SwissSign Signing Services CP/CPS

Certificate Policy and Certification Practice Statement of the “SwissSign Signature Services Root 2020 - 2” and its subordinated issuing CA.

Document Type:	Certificate Policy and Certification Practice Statement
OID:	2.16.756.1.89.1.4.2.1
Author:	Information Security and Compliance
Classification:	C0 (public)
Applicability:	Global
Owner:	CEO
Issue Date:	09 April 2021
Version:	1.0
Obsoletes:	-
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Review: This document is reviewed periodically at least once per calendar year. The owner is responsible for this review.

Compliance: The “SwissSign Signature Services Root 2020 – 2” and its subordinated SwissSign Qualified Electronic Signature ICA operating under this CP/CPS and issuing certificates under this CP/CPS are fully compliant with ZertES, VZertES and all stipulations therein.

Version Control

Date	Version	Comment	Author
09.04.2021	1.0	First public version	Michael Günther

Authorization

Date	Approved by	Approved by	Version
09.04.2021	Michael Günther	Markus Naef	1.0 / OID = 1

Michael Günther (Qualified Signature)

Digital unterschrieben von Michael Günther (Qualified Signature)
Datum: 2021.04.09 12:02:37 +02'00'

digital signature

digital signature

Table of Contents

1. Introduction

Since 2001 SwissSign AG offers several trust services such as SSL and mail certificates to customers all over the world, with a focus on Switzerland and Europe.

This Trust Service Provider (TSP) document describes the Certificate Policy / Certification Practice Statement CP/CPS of the trust services provided by SwissSign AG. The structure of this document corresponds to RFC3647. Under this CP/CPS the TSP operates all Trust Services published under the root “SwissSign Signature Services Root 2020-2”.

This Root Certificate Authority is operated by SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Switzerland (“SwissSign Switzerland”) and only issue certificates to its subordinated issuing CA.The offered services are non-discriminatory. They respect the applying export regulations.

The TSP can outsource partial tasks to partners or external providers. The TSP, represented by the management or its agents, 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.

These subordinate CA comply with the Swiss Digital Signature Law, 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 (2018): General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI TS 119 312 (2019): Cryptographic Suites
- 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)
- 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 In this CP/CPS, “this CA” refers to the “SwissSign Signature Services Root 2020 - 2” and all it subordinated issuing CA, unless stated differently.

The certificates are classified with the following Policy OIDs:

- QCP-n-qscd

In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.1 Overview

This certificate policy and certification practice statement (CP/CPS) describes:

- The certification and registration policy of this CA.
- Practices and procedures of this CA.
- Practices and procedures of the registration authorities for this CA.
- Terms and conditions under which this CA is made available.

The documents above are available in their current and all previous versions on the https://repository.swissign.com website.

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

SwissSign AG provides a detailed product overview on the website (swisssign.com) for Signature Services Certificates and for other services.

The TSP does not have and does not issue any cross certificates for this CA.

1.2 Document name and identification

This document is named ”SwissSign Signature Services CP/CPS” as indicated on the cover page of this document.

The applicable CP/CPS for each certificate can be found in the certificate field "cpsURI" (see chapter 7).

The Object identification number (OID) for this and only this document is: OID 2.16.756.1.89.1.4.2.1

The last position of the OID represents the document version.

1.3 PKI participants

1.3.1 Certification authorities

The TSP operates a Public Key Infrastructure, consisting of a “SwissSign Signature Services Root 2020 - 2” and its subordinated issuing CAs as listed in this document..

1.3.2 Registration authorities

The TSP operates a registration authority, called “SwissSign RA” that registers Subscribers of certificates issued by this CA.

Third parties may operate their own Registration Authority services, if these third parties abide by all the rules and regulations of this CP/CPS.

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

- The RA must have a contractual agreement with the TSP which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities.
- The registration process must meet the stipulations of Swiss Digital Signature Law. It must be documented, published, and distributed to all parties involved in the RA process.
- The RA must be certified according to Swiss Digital Signature Law. The RA must pass an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit may lead to the revocation of RA privileges.
- The information collected during the RA process is subject to applicable data protection regulations. Compliance with these provisions must be demonstrated (Chapters 9.3 and 9.4).

1.3.3 Subscribers

In the context of this CP/CPS, the term “Subscriber” encompasses all end users of certificates issued by this CA:

- Requesters are individuals or organizations that have requested (but not yet obtained) a certificate.
- Subscribers are individuals or organizations that have obtained a certificate.

Subscribers and Requesters are responsible for:

- having a basic understanding of the proper use of public key cryptography and certificates,
- providing only correct information without errors, omissions or misrepresentations,
- substantiating information by providing a properly completed registration form as specified in chapter 3.2,
- supplementing such information with a proof of identity and the provision of the information as specified in chapter 3.1 and 3.2,
- using a secure, and cryptographically sound key pair on a crypto device provided or approved by the registration authority,
- maintaining the crypto device unmodified and in good working order, if it is not a remote signature device,
- verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information,
- reading and agreeing to all terms and conditions of this CP/CPS, other relevant regulations and agreements,
- reading and agreeing to the general terms and conditions of the requested product,
- the maintenance of their certificates using the tools provided by the registration authority,
- deciding on creation of a certificate whether the respective certificate is to be published in the public directory: directory.swisssign.net,
- using SwissSign certificates exclusively for lawful and authorized purposes,
- ensuring that SwissSign certificates are exclusively used on behalf of the person or the organization specified as the subject of the certificate,
- protecting the private key from unauthorized access,
- using the private key only in secure computing environments that have been provided by trustworthy sources and that are protected by state-of-the-art security measures,
- ensuring complete control over the device containing the authentication means with the capability of generating activation data by not entrusting any person other than the certificate owner himself with the safekeeping of this device and data,

- notifying the registration authority of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate,
- revoking the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances makes the information in the certificate misleading or inaccurate,
- notifying the registration authority immediately of any suspected or actual compromise of the private key and requesting that the certificate be revoked,
- immediately ceasing to use the certificate upon (a) expiration or revocation of such a certificate, or (b) any suspected or actual damage/corruption or (c) any suspected or actual compromise of the private key corresponding to the public key in such a certificate, and immediately removing such a certificate from the devices and/or software onto which it has been installed,
- if the certificate or the corresponding issuing or root certificate has been revoked by the TSP, the TSP will inform the Subscriber who shall no longer use the certificate.
- refraining to use the Subscriber's private key that corresponds to the public key certificate to sign other certificates,
- using their own judgment about whether it is appropriate, given the level of security and trust provided by a certificate issued by this CA, to use such a certificate in any given circumstance,
- using the certificate with due diligence and reasonable judgment,
- complying with all laws and regulations applicable to a Subscriber's right to export, import, and/or use a certificate issued by this CA and/or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.
- submitting applications in form of either paper or electronic documentation which shall include the declaration of consent with the applicable legal documents such as:
    - PKI Disclosure Statement
    - Subscriber Agreement
    - Terms and Conditions under which this CA is made available.

1.3.4 Relying Parties

Relying Parties are individuals or organizations that use certificates of this CA to validate the signatures and verify the identity of Subscribers and/or to secure communication with these Subscribers. Relying Parties are allowed to use such certificates only in accordance with the terms and conditions set forth in this CP/CPS. It is in the sole responsibility of the Relying Party to verify revocation status, legal validity, transaction limits and applicable policies.

Relying Parties can also be Subscribers within this CA.

1.3.5 Other participants

Not applicable

1.4 Certificate usage

1.4.1 Appropriate certificate uses

(QCP-n-qscd) Qualified Electronic 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

The SwissSign Trust Service Practice Statement 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 Board of Directors of SwissSign AG determines the suitability of this CP/CPS document.

Changes or updates to relevant documents must be made in accordance with the stipulations of Swiss Digital Signature Law and the provisions contained in this CP/CPS and are therefore subject to review by the organization appointed by SAS.

1.5.4 CP/CPS approval procedures

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

1.6 Definitions and acronyms

Note: Aus der TSPS (gültig für alle Zertifikate). Es wird kein angepasstes Kapitel 1.6 mehr geben

Term	Abbrev.	Explanation
Advanced Digital Signature		A digital signature that can be associated with the owner and enables his identification. It is created using means that are under the sole control of the owner and makes any modification of the associated set of data obvious.
Algorithm		A process for completing a task. An encryption algorithm is merely the process, usually mathematical, to encrypt and decrypt messages.
Attribute		Information bound to an entity that specifies a characteristic of that entity, such as a group membership or a role, or other information associated with that entity.
Authentication		The process of identifying a user. User names and passwords are the most commonly used methods of authentication.
Baseline Requirements Guidelines	BRG	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

Term	Abbrev.	Explanation
Certification Authority Authorization	CAA	RFC 6844 defines a Certification Authority Authorization DNS Resource Record (CAA). A CAA allows a DNS domain name holder to specify the CAs authorized to issue certificates for that domain. Publication of the CAA gives domain holders additional controls to reduce the risk of unintended certificate misissuance.
CA Operator	CAO	A person responsible for CA operation, including establishment of certificate parameters for RA and RAO in accordance with certificate policy.
Certificate		Information issued by a trusted third party, often published in a directory with public access. The certificate contains at least a subject, a unique serial number, an issuer and a validity period.
Certification Authority	CA	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certification Authority Authorization	CAA	RFC 6844 defines a Certification Authority Authorization DNS Resource Record (CAA). A CAA allows a DNS domain name holder to specify the CAs authorized to issue certificates for that domain. Publication of the CAA gives domain holders additional controls to reduce the risk of unintended certificate miss issuance.
Certificate Extension		Optional fields in a certificate.
Certificate Policy	CP	A set of rules that a request must comply with in order for the RA to approve the request or a CA to issue the certificate.
Certificate Profile		A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software. Please see clause 7.1 of this Document.
Certification Authority Revocation List	CARL	Revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer
Certificate Revocation List	CRL	List of certificates that have been declared invalid. This list is issued by the CA at regular intervals and is used by applications to verify the validity of a certificate.
Certification Practice Statement	CPS	Document that regulates the rights and responsibilities of all involved parties (RA, CA, directory service, end entity, Relying Party).
Certification Service Provider	CSP	Individual or corporation that issues certificates to individual or corporate third parties.
Cipher		A cryptographic algorithm used to encrypt and decrypt files and messages.
Cipher Text		Data that has been encrypted. Cipher text is unreadable unless it is converted into plain text (decrypted) with a key.
Chief Security Officer	CISO	the senior-level executive within the TSP responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.
Coordinated Universal Time	UTC UTC(k)	Mean solar time at the prime meridian (0°). The time scale is based on seconds as defined in ETSI EN 319 421. Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.
Credentials		Evidence or testimonials governing the user's right to access certain systems (e.g. User name, password, etc.)
Certificate Transparency	CT	Is an experimental IETF open standard (RFC 6962) and open source framework for monitoring and auditing digital certificates. Through a system of certificate logs, monitors, and auditors, certificate transparency allows website users and domain owners to identify mistakenly or maliciously issued certificates and to identify certificate authorities (CAs) they issued such certificates.
Decryption		The process of transforming cipher text into readable plain text.

