SwissSign TSPS

Trust Services Practice Statement

Document Type:	Trust Services Practice Statement
OID:	n/a
Author:	Information Security and Compliance
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	08 November 2021
Version:	3.0
Obsoletes:	v2.0; 11.10.2021
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

Version Control

Date	Version	Comment	Author
14.06.2021	1.0	First public version.	Michael Guenther
11.10.2021	2.0	New Trusted Role, small clarifications	Michael Guenther
08.11.2021	3.0	Changes to retention time of audit logs and archival	Michael Guenther

Authorization

Date	Approved by	Approved by	Version
11.06.2021	Michael Günther	Markus Naef	1.0
07.10.2021	Michael Günther	Markus Naef	2.0
05.11.2021	Michael Günther	Markus Naef	3.0

Michael Frank Günther
5. November 2021
Qualified Electronic Signature by SwissID

digital signature

digital signature

Table of Contents

1. Introduction

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

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

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

The structure of this document corresponds to RFC3647 and is divided into nine parts. To preserve the outline specified by RFC 3647, section headings that do not apply or are not supported by the TSP have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them.

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

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

1.1 Overview

This TSPS describes the practices implemented by SiwssSign AG to comply with for the relevant services as well as the terms and conditions under which this CA is made available. SwissSign Trust Services Practices Statement (TSPS) presents the practices established by SwissSign to provide electronic Trust Services, which enhance trust and confidence in electronic transactions. SwissSign TSPS describes SwissSign practices of providing Qualified Trust Services in conformity with the Swiss Federal law ZertES, ETSI EN 319 401 , ETSI EN 319 411-1/2 and other related service-based standard requirements. Additionally, SwissSign follows CA/Browser Forum Baseline Requirements and Extended Validation Guidelines and Network and Certificate System Security Requirements for the Issuance and Management of Publicly-Trusted Certificates.

For the issuance of certificates within of this scope, SwissSign fully complies with different rules and regulations which are described in each service-based CPS.

The relevenat PKI used for different PKI is described are described in each service-related CPS.

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

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

In this CPS, “this CA” refers to both Root CA and all it subordinated issuing CA, unless stated differently.

In the event of conflict between the TSPS and the practice statements of specific services, the provisions of the practice statements of specific services shall prevail.

SwissSign AG provides a detailed product overview on the website (swisssign.com) for all provided Trust Services.

1.2 Document name and identification

This document is named “SwissSign TSPS - Trust Services Practice Statement as indicated on the cover page of this document.

1.3 PKI Participants

1.3.1 Certification Authorities

The TSP operates a Public Key Infrastructure, consisting of the CAs listed in the relevant service-based Policy and/or Practice Statement.

1.3.2 Registration Authorities

Registration Authority (RA) and its roles are defined in relevant service-based Policy and/or Practice Statement.

Obligations and warranties of RA are described in the clause 9.6.2 of this TSPS.

1.3.3 Subscribers

Subscriber is Specified in the relevant service-based Policy and/or Practice Statement.

Obligations and warranties of Subscriber are described in the clause 9.6.3 of this TSPS.

1.3.4 Relying Parties

Relying Party is defined in the clause 1.6 in this TSPS.

Obligations and warranties of Relying Party are described in the clause 9.6.4 of this TSPS.

1.3.5 Other participants

Not applicable

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Specified in the relevant service-based Policy and/or Practice Statement.

1.4.2 Prohibited Certificate Uses

Specified in the relevant service-based Policy and/or Practice Statement.

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 Management Board of SwissSign AG determines the suitability of this CPS document.

Changes or updates to relevant documents must be made in accordance with the stipulations of the regulatory requirements and the provisions contained in this TSPS. They are subject to review by the audit bodies (appointed by SAS in case of the ZertES audit).

1.5.4 TSPS approval procedures

This TSPS document and its related documentation are regularly reviewed by Information Security & Compliance and approved by the CEO of SwissSign AG. Following the approval by the CEO of SwissSign AG, the TSPS and its relevant documentation are published as stated in clause 2 of this TSPS and communicated to employees of SwissSign and external parties as relevant.

1.6 Definitions and acronyms

In this TSPS, the service related certificate policies and certification practice statements the following terms and acronyms have the following meaning:

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
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 public key, 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 mis-issuance.
Certificate Extension		Optional fields in a Certificate according to X.509 v3
Certificate Policy	CP	A set of rules that a CA must comply when providing the trust service.
Certificate Profile	CPR	A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with the applicable requirements. Please see clause 7.1 of this Document.
Certification Authority Revocation List	CARL	Revocation list containing a list of CA-certificates that have been revoked by the certificate issuer (Root CA).
Certificate Revocation List	CRL	Revocation list containing a list of leaf certificates that have been revoked by the certificate issuer (Issuing CA).

