SwissSign

SwissSign CPS eIDAS Signing Services

Certification Practice Statement for eIDAS Signing certificates

Document Type:	Certificate Practice Statement
OID:	n/a
Author:	Information Security and Compliance
Owner:	CEO
Applicability:	Global
Copyright:	Attribution-NoDerivs (CC-BY-ND) 4.0
Version:	3
Issue date:	02.10.2025
Obsoletes:	v2.0, 28.02.2025

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

Table of Contents

1. INTRODUCTION

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

Its affiliate SwissSign GmbH in Austria provides services according to the EU Regulation No 910/2014 (eIDAS) on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

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

- Certificate Policy which defines the policy that 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 [4], if the chapter refer to general practices of the TSP independent from the trust service.

The offered services are non-discriminatory, duly comply regarding accessibility with eIDAS [10] and the Austrian Federal Law on electronic signatures and trust services for electronic transactions (SVG) [11]. They respect the applying export regulations according to Swiss law. 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 in conjunction with the TSPS [4] describes the practices implemented by SwissSign GmbH to comply with the relevant services as well as the terms and conditions under which this CA is made available. The following certificate policies describe in detail the eIDAS Remote Signing Service based on qualified electronic certificates for Qualified Electronic Signatures and Advanced Electronic Signatures respectively:

“SwissSign CP eIDAS QCP-n-qscd RSS – Certificate Policy for eIDAS Qualified Electronic Signatures for Remote Signing Service” [1]

“SwissSign CP eIDAS QCP-n RSS – Certificate Policy for eIDAS Advanced Electronic Signatures for Remote Signing Service” [2]

SwissSign implements and operates the user registration and identification processes along with the issuance of qualified certificates. The qualified certificates issued are short-term certificates meant to be used for only one signing case. Short-term certificates expire before a revocation would take effect; therefore, no revocation service is offered to the subscriber. To publish the status of issued certificates in extraordinary cases, SwissSign does, however, offer an OCSP service as well as a certificate revocation list (CRL). The supported format of the generated signatures via the remote qualified signing service (RSS) is PAdES and can be used to sign PDF files. The electronic signature functionality provided to subscribers is facilitated through a dedicated mobile application installed on their smartphone. This application ensures that the subscriber retains exclusive control over the signature process.

SwissSign eIDAS signing service support signature with time. The time is provided by a time-stamp token on the signature. The time-stamp token is not an eIDAS qualified timestamp.

For the issuance of certificates within of this scope and its signing service, SwissSign fully complies with eIDAS, the Austrian Federal Law on electronic signatures and trust services for electronic transactions (SVG) [11], the related ordinance on electronic signatures and trust services for electronic transactions (SVV), the EUSCP policy of ETSI TS 119 431-1 (EU SSASC Policy: itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)) as well as further applicable specifications:

- eIDAS: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- SVG: Austrian Federal Law on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Law)
- SVV: Austrian Ordinance on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Ordinance)
- 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 EN 319 411-2 : Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/ SCDev
- ETSI TS 119 431-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting ADES digital signature creation.
- 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 (2022-02): 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 eIDAS RSS (qualified certificates for qualified signatures, RA is SwissSign)
- QCP-n eIDAS RSS (qualified certificates for advanced signatures, RA is SwissSign)

The relevant Issuing CA for these certificates under this CPS are shown in the PKI overview of SwissSign shown in figures 1 and 2.

The SwissSign ECC eIDAS Qualified Services Root 2023-2 CA is not currently used with the SwissSign eIDAS service. Its inclusion within the TSP will take place in a subsequent phase.

The SwissSign RSA eIDAS Qualified Services Root 2023–2 Root Certificate Authority as well as the Issuing CA are operated by SwissSign GmbH, Fleischmarkt 1, 1010 Vienna Austria.

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 GmbH with respect to certificates issued by this CA. This CPS also provides statements of the rights and obligations of SwissSign GmbH, authorized Registration Authorities and other third parties as far as applicable, 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 the Root CA “SwissSign RSA eIDAS Qualified Services Root 2023 - 1” and all it subordinated issuing CA for qualified certificates for signing as shown in Figure 1 above, unless stated differently.

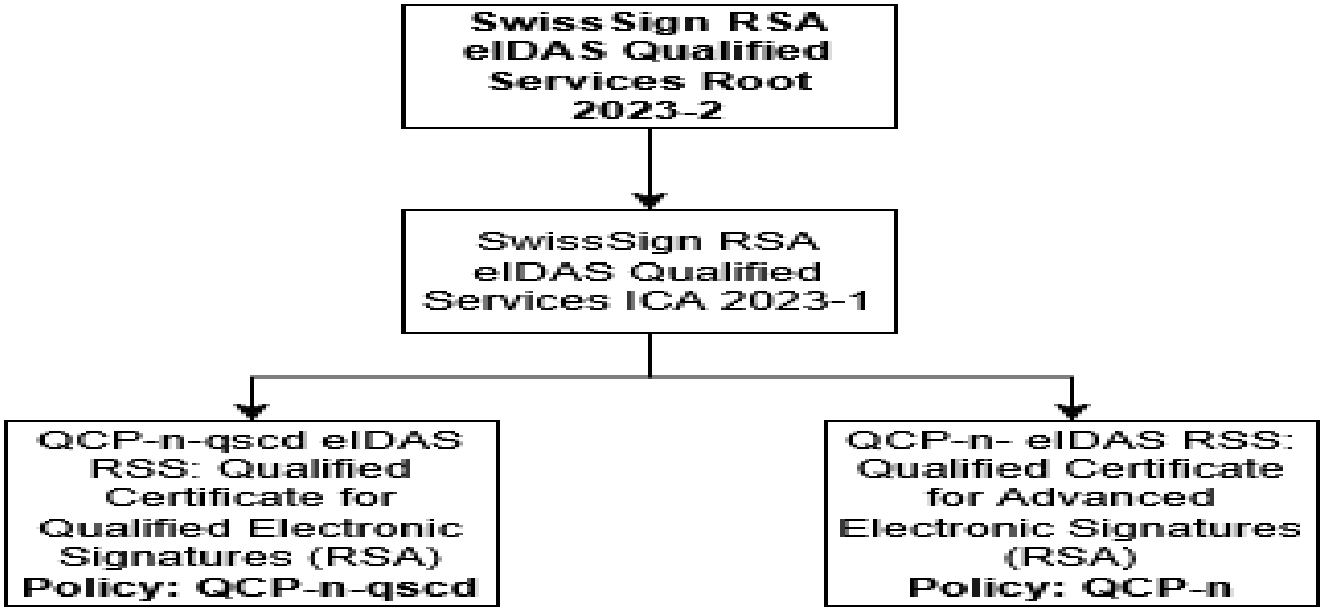

Figure 1: Picture showing SwissSign RSA eIDAS Qualified Services Root 2023–2 hierarchy

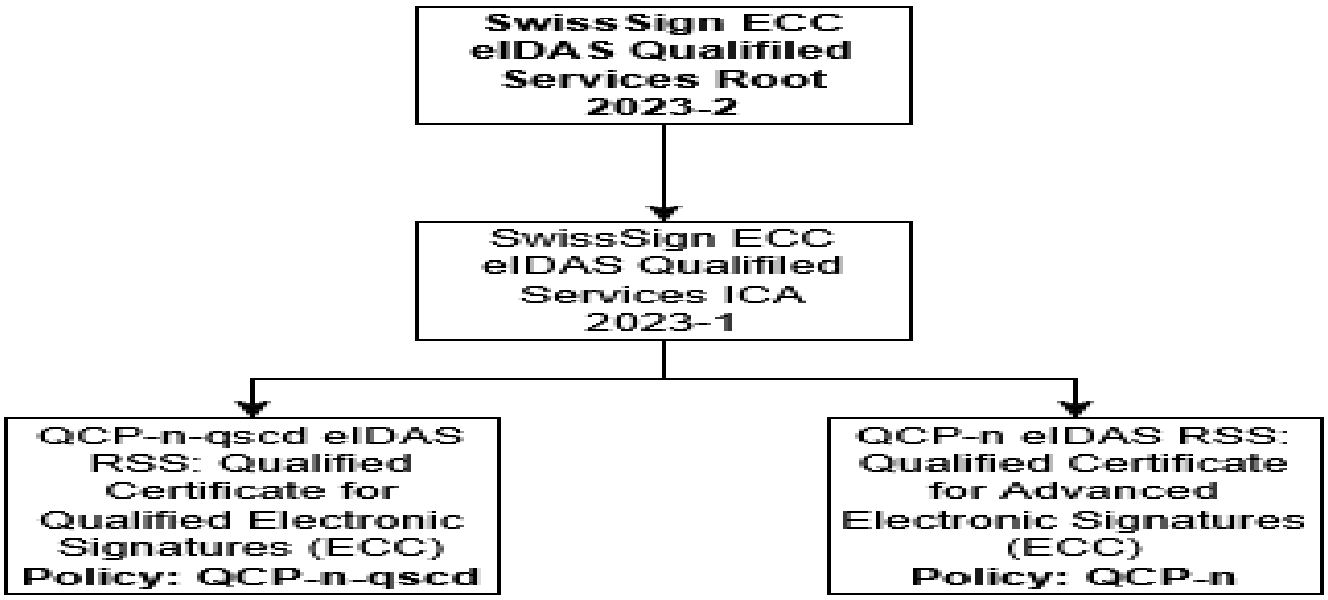

Figure 2: Picture showing SwissSign ECC eIDAS Qualified Services Root 2023-2 hierarchy

1.2 Document name and identification

This document is named “SwissSign CPS Signing Services - Certification Practice Statement for eIDAS 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 fixed Certificate Policy for each certificate type issued.

The TSPS [4] and the service-related Certification Practice Statements do not contain an OID.

1.2.1 Revisions

Version	Date	Author	Comment
1.0	16.02.2024	Adrian Müller, Luis Peñalosa	Initial version
2.0	28.02.2025	Luis Peñalosa, Raffaela Achermann	Change: Disclaimer. 1.5.3, 1.5.4 and 4.9.5
3.0	02.10.2025	Luis Peñalosa	Additional details about remote identity proofing in sections 1.3.2 and 3.2.3

1.3 PKI Participants

1.3.1 Certification Authorities

The TSP operates a Public Key Infrastructure, consisting of the following Root CAs “SwissSign RSA eIDAS Qualified Services Root 2023 – 1” and its subordinated issuing CAs as shown in Figure 1.

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

Another Registration Authority for these policies, called “External RA Partner” that registers subjects and subscribers is operated in conjunction with an external service provider who provides “automated identity verification” and “hybrid manual and automated identity verification” as independently eIDAS certified component/module.

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 [4] for Subject’s and Subscriber’s responsibilities.

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS 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 Certificate Profile document [3].

1.5 Policy administration

1.5.1 Organization administering the document

The CPS is written and updated by SwissSign GmbH.

SwissSign GmbH
Fleischmarkt 1
1010 Vienna
Austria
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

A member of the Management Board of SwissSign AG (in Switzerland) and as well as SwissSign GmbH for the eIDAS trust services determine the suitability of this CPS 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. They are subject to review by the Austrian supervisory body (RTR).

1.5.4 CPS approval procedures

This document shall be regularly reviewed by Information Security & Compliance and approved by a member of the SwissSign GmbH 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. In particular, changes to this document are notified to the Austrian eIDAS supervisory body (RTR).

1.6 Definitions and acronyms

Refer to clause 1.6 of the TSPS [4].

2. Publication and Repository Responsibilities

Refer to clause 2 of SwissSign TSPS [4].

2.1 Repositories

Refer to clause 2.1 of SwissSign TSPS [4].

Please note: No subscriber certificate issued according to this CPS is published in the directory.

2.2 Publication of certification information

Refer to clause 2.2 of SwissSign TSPS [4].

2.3 Time or frequency of publication

Refer to clause 2.2 of SwissSign TSPS [4].

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 [4].

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 are described in the Certificate Profile [3].

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

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. 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 any part of the subject information.

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

Furthermore:

- The use of a real name and its identifying information must be authenticated and authorized according to chapter 3.2.3
- The use of pseudonym is not permitted.
- All attributes in the DN and SAN, if applicable, must be validated and authorized.

3.1.2 Need for names to be meaningful

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 are described in the Certificate Profile document [3].

3.1.3 Anonymity or pseudonymity of Subscribers

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS): The use of pseudonyms is not permitted.

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.

Depending on the certificates issue the uniqueness of the Distinguished Name is achieved through different unique identifiers as defined in the Certificate Profile document [3].

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 Austrian 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.

3.2 Initial identity validation

The initial identity validation is part of the Certificate Application process as described in chapter 4.1. Existing evidence can be re-used to validate the identity depending on the validity of the evidence. The evidence is not used if older than 5 years.

3.2.1 Method to prove possession of private key

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS 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. Further details are described in chapter 6.1.2

3.2.2 Authentication of organization identity

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS 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. The process is conducted either in physical presence using a registration form or through an equivalent remote identification procedure in accordance with ETSI TS 119 461 [14]. Remote identification may involve unattended identity proofing with fully automated operation, or a hybrid approach combining automated and manual processes.

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS 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 names in the request have to be identical or a subset of the given name(s) and the family name of the identifying documents, irrespective of the order of these names (see 3.1.1).

The identification is performed 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, ETSI TS 119 461, chapters 8, 9.1 and 9.2. This step may be conducted by:
  - the registration authority processing the certificate request: “SwissSign RA”, see section 1.3.2
  - a trained and contracted partner for the identification service: “External RA Partner”, see section 1.3.2
- The individual must present a valid original of an official identification document as recognized by national law. If the identification is performed remotely, the system captures photos and videos of the identifying document. If an agent conducts the identification, a high-quality scanned copy of the document is obtained. In both cases, the agent or system confirms the proper execution of the identification either in writing or electronically, as agreed with the TSP.
- The identifying document information is compared and has to match (e.g., facial features, age) with the person present as described above. If the identification process is performed remotely, the face image to be compared against is captured from a video stream of the person present.
- When the identifying document presented by the subject is NFC-compliant, a fully unattended identity verification process will be performed. If the document does not support NFC, or if the automated NFC verification yields a score below the acceptance threshold, a human-assisted verification process will be initiated.

3.2.4 Non-verified Subscriber information

All Subscriber information and evidence 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

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS 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.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Only short-term certificates are issued. A new certificate has to be requested. The new certificate contains new validity and key information but retains subject information of the previously issued certificate if valid. The subscriber has to confirm that the information submitted during identification is still valid.

The Certificate Application process is described in chapter 4.1.

3.3.2 Identification and authentication for re-key after revocation

Only short-term certificates, i.e. certificates that expire before a revocation would take effect, are issued. No revocation can be requested by the subscriber, therefore the TSP does not support re-keying of certificates issued by this CA after revocation.

See also chapter 4.9

3.4 Identification and authentication for revocation request

Only short-term certificates, i.e. certificates that expire before a revocation would take effect, are issued. Therefore, no revocation can be requested by the subscriber. See also chapter 4.9

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.

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS) Certificate request can be applied via SwissSign registration 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 eIDAS, SVG [11] and SVV [12]:

- identity of the Subscriber 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 eIDAS RSS and QCP-n eIDAS 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) including a 2FA.
- 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,
- all documents and information are approved by the RA.

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

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

The subscribers must be fully identified and authenticated before they can proceed with any action related to signing operations or their keys.

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. The RA identifies the Subscriber on the basis of the identifying documents and evidence 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 sole 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 referred in chapter 7.1.

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:

- electronically provide the certificate to the Subscriber within its self-service portal or Remote Signing Service interface.

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 perform a signature. 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 [4], 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 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 eIDAS RSS) Qualified certificates can be used for qualified electronic signatures.
- (QCP-n eIDAS RSS) Qualified certificates can be used for advanced 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

Only short-term certificates are issued. Certificate renewal is not supported by the TSP. A new certificate has to be requested. Subscribers that have previously been registered by the TSP and for whom a certificate has been issued may apply for a new certificate. The new certificate contains new validity and key information but retains subject information of the previously issued certificate if valid. The subscriber has to confirm that the information submitted during identification is still valid.

The Certificate Application process is described in chapter 4.1.

4.7 Certificate re-key

Subscribers that have previously been registered by the TSP and for whom a certificate has been issued may apply for a new certificate. The new certificate contains new validity and key information but retains subject information of the previously issued certificate if valid. The subscriber has to confirm that the information submitted during identification is still valid.

The Certificate Application process is described in chapter 4.1.

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 has been in possession of strong authentication factors since the initial certificate application.
- The registration information about the Subscriber is correct.
- The verification of the identity and evidence 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.

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 requester uses strong authentication factors to confirm the validated information at the TSP.
- 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.

The TSP issues only short-term certificates for its eIDAS services. (QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS) There is no revocation system available for the subscribers of these certificates.

The CA or the Austrian supervisory body (RTR) can request for revocation of specific certificates under special circumstances.

The TSP logs all revocations in the CA Journal Database (5.4).

4.9.1 Circumstances for revocation

The CA revokes a Subscriber’s certificate if any of the following conditions are met:

- The Austrian supervisory body (RTR) requests in writing that the CA revoke the certificate
- 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 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.

4.9.2 Who can request revocation

This CA accepts certificate revocation requests from the following sources:

- the Austrian supervisory body (RTR).

4.9.3 Procedures for revocation request

For "short-term" certificates (with validity period, shorter than the maximum time to process a revocation request) the revocation procedures do not have to be offered. However, status services are offered for short-term certificates as well and the certificates are marked specifically as short-term (with extension ext-etsi-valassured-ST-certs).

4.9.3.1 Notification about revocation

This CA will communicate to the Austrian supervisory body (RTR) by e-mail.

4.9.4 Revocation request grace period

Not applicable

4.9.5 Time within which CA must process the revocation request

After the verification of the revocation request outlined in chapter 4.9.1 have been met, the CA will process revocation requests on working days between 9 and 17.

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

The following table has the format "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. CRLs are issued with a life-time of at least 10 days.

  - 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,
- 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 “directory.swisssign.net”. The certificate status services provide information on the status of certificates at all times, even after the certificate has expired or was revoked. The certificate status service ensures high availability including the corresponding databases. In case of an outage of more than 30 minutes this will be treated as an incident and reported to the Austrian supervisory body (RTR). 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 30 years after the expiry date of the last leaf-certificate in scope, not only until the end of the Issuing CA validity.

Please note: Certificate status services are provided for all certificates, including “short-term” certificates (with validity period, shorter than the maximum time to process a revocation request). Therefore, the specific marking of these certificates as short-term according to ETSI EN 319 411-1, chapter 6.6.1 will be present.

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 30 years after termination of a subscription according to SVV [12].

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 [4].

5.2 Procedural controls

Refer to clause 5.2 of SwissSign TSPS [4].

5.3 Personnel controls

Refer to clause 5.3 of SwissSign TSPS [4].

5.4 Audit logging procedures

Refer to clause 5.4 of SwissSign TSPS [4].

In addition to the events described in 5.4.1 of SwissSign TSPS [4], the lifecycle events key generation (see 6.1.1) and key destruction (see 6.2.10) for subscriber and their keys are logged.

The logging process includes recording the date and time of occurrence, event type, actor’s identity, and the outcome (success or failure) of the event.

5.5 Records archival

Refer to clause 5.5 of SwissSign TSPS [4].

5.6 Key changeover

Refer to clause 5.6 of SwissSign TSPS [4].

5.7 Compromise and disaster recovery

Refer to clause 5.7 of SwissSign TSPS [4].

5.8 CA or RA termination

Refer to clause 5.8 of SwissSign TSPS [4].

6. Technical Security Controls

Refer to clause 6 of SwissSign TSPS [4].

6.1 Key pair generation and installation

Refer to clause 6.1 of SwissSign TSPS [4].

6.1.1 Key pair generation

For Root and Issuing CA, refer to clause 6.1.1 of SwissSign TSPS [4].

The Subscriber key pairs are generated by the TSP.

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

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS) Subscriber keys are generated by the TSP on a QSCD in the secure environment of the TSP. In all cases the requirements of eIDAS, 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 eIDAS RSS and QCP-n eIDAS 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. Immediately after signature creation, the signing key pair is securely deleted in the QSCD.

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 [4].

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 RSA based eIDAS Root CA uses a 4096 bit RSA key.

The RSA based eIDAS Issuing CA use a 4096 bit RSA key.

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS):

- All RSA based 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)

The signing key of this CA and its subordinated issuing CAs are the only keys permitted for signing certificates and CRLs and have the keyCertSign and CRLSign key usage bit set. Subscribers can obtain certificates issued by this CA with the following key usage bit included, depending on the type of product selected.

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS):

Key usage:

- nonRepudiation

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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.1 of SwissSign TSPS [4] – Trust Services Practice Statement.

Subscriber key (QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS) Subscriber keys for qualified certificates are generated and stored on an HSM that meets Common Criteria EAL4+ requirements and certified as a QSCD.

The TSP has implemented organizational monitoring procedures to ensure that the device is certified during the whole certificate life cycle as well as to ensure that it fulfills the requirements of eIDAS.

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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.2 of SwissSign TSPS [4] – 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.3 of SwissSign TSPS [4] – 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.4 of SwissSign TSPS [4] – Trust Services Practice Statement.

Subscriber keys Subscriber keys are managed by the TSP within certified QSCD 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.5 of SwissSign TSPS [4] – Trust Services Practice Statement.

Subscriber keys Subscriber keys are managed by the TSP within certified QSCD 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.6 of SwissSign TSPS [4] – Trust Services Practice Statement.

Subscriber keys Subscriber keys are generated and managed by the TSP within certified QSCD 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.7 of SwissSign TSPS [4] – Trust Services Practice Statement.

Subscriber keys Subscriber keys are stored within certified QSCD 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.8 of SwissSign TSPS [4] – 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.9 of SwissSign TSPS [4] – Trust Services Practice Statement.

Subscriber keys Subscriber keys are activated for single use only under and are automatically deactivated by the certified QSCD 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 [4] – Trust Services Practice Statement.

Issuing CA keys Refer to clause 6.2.10 of SwissSign TSPS [4] – 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 certified QSCD after the signature is created following a compliant FIPS140-2 Level 3 destruction method.

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 [4].

6.3 Other aspects of key pair management

6.3.1 Public key archival

Refer to clause 6.3.1 of SwissSign TSPS [4].

6.3.2 Certificate operational periods and key pair usage periods

Refer to clause 6.3.2 of SwissSign TSPS [4].

End user certificates are short-terms certificates and have a lifetime of 10 minutes. The generated key pair is securely deleted in the certified QSCD after signature creation following a compliant FIPS140-2 Level 3 destruction method.

6.4 Activation data

6.4.1 Activation data generation and installation

Refer to clause 6.4.1 of SwissSign TSPS [4].

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
- activated using biometrics

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS 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 QSCD 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 [4].

Issuing CA keys Refer to clause 6.4.2 of SwissSign TSPS [4].

Subscriber keys Subscribers are obliged to keep the activation data secret at all times.

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS)

- The device containing the SIC authentication means must be protected with biometric activation. The activation data is created with the SIC authentication means with a nonce and reference to the data to be signed provided by the QSCD. This reference assures that the data to be signed is only signed by the signing key belonging to his signer. The SAD is verified by the QSCD within the tamper proof environment containing the subscriber keypair, not allowing access to other subscribers and protecting it against tampering. The SAD comprises one single DTBS/R, the signing key name and must be signed by the signer’s private authentication key. Measures are applied to secure the connection between the signature creation application and the QSCD.
- Appropriate measures are in place to prevent online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay, session hijacking, man-in-the middle, credential theft, spoofing and masquerading attacks. A session token is used during signing operations for protection against replay bypass and forgery attacks.

6.4.3 Other aspects of activation data

Refer to clause 6.4.3 of SwissSign TSPS [4].

(QCP-n-qscd eIDAS RSS and QCP-n eIDAS RSS)

- The QSCD is used in a tamper proof environment containing the subscriber key pair. The QSCD fulfills the requirements stated in CEN EN 419241-2.
- Mobile devices which SwissSign allows to use the service have to fulfill the following requirements:
  - Device is not rooted
  - Device PIN set and biometric authentication
  - Secure Element with TEE present
  - Apple devices:
    - iOS 17.0 or newer
  - Android devices:
    - Android 9.0 or newer
  - Fingerprint reader present or face recognition to unlock the secure element with strong biometrics
  - Subscribers agree to set a biometric authentication on the device.
- Communications are protected to prevent any forms of attacks tampering subscriber authentication methods.
- Throughout the signing process, the subscriber initiates by uploading the PDF document onto the SwissID Sign application platform, where the document becomes accessible for review. Within this interface, the subscriber peruses the document content and subsequently endorses it for signature. The subscriber retains the autonomy to designate the signing certificate and the signature placement within the document and affirm the transaction. The conclusive step involves the subscriber's confirmation of the signature, accomplished via their mobile device, which supplies the requisite activation data. Upon successful completion of the signing procedure, the subscriber gains access to download the signed document via the SCA user interface. The signing process involves the transmission of only the document's hash to the QSCD for signing purposes. This mechanism ensures that the document presented to the subscriber within the SCA remains unchanged and identical to the one that undergoes the signing process.

6.5 Computer security controls

Refer to clause 6.5 of SwissSign TSPS [4].

6.5.1 Specific computer security technical requirements

Refer to clause 6.5.1 of SwissSign TSPS [4].

6.5.2 Computer security rating

Refer to clause 6.5.2 of SwissSign TSPS [4].

6.6 Life cycle technical controls

6.6.1 System development controls

Refer to clause 6.6.1 of SwissSign TSPS [4].

6.6.2 Security management controls

Refer to clause 6.6.2 of SwissSign TSPS [4].

6.6.3 Life cycle security controls

Refer to clause 6.6.3 of SwissSign TSPS [4].

6.7 Network security controls

Refer to clause 6.7 of SwissSign TSPS [4].

6.8 Time-stamping

No timestamping service according to eIDAS is provided. For other timestamping implementations please refer to clause 6.8 of SwissSign TSPS [4].

7. Certificate, CRL and OCSP Profiles

7.1 Certificate profile

The Certificate profile is described in the Certificate Profile [3].

7.2 CRL profile

The CRL profile is described in the Certificate Profile [3].

7.3 OCSP profile

The OCSP profile is described in the Certificate Profile [3].

8. Compliance Audit and Other Assessments

The present CPS fulfills the requirements for certificates and services according to eIDAS, SVG, SVV and ETSI EN 319 401, ETSI EN 319 411-1/2, ETSI TS 119 431-/2 and ETSI TS 119 461. The terms and conditions of this CPS, the SVG [11], SVV [12] 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 [4].

8.2 Identity/qualifications of assessor

Refer to clause 8.2 of SwissSign TSPS [4].

The Austrian supervisory body (RTR) can request access to the SwissSign facilities and check on the TSP’s operations at any time.

8.3 Assessor’s relationship to assessed entity

Refer to clause 8.3 of SwissSign TSPS [4].

8.4 Topics covered by assessment

Refer to clause 8.4 of SwissSign TSPS [4].

8.5 Actions taken as a result of deficiency

Refer to clause 8.5 of SwissSign TSPS [4].

8.6 Communication of results

Refer to clause 8.6 of SwissSign TSPS [4].

9. Other Business and Legal Matters

9.1 Fees

Refer to clause 9.1 of SwissSign TSPS [4].

9.1.1 Certificate issuance or renewal fees

Refer to clause 9.1.1 of SwissSign TSPS [4].

9.1.2 Certificate access fees

Refer to clause 9.1.2 of SwissSign TSPS [4].

9.1.3 Revocation or status information access fees

Refer to clause 9.1.3 of SwissSign TSPS [4].

9.1.4 Fees for other services

Refer to clause 9.1.4 of SwissSign TSPS [4].

9.1.5 Refund Policy

Refer to clause 9.1.5 of SwissSign TSPS [4].

9.2 Financial responsibility

9.2.1 Insurance coverage

Refer to clause 9.2.1 of SwissSign TSPS [4].

9.2.2 Other assets

Refer to clause 9.2.2 of SwissSign TSPS [4].

9.2.3 Insurance or warranty coverage for end-entities

Refer to clause 9.2.3 of SwissSign TSPS [4].

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Refer to clause 9.3.1 of SwissSign TSPS [4].

9.3.2 Information not within the scope of confidential information

Refer to clause 9.3.2 of SwissSign TSPS [4].

9.3.3 Responsibility to protect confidential information

Refer to clause 9.3.3 of SwissSign TSPS [4].

9.4 Privacy of personal information

Refer to clause 9.4 of SwissSign TSPS [4].

9.4.1 Privacy Plan

Refer to clause 9.4.1 of SwissSign TSPS [4].

9.4.2 Information treated as private

Refer to clause 9.4.2 of SwissSign TSPS [4].

9.4.3 Information not deemed private

Refer to clause 9.4.3 of SwissSign TSPS [4].

9.4.4 Responsibility to protect private information

Refer to clause 9.4.4 of SwissSign TSPS [4].

9.4.5 Notice and consent to use private information

Refer to clause 9.4.5 of SwissSign TSPS [4].

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to clause 9.4.6 of SwissSign TSPS [4].

9.4.7 Other information disclosure circumstances

Refer to clause 9.4.7 of SwissSign TSPS [4].

9.5 Intellectual property rights

Refer to clause 9.5 of SwissSign TSPS [4].

9.6 Representations and warranties

9.6.1 CA representations and warranties

Refer to clause 9.6.1 of SwissSign TSPS [4].

9.6.2 RA representations and warranties

Refer to clause 9.6.2 of SwissSign TSPS [4].

9.6.3 Subscriber representations and warranties

Refer to clause 9.6.3 of SwissSign TSPS [4].

9.6.4 Relying Party representations and warranties

Refer to clause 9.6.4 of SwissSign TSPS [4].

9.6.5 Representations and warranties of other participants

Refer to clause 9.6.5 of SwissSign TSPS [4].

9.7 Disclaimers of warranties

Refer to clause 9.7 of SwissSign TSPS [4].

9.8 Liability

9.8.1 Liability of the TSP

Refer to clause 9.8.1 of SwissSign TSPS [4].

9.8.2 Liability of the Certificate Holder

Refer to clause 9.8.2 of SwissSign TSPS [4].

9.9 Indemnities

Refer to clause 9.9 of SwissSign TSPS [4].

9.10 Term and termination

9.10.1 Term

Refer to clause 9.10.1 of SwissSign TSPS [4].

9.10.2 Termination

Refer to clause 9.10.2 of SwissSign TSPS [4].

9.10.3 Effect of termination and survival

Refer to clause 9.10.3 of SwissSign TSPS [4].

9.11 Individual notices and communications with participants

Refer to clause 9.11 of SwissSign TSPS [4].

9.12 Amendments

9.12.1 Procedure for amendment

Refer to clause 9.12.1 of SwissSign TSPS [4].

9.12.2 Notification mechanism and period

Refer to clause 9.12.2 of SwissSign TSPS [4].

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 [4].

9.14 Governing law and place of jurisdiction

Refer to clause 9.14 of SwissSign TSPS [4].

9.15 Compliance with applicable law

Refer to clause 9.15 of SwissSign TSPS [4].

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Refer to clause 9.16.1 of SwissSign TSPS [4].

9.16.2 Assignment

Refer to clause 9.16.2 of SwissSign TSPS [4].

9.16.3 Severability

Refer to clause 9.16.3 of SwissSign TSPS [4].

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 [4].

9.17 Other provisions

9.17.1 Language

Refer to clause 9.17.1 of SwissSign TSPS [4].

9.17.2 Delegated or outsourced Services

Refer to clause 9.17.2 of SwissSign TSPS [4].

10. References

[1] SwissSign CP eIDAS QCP-n-qscd RSS – Certificate Policy for eIDAS Qualified Electronic Signatures for Remote Signing Service, published under: https://repository.swisssign.com

[2] SwissSign CP eIDAS QCP-n RSS – Certificate Policy for eIDAS Advanced Electronic Signatures for Remote Signing Service, published under: https://repository.swisssign.com

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

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

[5] 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.

[6] ETSI EN 319 411-2 V2.5.1 (2023-10) 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 .

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

[8] ETSI TS 119 431-1 v1.2.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/ SCDev

[9] ETSI TS 119 431-2 v1.1.1 (2018-12) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting ADES digital signature creation.

[10] eIDAS: Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[11] SVG: Austrian Federal Law on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Law)

[12] SVV: Austrian Ordinance on electronic signatures and trust services for electronic transactions (Signature- and Trust Services Ordinance)

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

[14] ETSI TS 119 461 V1.1.1 (2021-07): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects