included in this Issuing CA certificate)
- Certificate Policies:
  - 2.23.140.1.1 (CABF EV)

  - 0.4.0.2042.1.4 (ETSI EVCP)
  - 2.16.756.1.89.2.1.3 (SwissSign EVCP)
- CRL Distribution Points:
  - http://crl.swisssign.ch/cdp-9661c29f-9121-4f46-acd8-ead4a22f7160
- Authority Information Access:
  - caIssuers: http://aia.swisssign.ch/air-aeff374d-0f7a-4c55-a034-1440290cfa32

The CA certificate is identified via the following fingerprints:

- SHA1 Fingerprint: 60A957DD4C5AA0D6949F8D0F52F1A21773896205
- SHA256 Fingerprint: 6FA62783E0FFDF8A9B1579B5766B07FD6B2AF2DC44F9CB9D6068B3EEDEFE20DB

7.1.1.3 End-entity certificates

The TSP issues under this combined CP/CPS end-entity 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)

7.1.1.3.1 TLS Extended Validation Certificate (EVCP) issued by SwissSign RSA TLS EV ICA 2022 – 1 (EVCP)

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Name: CN=SwissSign RSA TLS EV ICA 2022 - 1,O=SwissSign AG,C=CH (Unique issuer distinguished name of the certificate)
- Subject DN: (Unique subject distinguished name of the certificate)
  - Common Name (CN): FQDN (mandatory)
  - SerialNumber: Unique Registration Number as stated in certificate application, a date of incorporation, formation, or establishment, “Government Entity”, OR language to indicate an International Organization Entity (like “International Organization”) (mandatory)
  - OrganizationName (O): Subject organization name as stated in certificate application. (mandatory)
  - Street: Name of the street as described in the certificate application. (optional)
  - PostalCode: Postal code as described in the certificate application. (optional)
  - LocalityName (L): Name of the locality as described in the certificate application (mandatory if ST-attribute is missing, otherwise optional) (optional)
  - State-Or-Province (ST): State or province name or code as described in certificate application and in accordance with ISO 3166-2 (mandatory if L-attribute is missing, otherwise optional) (optional)
  - Country (C): Country code in accordance with ISO 3166-1 (mandatory)
  - Business Category (BC): One of the following: “Private Organization”, “Government Entity”, “Business Entity”, or “Non-Commercial Entity” as described in certificate application. (mandatory)
  - Jurisdiction Locality Name (joiL): Name of the locality as described in the certificate application. (optional)
  - Jurisdiction State or Province Name (joiST): State or province name in accordance with ISO 3166-2. (optional)
  - Jurisdiction Country Name (joiC): Country code in accordance with ISO 3166-1. (mandatory)
- Valid from: Start of certificate validity.
- Valid to: End of certificate validity.
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Authority Key Identifier: 4952DF308692595F349C254824ABC0EBD106F2D6 (mandatory)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Key Usage (critical): digitalSignature (mandatory), keyEncipherment (mandatory)
- Extended Key Usage: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) (mandatory), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) (mandatory)

- Subject Alternative Name:
  - DNS: Must contain the subject CN and may contain additional DNS names (Wildcard entries are not allowed) (mandatory)
- Certificate Policies:
  - Policy OID: 2.23.140.1.1 (CABF EV) (mandatory)
  - Policy OID: 0.4.0.2042.1.4 (ETSI EN 319 411-1 EVCP) (mandatory)
  - Policy OID: 2.16.756.1.89.2.1.3 (SwissSign EVCP) (mandatory)
  - CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf (mandatory)
- OCSPmustStaple: ‘5’ (optional)
- CRL Distribution Point:
  - http://crl.swisssign.ch/cdp-9fdd910e-b9ff-4b2f-be38-2e93708c1b36 (mandatory)
- Authority Information Access:
  - caIssuer: http://aia.swisssign.ch/air-20350159-813d-4532-b988-8519eca57650 (mandatory)
  - ocsp: http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec (mandatory)
- SCT list: List of Signed Certificate Timestamps (SCT) (SCTs are provided by the CT-logs accessed)