Term	Abbrev.	Explanation
Certification Practice Statement	CPS	Document that describes the implemented practices of the CA when providing the trust service.
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 Information 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.
Cryptographically-secure pseudo-random number generator	CSPRNG	Pseudo-random number generator meeting the quality requirements for the use in cryptology.
Decryption		The process of transforming cipher text into readable plain text.
Digital signature		A system allowing individuals and organizations to electronically certify features such as their identity or the authenticity of an electronic document.
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'.
eIDAS		European ordinance on “electronic IDentification, Authentication and trust Services” or “REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC” Compliance with the trust servces part implies compliance with the following standards: ETSI EN 319 401, 319 411-1, 319 411-2

Term	Abbrev.	Explanation
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 certificate holder certificates.
Subscriber Agreement	SA	Contractual agreement between the CA and the Subscriber.
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.
EVCG		Extended Validation Certificate Guidelines as published by the CA/Browser Forum
Extended Validation	EV	Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.
FIPS 140		FIPS 140 (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	Hyper-Text Transfer Protocol over TLS/SSL
Key		The secret input for cryptographic algorithms that allows a message to be transformed. -> See Private Key, Public Key
Key password		Password used to encrypt the private key.
Key size		Length of private and public key. Regular key RSA sizes are 2048, 3072 and 4096. At least 2048 bit is the recommended key size according to NIST today.

Term	Abbrev.	Explanation
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
Managed PKI	M-PKI	Interface where the subscriber/subject can request leaf certificates. The content of the certificate as well as authorization of the subscriber is already verified by the SwissSign and the certificate is issued only if the CSR match to the verified content. Otherwise the certificate request is rejected.
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 certificate status 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.

Term	Abbrev.	Explanation
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 eIDAS and in ZertES article 2 e
Qualified Signature/Seal Creation Device	QSCD	Signature-creation device which meets the requirements specified in article 30 of eIDAS.
RA Operator	RAO	The person responsible for identifying the requester, collecting and verifying the identity substantiating evidence, authorizing the CSR, and forwarding the authorized CSR to the CA.
Recognition Body		The Recognition Body of Switzerland is accredited by the SAS and conducts the audits prescribed by Swiss Digital Signature Law.
Registration Authority	RA	A registration authority (RA) verifies the identity of entities requesting their digital certificates and approves the CSR to the Certificate Authority (CA) to issue the leaf-certificate.
Regulation No 910/2014 /EC		See eIDAS
Relying Party		Relying Parties are individuals or organizations that use certificates of this CA to validate the signatures and verify the identity of Subscribers and/or to secure communication with these Subscribers. Relying Parties are allowed to use such certificates only in accordance with the terms and conditions set forth in the CP, CPS and this TSPS. It is in the sole responsibility of the Relying Party to verify revocation status, legal validity, transaction limits and applicable policies.
Remote Signing Service	RSS	A service for signing documents operated by a TSP on behalf of (authenticated) users
Requester		Requesters are individuals or organization that have requested a certificate.
Revocation		Withdrawing the certificate status of 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	Secure signature creation device is a cryptohgraphic device which is certified and recognized for usage for the provision of trust services.

Term	Abbrev.	Explanation
Smartcard		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 and authenticate 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.
Single Sign On	SSO	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 is an organization providing trust services, e.g. issuing leaf-certificates for a subscriber.
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.
Traffic management		Management and surveillance of network traffic with domain names or IPs owned or controlled by third parties.

Term	Abbrev.	Explanation
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.
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 enterprise identification number	UID	The UID is an unique organization number, e.g. the number of the commercial register entry or the VAT number.
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.
VZertES		Swiss ordinance 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, TSPS, service-based Policy and/or Practice Statement, Subscriber agreement with terms and conditions, CRL, CA certificates and related documents for this CA publicly available. 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. Certificate status information is also available via OCSP Responder.

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

The TSP publishes information related to certificates issued by its CAs 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 its CAs.
- The certificate revocation list (CRLs) for its CAs. The CRLs may be downloaded from the swisssign.net web site. The exact URLs are documented in every certificate that is issued by the CA or the subordinated issuing CAs in the field: “CRL Distribution Point”. For details, please refer to clause 7.

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

2.2 Publication of certification information

The SwissSign TSPS is reviewed at least once a year. Even if no updates are required, a new version is published.

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

- the Trust Service Practice Statement
- the service-based Policy and Practice Statement (CP and CPS)
- Certificate Profile (CPR)
- PKI Disclosurer Statement (PDS)
- End User Agreement / Subscriber Agreement (EUA)
- Relying Party Agreement (RPA)

The TSPS and the service related CP’s and CPS’s are published in case of changes and changes are communicated as described in chapter 9.12.

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

2.3 Time or frequency of publication

Refer to clause 2.2 above.

Information on certification status is published in accordance with the relevant service-based Policies and Practice Statements.

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 TSPS is provided as public information on the swisssign.com web site.

Management access always requires two factor authentication.

2.5 Additional testing

Specified in the relevant service-based Policy and/or Practice Statement.

3. Identification and Authentication

3.1 Naming

Specified in the relevant service-based Policy and/or Practice Statement.

3.2 Initial identity validation

Specified in the relevant service-based Policy and/or Practice Statement.

3.3 Identification and authentication for re-key requests

Specified in the relevant service-based Policy and/or Practice Statement.

3.4 Identification and authentication for revocation request

Specified in the relevant service-based Policy and/or Practice Statement.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Specified in the relevant service-based Policy and/or Practice Statement.

4.1.2 Enrollment process and responsibilities

Specified in the relevant service-based Policy and/or Practice Statement.

4.1.3 Annual Control of QSCD

SwissSign has implemented organizational monitoring procedures to ensure that the QSCD in use are recognized regarding to ZertES, Regulation (EU) N° 910/2014 during the whole certificate life cycle as well as to ensure that it fulfills the requirements of ZertES/TAV.

4.2 Certificate application processing

Specified in the relevant service-based Policy and/or Practice Statement.

4.3 Certificate issuance

Specified in the relevant service-based Policy and/or Practice Statement.

4.4 Certificate acceptance

Specified in the relevant service-based Policy and/or Practice Statement.

4.5 Key pair and certificate usage

Specified in the relevant service-based Policy and/or Practice Statement.

4.6 Certificate renewal

Specified in the relevant service-based Policy and/or Practice Statement.

4.7 Certificate re-key

Specified in the relevant service-based Policy and/or Practice Statement.

4.8 Certificate modification

Specified in the relevant service-based Policy and/or Practice Statement.

4.9 Certificate revocation and suspension

Specified in the relevant service-based Policy and/or Practice Statement.

4.10 Certificate status services

Specified in the relevant service-based Policy and/or Practice Statement.

4.11 End of subscription

Specified in the relevant service-based Policy and/or Practice Statement.

4.12 Key escrow and recovery

Key Specified in the relevant service-based Policy and/or Practice Statement.

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 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 TSP's security policies to ensure an appropriate level of protection of all assets including information assets. Controls are implemented to avoid loss, damage or compromise of assets or information and interruption to business activities.

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

5.1 Physical controls

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

The SwissSign CA servers are located in 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 and ISO 2230 1 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 at different geo-locations.

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

5.1.2 Physical access

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

Swiss bank:	Physical access is only granted to a group of three 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. Every entry to the facility is logged and object to a montlhly audit review. The logs are object to a montlhly audit review. The TSP has a separate cage in the data center, with only the hardware used by the TSP.
RA	Physical access is restricted to authorized personnel. Electronic badge identification is required to enter the facility.

5.1.3 Power and air-conditioning

Swiss Bank:	Workspace with power facilities is available whenever needed.
Data center:	The data 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 Inergen-based fire extinguishing system.

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

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

This process guarantees that the off-site storage of all data from the PKI environment is fully encrypted.

5.2 Procedural controls

5.2.1 Trusted roles

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

5.2.1.1 Security Officer (SecOff) (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 trustworthy systems of SwissSign, including performing the system backup and recovery functions. Within this authorization group in SwissSign, the following subroles are defined:

5.2.1.2.1 Infrastructure Engineer (Infra Eng)

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

5.2.1.2.2 Application Engineer (App Eng)

Application Engineers have full control of TSP application software (i.e. all application level systems of the TSP above the operation system), but not of cryptographically relevant information such as the private keys of any of the TSP components. The Application Engineer is authorized to install, configure, and maintain the TSP's trustworthy systems for registration (of all identity data for certificate

issuance), certificate generation, subject-device provision and revocation management. The Application Engineer is responsible for operating the trustworthy systems on a day-to-day basis and supports system backup and recovery.

5.2.1.3 System Operator (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 subroles 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 Signing Service Operators (RSSO)

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

5.2.1.3.5 Remote Signing Service Revocation Operator (RSSRO)

RSSRO is responsible for signing certificate revocations of the RSS

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

The System Auditor has read-only access to some or all components of the SwissSign TSP to verify that the operation of these components complies with the rules and regulations of this TSPS. The System Auditor is authorized to view archives and/or audit logs of all of the TSP's trustworthy systems within the limitation of the audit scope. The System Auditor has no direct operative abilities on production environment .

5.2.2 Number of persons required per task

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

System Administrator: 2 employees for network access configuration and TSP maintenance and management tasks

System Operator: 2 employees for system administration and TSP operation

System Auditor: 1 auditor

The certificate store and all cryptographically relevant aspects of all TSP's signing operations can only be 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 following the internal documented procedure for appointing individuals to Trusted Roles. The requirements of the information security policy apply.

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

For authentication controls, SwissSign has implemented the following controls:

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

5.2.4 Roles requiring separation of duties

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

		Authorization Group	System Administrator		System Operator					System Auditor	Security Officer
		Trusted Role	Infrastructure Engineer	Application Engineer	CAM	RAO	CAO	RSSO	RSSRO	System Auditor	Security Officer
Infrastructure	Define changes to hardware and OS		C	C	R	C	C	C	C	C	A
	Execute changes to hardware and OS		R		I						A
	Verify changes to hardware and OS				I					R	A
Applications	Define changes to software		C	C	R	C	C	C	C	C	A
	Execute changes to software			R	I						A
	Verify changes to software				I					R	A
PKI Configuration	Define changes to PKI key pairs				R						A
	Execute changes to PKI key pairs			R	I						A
	Verify changes to PKI key pairs				I					R	A
Certificates	Define certificate profiles				R						A
	Process, accept certificate and mPKI applications					R					A
	Configure mPKI solutions						R				A
	Verify compliance of issued certificates				I					R	A
Signatures	Configure RSS solutions							R			A
	Revoke RSS certificates								R		A
	Verify compliance of RSS operations				I					R	A
Registration of identities	Process, accept LoT2 SwissID (ZertES, EPD) applications					R					A
	Verify compliance of IDP operations				I					R	A
Roles	Authorize role assignment				R						A
	Execution of role assignment by line management (not a trusted role function)										A
	Verify changes in role assignment				I					R	A

Illustration 1: Segregation of duties

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

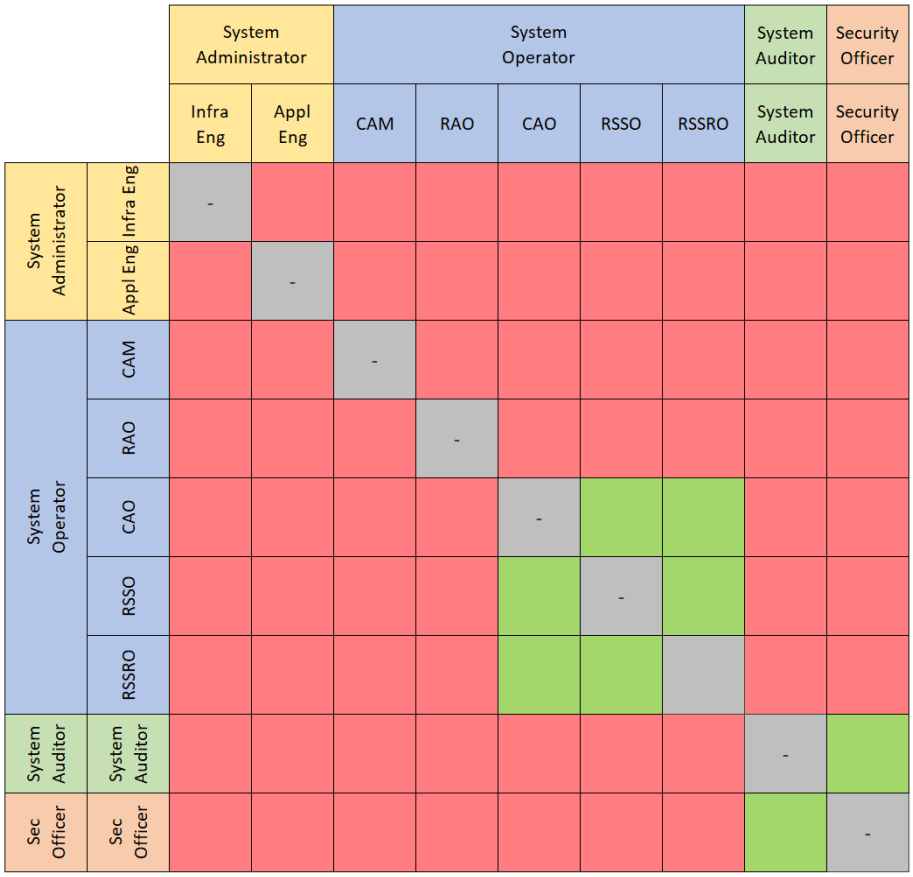

Illustration 2: Permitted combinations of roles

5.3 Personnel controls

The TSP fulfills the requirements for personnel from ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and BRG.

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

5.3.1 Qualifications, experience, and clearance requirements

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

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

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

5.3.2 Background check procedures

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

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

On their first day of work, all SwissSign employees receive an 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 the TSP.

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

5.4 Audit logging procedures

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

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

5.4.1 Types of events recorded

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

- account violations
- user account logon
- all events relating to the synchronisation of the clock to UTC, the detection of loss of synchronisation

- Any security events related to Sytems, Hardware, Network, and physical security including system start-up and shutdown, administration of the trustworthy systems, system crashes and hardware failures, firewall and router activities, and PKI system access attempts.

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

5.4.2 Frequency of processing log

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

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

5.4.3 Retention period for audit log

The log information is kept for one year. The log entries can be viewed with the role Auditor.

5.4.4 Protection of audit log

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

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

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

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

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

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

5.5.1 Types of records archived

The following records are archived:

- All events relating to the life-cycle of keys (CA or subject): key generation, backup, storage, recovery, archival and destruction where applicable,
- All events related to the life-cycle of certificates
- certificate requests (also for renewal, rekey)
- acceptance of terms and conditions
- rejected and approved certificate requests
- certificate signing (also for renewal, rekey)
- certificate revocation and the resulting action (CRL and OCSP entries)
- CRL signing
- CA rollover
- certificate expiration
- certificate downloads/installation
- CAA Check, if applicable
- signature requests (remote signing), if applicable
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles
- All verification activities in accordance with this TSPS and BRG requirements.

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

Protection of the archive is as follows:

- Archived information is only accessible to authorized employees according to the role model as presented in clause 5.2.
- Protection against modification: Archives of digital data are protected according to Swiss law to prevent unknown modification.
- Protection against data loss: The RA must ensure that at least two copies of the archived data is available at all times. The storage locations must be suitable for this purpose and must provide physical protection and access controls.

- Protection against the deterioration of the media on which the archive is stored: Digital data is to be migrated periodically to fresh media.
- Protection against obsolescence of hardware, operating systems, and other software: As part of the archive, the hardware (if necessary), operating systems, and/or other software is archived in order to permit access to and use of archived records over time.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

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

5.5.6 Archive collection system (internal or external)

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

5.5.7 Procedures to obtain and verify 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 CA are available for download on the swisssign.net website and in the public directory directory.swisssign.net. These CA certificates are directly signed by the long-living trust anchors (Root CA) of the SwissSign PKI.

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

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

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

The new Trust Service certificate is generated and distributed according to this TSPS and service-related practice statements.

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 HSM,
- Comporomise of QSCD/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 HSM or QSCD/SSCD 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. Furthermore, the TSP will schedule the revocation of the affected certificates.

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

- The TSP will inform the relevant governmental authorities, the corresponding auditor and the relevant Root Store maintainers of any trust-anchor compromise.
- The TSP informs the relying parties about the incident by means of information on the SwissSign homepage.
- All Subscriber certificates will be revoked.
- The OCSP responder certificate(s) will be revoked
- A last CRL will be issued
- The CA certificate will be revoked.

- A new CARL, i.e. the CRL of the Root CA will be issued and published.
- All Subscribers with certificates issued by either the revoked CA or one of its subordinated issuing CA will be informed by e-mail as soon as possible.
- The cause of the key compromise will be determined and the situation rectified.
- The TSP will generate a new key pair for the new CA and the resulting key certificate will be signed by the superior CA.
- The new CA certificate will be published on the swisssign.com or the swisssign.net web site.

5.7.4 Business continuity capabilities after a disaster

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

5.8 CA or RA termination

The TSP has an up-to-date termination plan to minimize potential 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 TSP terminates its services, the following actions will be executed:

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

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

- The TSP will revoke all Subscriber certificates and will issue for each issuing CA a last CRL.
- The TSP will revoke all issuing CA certificates and issue for each Root CA a last CARL.
- The TSP will transfer obligations for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period such as registration information, certificate status information, and event log archives that cover the respective time to the appropriate organization.
- The TSP will destroy all private keys, including backup copies of the private signing keys of the SwissSign Root CAs and Subordinated Issuing CAs such that the private keys cannot be retrieved, retained, or put back into use.
- All copies of documents which are required to be saved according to the stipulations of any applicable law will be stored under the conditions and for the duration as stipulated in this TSPS.

- The TSP will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period such as to make available the public keys or the trust service tokens to relying parties if applicable.

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

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

6. Technical Security Controls

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

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

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

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

6.1 Key pair generation and installation

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

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

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

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

6.1.1 Key pair generation

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

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

The HSMs are located in a high-security area and operated in FIPS mode, which guarantees that the private keys can never leave the HSM unencrypted. Following the TSP's documented procedures, the key pairs for the Root or subordinated issuing CA of 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.

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.

The Subscriber Private Key generation is specified in the relevant service-based Policy and/or Practice Statement.

6.1.2 Private key delivery to Subscriber

Specified in the relevant service-based Policy and/or Practice Statement.

6.1.3 Public key delivery to certificate issuer

Specified in the relevant service-based Policy and/or Practice Statement.

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.

Further possibilities are included in the relevant service-based Policy and/or Practice Statement.

6.1.5 Key sizes

Specified in the relevant service-based Policy and/or Practice Statement.

6.1.6 Public key parameters generation and quality checking

Specified in the relevant service-based Policy and/or Practice Statement.

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

Specified in the relevant service-based Policy and/or Practice Statement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

6.2.1 Cryptographic module standards and controls

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

Root CA keys	The HSM used for CA keys is kept offline at all times and meets at least FIPS 140-2 level 3 requirements.
Issuing CA keys	The HSM used for CA keys meets at least FIPS 140-2 level 3 requirements. These keys are online and access is strictly controlled by using the '4-eye' principle.

Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

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

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

Root CA keys	Root CA keys can only be accessed on the physical and on the logical level by adhering to '3 out of 6' control, meaning that 3 of the 6 persons are present.
Issuing CA keys	Management access to these keys is only possible using '4-eye' principle (2 out of m). Once the issuing CA is operable, signing operations can be authorized by a single RA operator.

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

Root CA keys	Root CA keys are not in escrow.
Issuing CA keys	The issuing CA keys are not in escrow.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.2.4 Private key backup

The following list shows how private key backup is implemented:

Root CA keys	Root CA keys have been backed up onto an HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access.
Issuing CA keys	The Issuing CA keys have been put into backup HSM, so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 2 persons are present in order to gain physical and logical access.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

Root CA keys	The Root CA keys are not archived.
Issuing CA keys	The Issuing CA keys are not archived.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.2.6 Private key transfer into or from a cryptographic module

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

Root CA keys	The Root CA keys are cloned only into other HSMs providing the same cryptographic security using the functionality provided by the HSM.
Issuing CA keys	The Issuing CA keys are cloned in the same manner as Root keys.

Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.2.7 Private key storage on cryptographic module

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

Root CA keys	The Root CA keys are stored on cryptographic modules so that they can be used only if properly activated.
Issuing CA keys	The Issuing CA keys are stored on cryptographic modules so that they can be used only if properly activated.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

The controls on these processes are explained in clause 6.2.4, Private Key Backup.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

Root CA keys	The Root CA keys are activated with a user key (physical), a user pin (knowledge) and 3 authentication keys (physical).
Issuing CA keys	The Issuing CA keys are activated with role-based access control requiring at least two persons.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

Root CA keys	The Root CA keys are deactivated at least under dual control either by logging out of the HSM, by terminating the session with the HSM, by removing the CA token from the computer or by powering down the system.
Issuing CA keys	The Issuing CA keys are deactivated at least under dual control by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

Root CA keys	The Root CA keys are destroyed at least under dual control by initializing the partition on the HSM.
Issuing CA keys	The Issuing CA keys are destroyed at least under dual control by initializing the partition on the HSM.
Subscriber keys	Specified in the relevant service-based Policy and/or Practice Statement.

All copies of SwissSign private keys are destroyed after their expiry or revocation so that further use or derivation thereof is impossible. If a HSM that was used within the TSP is no longer in use or replaced, the HSM will be physically destroyed.

6.2.11 Cryptographic Module Rating

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

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

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

6.3.2 Certificate operational periods and key pair usage periods

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

- The Root CAs as well as all trust-anchor certificates are valid up to 30 years.
- Issuing CA certificates are issued for a maximum lifetime of 15 years.
- For Subscriber certificates, the validity period is defined in relevant service-based Policy and/or Practice Statement.

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

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

Key changeover will be performed as described in clause 5.6.

6.4 Activation data

6.4.1 Activation data generation and installation

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

For subscriber certificates, the activation data generation and installation is defined in the relevant service-based Policy and/or Practice Statement.

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.
Subscribers keys	Specified in the relevant service-based Policy and/or Practice Statement.

6.4.3 Other aspects of activation data

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

Further aspects defined in in the relevant service-based Policy and/or Practice Statement, if applicable.

6.5 Computer security controls

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

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

6.5.1 Specific computer security technical requirements

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

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

6.5.2 Computer security rating

The TSP has applied procedures which ensure that security patches are applied within a reasonable time after they are available and no later than 6 months from when the security patches are made available. In the case that security patches will be not applied, because they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them, the reasons for not applying the security patches is documented.

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

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

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

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

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 to ensure that security requirements are carried out at the design. The development team adheres to the following principles:

- All software is stored in the Source Code Control System to keep track of software versions.
- The software archive is put onto backup regularly, and a copy is stored externally.

- A Software Life Cycle Control based on separate environments for Development, Test and Production is in place. This software life cycle control ensures adherence to controls and checkpoints within the organization.
- Internal software development policies specify standards and principles for software engineering and related tasks.
- Changes to the systems are accordingly documented.

6.6.2 Security management controls

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

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

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

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

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

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

The TSP monitors the certification status of cryptographic devices.

6.6.3 Life cycle security controls

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

6.7 Network security controls

The TSP has implemented a network concept based on its riks assessment considering functional, logical, and physical relationships between trustworthy systems and services. This ensures that the sensitive CA systems are operated in dedicated secure network zones to protect SwissSign's internal network domains from unauthorized access, including access from subscribers and third parties, or from attacks. For the network concept, a separate documentation is available, which can be viewed on the premises of the TSP in the relevant parts if there is justified interest. To protect the processes of the TSP, among others, firewalls and intrusion detection/prevention mechanisms are used, which only allow explicitly permitted connections. The TSP operates network segments in differentiated severity levels, thereby separating workstation networks from server networks. Same security controls are applied to all systems co-located in the same zone. Access and communication between zones is restricted to those necessary for the operation

of the TSP and communication is established only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure. All other connections, accounts, applications, services, protocols and ports that are not needed are explicitly forbidden or deactivated. Communication channels to external third parties are TLS encrypted.

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

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

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

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

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

The TSP performs:

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

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

6.8 Time-stamping

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

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 PKIs.

7. Certificate, CRL and OCSP Profiles

Specified in the relevant service-based Policy and/or Practice Statement.

7.1 Certificate profile

Specified in the relevant service-based Policy and/or Practice Statement.

7.2 CRL profile

Specified in the relevant service-based Policy and/or Practice Statement.

7.3 OCSP profile

Specified in the relevant service-based Policy and/or Practice Statement.

8. Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

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

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

Once a quarter, the TSP examines 3% of issued certificates for compliance with applicable standards and the quality of TSP services.

8.2 Identity/qualifications of assessor

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

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

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

8.5 Actions taken as a result of deficiency

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

8.6 Communication of results

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

9. Other Business and Legal Matters

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

The TSP charges a fee according to their pricing policy.

9.1.3 Revocation or status information access fees

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

9.1.4 Fees for other services

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

9.1.5 Refund Policy

The TSP has established a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

With regard to the certificates issued pursuant to service-based Policies and Practice statements TSP has entered into a contract for an insurance policy for liability claims against the TSP. The amount of insurance coverage meets the requirements of Article 3 para. 1 ZertES and VZertES Article 2, Baseline Requiremets and EV Guidelines.

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

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

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

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

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 to maintain the privacy of subject information. Information and data can be used where needed for professional handling of the services provided herein. Subscribers and other third parties have to comply with the privacy standards of the TSP.

9.4.1 Privacy Plan

The stipulations of clause 9.3 and 9.4 apply.

9.4.2 Information treated as private

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

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

9.6.2 RA representations and warranties

All registration authorities must warrant full compliance with all provisions stated in this TSPS, service-based Policies and Practice statements, related agreements, Swiss Digital Signature Law (as far as qualified and regulated certificates are concerned), and related regulations and rules.

Any RA operating under this TSPS must adhere to the following rules:

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

9.6.3 Subscriber representations and warranties

Subscribers warrant full compliance with all provisions stated in this TSPS, service-based Policies and Practice statements, related agreements, Swiss Digital Signature Law, CA/B Forum Requirements, Root Store Policies and related regulations and rules.

Subjects and Subscribers are responsible for:

- having a basic understanding of the proper use of public key cryptography and certificates,
- providing only correct information without errors, omissions or misrepresentations,
- substantiating information by providing a properly completed registration form as specified in chapter 3.2,
- supplementing such information with a proof of identity and the provision of the information as specified in chapter 3.1 and 3.2,
- using a secure, and cryptographically sound key pair on a crypto device provided or approved by the registration authority,
- maintaining the crypto device unmodified and in good working order, if applicable,
- verifying the content of a newly issued certificate before its first use and to refrain from using it, if it contains misleading or inaccurate information,
- reading and agreeing to all terms and conditions of this TSPS, other relevant regulations and agreements,
- reading and agreeing to the general terms and conditions of the requested product,
- the maintenance of their certificates using the tools provided by the RA,
- 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 private key by not sharing private keys and passwords and not using easily guessable passwords,
- ensuring complete control over the device containing the authentication means with the capability of generating activation data by not entrusting any person other than the certificate owner himself with the safekeeping of this device and data,
- notifying the registration authority of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate,
- revoking the certificate immediately if any information included in the certificate is misleading or inaccurate, or if any change of circumstances makes the information in the certificate misleading or inaccurate,
- notifying the registration authority immediately of any suspected or actual compromise of the private key and requesting that the certificate be revoked,
- immediately ceasing to use the certificate upon (a) expiration or revocation of such a certificate, or (b) any suspected or actual damage/corruption or (c) any suspected or actual compromise of the private key corresponding to the public key in such a certificate, and immediately removing such a certificate from the devices and/or software onto which it has been installed,
- if the certificate or the corresponding issuing or root certificate has been revoked by the TSP, the TSP will inform the certificate holder who shall no longer use the certificate,
- refraining to use the Subscriber's private key that corresponds to the public key certificate to sign other certificates,
- using their own judgment about whether it is appropriate, given the level of security and trust provided by a certificate issued by this CA, to use such a certificate in any given circumstance,
- using the certificate with due diligence and reasonable judgment,

- complying with all laws and regulations applicable to a Subscriber's right to export, import, and/or use a certificate issued by this CA and/or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.
- submitting applications in form of either paper or electronic documentation which shall include the declaration of consent with the applicable legal documents such as:
    - PKI Disclosure Statement
    - Subscriber Agreement
    - Terms and Conditions under which this CA is made available

9.6.4 Relying Party representations and warranties

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

9.6.5 Representations and warranties of other participants

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

9.7 Disclaimers of warranties

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

9.8 Liability

9.8.1 Liability of the TSP

The TSP is only liable for damages which are the result of SwissSign's failure to comply with this TSPS, service-based Policies and Practice statements and which were provoked deliberately or wantonly negligent.

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

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

9.8.2 Liability of the Subscriber and subject

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

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

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

This TSPS, service-based Policies and Practice statements 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 TSPS, service-based Policies and Practice statements.

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 TSPS, service-based Policies and Practice statements upon the approval of the executive board of the TSP.

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

9.12.2 Notification mechanism and period

The TSP executive board can decide to amend this TSPS, service-based Policies and Practice statements and respective amendments without notification for amendments that are non-material (with little or no impact).

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

All changes to the TSPS, service-based Policy and/or Practice Statement will be published after approval as described in chapter 2.

9.12.3 Circumstances under which OID must be changed

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

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

9.13 Dispute resolution provisions

Complaints regarding compliance with or implementation set forth in this TSPS and of the service-based Policies and Practice statements must be submitted in writing to the TSP in the contact details described in clause 1.5.2. In case of any dispute or controversy in connection with the performance, execution or interpretation of this agreement that can not be resolved within a period of four weeks after submission of the complaint, the parties are free to file action with the courts pursuant to clause 9.14.

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

9.14 Governing law 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 TSPS, service-based Policy and/or Practice Statement and rights or obligations related hereto are in accordance with the relevant provisions of the Swiss Digital Signature Law, CA/B Forum Requirements, Root Store Policies and of the other applicable standards. Compliance with the laws and regulations are verified within the annual external audit. The audits are carried out by an independent qualified auditor.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

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

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

9.16.2 Assignment

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

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

9.16.3 Severability

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

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

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

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

The TSP will communicate an appropriate change within 90 days.

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

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

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

9.17 Other provisions

9.17.1 Language

If this TSPS, service-based Policies and Practice Statements are provided in additional languages to English, the English version will prevail.

9.17.2 Delegated or outsourced Services

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