Term	Abbrev.	Explanation
DES		Data Encryption Standard. A cipher developed by the United States government in the 1970s as the official encryption algorithm of the U.S.
Digital signature		A system allowing individuals and organizations to electronically certify features such as their identity or the authenticity of an electronic document.
Directive No 910/2014 /EC		European digital signature law: Directive No 910/2014 /EC of the European Parliament and of the Council of 23 July 2014 on a community framework for electronic signatures. Compliance with this law always implies compliance with the following standards: ETSI EN 319 401, 319 411-1, 319 411-2, policy QCP-n-qscd
Distinguished Name	DN	-> Subject
DNS		Domain Name System. The Internet system of holding a distributed register of entity names. For example, the domain is the part of the email address to the right of the `@', e.g. `anytown.ac.uk'.
Electronic Signature		-> Digital Signature
Encryption		Encryption is the process of using a formula, called an encryption algorithm, to transform plain text into an incomprehensible cipher text for transmission.
End Entity		Used to describe all end users of certificates, i.e. Subjects and Relying Parties.
Subscriber Agreement	EUA	Contractual agreement between seller of certificates and the Subscriber.
Enterprise EV Certificate		An EV certificate that an enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original valid EV certificate issued to the enterprise RA.
Entropy		A numerical measure of the uncertainty of an outcome. The entropy of a system is related to the amount of information it contains. In PKI and mathematics, a cryptographic key contains a certain amount of information and tends to lose a small amount of entropy each time it is used in a mathematical calculation. For this reason, one should not use a key too frequently or for too long a period.
EV Certificate		A digital certificate that contains information specific in the EV guidelines and that has been validated in accordance with the guidelines.
Extended Validation	EV	Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.
Extension		-> Certificate Extension
FIPS 140		FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules.
FQDN	FQDN	Fully Qualified Domain Name.
FTA	FTA	Federal Tax Administration (Eidgenössische Steuerverwaltung, ESTV)
General Data Protection Regulation	GDPR	The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union.
Hardware Security Module	HSM	Hardware Security Module is a device that physically protects key material against unauthorized parties.
HTTP	HTTP	Hyper-Text Transfer Protocol used by the Internet. HTTP defines how data is retrieved or transmitted via the Internet and what actions should be taken by web servers and browsers.
HTTPS	HTTPS	Secure Hyper-Text Transfer Protocol using TLS/SSL
Key		The secret input for cryptographic algorithms that allows a message to be transformed. -> See Private Key, Public Key

Term	Abbrev.	Explanation
Key password		Password used to encrypt the private key.
Key size		Length of private and public key. Regular key sizes are 512, 768, 1024, 2048, 3072 and 4096.
Key usage		Key's intended purpose. This information is stored in the certificate itself to allow an application to verify that the key is intended for the specified use.
Leaf-certificate		A certificate issued under this TSPS that is not a CA Certificate.
Lightweight Directory Access Protocol	LDAP	LDAP is used to retrieve data from a public directory.
LDAP Secure	LDAPS	LDAP secured with TLS/SSL
Man-in-the-middle	MITM	Active eavesdropping of secure communications in which attacker/third party relays and controls messages between sender and receiver.
Online Certificate Status Protocol	OCSP	Method to verify the validity of a certificate in real time.
Participants		Entities like CAs, RAs, and repositories. These can be different legal entities.
PKCS		PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Laboratories.
Plain Text		The original message or file.
Privacy Level		Used to determine how the certificate can be accessed in the directory. Private, Public Lookup and Public Download are the available levels.
Private Key		One of two keys used in public key cryptography. The private key is known only to the owner and is used to sign outgoing messages or decrypt incoming messages.
Profile		A user profile is a personal area where end users can access and manage their digital identities and requests directly on the TSP web page. Access to this profile can be granted by means of user name and password.
Public Key		One of two keys used in public key cryptography. The public key can be known to anyone and is used to verify signatures or encrypt messages. The public key of a public-private key cryptography system is used to verify the “signatures” on incoming messages or to encrypt a file or message so that only the holder of the private key can decrypt the file or message.
Public Key Infrastructure	PKI	Processes and technologies that are used to issue and manage digital identities that may be used by third parties to authenticate individuals or organizations.
Qualified Certificate	QC	Certificate which meets the requirements of ETSI EN 319 411-1/2 and article 8 ZertES.
Qualified Certificate Policy	QCP	Certificate policy which incorporates the requirements laid down in ETSI EN 319-401 and ETSI EN 391 411-2.
Qualified Digital Signature		Qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures, as defined in article 3 (12) of the Directive No 910/2014 and in ZertES article 2 e
RA Operator	RAO	The person responsible for identifying the requester, collecting the identity substantiating evidence, authorizing the CSR, and forwarding the authorized CSR to the CA.
Recognition Body		The Recognition Body of Switzerland is accredited by the SAS and conducts the audits prescribed by Swiss Digital Signature Law.
Recognized Qualified Digital Signature		Qualified digital signature created with a certificate issued by a CA that has successfully been certified by a Swiss recognition body.

Term	Abbrev.	Explanation
Registration Authority	RA	A registration authority (RA) verifies the identity of entities requesting their digital certificates and tells the Certificate Authority (CA) to issue it.
Relying Party		Recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate.
Revocation		Invalidation of a certificate. Every CA regularly issues a list of revoked certificates called CRL. This list should be verified by all applications using certificates from that CA before trusting a certificate.
Rollover		To rollover a certificate means that a new certificate is issued while the old one is still valid and usable. The rollover is used to issue a new CA certificate while keeping the old one valid along with all the certificates issued with it.
RSA		A public key encryption algorithm named after its founders: Rivest-Shamir-Adleman.
S/MIME		Secure / Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail.
Secure Signature Creation Device	SSCD	Signature-creation device which meets the requirements specified in article 30 of Directive No 910/2014 /EC.
Smart-card		Credit Card or SIM-shaped carrier of a secure crypto processor with tamper-resistant properties intended for the secure storage and usage of private keys.
Signature		Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
Signature-creation data		Unique data, such as parameters of signature algorithms or private cryptographic keys, used by the signatory to create an electronic signature.
Signature-creation device		Configured software or hardware used to implement the signature-creation data
Signature-verification data		Data, such as parameters of signature algorithms or public cryptographic keys, used for the purpose of verifying an electronic signature.
SSO		Single Sign On: The user only needs to log in once to access various services.
Subject		Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
Subscriber		Legal or natural person bound by agreement with a trust service provider to any subscriber obligations.
TAV-BAKOM		Amendment to VZertES, technical and administrative directives on the issuance of digital signatures, issued November 23th, 2016. SR 943.032.1.
Time-stamping Authority	TSA	Authority which issues time-stamp tokens.
TLS		Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). A protocol that enables secure transactions via the Internet. URLs that require an TLS connection for HTTP start with https: instead of http:.
TSP	TSP	Trust Service Provider
Time-stamp Policy	TP	Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements.
Time-stamp Token	TST	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time-stamping Unit		Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.

Term	Abbrev.	Explanation
Traffic management		Management and surveillance of network traffic with domain names or IPs owned or controlled by third parties.
TSA Disclosure statement		Set of statements concerning the policies and practices of a TSA that require emphasis or disclosure to Subscribers and Relying Parties, for example, to meet regulatory requirements.
TSA practice statement	TPS	Statement of the practices that a TSA employs in issuing time-stamp tokens.
TSA system		Composition of IT products and components organized to support the provision of time-stamping services.
Transaction Limit		The transaction limit is detailing liability limits of the TSP, the Subscriber and Relying Parties. This limit is published in the respective certificate.
Triple DES		A method of improving the strength of the DES algorithm by using it three times in sequence with different keys.
Two-factor authentication		Two-factor authentication (also known as 2FA or 2-Step Verification) is a method of confirming a user's claimed identity by utilizing a combination of two different components.
Unique identification number	UID	The UID is an unique organization number, e.g. the number of the commercial register entry or the VAT number or a number assigned by SwissSign.
Uniform Resource Locator	URL	The global address of documents and other resources on the WWW, e.g. http://swisssign.net. The first part indicates the protocol to be used (http) and the second part shows the domain where the document is located.
USB Token		Secure crypto processor that appears like a common USB memory stick. It has tamper resistant properties and is intended for the secure storage and usage of private keys.
VZertES		Swiss directive for digital signatures, issued November 23th, 2016. SR 943.032.
ZertES		Swiss Digital Signature Law. Issued March 18, 2016. SR 943.03. Compliance with this law always implies adherence to VZertES and TAV-BAKOM.

2. Publication and Repository Responsibilities

The TSP makes its certificates, CP/CPS, CRL and related documents for this CA publicly available through the swisssign.com or swisssign.net web sites. To ensure both integrity and authenticity, all documents are digitally signed. To document the validity period of the document, a version history is included.

2.1 Repositories

The TSP publishes all current and past documentation on https://repository.swisssign.com (available 24h a day / 7 days a week).

The TSP publishes root certificates and CA certificates as well as Certificate Revocation Lists on https://www.swisssign.com/support/ca-prod.html

The TSP publishes information regarding public subscriber certificates in an LDAP directory (ldap://directory.swisssign.net:389/o=SwissSign,c=CH)

These web sites are the only source for up-to-date documentation. SwissSign AG reserves the right to publish newer versions of the documentation without prior notice.

2.2 Publication of certification information

Changes to the policies can be communicated to third parties via RSS feed, where applicable. Assessment bodies, supervisory or other regulatory bodies are informed via e-mail about changes on the policy documents.

For this CA, the TSP publishes an approved, current and digitally signed version of:

- the certificate policy and certification practice statement (CP/CPS)
- PKI Disclosurer Statement (PDS)
- End User Agreement / Subscriber Agreement (EUA)
- Nutzungsbedingungen SwissID Sign
- Relying Party Agreement (RPA)

The TSP publishes information related to certificates issued by this CA on the swisssign.net web site. The swisssign.net web site and the LDAP directory directory.swisssign.net are the only authoritative sources for:

- All publicly accessible certificates issued by this CA.
- The certificate revocation list (CRL) for this CA. The CRL may be downloaded from the swisssign.net web site. The exact URL is documented in every certificate that is issued by this CA or its subordinated issuing CA in the field: “CRL Distribution Point”. For details, please refer to chapter 7.

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

2.3 Time or frequency of publication

SwissSign AG will publish the most current version and all superseded versions of the following publications on its web site:

The SwissSign Signature Services CP/CPS is reviewed at least once a year. Even if no updates are required, a new version is published.

The TSP publishes this information on a regular schedule:

- CRLs are published according to the schedule detailed in chapter 4.10.7.
- 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

The LDAP, CRL and OCSP information is managed in a database system. All access to the data in this database system is managed through the swisssign.net web interface and requires sufficient authorization. The type of authorization required depends on how the process is executed.

This CP/CPS is provided as public information on the swisssign.com web site. Public documents are only valid if they are published as a PDF with the digital signatures of two officers of SwissSign AG.

Management access always requires two factor authentication.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) in a certificate issued by this CA complies with the X.509 standard and with RFC 5280.

For the distinguished name, a minimum of one field is required. This field must be /CN=.

To ensure uniqueness of the distinguished name, a unique identifier associated with the subscriber must be added as serialNumber (OID: 2.5.4.5)

For the common name (CN), SwissSign allows two types of names to be specified:

- given name(s) and surname,
- pseudonyms

Real names are specified as /CN='given name(s)' 'surname'.

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

Pseudonyms are specified as /CN='identifier': 'arbitrary string'. The SwissSign RA requires pseudonym certificates to use the string 'pseudo' as identifier. An example of a correctly formulated pseudonym is: "/CN=pseudo: John Doe". Other registration authorities may use other identifiers. The pseudonym may be added as /pseudonym (OID: 2.5.4.65)

The use of names in the /CN field must be authorized. This means:

- The use of a real name and its identifying information must be authenticated and authorized according to chapter 3.2.3.
- A pseudonym requires that the requester authenticates and authorizes the request containing identifying information according to chapter 3.2.3.

SubjectAltName is an optional field for certificates issued with real names or pseudonyms. If it is present, it contains at least an email address.

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

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of Subscribers

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

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

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

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

The TSP and its RAs reserve the right to reject certificate requests or revoke certificates containing offensive or misleading information or names protected by legislation and infringing rights of others. However, SwissSign AG and its registrations authorities are not obliged to verify lawful use of such names. SwissSign AG and its registrations authorities reserve the right to decline any request for anonymity or pseudonymity. Anonymous or pseudonymous common names are available on a "first come, first served" basis. Chapter 3.1.6 applies.

Other registrations authorities may use different identifiers to identify pseudonym certificates, if they meet the following requirements:

- The TSP has approved the identifier.
- The identifier and the resulting /CN= values are neither incorrect nor misleading.

- The identifier is alphabetical and can be used with the <identifier><colon><space> formatting.

3.1.4 Rules for interpreting various name forms

For all attributes in the distinguished name that are specified as UTF8 string, 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 issued under this CP/CPS enforce the uniqueness of certificate subject fields in such a manner that all certificates with identical subject fields must belong to the same individual or organization. The following rules are enforced:

- All certificates for individuals with identical subjects must belong to the same individual. This explicitly includes possession of revoked or expired certificates.
- To ensure uniqueness of the distinguished name, a unique identifier associated with the subscriber must be added as serialNumber (OID: 2.5.4.5)

3.1.6 Recognition, authentication, and role of trademarks

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

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

3.1.7 Test Certificates

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

3.2 Initial identity validation

The initial identity validation is part of the Certificate Application process as described in chapter 4.1. Existing evidences can be re-used to validate the identity depending on the validity of the evidence and on the product to be issued.

Other RA's may implement a different process that complies to the stipulations under chapter 4.1.2.

3.2.1 Method to prove possession of private key

The registration authorities operating under this CP/CPS must adhere to the stipulations of Swiss digital signature law and ensure possession of private key generated by:

SwissSign RA: The key pair is generated on a QSCD (HSM). Control over the user’s private keys on HSM is granted to the subscriber through authentication means fulfilling the requirements of ETSI EN 319 411-1 and SCAL2 of CEN EN 419241-1. Authentication means are created on a device provided by the subscriber during registration. The registration process verifies that the device fulfills the requirements posed on the authentication means.

3.2.2 Authentication of organization identity

This CA does not support use of organization names.

3.2.3 Authentication of individual identity (QCP-n-qscd)

Various individuals may need to authorize the use of names in different parts of the DN. The registration process of any registration authority operating under this CP/CPS must contain provisions to determine the identity of such individuals. To achieve this goal, all individuals must be identified according to the requirements of ETSI EN 319 411-1 and ETSI EN 319 411-2. The regulations defined in the registration forms may be summarized as follows:

- The registration form must carry original, personal handwritten signatures or it must be supplied electronically and digitally signed using a qualified certificate.

- The information on the identifying document must match the name on the registration form. In case the registration form carries the original, personal handwritten signature, this signature and the signature on the identifying document must also match.
- The wording in the request has to match the given name(s) and the family name of the identifying documents (see 3.1.1).
- The requester must present a valid original of an official identification document as recognized by ETSI EN 319 411-1.
- The requester must be present in person or in an equivalent procedure according to ETSI EN 319 411-1 6.2.2 and ZertES Art. 9. This step may be conducted by:
    - The registration authority processing the certificate request.
    - An accredited notary.
    - A trained and contracted partner for the identification service.
- The identifying agent is to make a high-quality copy, scan or photograph of the identifying document and to confirm proper execution of the identification in writing or electronically as agreed with the TSP.
- The photo in the identifying document is compared to and has to match (facial features, age, gender and size) the requester present as described above.

3.2.4 Non-verified subscriber information

All subscriber information required by the choosen certificate type is duly verified. Additional information given by the subscriber can be ignored.

3.2.5 Validation of authority

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.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

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

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

Revocation of a certificate that is issued by this CA requires that the Subscriber is authenticated according to one of the following methods:

- Through the revocation dialog after successful login to the SwissID profile.
- With a personal handwritten signature or a recognized qualified electronic signature according to ZertES regulation on a revocation form.
- Appearance in person at the registration authority.
- Providing a one-time revocation key on the web site of the registration authority.

Not all registration authorities must support all methods of revocation.

The process how the revocation request can be submitted is described in chapter 4.10.3.

4. Certificate Life-Cycle Operational Requirements

Each certificate issued by the TSP is securely stored in a database and has a unique reference to the certificate application data. If the TSP offers a certificate renewal, the data contained in the certificate are being used.

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, CP/CPS and relevant End-User Agreement. The applicable legal documents (Terms and Conditions, CP/CPS) are displayed to the subscriber during the application process.

4.1.2 Enrollment process and responsibilities

The registration authority must establish an enrollment process that meets the requirements of ETSI EN 319 411-1 and ETSI EN 319 411-2.

The RA has a valid contract with the TSP.

The 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.

The RA collects the following during its enrollment process:

- identity of the requester and of all persons authorizing the certificate request according to chapter 3.2.3,
- type of document(s) presented by the applicant to support registration,
- 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,
- name of receiving TSP and/or submitting RA.

The RA collects and verifies all the required documentation according to chapter 3.2.3.

The RA collects references to the following during its enrollment process to ensure sole control of the subscriber over the subscriber key pair:

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

Only if the RA fulfills these requirements it will be a trusted RA within the TSP.

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 CP/CPS and End-User Agreement have been accepted by the subscriber,
- all documents and information are approved by the SwissSign RA,
- SwissID authentication means are linked to the user profile,
- A Subscriber key pair is generated by the TSP,
- SIC authentication means are linked to the subscriber key pair.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

4.2.2 Approval or rejection of certificate applications

The RA will approve a certificate request if all of the following criteria are met:

- the requester 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,
- the requester has proven control over the SwissID and SIC authentication means.

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

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

4.2.3 Time to process certificate applications

RAs must design their processes in such fashion that the processing of a regular, fully documented certificate request takes no longer than two business days.

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

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

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

On successful verification, the CA will then issue the requested certificate and communication between RA and CA is via a secure channel.

4.3.2 Notification to Subscriber by the CA of issuance of certificate

The CA may notify the requester in different ways:

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

The CA may:

- email the certificate to the Subscriber,
- electronically provide the certificate to the requesting RA,
- email information permitting the Subscriber to download the certificate from a web site,
- email information permitting the RA to download the certificate from a web site.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Subscribers are not required to confirm the acceptance of the certificate.

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

4.4.2 Publication of the certificate by the CA

The Requester agrees that SwissSign AG 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.

4.5 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 1.3.3, summarized as follows:

- Qualified certificates can be used for qualified electronic signatures .
- Subscribers may only use a SwissSign certificate on behalf of the person listed as the subject of such a certificate.

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 CP/CPS and the End-User Agreement for Relying Parties,
- verify certificates issued by this CA, including use of revocation information, in accordance with the certification path validation procedure, taking into account any critical certificate extensions,
- 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,
- verify the transaction limit provided in the aforementioned certificate,
- comply with all laws and regulations applicable to a Relying Party's right to export, import, and/or use a certificate issued by this CA and/or related information. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.

4.6 Certificate renewal

Certificate renewal is not supported.

4.7 Certificate reissuance

Certificate reissuance is not supported.

4.8 Certificate re-key

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

4.8.1 Circumstance for certificate re-key

Fehler! Verweisquelle konnte nicht gefunden werden. The Subscriber may choose to re-key a certificate if the following conditions are met:

- The Subscriber owns a currently valid certificate from this CA.
- All information in the certificate is still correct.
- The verification of the identity is still within the time period allowed by legal and regulatory requirements governing this type of certificate.

4.8.2 Who may request certification of a new public key

Fehler! Verweisquelle konnte nicht gefunden werden. Re-key may be requested by the Subscriber. To-re-key a qualified certificate, Swiss Digital Signature law requires the Subscriber to digitally sign the renewal request with the certificate to be re-keyed.

4.8.3 Processing certificate re-keying requests

Fehler! Verweisquelle konnte nicht gefunden werden. The process of the application for re-key request will be conducted as follows:

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

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

• If any data has changed, the re-key application is treated as an initial certificate application. The applicable legal documents

(Terms and Conditions, CP/CPS) are communicated to and agreed by the subscriber during the re-key process.

4.8.4 Notification of new certificate issuance to Subscriber

The same stipulations as for certificate renewal apply, see **Fehler! Verweisquelle konnte nicht gefunden werden.**. The same stipulations as for initial certificate issuance apply, see 4.3.2.

4.8.5 Conduct constituting acceptance of a re-keyed certificate

Fehler! Verweisquelle konnte nicht gefunden werden. The same stipulations as for initial certificate issuance apply, see 4.4.1.

4.8.6 Publication of the re-keyed certificate by the CA

Fehler! Verweisquelle konnte nicht gefunden werden. The same stipulations as for initial certificate issuance apply, see 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

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

4.9 Certificate modification

The TSP does not support certificate modification.

4.10 Certificate revocation and suspension

The procedures of the TSP meet the requirements of ETSI EN 319 411-1. Certificate revocation is irreversible. Once a certificate has been revoked, the certificate can not be valid again, which is technically enforced by the CA.

Subscribers or Relying Parties are requested to apply for certificate revocation immediately if there is a suspicion that private keys have been compromised or the content of the certificate is no longer correct.

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

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

4.10.1 Circumstances for revocation

Subscribers may revoke their certificates at will.

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

- The Subscriber requests in writing that the CA revoke the certificate
- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization
- The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise
- The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.The private key of the issuing CA or any of its superior CAs has been compromised.

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

- The certificate issued does not comply with the terms and conditions of this CP/CPS.
- The CA obtains evidence that the Certificate was misused
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use and/or other applicable laws, rules and regulations. In addition, The TSP may investigate any such incidents and take legal action if required.

- The CA is made aware of a material change in the information contained in the Certificate, e.g.
    - Any part of the certificate subject has changed.
    - The certificate /CN= field is no longer valid (e.g. name change due to change in marital status or omission of domain registration renewal).
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement
- The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository
- The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed.

The CA must revoke 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 CP/CPS.
- The Issuing CA obtains evidence that the Certificate was misused.
- The Issuing CA is made aware that the Certificate was not issued in accordance with this CP/CPS.
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading.
- The Issuing CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
- The Issuing CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository.
- Revocation is required by this CP/CPS.

4.10.2 Who can request revocation

This CA accepts certificate revocation requests from the following sources:

- the owner of the profile used to issue the initial registration request,
- the owner of the private key,
- a properly authorized RAO,
- a properly authorized CAO,
- a properly authorized RSSO,
- a Swiss court of law.

4.10.3 Procedures for revocation request

Any one of these procedures can be used to successfully revoke a certificate:

- The Subscriber can personally visit the RA offices and request the revocation of a certificate off line. The Subscriber must present either a valid passport or Swiss identity card.
- The RAO of an RA can revoke certificates applied for through the RA.
- The Subscriber can submit an offline revocation form and send it to the TSP. After checking the validity of the revocation request, the TSP revokes the certificate.

4.10.3.1 Notification about revocation

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

4.10.4 Revocation request grace period

No stipulations.

4.10.5 Time within which CA must process the revocation request

After the formal requirements as detailed in chapters 4.10.1 and 4.10.2 have been met, the registration authority will process any written revocation requests within 24 hours (Monday through Friday, except public holidays in the canton of Zurich, Switzerland) and without unnecessary delay. If the subscriber requires the revocation on an appointed date, this will be noted accordingly and the certificate concerned will be revoked at the time required.

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

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

4.10.6 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.

4.10.7 CRL issuance frequency

CA	Information	Frequency
SwissSign Signature Services Root 2020-2 (Root CA)	CRL	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 CRL.
	OCSP Information	Real-time. The OCSP responder will report a certificate's revocation immediately after the revocation has been completed.
Subordinated issuing CAs	CRL	At least once every 24 hours. At most, one hour may pass from the time a certificate is revoked until the revocation is reported on the CRL.
	OCSP Information	Real-time. The OCSP responder will report a certificate's revocation immediately respectively 10 minutes after the revocation has been completed.

4.10.8 Maximum latency for CRLs

The CRL of this CA and all its subordinated issuing CAs is issued according to chapter 4.10.7 and published without delay.

4.10.9 On-line revocation/status checking availability

This CA and all its subordinated issuing CAs support the OCSP protocol for on line revocation checking. The OCSP responder URL is stored in every certificate issued by one of the subordinated issuing CAs of the “SwissSign Signature Services Root 2020-2” (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.

4.10.10 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.

4.10.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.10.12 Special requirements regarding key compromise

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

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

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

4.10.13 Circumstances for suspension

Certificates may not be suspended.

4.10.14 Who can request suspension

Certificates may not be suspended.

4.10.15 Procedure for suspension request

Certificates may not be suspended.

4.10.16 Limits on suspension period

Certificates may not be suspended.

4.11 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. 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. Revocation information remains in the CRL until the end of the issuing CA validity.

The last CRL will only be issued after all certificates in the scope of the CRL are either expired or revoked.

A certificate can only be revoked by authorized persons using the required credentials.

4.11.1 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 (QCP-n-qscd, QCP-l-qscd, QCP-n, QCP-l). CRL are issued regularly and until the end of the validity of the issuing CA. If a certificate is revoked a new CRL will be created and published within one hour.

4.11.2 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.

4.11.3 Optional features

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

4.12 End of subscription

End of subscription occurs after:

- successful revocation of the last certificate of a Subscriber,
- expiration of the last certificate of a Subscriber.

For reasons of legal compliance, the SwissSign CA and all registration authorities must keep all Subscriber data and documentation for a minimum period of 11 years after termination of a subscription.

4.13 Key escrow and recovery

4.13.1 Key escrow and recovery policy and practices

Key escrow is not supported for certificates under this CP/CPS.

4.13.2 Session key encapsulation and recovery policy and practices

This CA does not support session key encapsulation.

5. Facility, Management, and Operations Controls

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

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

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

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

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

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

5.1 Physical controls

Two identical clones of the SwissSign Signature Services Root 2020-2 keys are stored offline in Swiss bank safe deposit boxes.

The SwissSign CA servers are located in a commercial data center that

- meets the requirements of ETSI EN 319 411-1 and ETSI EN 319-411-2.
- complies with the IT-Security outsourcing requirements (99/2) of the Swiss banking committee.
- is ISO 27001 & ISO 22301 certified.
- is annually reviewed by a qualified Auditor.

5.1.1 Site location and construction

Swiss bank:	The Swiss bank safe deposit boxes have been opened with different Banks
Data center:	The SwissSign electronic data processing center is located in a data center in the greater Zurich area in Switzerland.
SwissSign RA	The SwissSign RA is located in a dedicated building in the greater Zurich area in Switzerland. The requirements of ETSI EN 319 401 are fulfilled.

5.1.2 Physical access

Swiss bank:	Physical access is only granted to a group of three persons by a member of the board of directors or a member of the SwissSign executive management. Identification documentation (Passport, ID) and the personal signature of every employee are checked by the personnel of the Swiss Bank. Swiss bank personnel does not have access to the safe deposit box.
Data center:	Physical access is restricted to system administrators and authorized data center personnel. Biometric and electronic badge identification is required to enter the facility in which all movements are recorded and logged by video and access control points.The logs are object to a monthly audit review. The TSP has a separate cage in the data center, with only the hardware used by the TSP.

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

5.1.3 Power and air-conditioning

Swiss Bank:	Workspace with power facilities is available whenever needed.
Data center:	The data center is air-conditioned so as to create an optimal environment for the system according to generally accepted best practices. Power relies on two independent local power suppliers as well as on independent emergency diesel generators and on emergency battery power.

5.1.4 Water exposure

Swiss bank:	The two Swiss banks are not located in the same zone of exposure.
Data center:	The data center has water sensors in all double floors. Adequate alarming is ensured. The data center is located in an area that has no special exposures.

5.1.5 Fire prevention and protection

Swiss bank:	Both Swiss banks have fire prevention and protection.
Data center:	The fire prevention system is an advanced VESDA (very early smoke detection system) and gas-type system. The data center has an Energen-based fire extinguishing system.

5.1.6 Media storage

The TSP media are reliably protected against damage, loss or compromise. The TSP fulfills the requirements of ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

5.1.7 Waste disposal

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

Application documents that are no longer required will also be physically destroyed.

5.2 Procedural controls

5.2.1 Trusted roles

In order to guarantee a segregation of duties in conflicting areas of responsibility to reduce opportunities for unauthorized or unintentional modification or missuse of the TSP's assets, the roles within the SwissSign TSP are operated by four separated authorization groups: Security Officer, System Administrators, System Operators and System Auditors. Access to any of the systems in the TSP requires 2-factor authentication. Any person may only be part of one of these authorization groups with the exception of the Security Officer and System Auditors. Within these authorization groups, multiple roles are defined (see picture below).

5.2.1.1 Security Officer (SecOff) (Read only System Configuration, Read only Data)

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

5.2.1.2 System Administrator (Read/Write System Configuration, Read only Data)

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

5.2.1.2.1 Infrastructure Engineer (Infra Eng)

Infrastructure Engineers install, configure and maintain the TSP's trustworthy systems, including recovery of the systems. Infra Eng have full control over the network access to all the systems as well as full control of the layers from hardware up to operation systems.

5.2.1.2.2 Application Engineer (App Eng)

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

is authorized to install, configure, and maintain the TSP's trustworthy systems for registration (of all identity data for certificate issuance), certificate generation, subject-device provision and revocation management. The App Eng is responsible for operating the trustworthy systems on a day-to-day basis and supports system backup and recovery. Regular recovery tests are carried out, the results are recorded and evaluated.

5.2.1.3 System Operator (Read only System Configuration, Read/Write Data)

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

5.2.1.3.1 CA Manager (CAM)

The CAM defines, creates, changes, deletes, and thus has full control over one or more of the actual TSP's keying material.

5.2.1.3.2 Certification Authority Operators (CAO)

CAO is responsible for the management of the configuration of the registration authorities in the TSP. The rules of access to the TSP for the CAO are defined by the Certification Authority Manager (CAM).

5.2.1.3.3 Registration Authority Operators (RAO)

RAO can manage a subset of certificates and requests as described by the RA application policies and the operator access rules. The RAO works with the RA application as defined by the CAM and cannot change the definition of the RA application. The RAO is responsible for operating the RA application on a day-to-day basis and is authorized to perform revocation requests.

5.2.1.3.4 Remote Signature Service Operators (RSSO)

RSSO is responsible for the management of the RSS and for operating the RSS application on a day-to-day basis.

5.2.1.4 System Auditor (Read only System Configuration, Read only Data)

The System Auditor has read-only access to all components of the SwissSign TSP to verify that the operation of these components complies with the rules and regulations of this CP/CPS. The System Auditor is authorized to view archives and audit logs of all of the TSP's trustworthy systems. The System Auditor has no direct operative abilities, but must inform SwissSign executive management, after the fact, of any irregularities in the processes.

5.2.2 Number of persons required per task

The operation of this CA is entirely role-driven and therefore requires at least:

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

The certificate store and all cryptographically relevant aspects of all TSPs signing operations can only be perfomed under four-eye-principle..

5.2.3 Identification and authentication for each role

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

Access to systems is always limited to authorized individuals following the 'least privilege' principle and based on 2-factor authentication. Internal procedures are in place to ensure timely assigning or removal of access for all employees and all personnel is identified and authenticated before using critical applications related to the service. Access to information and application system functions is restricted in accordance with the access control policy.

5.2.4 Roles requiring separation of duties

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

	Authorization Group	Security Officer	System Operator				System Administrator		System Auditor
	Role	SecOff	CAM	RAO	CAO	RSSO	Infra Eng	App Eng	SysAud
Infrastructure	Define Changes to Hardware and OS	A	R	C	C	C	C	C	C
	Execute Changes to Hardware and OS	A	I				R		
	Verify Changes to Hardware and OS	A	I						R
Applications	Define Changes to Software	A	R	C	C	C	C	C	C
	Execute Changes to Software	A	I					R	
	Verify Changes to Software	A	I						R
PKI Configuration	Define Changes to PKI Key Pairs	A	R						
	Execute Changes to PKI Key Pairs	A	I					R	
	Verify Changes to PKI Key Pairs	A	I						R
Certificates	Define Certificate Profiles	A	R						
	Process, Accept Certificate & MPKI Applications	A		R					
	Configure MPKI Solutions	A			R				
	Verify Compliance of Issued Certificates	A	I						R
Signatures	Configure RSS Solutions	A				R			
	Verify Compliance of RSS Operations	A	I						R
Registration of Identities	Process, Accept LoT2 SwissID (ZertES, EPD) applications	A		R					
	Verify Compliance of IDP Operations	A	I						R
Roles	Authorize Role Assignment	A	R						
	Execution of Role Assignment by Line Management (no trusted role function)	A							
	Verify Changes in Role Assignment	A	I						R

Illustration 1: Segregation of duties

Abbreviatons used: R: Responsible, A: Accountable, C: Consulted, I: Informed

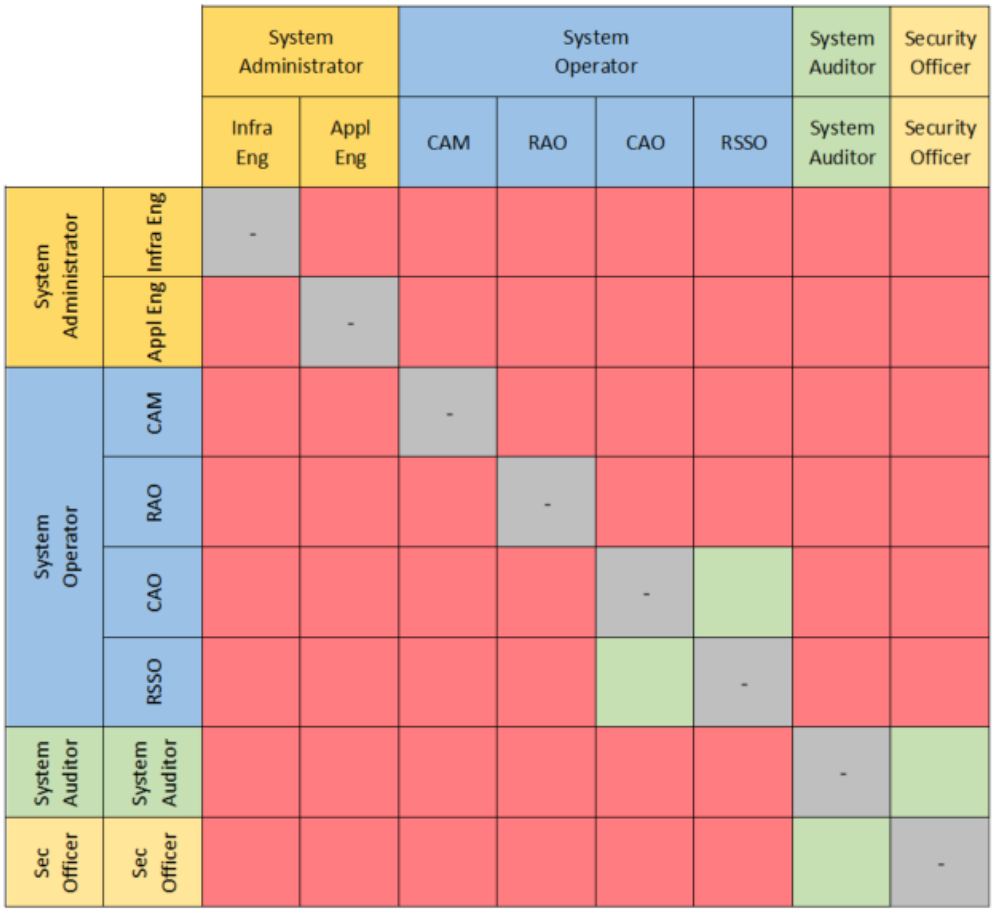

Illustration 2: Permitted combinations of roles

RA Data / CA Data / Role Definition	Infra / Application Config: no access	Infra / Application Config: read only	Infra / Application Config: read / write
own data only	non-trusted roles	-	-
read only	-	**Sec Of Sys Auditor**	**Sys Admin** Infra Eng App Eng
read / write	-	**Sys Ops** CAM RAO / CAO RSSO	-

Illustration 3: Data Access

5.3 Personnel controls

The TSP fulfills the requirements for personnel from ETSI EN 319 401, ETSI EN 319 411-1 and BRG.

TSP personnel is formally appointed to trusted roles by senior management responsible for security. In doing so, the principle of "least privilege", when accessing or when configuring access privileges, is applied. The personnel does not have access to the trusted functions until all necessary checks are completed.The permissions of the individual roles are restricted to those who need them to perform their tasks. The assignment of the authorizations is documented, assigned and periodically reviewed, and withdrawn immediately after the need has been removed. All employees of the TSP act within the framework of their respective policies only and are free from any constraints.

The TSP personnel is accountable for their activities. The actions of the personnel are stored by appropriate logging. The logs are backed up and examined for anomalies or unauthorized actions.

5.3.1 Qualifications, experience, and clearance requirements

SwissSign ensures to employ staff and subcontractors who possess the necessary expertise, reliability, experience, and qualifications to perform a service/job function and support the trustworthiness of the TSP's operations. Additionally, TSP staff and, if applicable, subcontractors, have received training regarding security and personal data protection rules as appropriate for the offered services and job function.

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

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

Before starting work at SwissSign AG, new staff members must sign confidentiality (non-disclosure) agreements and independence statements.

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

5.3.2 Background check procedures

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

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

Retraining of employees is done as necessity arises, depending on the needs of the organization or the needs of the individual, but at least once a year.

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

The TSP reserves the right to prosecute unauthorized actions to the fullest extent of applicable law. The TSP excludes unreliable employees from the activities in the certification service.

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

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

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

5.4 Audit logging procedures

The SwissSign CA software is built to journal all events that occur in the SwissSign Signature Services Root 2020 - 2. The journal is stored in the SwissSign CA database and is accessible through the SwissSign CA Web Interface. All other TSP systems involved in the remote signing service (including the IDP) do log into a centralized infrastructure.

5.4.1 Types of events recorded

The following events are recorded in either of the above mentioned audit log systems :

- key generation (certificate / signature)
- certificate requests (rekey)
- rejected certificate requests
- account violations (all involved systems)
- certificate signing (rekey)
- signer management
- certificate life cycle (creation, usage, deletion, revocation, expiration)
- key life cycle (certificate / signature key; if applicable: creation/activation, usage, deletion)

- authentication (failure, success; internal and user roles)
- Authorization (creation, change, withdrawing of rights; internal and user roles)
- CRL signing
- CA rollover
- signature requests
- start-up and shutdown of audit functions
- changes in system configuration

The above list is non-conclusive, and it is limited to events that are directly related to certificate management or trust-related functions. In particular, it does not include technical events that are logged elsewhere. All technical events are logged in conformance to ETSI EN 319 411-1.

5.4.2 Frequency of processing log

Logs are processed continuously and audited on a quarterly basis. The audit report covers the following aspects:

- list of the audit accomplished with the results of the review of each individual item,
- list of open audit issues including status, escalation, deadline, responsible person/organization,
- prioritized list of actions to be taken.

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

5.4.3 Retention period for audit log

The journal information in the “SwissSign Signature Services Root 2020 - 2” database is never deleted. The journal entries can be viewed with the role Auditor. A corresponding request for information can be made via the contact given in this CP/CPS. The TSP then checks the authorization and provides the required information.

5.4.4 Protection of audit log

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

- System Auditor - audit logs
- RAO - logs concerning only the RAO application (user logs)
- CAO - system logs
- RSSO - system logs
- CAM - system logs

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

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

5.5.1 Types of records archived

The following records are archived:

- a daily backup of any information that this CA and its subordinated issuing CAs produce
- journal
- all registration information of end entities as specified in chapter 4.1.2

5.5.2 Retention period for archive

Archived information is kept at least 11 years beyond the end of subscription, as specified in chapter 4.12.

5.5.3 Protection of archive

Protection of the archive is as follows:

- Archived information is only accessible to authorized employees according to the role model as presented in chapter 5.2.
- Protection against modification: Archives of digital data are digitally signed to prevent unknown modification.
- Protection against data loss: The RA must ensure that at least two copies of the archived data is available at all times. The storage locations must be suitable for this purpose and must provide physical protection and access controls.
- Protection against the deterioration of the media on which the archive is stored: Digital data is to be migrated periodically to fresh media.
- Protection against obsolescence of hardware, operating systems, and other software: As part of the archive, the hardware (if necessary), operating systems, and/or other software is archived in order to permit access to and use of archived records over time.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

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

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify archived information

In the event of a court order, a high-quality copy is made of the archived information and the original is temporarily made available to the court. When the original information is returned, the high-quality copy is destroyed. This process is logged and audited.

5.6 Key changeover

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

To manage a crisis or catastrophe, the TSP has a Business Continuity Management plan. Once this plan goes into action, the Emergency Management Team assumes managerial duties of the TSP until the crisis is dealt with.

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

- Loss of one computing facility
- System or server compromise
- CA key compromise
- Algorithm compromise
- Compromise of SSCD

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

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

5.7.2 Computing resources, software and/or data are corrupted

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

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

5.7.3 Entity private key compromise procedures

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

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

- The TSP will inform the relevant governmental authorities, the corresponding auditor and the relevant Root Store maintainers of any trust-anchor compromise.
- The TSP informs the relying parties about the incident by means of information on the SwissSign homepage.
- All Subscriber certificates will be revoked.
- The OCSP responder certificate(s) will be revoked
- A last CRL will be issued (compare 7.2).
- The CA certificate will be revoked.
- A new CARL, i.e. the CRL of the Root CA will be issued and published.
- All Subscribers with certificates issued by either the revoked CA or one of its subordinated issuing CA will be informed by e-mail as soon as possible.
- The cause of the key compromise will be determined and the situation rectified.
- The TSP will generate a new key pair for the new CA and the resulting key certificate will be signed by the superior CA.
- The new CA certificate will be published on the swisssign.com or the swisssign.net web site.

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

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

Before the SwissSign Signature Services CSP terminates its services, the following actions will be executed:

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

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

- The TSP will revoke all Subscriber certificates and will issue for each issuing CA a a CRL with a validity synchronized with the corresponding issuing certificate validity In addition for all certifcates a OCSP-Response will be issued where the nextUpdate field is sychronized with corresponding issuing certificate validity.
- The TSP will revoke all issuing CA certificates and issue for each Root CA a CRLwith a validity synchronized with the corresponding Root certificate validity. In addition for all certifcates a OCSP-Response will be issued where the nextUpdate field is sychronized with corresponding issuing certificate validity.
- The TSP will transfer obligations for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period such as registration information, certificate status information, and event log archives that cover the respective time to the appropriate organization.
- The TSP will destroy all backup copies and escrow copies of the private signing keys of the SwissSign Signature Services Root 2020-2, such that the private keys cannot be retrieved, retained, or put back into use.
- All copies of documents which are required to be saved according to the stipulations of any applicable law will be stored under the conditions and for the duration as stipulated in this CP/CPS.

The TSP will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period. RA termination is subject to negotiations with other equivalent RAs. Another RA may offer to assume the RA function for the Subscribers of the terminating RA. Regardless of whether or not an RA assumes the role of a terminating RA, the TSP will guarantee the safekeeping of any RA documents as stipulated in this document. To ensure that these activities can be carried out, the TSP has entered into an insurance policy.

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

6. Technical Security Controls

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

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

Exchanged devices or obsolete data carriers are taken out of service and disposed of in such a way that functionality or data misuse is excluded.

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

Penetration tests and vulnerability scans are carried out regularly by an independent and expert body. Furthermore, vulnerability assessments are regularly conducted.

6.1 Key pair generation and installation

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

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

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

6.1.1 Key pair generation

The signing keys of SwissSign Trust Services are created in an offline HSM that meets the requierements of ETSI EN 119 312, in accordance with internal procedures.

The HSMs are located in a high-security area. The HSM for Root or subordinated Issuing CAs are operated in FIPS mode which guarantees that the private keys can never leave the HSM.

Following the TSP's documented procedures, the key pairs for the Root or subordinated issuing CA of the SwissSign have been generated in HSMs that meet at least FIPS 140-2 level 3 requirements. Subsequently, the Issuing CA keys have been cloned into an online HSM meeting at least FIPS 140-2 level 3 requirements. In the case of key generation, the implementation of the role concept and the principle of double control are enforced.

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

SwissSign follows the abovementioned documented procedures for conducting key pair generation in accordance with ETSI EN 319 411-1. The Ceremony Master creates a report proving that the ceremony was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured. Report is signed by the Ceremony Master, Key Access Operators and external auditors if applicable. The more detailed procedures for key ceremony, roles and responsibilities of participants during and after procedure, requirements for report and collected evidences are defined in internal key ceremony procedures.

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

All life cycle events for the keys such as root ca, issuing ca and subscriber keys are logged.

6.1.2 Private key delivery to Subscriber

Subscriber private keys are maintained by the TSP on behalf of the subscriber and are not delivered. Subscriber private keys are only used by the TSP for signing the certificate signing request required for issuing the subscriber certificate. Immediately after certificate issuance, the public key of the SIC authentication means is registered within the SAM, whereby control over the private key is transfered to the SIC authentication means described in 4.1.2.

SIC authentication means use a 256 bit ECDSA key (NIST P-256 curve, OID 1.2.840.10045.3.1.7)

6.1.3 Public key delivery to certificate issuer

Subscriber public keys are generated and maintained by the TSP who is also the certificate issuer.

6.1.4 CA public key delivery to Relying Parties

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

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

Signatures created with the SwissSign RSS 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	https://www.nist.gov/publications

The "SwissSign Signature Services Root 2020 - 2" uses a 4096 bit RSA key.

The subordinate CAs use a 4096 bit RSA key.

All issuing CAs allow Subscribers to use RSA keys with a size of at least 3072 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

Key pairs are generated on SwissSign-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.

6.1.7.1 Qualified Electronic Signature Certificate (QCP-n-qscd)

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	The HSM used for CA keys is kept offline at all times and meets at least FIPS 140-2 level 3 requirements..
Issuing CA keys	The HSM used for CA keys meets at least FIPS 140-2 level 3 requirements. These keys are online and access is strictly controlled by using the '4-eye' principle.
QCP-n-qscd	Subscriber keys for qualified certificates must be generated and stored on an HSM that meets at least FIPS 140-2 level 3 or Common Criteria EAL4+ requirements.

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

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

Root CA keys	Root CA keys can only be accessed on the physical and on the logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.
Issuing CA keys	Management access to these keys is only possible using '4-eye' principle (2 out of m). Once the issuing CA is operable, signing operations can be authorized by a single RA operator.
QCP-n-qscd	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	Root CA keys are not in escrow.
Issuing CA keys	The issuing CA keys are not in escrow.
QCP-n-qscd	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	Root CA keys have been backed up onto an HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access. At least one of these persons must be a member of the Board of Directors of the TSP.
Issuing CA keys	The Issuing CA keys have been put into backup HSM, so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 2 persons are present in order to gain physical and logical access.
QCP-n-qscd	Subscriber keys are managed by the TSP within secure HSM and are not in backup.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

Root CA keys	The Root CA keys are not archived.
Issuing CA keys	The Issuing CA keys are not archived.
QCP-n-qscd	Subscriber keys are managed by the TSP within secure HSM and are not archived.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Root CA keys	Root CA keys have been backed up onto an HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access. At least one of these persons must be a member of the Board of Directors of the TSP.
Issuing CA keys	The Issuing CA keys are cloned in the same manner as Root keys.
QCP-n-qscd	Subscriber keys are are generated and managed by the TSP within secure HSM and are not transferred.

6.2.7 Private key storage on cryptographic module

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

Root CA keys	The Root CA keys are stored on cryptographic modules so that they can be used only if properly activated.
Issuing CA keys	The Issuing CA keys are stored on cryptographic modules so that they can be used only if properly activated.
QCP-n-qscd	Subscriber keys are stored within secure HSM and can be used only if properly activated.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

Root CA keys	The Root CA keys are activated with a user key (physical), a user pin (knowledge) and 3 authentication keys (physical).
Issuing CA keys	The Issuing CA keys are activated with role-based access control requiring at least two persons and an SSCD PIN.
QCP-n-qscd	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	The Root CA keys are deactivated either by logging out of the HSM, by terminating the session with the HSM, by removing the CA token from the computer or by powering down the system.
Issuing CA keys	The Issuing CA keys are deactivated by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.
QCP-n-qscd	Subscriber keys are activated for single use only and are automatically deactivated by the SAM after every use.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

Root CA keys	The Root CA keys are destroyed by initializing the partition on the HSM.
Issuing CA keys	The Issuing CA keys are destroyed by initializing the partition on the HSM.
QCP-n-qscd	Private key are managed by the TSP within secure HSM and cannot be extracted decrypted. Subscriber keys are destroyed through the key management functionality of the HSM when the associated certificate is revoked or after the associated certificate has expired.

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

6.2.11 Cryptographic Module Rating

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

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

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

6.3.2 Certificate operational periods and key pair usage periods

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

- The “SwissSign Signature Services Root 2020-2” as well as all trust-anchor certificates are valid 30 years. Key changeover shall be performed based on a current risk assessment taking into consideration the latest risks.
- Issuing CA certificates are issued for a maximum lifetime of 15 years.
- The rollover of CA certificates will be done manually and is after 13 years of the lifetime of the most recent CA certificate.
- End user certificates can have according to PKI “best practices” a lifetime of up to 2 years and up to the maximum remaining lifetime of the issuing CA certificate minus 10 days.

6.4 Activation data

6.4.1 Activation data generation and installation

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

Activation data used to protect private keys inside SwissSign-approved crypto devices is generated in accordance with the requirements of this CP/CPS.

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

6.4.2 Activation data protection

Root CA keys	The activation data is distributed over multiple physical keys. The owners of a part are required to store this part in a private safe deposit of a Swiss bank.
Issuing CA keys	The activation data is known to trusted individuals at the TSP. An escrow copy is stored in a safe deposit with dual controls access.
QCP-n-qscd	The device containing the SIC authentication means must be protected with a PIN or password of at least six characters which must not be easily guessable. Biometric protection may be used. Subscribers are obliged to keep the SIC authentication means for generating activation data secret at all times. The activation data is created with the SIC authentication means with a nonce and reference to the data to be

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

6.4.3 Other aspects of activation data

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

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

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

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

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

6.5 Computer security controls

The CA servers are protected by internal and external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. System Administrator access to the system is granted only over secure and restricted protocols using strong public-key authentication.

6.5.1 Specific computer security technical requirements

SwissSign uses a layered security approach to ensure the security and integrity of the computers used to run the SwissSign CA software. The following controls ensure the security of SwissSign-operated computer systems:

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

6.5.2 Computer Security rating

The TSP has applied procedures which ensure that security patches are applied within a reasonable time after they are available. In the case that security patches will be not applied, because they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them, the reasons for not applying the security patches is documented.

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

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

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

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

6.6 Life cycle technical controls

6.6.1 System development controls

To ensure quality and availability of the the TSP software, SwissSign implements the ITIL model and the development team adheres to the following principles:

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

6.6.2 Security management controls

Continuous monitoring is used to ensure that systems and networks are operated in compliance with the specified security policy. All processes are logged and audited according to applicable law and normative requirements. In particular, the TSP monitors the start-up and shutdown of the logging functions, the availability and utilization of needed services within the TSP network. The TSP has implemented automatic mechanisms to process the audit logs and alert personnel of possible critical security events. Each vulnerability identified by the TSP is examined and treated within 48 hours according to the ISMS guidelines for the treatment of security events. The TSP monitors ocsp requests concerning in terms of utilization and the request for unknown certificates on the ocsp responder as part of the business continuity and security controls. The TSP monitors the list of QSCD under Art. 31 and QSealCD under Art. 39 eIDAS and informs the Subscriber about replacement measures if necessary.

6.6.3 Life cycle security controls

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

6.7 Network security controls

The TSP has implemented a network concept, which ensures that the sensitive CA systems are operated in dedicated secure network zones. For the network concept, a separate documentation is available, which can be viewed on the premises of the TSP in the relevant parts if there is justified interest. To protect the processes of the TSP, among others, firewalls and intrusion detection mechanisms are used, which only allow explicitly permitted connections. The TSP operates network segments in differentiated severity levels, thereby separating workstation networks from server networks. The TSP uses dedicated systems used for administration of the security policy implementation.

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

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

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

The TSP performs quarterly vulnerability scans and annual penetration tests on public and private IP addresses identified by the TSP and records evidence for each vulnerability scan and penetration test that was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

6.8 Time-stamping

The TSP operates an internal time service using various sources from the Internet, a GPS receiver and a DCF77 receiver.

Based on this internal time service, The TSP offers a timestamping service that can be used to create a timestamp for arbitrary documents. This service is implemented in accordance with ETSI EN 319 421.

SwissSign may charge a fee for this service. The keys used for the creation of timestamping signatures are treated in exactly the same fashion as the keys of the subordinated issuing CAs of the “SwissSign Signature Services Root 2020-2”.

7. Certificate, CRL and OCSP Profiles

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions.

7.1 Certificate profile

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

The structure of such a certificate is:

Certificate Field	Value	Comment
Version	X.509 Version 3	See Chapter 7.1.1
Serial number	Unique number	Will be used in CRL
Signature algorithm identifier	OID	See Chapter 7.1.3
Validity period	Start date, expiration date	
Subject Public Key Info	Public Key algorithm, Subject Public Key	See Chapter 7.1.3
Extensions	X509V3 Extensions	See Chapter 7.1.2
Signature	Certificate Signature	See Chapter 7.1.3

7.1.1 Version number(s)

Version of X.509 certificates: version 3.

7.1.2 Certificate Extensions

7.1.2.1 SwissSign Signature Services Root 2020-2 Certificates

CA Type	Subject	Issuer
Root CA	CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH organizationIdentifier=NTRCH-CHE-109.357.012	CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH organizationIdentifier=NTRCH-CHE-109.357.012
Issuing CA	CN=SwissSign Qualified Electronic Signature ICA 2021 - 2 O = SwissSign AG C = CH organizationIdentifier=NTRCH-CHE-109.357.012	CN=SwissSign Signature Services Root 2020 - 2 O=SwissSign AG C=CH organizationIdentifier=NTRCH-CHE-109.357.012

7.1.2.1.1 Extension of the Root CA Certificate: SwissSign Signature Services Root 2020 – 2

Field/Extension	**Value(s)**	**Comment**
Version	Version 3	Certificate format version
Serial Number	002FDBA9B88D001EBCE7B99C2D23EF4A	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	CN=SwissSign Signature Services Root 2020 - 2, O=SwissSign AG, C=CH, organizationIdentifier=NTRCH-CHE-109.357.012	Distinguished name of the certificate issuer
Subject Distinguished name	CN=SwissSign Signature Services Root 2020 - 2, O=SwissSign AG, C=CH, organizationIdentifier=NTRCH-CHE-109.357.012	Unique Subject name of the certificate issuer
Valid from	07 Oct 2020 10:19:32 UTC	First date of certificate validity.
Valid to	30 Sep 2050 10:19:32 UTC	The last date of certificate validity.
Basic Constraints	CA: TRUE	Critical
Key Usage	Certificate Sign, CRL Sign	Critical
Subject Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Certificate Policies	not included in Root CA certificate	
CRL Distribution Points	not included in Root CA certificate	

7.1.2.1.2 Extensions of the Issuing CA Certificates

SwissSign Qualified Electronic Signature ICA 2021 - 2

Field/Extension	Value(s)	Comment
Version	Version 3	Certificate format version
Serial Number	00CE3774E62AA97F1F3D6D8801DB4AC4	Unique serial number of the certificate
SignatureAlgorithm	sha256WithRSAEncryption	
Issuer Distinguished name	CN=SwissSign Signature Services Root 2020 - 2, O=SwissSign AG, C=CH, organizationIdentifier=NTRCH-CHE-109.357.012	Distinguished name of the certificate issuer
Subject Distinguished name	CN=SwissSign Qualified Electronic Signature ICA 2021 - 2, O = SwissSign AG, C = CH, organizationIdentifier=NTRCH-CHE-109.357.012	Unique Subject name of the certificate issuer
Valid from	2021-03-31 12:28:00 UTC	First date of certificate validity.
Valid to	2036-03-31 12:28:00 UTC	The last date of certificate validity.
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	069B3BD514ECA62EFB76573C9923EA1D2DDE2C00	
Authority Key Identifier	C99B6176377D397796F4A1E97BCDEB2070F2E084	
Certificate Policies	Policy: 2.16.756.1.89.1.4.2.1 CPS: https://repository.swisssign.com/SwissSign-Signing-Services-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/C99B6176377D397796F4A1E97BCDEB2070F2E084 ldap://directory.swisssign.net/CN=C99B6176377D397796F4A1E97BCDEB2070F2E084%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	

7.1.2.1.3 Extensions of Leaf Certificates

7.1.2.1.3.1 Qualified Electronic Signature Certificates issued by SwissSign Qualified Electronic Signature ICA 2021 - 2 (QCP-n-qscd)

Field/Extension	Values	Comment
Version	Version 3	Certificate format version
SignatureAlgorithm	SHA256withRSAEncryption	
Subject	/CN=(/GN /SN) or pseudo: Pseudonym (mandatory) /GN (mandatory if CN without Pseudonym) /SN (mandatory if CN without Pseudonym) /Pseudonym (optional) /serialNumber (mandatory) /C (mandatory)	See Definitions in Chapter 1.6
Issuer Name	/CN=SwissSign Qualified Electronic Signature ICA 2021 - 2 /organizationIdentifier=NTRCH-CHE-109.357.012 /O=SwissSign AG /C=CH	DN of the issuing CA
Authority Key Identifier	069B3BD514ECA62EFB76573C9923EA1D2DDE2C00	

Field/Extension	Values	Comment
CRL Distribution Points	http://crl.swisssign.net/069B3BD514ECA62EFB76573C9923EA1D2DDE2C00 ldap://directory.swisssign.net/CN=069B3BD514ECA62EFB76573C9923EA1D2DDE2C00%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.4.2.1 CPS: https://repository.swisssign.com/SwissSign-Signing-Services-CP-CPS.pdf Policy: 0.4.0.194112.1.2 (QCP-n-qscd)	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/069B3BD514ECA62EFB76573C9923EA1D2DDE2C00 http://ocsp.swisssign.net/069B3BD514ECA62EFB76573C9923EA1D2DDE2C00	URL to OCSP responder and optional URL to CA issuer certificate
QC Statements	0.4.0.1862.1.4 Secure Signature Creation Device Qualified Certificate 0.4.0.1862.1.5 PDS=http://repository.swisssign.com/PDS.pdf 0.4.0.1862.1.6 QC Type=0.4.0.1862.1.6.1 (Certificate for electronic signatures) 0.4.0.1862.1.7 QC CC Legislation=CH	
Key Usage	nonrepudiation	Critical

7.1.2.2 User Notices

The following certificates issued respectively have an according User Notice:

- Under “SwissSign Qualified Electronic Signature ICA 2021 - 2”, the user notice is “Qualified Certificate”
- The Issuing CA “SwissSign Signature ICA 2021 - 2” has the user notice “regulated certificate”.

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA and its subordinates issuing CAs are:

Algorithm	Object Identifier
SHA256withRSAEncryption	1.2.840.113549.1.1.11

7.1.4 Name forms

Certificates issued by the subordinated issuing CAs of this CA contain the full X.509 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 Name constraints

Name constraint is only implemented for the TSA Issuing CA and all other Issuing CA are not technically constrained.

7.1.6 Certificate policy object identifier

Each certificate must reference a policy OID, and may contain several as long as none of the policy constraints conflict.

For information see chapter 7.1.2 of this document.

7.1.7 Usage of Policy Constraints extension

Not implemented.

7.1.8 Policy qualifiers syntax and semantics

The policy qualifier is an OID that identifies this document and a URL that points to this document, adhering to the semantics for the critical Certificate Policies extension.

7.1.9 Processing semantics for the critical Certificate Policies extension

PKI client applications must process extensions marked as critical.

7.2 CRL profile

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

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

Extension Attribute	Values	Comment
Version Number	V2	CRL format version pursuant to X.509.
Signature Algorithm	sha256WithRSAEncryption	Hash method and the signature algorithm used to sign the CRL pursuant to RFC 5280.
Issuer Distinguished Name	Distinguished name of certificate issuer	
Effective Date		Date and time of CRL issuance.
This Update		Date and time of issuance of this CRL was published.
Next Update		Date and time of issuance of the next CRL. Maximum validity for CARL of the Root CA is 1 year after the publication of the CRL. The validity for CRLs provided by the Issuing CAs is 10 days. If it is the last CRL issued for those certificates in the scope of this CRL, the nextUpdate field in the CRL will be set to "99991231235959Z" as required by IETF RFC 5280.
Revocation List Number		CRL sequence number
Revoked Certificates:		List of revoked Certificate serial numbers.
Serial Number		Serial number of the certificate revoked.
Revocation Date		Date and time of revocation of the certificate.
reasonCode		Reason code for certificate revocation. Not applicable for end-entity certificates. For CARL issued by the Root CA - reasonCode extension is present and not marked critical - possible reason codes in CARL: - cACompromise (2), or - cessationOfOperation (5)
Authority Key Identifier		Matching the subject key identifier of the certificate
ExpiredCertsOnCRL		Populated as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 if there are expired certficates on the CRL that have been revoked
Signature		Confirmation signature of the authority issued the CRL.

7.3 OCSP profile

The SwissSign OCSP functionality is built according to RFC 6960.

OCSP response Field	Values	Comment
Response Status	0 for successful or error code	Result of the query
Version	V1	
Responder Id	DN	Distinguished name of the OCSP responder
Produced At	Date	Date when the OCSP response was signed
Cert Status	Good, revoked, or unknown	Indicates the response for certificate status (mandatory)
This Update	Date when the status was queried from database	
Next Update	The time at or before which newer information will be available about the status of the certificate.	The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate.
Signature Algorithm:	sha256WithRSAEncryption	
Certificate		Details of certificate
revocationReason		For revoked certificates, the reasonCode is omitted.

7.3.1 OCSP extensions

The OCSP extensions used are specified below:

- Nonce
- ServiceLocator

The ArchiveCutOff extension is not set in the OCSP responses.

8. Compliance Audit and Other Assessments

The present CP/CPS fulfills the requirements for certificates and services according to EN 319 401, EN 319 411-1, EN 319 411-2, EN 419241-1 and TS 119431-1. The terms and conditions of this CP/CPS, Swiss Digital Signature Law and all dependent rules and regulations will be used to conduct compliance audits for:

- The qualified subordinate CA
- All registration authorities that process requests for issuance by the qualified subordinate CA

8.1 Frequency or circumstances of assessment

The compliance audit is conducted annually as prescribed by Swiss Digital Signature Law.

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

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

The independent and qualified auditors will conduct the compliance audits according to the stipulations of ZertES.

The qualified auditor has the right to withdraw the certification of the TSP if a compliance audit reveals a severe deficiency in the operation of the TSP.

Internal audit generates objective evidence that is presented to auditor for the annual assessment.

8.4 Topics covered by assessment

The auditor will choose the control objectives that are to be covered by the assessment in accordance with ZertES. Objective evidence as generated by the internal audit is covered by the annual assessment of the qualified auditor.

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

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

Within 30 days of receiving the compliance audit results, the TSP will prepare a statement regarding the open issues and present SwissSign executive management and the ZertES Recognition Body a plan how the issues are going to be addressed.

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

8.7 Risk assessment

The TSP carries out a regular risk analysis which comprehensively analyzes the threat to the company as well as requirements and countermeasures. A residual risk analysis is carried out and documented in which the legibility of the residual risk is identified and, where appropriate, accepted. The relevant assets are adequately recorded and changes to these assets are reviewed at least yearly or, if applicable, released by the management team. The risk analysis is carried out annually, based on the requirements of the ISO 27001:2013 standard and released by SwissSign management body.

9. Other Business and Legal Matters

9.1 Fees

The TSP must 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 can 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 its pricing policy.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

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

9.1.5 Refund Policy

The TSP may establish a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

With regard to the qualified certificates issued pursuant to this CP/CPS document according to ZertES SwissSign Switzerland has entered into a contract for an insurance policy for liability claims against the TSP. The amount of insurance coverage meets the requirements of Article 3 para. 1 ZertES and VZertES Article 2.

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

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

It is in 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 Swiss Digital Signature Law.

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

9.3.2 Information not within the scope of confidential information

Any information that is already publicly available or contained in certificates is not considered confidential, nor is any information considered confidential which the TSP is explicitly authorized to disclose (e.g. by written consent of involved party, by law or because it is

part of the publicly available certificate information). In accordance with the RFC 5280 the information of the certificate status information (CRL and OCSP) is not considered as confidential data.

9.3.3 Responsibility to protect confidential information

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

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

9.4 Privacy of personal information

The TSP fully complies with the Swiss Data Protection Law. Information and data can be used where needed for professional handling of the services provided herein.

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

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

Certain third party software is used by the TSP in accordance with applicable license provisions.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The TSP warrants full compliance with all provisions stated in this CP/CPS, Swiss Digital Signature Law (as far as qualified certificates are concerned), and related regulations and rules.

9.6.2 RA representations and warranties

All registration authorities must warrant full compliance with all provisions stated in this CP/CPS, related agreements, Swiss Digital Signature Law (as far as qualified certificates are concerned), and related regulations and rules.

9.6.3 Subscriber representations and warranties

Subscribers warrant full compliance with all provisions stated in this CP/CPS, other related agreements, Swiss Digital Signature Law, and related regulations and rules.

9.6.4 Relying Party representations and warranties

Relying Parties warrant full compliance with the provisions of this CP/CPS, related agreements, Swiss Digital Signature Law, and related regulations and rules.

9.6.5 Representations and warranties of other participants

Any other participant warrants full compliance with the provisions set forth in this CP/CPS, related agreements, Swiss Digital Signature Law, 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

As far as qualified certificates are concerned the TSP is liable for damages which are the result of the TSP's failure to comply with Swiss Digital Law (Art. 17 ZertES).

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 or the Relying Party on the applicable terms and conditions including the exceeding of the transaction limit.

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

9.8.2 Liability of the Subscriber

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

The Subscriber of a qualified certificate is also liable according to Article 59a OR (Swiss Code of Obligations).

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This Certificate Policy and Certification Practice Statement and respective amendments become effective as they are published on the SwissSign website at "https://repository.swisssign.com".

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

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

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

9.12 Amendments

9.12.1 Procedure for amendment

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

Changes with material impact will be first submitted to the Supervisory Body to obtain the required approval.

Updated CP/CPS become final and effective by publication on the SwissSign website and will supersede all prior versions of this CP/CPS.

9.12.2 Notification mechanism and period

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

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

All changes to the CP/CPS will be published according to chapter 2. of this CP/CPS. Material changes for the Subscriber will be sent to the respective parties via email 30 days before the changes become effective, provided that email addresses are known.

9.12.3 Circumstances under which OID must be changed

Changes of this CP/CPS that do affect Subscribers and/or Relying Parties do require the OID of this CP/CPS to be updated.

9.13 Dispute resolution provisions

Complaints regarding compliance with or implementation of these CP/CPS must 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 can not be resolved within a period of four weeks after submission of the complaint, the parties are free to file action with the competent courts at the place of jurisdiction pursuant to clause 9.14.

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/CPS and rights or obligations related hereto are in accordance with the relevant provisions of the EU Regulation No 910/2014 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 SwissSign AG state the agreement between the TSP and the Subscriber:

- the CP/CPS, as indicated in the certificate,
- the registration form, including the application documentation as required for the type of certificate,
- the SwissSign 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 is not permitted to assign this agreement or its rights or obligations arising hereunder, in whole or in part.

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

9.16.3 Severability

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

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

When the Law no longer applies, or the Requirements are modified the TSP will modify these requirements to make it possible to comply with both them and the Law simultaneously.

The TSP will communicate an appropriate change within 90 days.

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

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

The TSP 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/CPS is provided in additional languages to English, the English version will prevail.

9.17.2 Delegated or outsourced Services

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