SwissSign CP QCP-n-qscd RSS

Certificate Policy for Qualified Signature certificates for RSS

Document Type:	Certificate Policy
OID:	2.16.756.1.89.2.1.21
Author:	Information Security and Compliance
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	12.12.2022
Version:	2.0
Obsoletes:	Version 1.0, 14 July 2021
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Version Control

Date	Version	Comment	Author
14.07.2021	1.0	First public edition.	Michael Guenther
12.12.2022	2.0	Minor redactional changes	Roman Fischer, Adrian Müller

Authorization

Date	Approved by	Approved by	Version
08.07.2021	Michael Günther	Markus Naef	1.0
12.12.2022	Michael Günther	Michael Widmer	2.0

Michael Frank Günther

December 7, 2022

Qualified Electronic Signature by SwissID

digital signature

Michael Peter Widmer

7. Dezember 2022

Qualified Electronic Signature by SwissID

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

The structure of this document corresponds to RFC3647 and is divided into nine parts. To preserve the outline specified by RFC 3647, section headings that do not apply or are not supported by the TSP have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them. Each top-level chapter includes references to the relevant specifications ETSI EN 319 411-1 [4] and ETSI EN 319 411-2 [5].

The services offered duly comply e.g. regarding the accessibility with the Swiss law. The offered services are non-discriminatory. They respect the applying export regulations. The TSP may outsource partial tasks to partners or external providers. The TSP, represented by the management or its agents, shall remain 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 document, named ”SwissSign CP QCP-n-qscd RSS - Certificate Policy for Qualified Signature certificates for RSS“ (hereinafter referred to as CP), defines procedural and operational requirements that SwissSign AG adheres to and requires entities to adhere to when issuing and managing certificates according ZertES/VZertES, i.e.

- 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 (2021): General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 (2021): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 (2021):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 (2022): 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 (May 2008): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

This CP 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 CP 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 the event of any inconsistency between this document and the Requirements listed above, the Requirements take precedence over this document.

1.2 Document name and identification

This document is named ”SwissSign CP QCP-n-qscd RSS - Certificate Policy for Qualified Signature certificates for RSS“ as indicated on the cover page of this document.

This CP is identified by OID: 2.16.756.1.89.2.1.21

The OID is composed according to the contents of the following table:

Meaning	Position 1	Position 2	Position 3	Position 4	Position 5	Position 6	Position 7	Position 8
Joint ISO-CCITT Tree	2							
Country		16						
Switzerland			756					
RDN				1				
SwissSign					89			
TSP Tree						2		
Document Type							1	
Product								21

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

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

The OID used by SwissSign to identify the QCP-n-qscd certificates shall be used in the QCP-n-qscd RSS certificate profile.

1.3 PKI Participants

Refer to clause 5.4 of ETSI EN 319 411-1/2 [4]/[5].

1.3.1 Certification Authorities

The TSP shall have a clear structure of its PKI including the Root and Issuing CA operated.

1.3.2 Registration Authorities

The TSP shall operate an internal registration authority, called “SwissSign RA” that registers Subscribers of certificates issued by this CA.

Third parties may operate their own external Registration Authority services, if these third parties abide by all the rules and regulations of this CP, the services related CPS [1] and TSPS [3] clause 9.6.2. The external RA shall have a contract with the TSP and shall be allowed to execute their registration process if the TSP has audited and approved the process as equivalent to the registration process of the SwissSign RA.

In particular, other RA's may implement a different process if they meet the following requirements:

- The registration process must be documented and presented to the TSP.
- The other RA is only allowed to execute their registration process if the TSP has audited and approved the process as equivalent to the registration process of the SwissSign RA.
- RA’s other than the SwissSign RA may choose to accept different identifying documents or information sources. Such documents or information sources may contain name forms that differ from official identity documents.
- Any RA operating under this CP must implement a registration process that meets the requirements of the ZertES/VZertES as well ETSI EN 319 411-1/2 and that authenticates the individual identity in accordance with these guidelines.