7.1.1.3.2 TLS Organization Validated Certificates (OVCP) issued by SwissSign RSA TLS OV ICA 2022 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Name: CN=SwissSign RSA TLS OV ICA 2022 - 1,O=SwissSign AG,C=CH (Unique issuer distinguished name of the certificate)
- Subject DN: (Unique subject distinguished name of the certificate)
  - Common Name (CN): FQDN (mandatory)
  - OrganizationName (O): Subject organization name as stated in certificate application. (mandatory)
  - LocalityName (L): Name of the locality as described in the certificate application (mandatory if ST-attribute is missing, otherwise optional) (optional)
  - State-Or-Province (ST): State or province name or code as described in certificate application and in accordance with ISO 3166-2 (mandatory if L-attribute is missing, otherwise optional) (optional)
  - Country (C): Country code in accordance with ISO 3166-1 (mandatory)
- Valid from: Start of certificate validity.
- Valid to: End of certificate validity.
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Authority Key Identifier: 7C6F0A6F130FD98C246F2634F35C6B436DB723B6 (mandatory)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Key Usage (critical): digitalSignature (mandatory), keyEncipherment (mandatory)
- Extended Key Usage: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) (mandatory), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) (mandatory)
- Subject Alternative Name:
  - DNS: Must contain the subject CN and may contain additional DNS names (Wildcard entries are allowed) (mandatory)
- Certificate Policies:
  - Policy OID: 2.23.140.1.2.2 (CABF OV) (mandatory)
  - Policy OID: 0.4.0.2042.1.7 (ETSI EN 319 411-1 OVCP) (mandatory)
  - Policy OID: 2.16.756.1.89.2.1.2 (SwissSign OVCP) (mandatory)
  - CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf (mandatory)
- OCSPmustStaple: ‘5’ (optional)
- CRL Distribution Point:
  - http://crl.swisssign.ch/cdp-96b62f5a-6b73-4da4-87f7-ce4002c1cd34 (mandatory)
- Authority Information Access:
  - caIssuer: http://aia.swisssign.ch/air-0f2bf9a5-dd37-48c9-a85b-12acdcb8be45 (mandatory)

  - ocsp: http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec (mandatory)
- SCT list: List of Signed Certificate Timestamps (SCT) (SCTs are provided by the CT-logs accessed)

7.1.1.3.3 TLS Domain Validated Certificates (DVCP) issued by SwissSign RSA TLS DV ICA 2022 - 1

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Name: CN=SwissSign RSA TLS DV ICA 2022 - 1,O=SwissSign AG,C=CH (Unique issuer distinguished name of the certificate)
- Subject DN: (Unique subject distinguished name of the certificate)
  - Common Name (CN): FQDN (mandatory)
- Valid from: Start of certificate validity.
- Valid to: End of certificate validity.
- SubjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Authority Key Identifier: EBBD7F49938CC9EEECA2BAF71CD267F083B1EADE (mandatory)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC5280 chapter 4.2.1.2 (mandatory)
- Key Usage (critical): digitalSignature (mandatory), keyEncipherment (mandatory)
- Extended Key Usage: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth) (mandatory), 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth) (mandatory)
- Subject Alternative Name:
  - DNS: Must contain the subject CN and may contain additional DNS names (Wildcard entries are allowed) (mandatory)
- Certificate Policies:
  - Policy OID: 2.23.140.1.2.1 (CABF DV) (mandatory)
  - Policy OID: 0.4.0.2042.1.6 (ETSI EN 319 411-1 DVCP) (mandatory)
  - Policy OID: 2.16.756.1.89.2.1.1 (SwissSign DVCP) (mandatory)
  - CPSURI: https://repository.swisssign.com/SwissSign_CPS_TLS.pdf (mandatory)
- OCSPmustStaple: ‘5’ (optional)
- CRL Distribution Point:
  - http://crl.swisssign.ch/cdp-679723b2-8641-4642-8500-f6d2ff37e6ba (mandatory)
- Authority Information Access:
  - caIssuer: http://aia.swisssign.ch/air-1b863385-f4a9-47fa-88a5-2a5abfd4a167 (mandatory)
  - ocsp: http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec (mandatory)
- SCT list: List of Signed Certificate Timestamps (SCT) (SCTs are provided by the CT-logs accessed)

7.2 CRL profile

SwissSign issues CRLs in accordance to the guides of RFC 5280.

The CRL profile is applicable to the Root CA and its subordinated issuing CAs.

This list has the format “Field/Extension”: “Values” (Comment):

- Version Number: V2 (CRL format version pursuant to X.509.)
- Signature Algorithm: sha256WithRSAEncryption (Hash method and the signature algorithm used to sign the CRL pursuant to RFC 5280.)
- Issuer Distinguished Name: Unique issuer distinguished name of the certificate
- Effective Date: Date and time of CRL issuance.
- Next Update: Date and time of issuance of the next CRL. Maximum validity for CARL of the Root CA is 1 year after the publication of the CRL. The validity for CRLs provided by the Issuing CAs is 10 days. If it is the last CRL issued for those certificates in the scope of this CRL, the nextUpdate field in the CRL will be set to “99991231235959Z” as required by IETF RFC 5280.
- Revocation List Number: CRL sequence number

- Revoked Certificates: List of the serial numbers and revocation dates of the revoked Certificate.
- Serial Number: Serial number of the revoked certificate.
- Revocation Date: Date and time of revocation of the certificate.
- reasonCode: Reason code for certificate revocation. Optional for end-entity certificates (please note: reason code 0 for “unspecified” is not set). If present, the possible values are as follows:
  - keyCompromise (1)
  - affiliationChanged (3)
  - superseded (4)
  - cessationOfOperation (5) or
  - privilegeWithdrawn (9)
  - For CARL issued by the Root CA:
    * reasonCode extension is present and not marked critical
    * possible reason codes in CARL:
    * cACompromise (2), or
    * cessationOfOperation (5)
- Signature: Confirmation signature of the authority issued the CRL.
- Authority Key Identifier: The Authority key identifier of the Issuing CA

The ExpiredCertsOnCRL extension is not set as expired certificates are removed from the CRL.

7.2.1 Version number(s)

See section 7.2.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)

See section 7.3.3

7.3.2 OCSP extensions

No stipulation.

7.3.3 OCSP Response Profile

SwissSign OCSP v1 is built according to RFC 6960 [12].

This list has the format “Field/Extension”: “Values” (Comment):

- Response Status: 0 for successful or error code (Result of the query)
- Response Type: id-pkix-ocsp-basic (mandatory, Type of the response)
- Version: V1 (mandatory)
- Responder Id: DN (mandatory, Distinguished name of the OCSP responder)
- Produced At: Date (mandatory, Date when the OCSP response was signed)
- CertID: Unique ID for requested certificate (The CertID from the OCSP request is included in the response)
- Cert Status: Good, revoked, or unknown (mandatory, Indicates the response for certificate status)
- Revocation Time: (optional, Date of revocation of certificate, January 1, 1970 for non-issued certificates according to chapter 2.2 of RFC 6960)
- revocationReason: (Optional for end-entity certificates. If present, the possible values are as follows:)
  - unspecified (0)

  - keyCompromise (1)
  - affiliationChanged (3)
  - superseded (4)
  - cessationOfOperation (5) or
  - privilegeWithdrawn (9)
  - For CA certificates: Only present if issuing CA is revoked, The extension is set as described in BRG clause 7.2.2 and 7.3
- This Update: Date when the status was queried from database (mandatory)
- Next Update: The time at or before which newer information will be available about the status of the certificate. The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate.
  For Root and Issuing CA: The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate.
- Nonce: Value is copied from request if it is included. (optional)
- Extended Revoked Definition: Extended revoked extension according to chapter 2.2 and 4.4.8 of RFC 6960 (optional)
- SCT: SCTs for requested certificate (Optional, the Signed Certificate Timestamps (SCTs) for the requested certificate may be included in the response)
- Signature Algorithm: sha256WithRSAEncryption (mandatory)
- Certificate: Details of certificate used to sign the response (mandatory)

The OCSP extensions used are specified below:

- Nonce

The ArchiveCutOff extension is not set in the OCSP responses.

7.3.4 OCSP Responder Certificate

This list has the format “Field/Extension”: “Values” (Comment):

- Version: Version 3 (Certificate format version)
- Serial Number: Unique serial number of the certificate
- SignatureAlgorithm: sha256WithRSAEncryption
- Issuer Distinguished name: Unique issuer distinguished name of the certificate (Root CA for the Issuing CA and the Issuing CA for the end entity certificate)
- Subject Distinguished name: (Unique subject distinguished name of the OCSP Signer certificate.)
  - CommonName (CN): (The CN should include the string “OCSP” and the reference to the Issuer. The CN may contain an ID unique to the specific OCSP responder certificate.)
  - OrganizationName (O): SwissSign AG
  - Country (C): CH
- Valid from: Start of certificate validity
- Valid to: End of certificate validity
- subjectPublicKeyInfo: rsaEncryption (OID: 1.2.840.113549.1.1.1), RSA key (length 2048 bit or higher)
- Key Usage: digitalSignature (mandatory, critical)
- Subject Key Identifier: SHA-1 hash value of Public Key according to RFC 5280 chapter 4.2.1.2 (mandatory)
- Authority Key Identifier: SHA-1 hash value of Issuing CA’s Public Key according to RFC 5280 chapter 4.2.1.2 (mandatory)
- Extended Key Usage: id-kp-ocspSigning (mandatory)
- Certificate Policies: (Not included in this certificate)
- ocspNoCheck: NULL value (mandatory)
- CRL Distribution Points: (Not included in this certificate)
- Authority Information Access: (Not included in this certificate)

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The present combined CP/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 combined CP/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

The conformity of information system, policies and practices, facilities, personnel, and assets of SwissSign are assessed annually by a conformity assessment body in accordance to the corresponding legislation and standards or whenever a major change is made to the Trust Service operations.

More than one compliance audit per year is possible if this is requested by the audited party or is a result of unsatisfactory results of a previous audit.

Once a quarter, the TSP examines 3% of issued certificates for compliance with applicable standards and the quality of TSP services. The TSP examines at least 3% of issued EV certificates each year.

The TSP uses a Linting process to verify the technical accuracy of Certificates within the selected sample set independently of previous linting performed on the same Certificates.

8.2 Identity/qualifications of assessor

An independent qualified auditor will conduct the compliance audits according to the stipulations of corresponding law, CA Browser Forum, and applicable Root Store Policies. The scope of the audit and reporting will be fully in line with the rules set out before.

8.3 Assessor’s relationship to assessed entity

The independent and qualified auditors will conduct the compliance audits according to the stipulations of ETSI and the CA Browser Forum. The qualified auditors have the right to withdraw the certification of the TSP if a compliance audit reveals a severe deficiency in the operation of the TSP.

8.4 Topics covered by assessment

The auditor will assess the control objectives that are to be covered by the assessment in accordance with ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, TLS BR, and EV Guidelines, as well as Root Store Policies.

Internal audits are performed regularly and objective evidence as generated by the internal audit is covered by the annual assessment of the qualified auditor.

8.5 Actions taken as a result of deficiency

The TSP has implemented a ISO27001 System. The results of a compliance audit are handled within this framework. Depending on severity and urgency, all issues will be entered into the ISMS system either as incidents or as risks and tracked accordingly. Through the use of a supporting tool, the TSP ensures that all issues are being tracked and resolved in due course. Management reporting and escalation are part of the system.

8.6 Communication of results

The results of the compliance audit shall be communicated to SwissSign executive management in a timely manner.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The TSP provides a price list for certification and registration services on their website www.swisssign.com.

9.1.1 Certificate issuance or renewal fees

The TSP charges fees for issuing certificates according to the respective price list published on their website or made available upon request.

9.1.2 Certificate access fees

The TSP charges a fee according to their pricing policy.

9.1.3 Revocation or status information access fees

There is no charge for certificate revocation and the provision of certificate status information.

9.1.4 Fees for other services

The TSP reserves the right to charge an hourly rate or a fee, depending on the services rendered, additional to the fees mentioned above.

9.1.5 Refund policy

The TSP has established a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

With regard to the certificates issued pursuant to service-based Policies and Practice statements TSP has entered into a contract for an insurance policy for liability claims against the TSP. The amount of insurance coverage meets the requirements of Baseline Requirements and EV Guidelines.

The TSP has the necessary resources and the financial stability to properly operate the trust services.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

Upon request, the TSP will give advice about adequate insurances to cover potential risks.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Any information or data the TSP obtains in the course of business transactions is considered confidential, except for information defined in clause 9.3.2. This includes, but is not limited to business plans, sales information, trade secrets, organizational names, registration information, and Subscriber data. No breach of the duty of confidentiality shall be deemed to have taken place where confidential information has been disclosed within the TSP to its contracted third parties (see 9.3.3).

9.3.2 Information not within the scope of confidential information

Any information that is already publicly available or contained in certificates is not considered confidential, nor is any information considered confidential which the TSP is explicitly authorized to disclose (e.g. by written consent of involved party, by law or because it is part of the publicly available certificate information). In accordance with the RFC 5280 the information of the certificate status information (CRL and OCSP) is not considered as confidential data.

9.3.3 Responsibility to protect confidential information

The TSP is responsible to take all required measures to comply with the Swiss Data Protection Law or GDPR.

The TSP is responsible to take all required measures to comply with the applicable Data Protection Laws, in particular for authentication as a service. The TSP is processing only such identification data which are adequate, relevant and not excessive to grant access to that service.

9.4 Privacy of personal information

The TSP fully complies with, the Swiss Data Protection Law or GDPR to maintain the privacy of subject information. Information and data can be used where needed for professional handling of the services provided herein. Subscribers and other third parties have to comply with the privacy standards of the TSP.

9.4.1 Privacy plan

The stipulations of clause 9.3 and 9.4 apply.

SwissSign's privacy plan is available at https://www.swisssign.com/en/datenschutz.html.

9.4.2 Information treated as private

Any information about Subscribers and Requesters that is not already publicly available or contained in the certificates issued by this CA, the CRL, or the LDAP directory's content is considered private information.

In particular, data to be signed and the signed document provided during the signing service are considered personal data which are made available only to the signer and to the relying party which initially provided the data to be signed.

9.4.3 Information not deemed private

Any information already publicly available or contained in a certificate issued by this CA, or its CRL, or by a publicly available service shall not be considered confidential.

9.4.4 Responsibility to protect private information

Participants that receive private information secure it from compromise and refrain from using it or disclosing it to third parties. The data protection policy valid for SwissSign and its suppliers or other external parties is available at https://www.swisssign.com/en/datenschutz/datenschutzpolitik.html.

9.4.5 Notice and consent to use private information

The TSP will only use private information if a Subscriber has given full consent in the course of the registration process.

9.4.6 Disclosure pursuant to judicial or administrative process

The TSP will release or disclose private information on judicial or other authoritative order.

9.4.7 Other information disclosure circumstances

The TSP will solely disclose information protected by, the Swiss Data Protection Law or GDPR, with prior consent or on judicial or other authoritative order.

9.5 Intellectual property rights

All intellectual property rights of the TSP including all trademarks and all copyrights remain the sole property of SwissSign AG. Certain third party software is used by the TSP in accordance with applicable license provisions.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The TSP warrants full compliance with all provisions stated in this combined CP/CPS, service-based Policies and Practice statements, Swiss Digital Signature Law (as far as qualified and regulated certificates are concerned), CA/B Forum Requirements, Root Store Policies and related regulations and rules. In accordance with the relevant legislation and taking into consideration standards on accessibility such as ETSI EN 301 549, SwissSign does its best to make its services available to all potential service users, including people with disabilities as far as possible.

9.6.2 RA representations and warranties

All registration authorities must warrant full compliance with all provisions stated in this combined CP/CPS, related agreements, and related regulations and rules.

Any RA operating under this combined CP/CPS must adhere to the following rules:

- The RA must have a contractual agreement with the TSP which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities.
- The registration process must meet the stipulations of Swiss Digital Signature Law, the BR and EV Guidelines or eIDAS. It must be documented, published, and distributed to all parties involved in the RA process.
- RAs are only allowed to execute their registration process if the TSP has audited and approved the process as meeting the quality requirements of this combined CP/CPS and the service-based Policies and Practice statements and therefore being equivalent to the registration process of the SwissSign RA.
- The RA must pass an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit may lead to the revocation of RA privileges.
- The information collected during the RA process is subject to applicable data protection regulations. Compliance with these provisions must be demonstrated as described in clauses 9.3 and 9.4.

9.6.3 Subscriber representations and warranties

Subscribers warrant full compliance with all provisions stated in this combined CP/CPS, related agreements, CA/B Forum Requirements, Root Store Policies and related regulations and rules.

Subjects and Subscribers are responsible for:

- having a basic understanding of the proper use of public key cryptography and certificates,
- providing only correct information without errors, omissions or misrepresentations,
- substantiating information by providing a properly completed registration form as specified in chapter 3.2,
- supplementing such information with a proof of identity and the provision of the information as specified in chapter 3.1 and 3.2,
- using a secure, and cryptographically sound key pair on a crypto device provided or approved by the registration authority,
- maintaining the crypto device unmodified and in good working order, if applicable,
- verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information,

- reading and agreeing to all terms and conditions of this document, other relevant regulations and agreements,
- reading and agreeing to the general terms and conditions of the requested product,
- the maintenance of their certificates using the tools provided by the RA,
- using SwissSign certificates exclusively for lawful and authorized purposes,
- ensuring that SwissSign certificates are exclusively used on behalf of the person or the organization specified as the subject of the certificate,
- protecting the private key from unauthorized access,
- using the private key only in secure computing environments that have been provided by trustworthy sources and that are protected by state-of-the-art security measures,
- ensuring complete control over the private key by not sharing private keys and passwords and not using easily guessable passwords,
- ensuring complete control over the device containing the authentication means with the capability of generating activation data by not entrusting any person other than the certificate owner himself with the safekeeping of this device and data,
- notifying the registration authority of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate,
- revoking the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances makes the information in the certificate misleading or inaccurate,
- notifying the registration authority immediately of any suspected or actual compromise of the private key and requesting that the certificate be revoked,
- immediately ceasing to use the certificate upon (a) expiration or revocation of such a certificate, or (b) any suspected or actual damage/corruption or (c) any suspected or actual compromise of the private key corresponding to the public key in such a certificate, and immediately removing such a certificate from the devices and/or software onto which it has been installed,
- if the certificate or the corresponding issuing or root certificate has been revoked by the TSP, the TSP will inform the certificate holder who shall no longer use the certificate,
- refraining to use the Subscriber's private key that corresponds to the public key certificate to sign other certificates,
- using their own judgment about whether it is appropriate, given the level of security and trust provided by a certificate issued by this CA, to use such a certificate in any given circumstance,
- using the certificate with due diligence and reasonable judgment,
- complying with all laws and regulations applicable to a Subscriber's right to export, import, and/or use a certificate issued by this CA and/or related information. Subscribers 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.
- submitting applications in form of either paper or electronic documentation which shall include the declaration of consent with the applicable legal documents such as:
  - PKI Disclosure Statement
  - Subscriber Agreement
  - Terms and Conditions under which this CA is made available

9.6.4 Relying party representations and warranties

Relying Parties warrant full compliance with the provisions of this combined CP/CPS, service-based Policies and Practice statements, related agreements, Swiss Digital Signature Law, CA/B Forum Requirements, Root Store Policies and related regulations and rules.

9.6.5 Representations and warranties of other participants

Any other participant warrants full compliance with the provisions set forth in this combined CP/CPS, service-based Policies and Practice statements, related agreements, Swiss Digital Signature Law, CA/B Forum Requirements, Root Store Policies and related regulations and rules.

9.7 Disclaimers of warranties

Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, the TSP disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use.

9.8 Limitations of liability

9.8.1 Liability of the TSP

The TSP is only liable for damages which are the result of SwissSign's failure to comply with this combined CP/CPS and which were provoked deliberately or through gross negligence.

The TSP shall not in any event be liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law. SwissSign AG shall not be liable for any damages resulting from infringements by the Certificate Holder or the Relying Party on the applicable terms and conditions including the exceeding of the transaction limit.

The TSP shall not in any event be liable for damages that result from force majeure events. SwissSign AG shall take commercially reasonable measures to mitigate the effects of force majeure in due time. Any damages resulting of any delay caused by force majeure will not be covered by the TSP.

9.8.2 Liability of the Certificate Holder

The subscriber and subject are liable to the TSP and the Relying Parties for any damages resulting from misuse, willful misconduct, failure to meet regulatory obligations, or noncompliance with other provisions for using the certificate.

The subscriber confirms to SwissSign until revocation that his organization wishes to continue to obtain and issue certificates from SwissSign.

The Subscriber and subject of a qualified or regulated signature or seal certificate is also liable according to Article 59a OR (Swiss Code of Obligations).

9.9 Indemnities

Indemnities are already defined in the provisions stated in this combined CP/CPS and other related documents.

9.10 Term and termination

9.10.1 Term

This combined CP/CPS and respective amendments become effective as they are published on the SwissSign website at https://repository.swisssign.com and will supersede all prior versions of this combined CP/CPS, service-based Policies and Practice statements and respective amendments.

9.10.2 Termination

This combined CP/CPS will cease to have effect when a new version is published on the SwissSign website.

9.10.3 Effect of termination and survival

All provisions regarding confidentiality of personal and other data will continue to apply without restriction after termination. Also, the termination shall not affect any rights of action or remedy that may have accrued to any of the parties up to and including the date of termination.

9.11 Individual notices and communications with participants

The TSP has established procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided or the personal data maintained therein within 24 hours of the breach being identified.

Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP also in particular notifies such person without undue delay.

The TSP can provide notices by email, postal mail, voice message or on web pages unless specified otherwise in this combined CP/CPS.

9.12 Amendments

9.12.1 Procedure for amendment

The TSP will implement changes with little or no impact for Subscribers and Relying Parties to this combined CP/CPS upon the approval of the executive board of the TSP.

Changes with material impact will be first submitted to the Audit Body to obtain the required approval, if applicable.

9.12.2 Notification mechanism and period

The TSP executive board can decide to amend this combined CP/CPS and respective amendments without notification for amendments that are non-material (with little or no impact).

The TSP executive board, at its sole discretion, decides whether amendments have any impact on the Subscriber and/or Relying Parties.

All changes to the combined CP/CPS will be published after approval as described in chapter 2.

9.12.3 Circumstances under which OID must be changed

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

In case the scope of a certificate profile changes, the OID will be changed.

9.13 Dispute resolution provisions

Complaints regarding compliance with or implementation set forth in this combined CP/CPS must be submitted in writing to the TSP in the contact details described in clause 1.5.2. In case of any dispute or controversy in connection with the performance, execution or interpretation of this agreement that cannot be resolved within a period of four weeks after submission of the complaint, the parties are free to file action with the courts pursuant to clause 9.14.

Complaints regarding the content or format of a certificate must be submitted in writing or over the contact form on the SwissSign home page. According to the requirements of the CA/Browser Forum, SwissSign will react to a notification of a failure or mis-issuance of a certificate within 24 hours.

9.14 Governing law

The laws of Switzerland shall govern the validity, interpretation and enforcement of this contract, without regard to its conflicts of law. The application of the United Nations Convention on Contracts for International Sale of Goods shall be excluded.

Exclusive place of jurisdiction shall be the commercial court of Zurich (Handelsgericht Zürich), Switzerland.

9.15 Compliance with applicable law

This combined CP/CPS and rights or obligations related hereto are in accordance with the relevant provisions of the Swiss Digital Signature Law, CA/B Forum Requirements, eIDAS, SVG and SVV (for its eIDAS trust services), Root Store Policies and of the other applicable standards. Compliance with the laws and regulations are verified within the annual external audit. The audits are carried out by an independent qualified auditor.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The following documents and the Subscriber-Agreement of the TSP state the agreement between the TSP and the Certificate Holder (Subject) as well as Subscriber, if applicable:

- This combined CP/CPS,
- the registration form, including the application documentation as required for the type of certificate,
- the Subscriber Agreement and Terms and Conditions, valid at the time of the application or the applicable effective version thereof.

9.16.2 Assignment

The Certificate Holder and/or Subscriber is not permitted to assign this agreement or its rights or obligations arising hereunder, in whole or in part.

The TSP can fully or partially assign this agreement and/or its rights or obligations hereunder.

9.16.3 Severability

In the case of a conflict between the SMIME BR, TLS BR or EV Guidelines, and the applicable law or national regulation (herein after law) of any jurisdiction in which the TSP operates or issues certificates, the TSP will modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal according to national regulation.

This applies only to operations or certificate issuances that are subject to that law. In such an event the TSP will immediately and prior to the issuing of such certificates under the modified requirements include a detailed reference to the law requiring the modification. The specific modification to the Requirements implemented by the TSP will be described in this clause of the combined CP/CPS and Practice Statements.

Also in case of public trusted certificates, the TSP will prior to issuing a certificate under the modified requirement notify the CA/Browser Forum by sending a message to public@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/about/email-lists/.

When the law no longer applies, or the requirements are modified the TSP will modify these requirements to make it possible to comply with all applicable requirements.

The TSP will communicate an appropriate change within 90 days.

Invalidity or non-enforceability of one or more provisions of this agreement and its related documents shall not affect any other provision of this agreement, provided that only non-material provisions are severed.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

The TSP shall not be in default and the customer cannot hold the TSP responsible and/or liable for any damages that result from (but are not limited to) the following type of events: any delay, breach of warranty, or cessation in performance

caused by any natural disaster, power or telecommunication outage, fire, unpreventable third-party interactions such as virus or hacker attacks, governmental actions, or labor strikes.

The TSP takes commercially reasonable measures to mitigate the effects of force majeure in due time.

9.17 Other provisions

9.17.1 Language

If this combined CP/CPS is provided in additional languages to English, the English version will prevail.

9.17.2 Delegated or outsourced Services

The TSP has a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements. All services offered have to comply with the regulations stipulated in this combined CP/CPS. The TSP may require compliance with applicable policies to be verified by an approved auditor.

10. References

[1] TLS BR: current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates https://cabforum.org/working-groups/server/baseline-requirements/requirements/;

[2] EVCG: current version of the Guidelines for the Issuance and Management of Extended Validation Certificates" https://cabforum.org/working-groups/server/extended-validation/guidelines/;

[3] ETSI EN 119 312 V1.5.1 (2024-12) Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites;

[4] 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;

[5] ETSI EN 319 411-2 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[6] ETSI EN 319 401 V3.1.1 (2024-06) Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

[7] NIST: SP 800-89 https://csrc.nist.gov/pubs/sp/800/89/final

[8] RFC 3647 – https://www.rfc-editor.org/rfc/rfc3647;

[9] RFC 5280 - https://www.rfc-editor.org/rfc/rfc5280

[10] RFC 6962 – Certificate Transparency;

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

[12] RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP