SwissSign CPS Signing Services

Certification Practice Statement for Signing certificates

Document Type:	Certification Practice Statement
OID:	n/a
Author:	Information Security and Compliance
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	14 July 2021
Version:	1.0
Obsoletes:	n/a
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Disclaimer: The electronic version of this document and all its stipulations are considered binding if saved in Adobe PDF Format and signed by two legal representatives of SwissSign. All other copies and media are null and void.

Version Control

Date	Version	Comment	Author
14.07.2021	1.0	Initial CPS	Michael Guenther

Authorization

Date	Approved by	Approved by	Version
08.07.2021	Michael Günther	Markus Naef	1.0

Michael Günther (Qualified Signature)

Digital unterschrieben von Michael Günther (Qualified Signature)
Datum: 2021.07.08 10:20:53 +02'00'

digital signature

Markus Naef (Qualified Signature)

Digital unterschrieben von Markus Naef (Qualified Signature)
Datum: 2021.07.08 14:24:13 +02'00'

digital signature

Table of Contents

1. Introduction

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

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

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

The structure of this document corresponds to RFC3647 and is divided into nine parts. To preserve the outline specified by RFC 3647, section headings that do not apply or are not supported by the TSP have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them. Each top-level chapter includes references to the relevant sections the TSPS [3], if the chapter refer to general practices of the TSP independent from the trust service.

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

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

1.1 Overview

This CPS respectively the TSPS [3] describes the practices implemented by SiwssSign AG to comply with for the relevant services as well as the terms and conditions under which this is CA is made available:

- “SwissSign CP QCP-n-qscd RSS – Certificate Policy for Qualified Signature certificates for RSS” [1]

For the issuance of certificates within of this scope, SwissSign fully complies with the rules and regulations of the ZertES/VZertES as well as further applicable specifications:

- ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)
- VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)
- TAV-BAKOM: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
- ETSI EN 319 401 (2018): General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-1 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 (2018):Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 (2016): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

- DIN EN 419 241-1 (2018): Vertrauenswürdige Systeme, die Serversignaturen unterstützen – Teil 1: Allgemeine Sicherheitsanforderungen (CEN EN 419 241-1, 2018: Trustworthy Systems Supporting Server Signing, Part 1: General System Security Requirements)
- ETSI TS 119 312 (2019): Cryptographic Suites
- IETF RFC 6960 (2013): Online Certificate Status Protocol - OCSP
- IETF RFC 3647 (2003): Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- IETF RFC 5280 (2008): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

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

- QCP-n-qscd RSS (qualified certificates for qualified signatures, RA is SwissSign)

The relevenat Issuing CA for these certificates under this CPS are marked in green in the PKI overview of SwissSign:

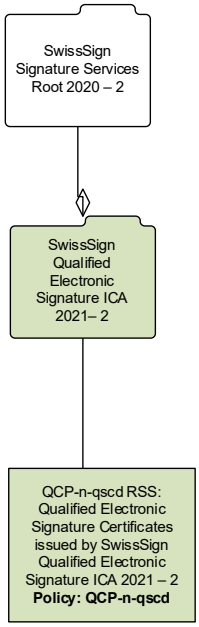

Figure 1: SwissSign Signature Services Root 2020 – 2

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

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

In this CPS, “this CA” refers to both Root CA “SwissSign Signature Services Root 2020 – 2” and all it subordinated issuing CA for qualified and non-qualified signing certificates as shown in Figure 1 above, unless stated differently.

1.2 Document name and identification

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

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

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

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

1.3 PKI Participants

1.3.1 Certification Authorities

The TSP operates a Public Key Infrastructure, consisting of both Root CA “SwissSign Signature Services Root 2020 – 2” and its subordinated issuing CAs as shown in Figure 1 and 2. The issuing CAs shown in the overview are the only public CAs operated by the TSP that issue S/MIME certificates under this CPS.

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

1.3.2 Registration Authorities

(QCP-n-qscd RSS) The TSP operates a Registration Authority, called “SwissSign RA” that registers Subscribers of certificates issued by this CA for these policies.

1.3.3 Subscribers

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

Please refer to clause 9.6.3 of the TSPS [3] for Subject’s and Subscriber’s responsibilities.

(QCP-n-qscd RSS) For these policies, the Subject is a natural person.

1.3.4 Relying Parties

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

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

Relying Parties can also be Subscribers within this CA.

1.3.5 Other participants

Not applicable

1.4 Certificate usage

The certificate usage in relation of the key usage as well extended key usage are defined within the CPR [2].

1.5 Policy administration

1.5.1 Organization administering the document

The CPS is written and updated by SwissSign AG.

SwissSign AG

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

1.5.2 Contact persons

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 determines the suitability of this CPS document.

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

1.5.4 CPS approval procedures

This CPS document and its related documentation are reviewed by Information Security & Compliance and approved by the CEO of SwissSign AG.

Following the approval by the CEO of SwissSign AG, the CPS and its relevant documentation are published as stated in clause 2 and communicated to employees of SwissSign and external parties as relevant.

1.6 Definitions and acronyms

Refer to clause 1.6 of the TSPS [3].

2. Publication and Repository Responsibilities

Refer to clause 2 of SwissSign TSPS [3].

2.1 Repositories

Refer to clause 2.1 of SwissSign TSPS [3].

2.2 Publication of certification information

Refer to clause 2.2 of SwissSign TSPS [3].

2.3 Time or frequency of publication

Refer to clause 2.2 of SwissSign TSPS [3].

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.

2.4 Access controls on repositories

Refer to clause 2.4 of SwissSign TSPS [3].

2.5 Additional testing

No stipulation

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

Type of names assigned to the Subscriber is described in the Certificate Profile [2].

(QCP-n-qscd RSS) The common name contains the given name and the surname of the Subject or pseudonym.

Real names are specified as /CN='given name(s)' 'surname'. Given name(s) and surname in the CN have to be identical to the names as they appear in the identifying documentation provided. In case the subject has more than one given name, he is free to choose one or several of his given names in any sequence. Given names joined with a hyphen are considered as one single given name. Characters are encoded according to chapter 3.1.4. Abbreviations or nicknames without substantiating identifying documentation are prohibited. Names consisting of multiple words are permissible.

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

The use of academic and/or job titles are not allowed in any part of the subject information.

Furhtermore:

- The use of a real name and its identifying information must be authenticated and authorized according to chapter 3.2.3.
- A pseudonym requires that the subject authenticates and authorizes the request containing identifying information according to chapter 3.2.3.
- The use of organizational name, where applicable must be authorized according to chapter 3.2.2.
- All attributes in the DN and SAN, if applicable, must be validated and authorized.

3.1.2 Need for names to be meaningful

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

Meaning of names in different fields of the Certificates is described in the Certificate Profile [2].

3.1.3 Anonymity or pseudonymity of Subscribers

(QCP-n-qscd RSS): Pseudonyms are specified as /CN='identifier': 'arbitrary string'. Pseudonyms are specified as /CN='pseudo': 'pseudonym'. An example of a correctly formulated pseudonym is: "/CN=pseudo: John Doe". Other registration authorities may use other identifiers.

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

- Identifier is a string that clearly indicates the nature of the CN,
- The identifier and the resulting /CN= values are neither incorrect nor misleading,
- The identifier and the remainder of the /CN= attribute must be separated with a <colon> <space> sequence.

A Subscriber can use any string of characters as a pseudonym. Proof of eligibility to use the pseudonym, e.g. an excerpt from the national trademark registry, is required when requesting certificates with pseudonyms.

The TSP and its RAs reserve the right to reject certificate requests or revoke certificates containing offensive or misleading information or names protected by legislation and infringing rights of others. However, the TSP and its RAs are not obliged to verify lawful use of

such names. The TSP and its RAs reserve the right to decline any request for anonymity or pseudonymity. Anonymous or pseudonymous common names are available on a “first come, first served” basis. Chapter 3.1.6 applies.

3.1.4 Rules for interpreting various name forms

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

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

- In general, national characters are represented by their ASCII equivalent, e.g. é, è, à, ç are represented by e, e, a, c.
- The German “Umlaut” characters ä, ö, ü are represented by either ae, oe, ue or a, o, u.

3.1.5 Uniqueness of names

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

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

Depending on the certificates issue the uniqueness of the Distinguished Name is achieved through different unique identifiers as defined in the CPR [2].

3.1.6 Recognition, authentication, and role of trademarks

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

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

3.1.7 Test Certificates

The TSP issues certificates for the purpose of tests. The purpose of these certificates is limited to tests needed for system integration and system releases. The CN of the certificate is prefixed with the string “TEST”.

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.

3.2.1 Method to prove possession of private key

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

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

3.2.2 Authentication of organization identity

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

- To validate the name and location of the organization, the Subscriber must provide official documentation about the organization provided by a government agency in the jurisdiction of the organization's legal creation, existence, or recognition or by any other official source that is considered a reliable data source.
- Organizations with an entry in the federal or a nationally recognized commercial register must supply verifiably current excerpt. All other organizations must supply either the certificate of registration with the FTA or a current VAT invoice.
- Government entities must supply official documentation to prove the existence and the correct spelling of the 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.

(QCP-n-qscd RSS) This CA does not support use of organization names.

3.2.3 Authentication of individual identity

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

The registration process of any registration authority operating under this CPS contain provisions to determine the identity of such individuals.

(QCP-n-qscd RSS)The regulations defined in the registration forms are summarized as follows:

- The registration form must carry original, personal handwritten signatures or it must be supplied electronically and digitally signed using a qualified certificate .
- The information on the identifying document must match the name on the registration form. In case the registration form carries the original, personal handwritten signature, this signature and the signature on the identifying document must also match.
- The wording in the request has to be identical to the given name(s) and the family name of the identifying documents (see 3.1.1).

The identification is performed by physical presence as follows:

- The Subject must be present in person or in an equivalent procedure according to ETSI EN 319 411-1/2, clause 6.2.2 and ZertES Art. 9. This step may be conducted by:
    - the registration authority processing the certificate request,
    - a trained and contracted partner for the identification service.
- The individual must present a valid original of an official identification document as recognized by national law. The identifying agent is to make a high-quality copy, scan or photograph of the identifying document and to confirm proper execution of the identification in writing or electronically as agreed with the TSP.
- The photo in the identifying document is compared and has to match (facial features, age and size) the person present as described above.

3.2.4 Non-verified Subscriber information

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

3.2.5 Validation of authority

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

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

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

These individuals must be identified according to the stipulations given in chapter 3.2.3.

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

(QCP-n-qscd RSS) Individuals must be identified according to the stipulations given in chapter 3.2.3.

3.2.6 Criteria for interoperation

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-keying requests for qualified certificates require the re-keying request to be digitally signed with the qualified certificate that is to be re-keyed.

For other re-keying requests, the requester is identified according to the stipulations for initial identity validation and authentication.

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:

- Through the revocation dialog after successful login to the SwissID profile.
- Providing proof of the possession of the authenticators to access the SwissID profile
- With a personal handwritten signature or a recognized qualified electronic signature according to the ZertES regulation on a revocation form.

- Appearance in person at the registration authority,
- Providing a one-time revocation key on the web site of the registration authority.

Not all methods are supported for all types of certificates.

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

4. Certificate Life-Cycle Operational Requirements

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

4.1 Certificate application

4.1.1 Who can submit a certificate application

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

4.1.2 Enrollment process and responsibilities

The RA collects and verifies the following during its enrollment process according to the ETSI EN 319 411-1 and ETSI EN 319 411-2 as well as ZertES:

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

(QCP-n-qscd RSS) The RA collects references to the following during its enrollment process to ensure sole control of the subscriber over the subscriber key pair:

- Authentication means provided by the TSP or provided by the subscriber for accessing the user profile (SwissID).
- Authentication means created by the TSP on a device provided by the subscriber for signature activation (SIC).

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

- Valid identification documentation is provided and complete registration forms have been signed, and the CPS and End-User Agreement have been accepted by the Subscriber,
- Registration forms can also be signed electronically with a qualified electronic signature in accordance with the Swiss Digital Law (ZertES). 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 RA.

(QCP-n-qscd RSS) On top, for this policy the following steps are successfully performed before the certificate is issued:

- SwissID authentication means are linked to the user profile,
- A Subscriber key pair is generated by the TSP,
- SIC authentication means are linked to the subscriber key pair.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

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.
- (QCP-n-qscd RSS) the Subject/Subscriber has proven control over the SwissID and SIC authentication means.

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

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

4.2.3 Time to process certificate applications

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

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

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

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

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

4.3.2 Notification to Subscriber by the CA of issuance of certificate

The CA may notify the Subscriber in different ways:

- If the certificate is presented to the Subscriber immediately, special notification may not be necessary.

The CA uses one of the following methods:

- email the certificate to the Subscriber,
- electronically provide the certificate to the Subscriber within its self service portal or Remote Signing Service interface,
- email information permitting the Subscriber to download the certificate from a web site or repository,
- email information permitting the RA 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.

The registration authority ensures that certificates are only issued when the Subscriber attempts to download and install the certificate for the first time. This step is considered sufficient, and no further confirmation is required.

4.4.2 Publication of the certificate by the CA

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

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.4.4 Certificate Transparency

Not applicable under this CPS.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The use of certificates by Subscribers must adhere to the obligations stipulated in chapter 9.6.3 of the TSPS [3], summarized as follows:

- Certificates issued under this CPS may only be used in accordance with the key usage declaration contained in the certificate.
- Subscribers may only use SwissSign certificates for intended, legal, and authorized purposes.
- Subscribers may only use a SwissSign certificate on behalf of the person or the organization listed as the Subject of such a certificate.
- Subscribers must read and agree to the General Terms and Conditions and the applicable End-User Agreement,
- (QCP-n-qscd RSS) Qualified certificates can be used for qualified electronic signatures.

4.5.2 Relying Party public key and certificate usage

Relying Parties shall:

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

4.6 Certificate renewal

Certificate renewal is not supported by the TSP. If the subscriber is known to the TSP, a new certificate will be issued following the practices defined for re-key.

4.7 Certificate re-key

Certificate re-keying is a process in which a new certificate is issued to a Subscriber based on an existing valid certificate and a new key pair, if proof of key possession of the existing valid certificate can be provided. The new certificate contains new validity and key information, but retains subject information of the existing valid certificate.

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.

If one of the conditions are not fulfilled, the initial certificate application and issuance is followed.

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.

(QCP-n-qscd RSS) To-re-key a qualified certificate, the subject has to sign digitally sign the re-key request with the valid qualified certificate issued previously.

4.7.3 Processing certificate re-keying requests

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

The process of the application for re-key request will be conducted as follows:

- The identification of the requester will be performed with the verification of the digital signature on the request form.

- Validation results from previous requests are considered valid if the validated information has not changed.

If any data has changed, the re-key application is treated as an initial certificate application. The applicable legal documents (Terms and Conditions, CPS) are communicated to and agreed by the subscriber during the re-key process.

4.7.4 Notification of new certificate issuance to Subscriber

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

4.7.5 Conduct constituting acceptance of a re-keyed certificate

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

4.7.6 Publication of the re-keyed certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

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

4.8 Certificate modification

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

4.9 Certificate revocation and suspension

The procedures of the TSP meet the requirements of ETSI EN 319 411-1/2. 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.

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

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

4.9.1 Circumstances for revocation

Subscribers may revoke their certificates at will.

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

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

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

- The certificate issued does not comply with the terms and conditions of this CPS.
- The CA obtains evidence that the Certificate was misused
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use and/or other applicable laws, rules and regulations. In addition, The TSP may investigate any such incidents and take legal action if required.
- The CA is made aware of 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. name change due to change in marital status or omission of domain registration renewal).
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement
- The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository
- Revocation is required by this CPS
- The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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

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

4.9.2 Who can request revocation

This CA accepts certificate revocation requests from the following sources:

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

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

4.9.3 Procedures for revocation request

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

- The Subscriber can personally visit the RA offices and request the revocation of a certificate off line. The Subscriber must present either a valid passport or Swiss identity card.
- 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 with a qualified electronic signature in accordance with the Swiss Digital Law (ZertES). In this case RAO check, validates and keeps all necessary records regarding the qualified electronic signature.

4.9.3.1 Notification about revocation

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

4.9.4 Revocation request grace period

The Subscriber is required to request a revocation request immediately if one of reasons listed in the subscriber agreement occur. Please see clause 9.6.3 of the TSPS [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, this will be noted accordingly and the certificate concerned will be revoked at the time required.

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

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

4.9.6 Revocation checking requirement for Relying Parties

Relying Parties must, when working with certificates issued by 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	Not applicable
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

All issuing CAs support the OCSP protocol for online revocation checking. The OCSP responder URL is stored in every certificate issued by one of the subordinated issuing CAs (field “Authority Information Access”). The OCSP response is signed by a dedicated OSCP Responder, whose certificate is signed by the CA which issued the certificate whose revocation status is being checked.

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.

4.9.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.9.12 Special requirements regarding key compromise

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

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

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

4.9.13 Circumstances for suspension

The TSP does not provide suspension.

4.9.14 Who can request suspension

The TSP does not provide suspension.

4.9.15 Procedure for suspension request

The TSP does not provide suspension.

4.9.16 Limits on suspension period

The TSP does not provide suspension.

4.10 Certificate status services

The TSP provides CRL and OCSP status service. Access to these services is provided through the web site “swisssign.net” and the online LDAP directory “directory.swisssign.net”. The certificate status services provide information on the status of certificates for at least 11 years after the certificate has expired or was revoked. The integrity and authenticity of the online status information (OCSP) is protected by a digital signature of the dedicated OCSP responder certificate which is signed from the appropriate issuing CA. The CRL is directly signed by the appropriate issuing CA. Integrity and authenticity of the revocation information is guaranteed by a signature of the CRL or the OCSP response.

Before revoking an Issuing CA certificate, the TSP makes sure that all leaf-certificates in the scope of the CRL are either expired or revoked. Afterwards, a last CRL will be issued and will be available for download at least 11 years after the expiry date of the last leaf-certificate in scope, not only until the end of the Issuing CA validity.

4.10.1 Operational characteristics

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. CRL 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 an URL in the certificates.

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

This CA does not support session key escrow and key recovery.

4.12.2 Session key encapsulation and recovery policy and practices

This CA does not support session key encapsulation.

5. Facility, Management, and Operations Controls

5.1 Physical controls

Refer to clause 5.1 of SwissSign TSPS [3].

5.2 Procedural controls

Refer to clause 5.2 of SwissSign TSPS [3].

5.3 Personnel controls

Refer to clause 5.3 of SwissSign TSPS [3].

5.4 Audit logging procedures

Refer to clause 5.4 of SwissSign TSPS [3].

5.5 Records archival

Refer to clause 5.5 of SwissSign TSPS [3].

5.6 Key changeover

Refer to clause 5.6 of SwissSign TSPS [3].

5.7 Compromise and disaster recovery

Refer to clause 5.7 of SwissSign TSPS [3].

5.8 CA or RA termination

Refer to clause 5.8 of SwissSign TSPS [3].

6. Technical Security Controls

Refer to clause 6 of SwissSign TSPS [3].

6.1 Key pair generation and installation

Refer to clause 6.1 of SwissSign TSPS [3].

6.1.1 Key pair generation

For Root and Issuing CA, refer to clause 6.1.1 of SwissSign TSPS [3].

The Subscriber key pairs are generated by the TSP.

The TSP generates the subject keys a key length and a public key algorithm as specified in ETSI TS 119 312 are used. The Subject Keys generated by TSP are generated and stored securely while held by the TSP as follows:

(QCP-n-qscd RSS) Subscriber keys are generated at time of registration by the TSP on a QSCD in the secure environment of the TSP. In all cases the requirements of ZertES, EN 319 411-2, CEN EN 419241-1 and TS 119 431-1 are met.

6.1.2 Private key delivery to Subscriber

The delivery of private keys generated by the TSP is implemented as follows:

(QCP-n-qscd RSS) Subscriber keys are not delivered to the Subscriber and are managed on behalf of the Subscriber by the TSP as these services are remote signing services. Subscriber private keys are only used by the TSP for signing the certificate signing request required for issuing the subscriber certificate. Immediately after certificate issuance, the public key of the SIC authentication means is registered within the SAM, whereby control over the private key is transfered to the SIC authentication means described in 4.1.2. SIC authentication means use a 256 bit ECDSA key (NIST P-256 curve, OID 1.2.840.10045.3.1.7).

6.1.3 Public key delivery to certificate issuer

As the keys are generated and maintained by the TSP on behalf of the Subscriber, no public key delivery method is required. The TSP issues also the corresponding certificate.

6.1.4 CA public key delivery to Relying Parties

Refer to clause 6.1.4 of SwissSign TSPS [3].

Signatures created with the qualified certificate contain the Subscriber’s certificate.

6.1.5 Key sizes

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

ETSI: ETSI TS 119 312 http://www.etsi.org/standards-search

NIST: SP 800-57

The Root CA uses a 4096 bit RSA key.

The Issuing CAs use a 4096 bit RSA key.

(QCP-n-qscd RSS) All issuing CAs allow Subscribers to use RSA keys with a size of at least 3072 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

Key pairs are generated by TSP only on approved secure crypto devices and parameters have been specified to meet all certification and security requirements.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

Root CA keys	Refer to clause 6.2.1 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.1 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber key	(QCP-n-qscd RSS) Subscriber keys for qualified certificates are generated and stored on an HSM that meets at least FIPS 140-2 level 3 or Common Criteria EAL4+ requirements. The TSP has implemented organizational monitoring procedures to ensure that the device is certified during the whole certificate life cycle aswell as to ensure that it fulfills the requirements of ZertES/TAV.

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

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

Root CA keys	Refer to clause 6.2.2 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.2 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	The registration process ensures that the Subscriber is the only person with access to the device containing the activation keys for activating the subscriber keys. The signer may give consent to signature activation by authenticating with the SIC authentication means described in chapter 4.1.2.

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

Root CA keys	Refer to clause 6.2.3 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.3 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber key escrow is not allowed.

6.2.4 Private key backup

The following list shows how private key backup is implemented:

Root CA keys	Refer to clause 6.2.4 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.4 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber keys are managed by the TSP within certified SSCD (HSM) and are not in any backup.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

Root CA keys	Refer to clause 6.2.5 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.5 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber keys are managed by the TSP within certified SSCD (HSM) and are not archived.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Root CA keys	Refer to clause 6.2.6 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.6 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber keys are generated and managed by the TSP within certified SSCD (HSM) and are not transferred.

6.2.7 Private key storage on cryptographic module

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

Root CA keys	Refer to clause 6.2.7 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.7 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber keys are stored within certified QSCD (HSM) and can be used only if properly activated.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

Root CA keys	Refer to clause 6.2.8 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.8 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber keys are activated with the SIC authentication means described in chapter 4.1.2. Details regarding the activation data are described in chapter 6.4.1 and 6.4.2.

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

Root CA keys	Refer to clause 6.2.9 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.9 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Subscriber keys	Subscriber keys are activated for single use only under and are automatically deactivated by the SAM after every use.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

Root CA keys	Refer to clause 6.2.10 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.
Issuing CA keys	Refer to clause 6.2.10 of SwissSign TSPS SwissSign TSPS - Trust Services Practice Statement.

Subscriber keys	Private key are managed by the TSP within secure QCSD and cannot be extracted decrypted. Subscriber keys are destroyed through the key management functionality of the HSM when the associated certificate is revoked or after the associated certificate has expired.

If a HSM that was used within the TSP is no longer in use or has been replaced, the HSM is physically destroyed.

6.2.11 Cryptographic Module Rating

Refer to clause 6.2.11 of SwissSign TSPS [3].

6.3 Other aspects of key pair management

6.3.1 Public key archival

Refer to clause 6.3.1 of SwissSign TSPS [3].

6.3.2 Certificate operational periods and key pair usage periods

Refer to clause 6.3.2 of SwissSign TSPS [3].

End user certificates can have according to PKI “best practices” a lifetime of up to 2 years and up to the maximum remaining lifetime of the issuing CA certificate minus 10 days.

6.4 Activation data

6.4.1 Activation data generation and installation

Refer to clause 6.4.1 of SwissSign TSPS [3].

Activation data used to protect private keys inside QSCD is generated in accordance with the requirements of this CPS. It must:

- be generated by and known to the Subscriber only
- have at least six characters
- not be easily guessable

(QCP-n-qscd-RSS)	The activation data is generated per signature with the SIC authentication means. The SIC authentication means consist of a key pair generated on a SwissSign-approved mobile device with a TEE provided by the Subscriber during registration as described in chapters 3.2.1 and 4.1.2. The activation data is verified by the SAM with the public key linked to the signing key pair during registration.

6.4.2 Activation data protection

Root CA keys	Refer to clause 6.4.2 of SwissSign TSPS [3].
Issuing CA keys	Refer to clause 6.4.2 of SwissSign TSPS [3].
Subscriber keys	Subscribers are obliged to keep the activation data secret at all times.
(QCP-n-qscd-RSS)	The device containing the SIC authentication means must be protected with a PIN or password of at least six characters which must not be easily guessable. Biometric protection may be used. Subscribers are obliged to keep the SIC authentication means for generating activation data secret at all times. The activation data is created with the SIC authentication means with a nonce and reference to the data to

be signed provided by the SAM. The SAD are verified by the SAM within the tamper proof environment of the SSCD containing the subscriber keypair.

6.4.3 Other aspects of activation data

Refer to clause 6.4.3 of SwissSign TSPS [3].

(QCP-n-qscd-RSS) The SAM is used in a tamper proof environment provided by the HSM containing the subscriber key pair. The HSM fulfills the requirements stated in CEN EN 419241-1.

Mobile devices which SwissSign allows to use the service have to fulfill the following requirements:

- Device is not rooted
- Device PIN set
- Secure Element with TEE present
- Apple devices:
  - iPhone 5S or newer
  - iOS 11 or newer
- Android devices:
  - Android 7 or newer
  - Fingerprint reader present

Subscribers agree to set a device PIN or passcode with at least 6 characters.

6.5 Computer security controls

Refer to clause 6.5 of SwissSign TSPS [3].

6.5.1 Specific computer security technical requirements

Refer to clause 6.5.1 of SwissSign TSPS [3].

6.5.2 Computer security rating

Refer to clause 6.5.2 of SwissSign TSPS [3].

6.6 Life cycle technical controls

6.6.1 System development controls

Refer to clause 6.6.1 of SwissSign TSPS [3].

6.6.2 Security management controls

Refer to clause 6.6.2 of SwissSign TSPS [3].

6.6.3 Life cycle security controls

Refer to clause 6.6.3 of SwissSign TSPS [3].

6.7 Network security controls

Refer to clause 6.7 of SwissSign TSPS [3].

6.8 Time-stamping

Refer to clause 6.8 of SwissSign TSPS [3].

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

The Certificate profile is described in the Certificate Profile [2].

7.2 CRL profile

The CRL profile is described in the Certificate Profile [2].

7.3 OCSP profile

The OCSP profile is described in the Certificate Profile [2].

8. Compliance Audit and Other Assessments

The present CPS fulfills the requirements for certificates and services according to ZertES and EN 319 401, EN 319 411-1/2. The terms and conditions of this CPS, Swiss Digital Signature Law and all dependent rules and regulations are used to conduct compliance audits for:

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

8.1 Frequency or circumstances of assessment

Refer to clause 8.1 of SwissSign TSPS [3].

8.2 Identity/qualifications of assessor

Refer to clause 8.2 of SwissSign TSPS [3].

8.3 Assessor's relationship to assessed entity

Refer to clause 8.3 of SwissSign TSPS [3].

8.4 Topics covered by assessment

Refer to clause 8.4 of SwissSign TSPS [3].

8.5 Actions taken as a result of deficiency

Refer to clause 8.5 of SwissSign TSPS [3].

8.6 Communication of results

Refer to clause 8.6 of SwissSign TSPS [3].

9. Other Business and Legal Matters

9.1 Fees

Refer to clause 9.1 of SwissSign TSPS [3].

9.1.1 Certificate issuance or renewal fees

Refer to clause 9.1.1 of SwissSign TSPS [3].

9.1.2 Certificate access fees

Refer to clause 9.1.2 of SwissSign TSPS [3].

9.1.3 Revocation or status information access fees

Refer to clause 9.1.3 of SwissSign TSPS [3].

9.1.4 Fees for other services

Refer to clause 9.1.4 of SwissSign TSPS [3].

9.1.5 Refund Policy

Refer to clause 9.1.5 of SwissSign TSPS [3].

9.2 Financial responsibility

9.2.1 Insurance coverage

Refer to clause 9.2.1 of SwissSign TSPS [3].

9.2.2 Other assets

Refer to clause 9.2.2 of SwissSign TSPS [3].

9.2.3 Insurance or warranty coverage for end-entities

Refer to clause 9.2.3 of SwissSign TSPS [3].

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Refer to clause 9.3.1 of SwissSign TSPS [3].

9.3.2 Information not within the scope of confidential information

Refer to clause 9.3.2 of SwissSign TSPS [3].

9.3.3 Responsibility to protect confidential information

Refer to clause 9.3.3 of SwissSign TSPS [3].

9.4 Privacy of personal information

Refer to clause 9.4 of SwissSign TSPS [3].

9.4.1 Privacy Plan

Refer to clause 9.4.1 of SwissSign TSPS [3].

9.4.2 Information treated as private

Refer to clause 9.4.2 of SwissSign TSPS [3].

9.4.3 Information not deemed private

Refer to clause 9.4.3 of SwissSign TSPS [3].

9.4.4 Responsibility to protect private information

Refer to clause 9.4.4 of SwissSign TSPS [3].

9.4.5 Notice and consent to use private information

Refer to clause 9.4.5 of SwissSign TSPS [3].

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to clause 9.4.6 of SwissSign TSPS [3].

9.4.7 Other information disclosure circumstances

Refer to clause 9.4.7 of SwissSign TSPS [3].

9.5 Intellectual property rights

Refer to clause 9.5 of SwissSign TSPS [3].

9.6 Representations and warranties

9.6.1 CA representations and warranties

Refer to clause 9.6.1 of SwissSign TSPS [3].

9.6.2 RA representations and warranties

Refer to clause 9.6.2 of SwissSign TSPS [3].

9.6.3 Subscriber representations and warranties

Refer to clause 9.6.3 of SwissSign TSPS [3].

9.6.4 Relying Party representations and warranties

Refer to clause 9.6.4 of SwissSign TSPS [3].

9.6.5 Representations and warranties of other participants

Refer to clause 9.6.5 of SwissSign TSPS [3].

9.7 Disclaimers of warranties

Refer to clause 9.7 of SwissSign TSPS [3].

9.8 Liability

9.8.1 Liability of the TSP

Refer to clause 9.8.1 of SwissSign TSPS [3].

9.8.2 Liability of the Certificate Holder

Refer to clause 9.8.2 of SwissSign TSPS [3].

9.9 Indemnities

Refer to clause 9.9 of SwissSign TSPS [3].

9.10 Term and termination

9.10.1 Term

Refer to clause 9.10.1 of SwissSign TSPS [3].

9.10.2 Termination

Refer to clause 9.10.2 of SwissSign TSPS [3].

9.10.3 Effect of termination and survival

Refer to clause 9.10.3 of SwissSign TSPS [3].

9.11 Individual notices and communications with participants

Refer to clause 9.11 of SwissSign TSPS [3].

9.12 Amendments

9.12.1 Procedure for amendment

Refer to clause 9.12.1 of SwissSign TSPS [3].

9.12.2 Notification mechanism and period

Refer to clause 9.12.2 of SwissSign TSPS [3].

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

9.12.3 Circumstances under which OID must be changed

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

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

9.13 Dispute resolution provisions

Refer to clause 9.13 of SwissSign TSPS [3].

9.14 Governing law and place of jurisdiction

Refer to clause 9.14 of SwissSign TSPS [3].

9.15 Compliance with applicable law

Refer to clause 9.15 of SwissSign TSPS [3].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Refer to clause 9.16.1 of SwissSign TSPS [3].

9.16.2 Assignment

Refer to clause 9.16.2 of SwissSign TSPS [3].

9.16.3 Severability

Refer to clause 9.16.3 of SwissSign TSPS [3].

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

Refer to clause 9.16.5 of SwissSign TSPS [3].

9.17 Other provisions

9.17.1 Language

Refer to clause 9.17.1 of SwissSign TSPS [3].

9.17.2 Delegated or outsourced Services

Refer to clause 9.17.2 of SwissSign TSPS [3].

10. References

[1] SwissSign CP QCP-n-qscd RSS – Certificate Policy for Qualified Signature certificates for RSS, published under: https://repository.swisssign.com

[2] SwissSign CPR Sign - Certificate, CRL and OCSP Profiles for Signing certificates, published under: https://repository.swisssign.com

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

[4] ETSI EN 319 411-1 v1.2.2 (2018-04) 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 (2018):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 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

[7] ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)

[8] VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)

[9] TAV-BAKOM: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)

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

[11] SwissSign Platinum CP/CPS - Certificate Policy and Certification Practice Statement of the SwissSign Platinum CA and its subordinated issuing CA, published under: https://repository.swisssign.com