1.3.3 Subscribers

The TSP shall define who is allowed to be Subscriber and Subject in the corresponding CPS [1] that belongs to the certificate.

1.3.4 Relying Parties

The TSP shall define who is relying parties in the corresponding CPS [1] that belongs to the certificate.

Relying Parties may also be Subscribers within this CA.

1.3.5 Other participants

The TSP shall state if any other participants are involved for the provision of the service in the corresponding CPS CPS [1] that belongs to the certificate.

1.4 Certificate usage

Refer to clause 5.5 of ETSI EN 319 411-1/2 [4]/[5].

1.4.1 Appropriate certificate uses

The following certificates shall be issued under this CP:

(QCP-n-qscd) Qualified certificates used for qualified signature under the ZertEs/VZertES [8]/[9]. Qualified Signature Certificates are intended for use in Qualified Electronic Signatures according to Swiss Digital Signature law with legal equivalence to handwritten signatures, and may be restricted to usage with certain contracting parties only.

1.4.2 Prohibited certificate uses

Any other use than defined in chapter 1.4.1 is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

This CP 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 shall determine the suitability of this CP 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 CP.

1.5.4 CP approval procedures

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

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

1.6 Definitions and acronyms

Refer to clause 1.6 of the TSPS [2].

2. Publication and Repository Responsibilities

Refer to clause 6.1 of ETSI EN 319 411-1/2 [4]/[5].

2.1 Repositories

The TSP shall publish all current and past documentation.

The TSP shall publish root certificates and CA certificates as well as certificate status information.

The TSP shall publish information regarding public Subscriber certificates.

These web sites shall publish the only source for up-to-date documentation.

2.2 Publication of certification information

Public documents shall only be valid if they are published as a PDF with the digital signatures of the for the approval responsible persons.

The TSP shall notify notice of changes it intends to make in its CP and referred documents.

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

2.3 Time or frequency of publication

This CP, the service-based CPS and the TSPS and their amendments shall be reviewed at least once a year. Even if no updates are required, a new version shall be published.

2.4 Access controls on repositories

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

2.5 Additional testing

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

3. Identification and Authentication

Refer to clause 6.2 of ETSI EN 319 411-1/2 [4]/[5].

3.1 Naming

3.1.1 Types of Names

The types of names allowed to be included in the QCP-n-qscd RSS Certificates shall be compiled in accordance with the Certificate Profile [2].

3.1.2 Need for names to be meaningful

All the values in the Subject information section of a Certificate shall be meaningful and authorized.

3.1.3 Anonymity or pseudonymity of Subscribers

The TSP may use pseudonyms in the issued certificates.

3.1.4 Rules for interpreting various name forms

The practices for interpreting names shall be described in chapter 3.1.4 of the respective CPS [1] that belongs to the certificate, if applicable.

3.1.5 Uniqueness of names

SwissSign shall not issue the Certificate with an identical Subject's Distinguished Name to different Subjects.

Additional practices shall be described in chapter 3.1.5 of the respective CPS [1] that belongs to the certificate, if applicable.

3.1.6 Recognition, authentication, and role of trademarks

The TSP and its RAs shall 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 shall not be obliged to verify lawful use of names. It shall be the sole responsibility of the Subscriber to ensure lawful use of chosen names.

The TSP shall 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 CP.

3.2 Initial identity validation

The TSP shall verify the identity of the Subject and/or Subscriber in an appropriate process. Furthermore, the TSP shall verify the attributes requested by the Subscriber to be included in the certificate and shall collect evidence providing the confirmation that the attributes are correct and allowed to be used for the Subject. For this the TSP shall define what kind of evidences for the different attributes are allowed to be provided by the Subscriber.

3.2.1 Method to prove possession of private key

The TSP shall verify that the Subscriber have possession over the private key.

3.2.2 Authentication of organization identity

Any RA operating for the TSP under this CP shall implement a registration process that meets the requirements of the ETSI EN 319 411-1/2 and that authenticates the organization identity in accordance with these requirements.

3.2.3 Authentication of individual identity

If applicable for a given certificate application, the RA shall identify the representative individual of the Subscriber.

The identification process for a natural person shall be performed by physical process or by recognized equivalent identification process.

3.2.4 Non-verified Subscriber information

All Subject and/or Subscriber information required shall be duly verified. Additional information given by the Subscriber may be ignored.

3.2.5 Validation of authority

Any RA operating for the TSP under this CP shall implement a registration process that meets the requirements of the ETSI EN 319 411-1/2 and that verifies authorization for use of the organization identity in accordance with these requirements.

3.2.6 Criteria for interoperation

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

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The Subject and/or Subscriber shall be identified by the SwissSign RA using valid identity information and evidences from the original request, in case they are not changed.

The validity period for the data included in a the certificate shall be limited within an appropriate period. After this period (determined by the date on the substantiating documentation provided), the data provided in the certificate as well as provided evidences shall be validated again.

3.3.2 Identification and authentication for re-key after revocation

The TSP shall not allow re-keying of certificates issued by this CA after revocation.

3.4 Identification and authentication for revocation request

The TSP shall define how the Subject and/or Subscriber is identified to be authorized to request revocation of the certificate.

4. Certificate Life-Cycle Operational Requirements

Refer to clause 6.2 and 6.3 of ETSI EN 319 411-1/2 [4]/[5].

4.1 Certificate application

4.1.1 Who can submit a certificate application

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.1.2 Enrollment process and responsibilities

The RA must establish an enrollment process that meets the requirements of ETSI EN 319 411-1/2 [4]/[5].

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The RA shall describe how the data information and evidences are verified during the registration process.

4.2.2 Approval or rejection of certificate applications

The RA shall approve a certificate request only if the identity and all attributes as well as authorization are verified successfully according ETSI EN 319 411-1/2. Otherwise the RA shall reject the certificate request.

4.2.3 Time to process certificate applications

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA shall prove the integrity and authenticity of the approved CSR before issuance of the certificate.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.4.2 Publication of the certificate by the CA

The TSP shall publish certificates only with the consent of the Subject and/or Subscriber.

4.4.3 Notification of certificate issuance by the CA to other entities

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.4.4 Certificate Transparency

Not applicable for this policy.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

4.5.2 Relying Party public key and certificate usage

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

4.6 Certificate renewal

Certificate renewal shall not be supported.

4.7 Certificate re-key

Certificate re-key may be supported.

4.7.1 Circumstance for certificate re-key

The TSP shall define under which circumstance a certificate re-key is allowed.

4.7.2 Who may request certification of a new public key

The TSP shall define who is authorized to request a certificate re-key.

4.7.3 Processing certificate re-keying requests

The TSP shall define the process of processing a certificate re-key request.

4.7.4 Notification of new certificate issuance to Subscriber

The same stipulations as for initial certificate issuance shall apply.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The same stipulations as for initial certificate issuance shall apply.

4.7.6 Publication of the re-keyed certificate by the CA

The same stipulations as for initial certificate issuance shall apply.

4.7.7 Notification of certificate issuance by the CA to other entities

The same stipulations as for initial certificate issuance shall apply.

4.8 Certificate modification

Certificate modification shall not be supported.

4.9 Certificate revocation and suspension

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.1 Circumstances for revocation

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

4.9.2 Who can request revocation

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.3 Procedures for revocation request

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

4.9.3.1 Notification about revocation

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

4.9.4 Revocation request grace period

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.5 Time within which CA must process the revocation request

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.6 Revocation checking requirement for Relying Parties

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.7 CRL issuance frequency

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.8 Maximum latency for CRLs

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.9 On-line revocation/status checking availability

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.10 On-line revocation checking requirements

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.11 Other forms of revocation advertisements available

The TSP may have other forms of revocation advertisements available.

4.9.12 Special requirements regarding key compromise

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.13 Circumstances for suspension

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.14 Who can request suspension

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.15 Procedure for suspension request

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.9.16 Limits on suspension period

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.10 Certificate status services

4.10.1 Operational characteristics

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.10.2 Service availability

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.10.3 Optional features

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

4.11 End of subscription

End of subscription shall occur after:

- successful revocation of the last certificate of a Subject and/or Subscriber,
- expiration of the last certificate of a Subject and/or Subscriber.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

4.12.2 Session key encapsulation and recovery policy and practices

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5. Facility, Management, and Operations Controls

The TSP shall set up technical, organizational and logical security controls that meet with the requirements of ETSI EN 319 411-1/2 [4]/[5].

The latest information on facility, management, and operations controls can be found in the TSPS [3] section 5.

5.1 Physical controls

5.1.1 Site location and construction

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.2 Physical access

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.3 Power and air-conditioning

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.4 Water exposure

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.5 Fire prevention and protection

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.6 Media storage

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.7 Waste disposal

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.1.8 Off-site backup

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.2 Procedural controls

5.2.1 Trusted roles

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.2.2 Number of persons required per task

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.2.3 Identification and authentication for each role

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.2.4 Roles requiring separation of duties

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.2 Background check procedures

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.3 Training requirements

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.4 Retraining frequency and requirements

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.5 Job rotation frequency and sequence

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.6 Sanctions for unauthorized actions

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.7 Independent contractor requirements

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.3.8 Documentation supplied to personnel

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4 Audit logging procedures

5.4.1 Types of events recorded

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.2 Frequency of processing log

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.3 Retention period for audit log

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.4 Protection of audit log

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.5 Audit log backup procedures

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.6 Audit collection system (internal vs. external)

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.7 Notification to event-causing Subject

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.4.8 Vulnerability assessments

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5 Records archival

5.5.1 Types of records archived

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5.2 Retention period for archive

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5.3 Protection of archive

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5.4 Archive backup procedures

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5.5 Requirements for time-stamping of records

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5.6 Archive collection system (internal or external)

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.5.7 Procedures to obtain and verify archived information

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.6 Key changeover

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.7.2 Computing resources, software and/or data are corrupted

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.7.3 Entity private key compromise procedures

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.7.4 Business continuity capabilities after a disaster

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

5.8 CA or RA termination

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6. Technical Security Controls

The TSP shall set up technical, organizational and logical security controls that meet with the requirements of ETSI EN 319 411-1/2 [4]/[5]. The latest information on the signature and encryption algorithms used can be found in the CPR [2].

Subscribers and relying parties shall use trusted computers and software.

These rules are described in chapter 6 of the respective CPS [1] that belongs to the certificate

6.1 Key pair generation and installation

Refer to clause 6.1 of SwissSign CPS [1].

6.1.1 Key pair generation

The Subscriber keys shall be generated only by the TSP.

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.1.2 Private key delivery to Subscriber

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.1.3 Public key delivery to certificate issuer

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.1.4 CA public key delivery to Relying Parties

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.1.5 Key sizes

Allowed key sizes shall be used as described in the Certificate Profile [2].

6.1.6 Public key parameters generation and quality checking

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

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

Allowed key usage as well as extended key usage shall be as described in the Certificate Profile [2].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

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

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.3 Private key escrow

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.4 Private key backup

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.5 Private key archival

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.6 Private key transfer into or from a cryptographic module

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.7 Private key storage on cryptographic module

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.8 Method of activating private key

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.9 Method of deactivating private key

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.10 Method of destroying private key

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.2.11 Cryptographic Module Rating

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.3.2 Certificate operational periods and key pair usage periods

The validity period of Subscriber certificates shall be as defined in the Certificate Profile [2].

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

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data used to protect private keys inside SwissSign-approved crypto devices shall be generated in accordance with the requirements of this CP. It must:

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

6.4.2 Activation data protection

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.4.3 Other aspects of activation data

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.5 Computer security controls

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.5.1 Specific computer security technical requirements

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

6.5.2 Computer security rating

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.6 Life cycle technical controls

6.6.1 System development controls

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

6.6.2 Security management controls

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.6.3 Life cycle security controls

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

6.7 Network security controls

No additional requirements on top of the ETSI EN 319 411-1/2 are defined.

6.8 Time-stamping

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

7. Certificate, CRL and OCSP Profiles

Refer to Clause 6.6 of ETSI EN 319 411-1/2 [4]/[5].

7.1 Certificate profile

The Certificate shall comply with the profile described in the Certificate Profile [2].

7.2 CRL profile

The CRL shall comply with the profile described in the Certificate Profile [2].

7.3 OCSP profile

The OCSP response shall comply with the profile described in the Certificate Profile [2].

8. Compliance Audit and Other Assessments

Refer to clause 6.7 of ETSI EN 319 411-1/2 [4]/[5].

8.1 Frequency or circumstances of assessment

The compliance audit shall be conducted annually.

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

8.2 Identity/qualifications of assessor

An independent qualified auditor shall conduct the compliance audits according to the stipulations of corresponding law, ZertES/VZertES and the applicable ESTI EN standards. The scope of the audit and reporting shall be fully in line with the rules set out before.

8.3 Assessor's relationship to assessed entity

The independent and qualified auditors shall conduct the compliance audits according to the stipulations of ETSI standards and ZertES/VZertES. The qualified auditors shall have the right to withdraw the certification of the TSP if a compliance audit reveals a severe deficiency in the operation of the TSP.

8.4 Topics covered by assessment

The auditor shall choose the control objectives that are to be covered by the assessment in accordance with ETSI EN 319 401 [6], ETSI EN 319 411-1 [4] and ETSI EN 319 411-2 [5].

Internal audits shall be performed regularly. Objective evidence as generated by the internal audit shall be covered by the annual assessment of the qualified auditor.

8.5 Actions taken as a result of deficiency

No additional requirements on top to the ETSI EN 319 411-1/2 are defined.

8.6 Communication of results

The results of the compliance audit shall be communicated to SwissSign executive management in a timely manner along with an action plan regarding issues to be addressed.

Within 30 days of presenting the action plan, The TSP shall publish a summarized result of the compliance audit on the SwissSign web site.

9. Other Business and Legal Matters

Refer to Clause 6.8 of ETSI EN 319 411-1/2 [4]/[5].

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

The TSP may charge a fee according to their pricing policy.

9.1.3 Revocation or status information access fees

The TSP shall not charge for certificate revocation and the provision of certificate status information.

In case of special SLA requested by the Subscriber, the TSP may charge the provision of the certificate status information for the specific SLA.

9.1.4 Fees for other services

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

9.1.5 Refund Policy

The TSP may establish a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

The amount of insurance coverage of the TSP shall meet the requirements of Article 3 para. 1 ZertES and VZertES Article 2.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

It shall be the sole responsibility of Subscribers and Relying Parties to ensure an adequate insurance, to cover risks using the certificate or rendering respective services, according to the ZertES/VZertES and respectively ETSI EN 319 411-1/2.

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

The TSP shall comply with the Swiss Data Protection Law.

The TSP is processing only such identification data which are adequate, relevant and not excessive to grant access to that service.

9.4 Privacy of personal information

The TSP shall comply with the Swiss Data Protection Law. Information and data can be used where needed for professional handling of the services provided herein. Subscribers and other third parties shall comply with the privacy standards of the TSP.

9.4.1 Privacy Plan

The stipulations of chapter 9.3 and 9.4 apply.

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

Participants that receive private information shall secure it from compromise and refrain from using it or disclosing it to third parties.

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

All intellectual property rights of the TSP including all trademarks and all copyrights shall remain the sole property of SwissSign AG.

Certain third party software may be used by the TSP in accordance with applicable license provisions

9.6 Representations and warranties

9.6.1 CA representations and warranties

The TSP shall comply with all provisions stated in this CP, ZertES/VZertES, and related regulations and rules.

9.6.2 RA representations and warranties

All registration authorities shall comply with all provisions stated in this CP, ZertES/VZertES, and related regulations and rules.

9.6.3 Subscriber representations and warranties

Subscribers shall comply with all provisions stated in this CP, ZertES/VZertES, and related regulations and rules.

9.6.4 Relying Party representations and warranties

Relying Parties shall comply with all provisions stated in this CP, ZertES/VZertES, and related regulations and rules.

9.6.5 Representations and warranties of other participants

Any other participant shall comply with all provisions stated in this CP, ZertES/VZertES, and related regulations and rules.

9.7 Disclaimers of warranties

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

9.8 Liability

9.8.1 Liability of the TSP

The TSP shall only be liable for damages which are the result of SwissSign's failure to comply with this CP and which were provoked deliberately or wantonly negligent.

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

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

9.8.2 Liability of the Subscriber

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

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This Certificate Policy and respective amendments shall become effective as they are published on the SwissSign website at “http://repository.swisssign.com”.

9.10.2 Termination

This CP shall cease to have effect when a new version is published on the SwissSign website.

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

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

The TSP may provide notices by email, postal mail, fax or on web pages unless specified otherwise in this CP.

9.12 Amendments

9.12.1 Procedure for amendment

Refer to Clause 1.5.4 of this CP.

9.12.2 Notification mechanism and period

Refer to Clause 1.5.4 of this CP.

9.12.3 Circumstances under which OID must be changed

The OID of this CP shall be change when the scope of this CP is changed.

9.13 Dispute resolution provisions

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

Complaints regarding the content or format of a certificate shall be submitted in writing or over the contact stated in this CP.

9.14 Governing law and place of jurisdiction

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

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

9.15 Compliance with applicable law

This CP and rights or obligations related hereto shall be in accordance with the relevant provisions of the ZertES/VZertES and of the other applicable laws. Compliance with the laws and regulations are verified within the annual external audit. The audits are carried out by an independent qualified auditor.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The following documents and the Subscriber-Agreement of the TSP shall state the agreement between the TSP and the Subject and/or Subscriber:

- TSPS [3]
- the CP, as indicated in the certificate
- the related CPS [1]

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

9.16.2 Assignment

The Subscriber shall not assign this agreement or its rights or obligations arising hereunder, in whole or in part.

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

9.16.3 Severability

In the case of a conflict between the ETSI EN 319 411-1/2 and the applicable law or national regulation (herein after law) of any jurisdiction in which the TSP operates or issues certificates, the TSP shall modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal according to national regulation.

This applies only to operations or certificate issuances that are Subject to that law. In such an event the TSP shall immediately and prior to the issuing of such certificates under the modified requirements include a detailed reference to the law requiring the modification. The specific modification implemented by the TSP shall be described in this chapter of the CP.

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

The TSP shall communicate an appropriate change within 90 days.

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

The TSP shall not be in default and the customer cannot hold the TSP responsible and/or liable for any damages that result from (but are not limited to) the following type of events: any delay, breach of warranty, or cessation in performance caused by any natural disaster, power or telecommunication outage, fire, unpreventable third-party interactions such as virus or hacker attacks, governmental actions, or labor strikes.

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

9.17 Other provisions

9.17.1 Language

If this CP, the related CPS, TSPS and their amendments are provided in additional languages to English, the English version shall prevail.

9.17.2 Delegated or outsourced Services

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

10. References

[1] SwissSign CPS Sign – Certificate Practice Statement for Signing Certificates, 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 v1.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements;

[5] ETSI EN 319 411-2 v2.3.1 (2021-05):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 v2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;

[7] 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

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

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

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

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