SwissSign Gold CP/CPS

Certificate Policy and Certification Practice Statement of the SwissSign Gold CA and its subordinated issuing CA.

Document Type:	Certificate Policy and Certification Practice Statement
OID:	2.16.756.1.89.1.2.1.12
Author:	Information Security and Compliance
Classification:	C1 (public)
Applicability:	Global
Owner:	CEO
Issue Date:	November 25th, 2019
Version:	2.8.0.
Obsoletes:	Version 2.7.0, December 17th, 2018
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

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

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

© SwissSign AG, 25.11.2019

Version Control

Date	Version	Comment	Author
24.03.2004	0.0.0	Pre-certification version	Joseph A. Doekbrijder
12.07.2006	2.0.0	Revision	Melanie Raemy
24.07.2006	2.0.1	Review	Michael Doujak
19.10.2006	2.0.2	Review, Minor changes	Björn Kanebog
21.12.2006	2.0.3	Review	Melanie Raemy, Michael Doujak
11.05.2007	2.0.4	Review, Minor changes	Björn Kanebog
27.06.2007	2.0.5	Extensions : code signing certificates, domain validation	Melanie Raemy
09.04.2008	2.1.0	New layout, Review, added changes about life cycle management	Björn Kanebog
10.04.2008	2.1.0	Review	Michael Doujak
10.07.2008	2.1.1	Added additional validation procedures for Extended Validation SSL certificates. Minor other changes	Björn Kanebog
14.10.2008	2.2.0	Update for Extended Validation SSL Certificates	Michael Doujak
19.11.2008	2.2.1	Update for flexible pseudonym identifiers.	Michael Doujak
03.02.2009	2.2.2	Amended EV OID	Michael Doujak
02.11.2009	2.2.3	Service Availability, Organization Certificates, key sizes,	Michael Doujak
06.05.2010	2.3.0	Added UCC certificates and G3 Root certificates	Michael Doujak
11.08.2011	2.3.1	Domain validation, alternative name forms, SSL Server validation, revocation circumstances, identification document	Michael Doujak
26.03.2012	2.3.2	prohibit MitM and traffic management	Michael Doujak
26.06.2012	2.3.3	Adjustments to the CA/Browser Forum Baseline Requirements	Christoph Stalder
30.09.2014	2.4.0	Added new Issuing CAs; Adjustment for Multidomain Certificates	Cornelia Enke
13.10.2014	2.4.1	Requirements for Organization Validation improved	Cornelia Enke
30.04.2015	2.4.2	added CT-Log and CAA	Cornelia Enke
13.09.2017	2.4.3	Updated CT-LOG and CAA	Cornelia Enke
12.10.2017	2.4.4	Updated after auditor review	Cornelia Enke
16.07.2018	2.5.0	Update regarding ETSI Regulations	Cornelia Enke
18.10.2018	2.6.0	Updated after auditor review	Jürg Eiholzer
17.12.2018	2.7.0	Correction CA hierarchy, Removal G3 CA hierarchy	Michael Guenther
25.11.2019	2.8.0	Improvement CA hierarchy, Removal revoked Issuing CA	Nathalie Weiler

© SwissSign AG, 25.11.2019

© SwissSign AG, 25.11.2019

Authorization

Date	Approved by	Approved by	Version
~~24.07.2006~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~2.0.0 / OID=1~~
~~21.05.2007~~	~~Melanie Raemy~~	~~Björn Kanebog~~	~~2.0.4 / OID=1~~
~~26.07.2007~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~2.0.5 / OID=2~~
~~17.04.2008~~	~~Adrian Humbel~~	~~Björn Kanebog~~	~~2.1.0 / OID=3~~
~~19.11.2008~~	~~Freddy Kaiser~~	~~Michael Doujak~~	~~2.2.1 / OID=4~~
~~28.02.2009~~	~~Freddy Kaiser~~	~~Michael Doujak~~	~~2.2.2 / OID=4~~
~~15.05.2010~~	~~Adrian Humbel~~	~~Michael Doujak~~	~~2.3.0 / OID=5~~
~~24.08.2011~~	~~Adrian Humbel~~	~~Michael Doujak~~	~~2.3.1 / OID=5~~
~~20.04.2012~~	~~Urs Fischer~~	~~Reinhard Dietrich~~	~~2.3.2 / OID=5~~
~~28.06.2012~~	~~Urs Fischer~~	~~Reinhard Dietrich~~	~~2.3.3 / OID=5~~
~~30.09.2014~~	~~Cornelia Enke~~	~~Reinhard Dietrich~~	~~2.4.0 / OID=6~~
~~13.10.2014~~	~~Reinhard Dietrich~~	~~Urs Fischer~~	~~2.4.1 / OID=6~~
~~30.04.2015~~	~~Reinhard Dietrich~~	~~Urs Fischer~~	~~2.4.2 / OID=6~~
~~14.09.2017~~	~~Reinhard Dietrich~~	~~Markus Naef~~	~~2.4.3 / OID=7~~
~~12.10.2017~~	~~Reinhard Dietrich~~	~~Markus Naef~~	~~2.4.4 / OID=8~~
~~16.07.2018~~	~~Reinhard Dietrich~~	~~Markus Naef~~	~~2.5.0 / OID=9~~
~~22.10.2018~~	~~Matthias Bartholdi~~	~~Markus Naef~~	~~2.6.0 / OID=10~~
~~17.12.2018~~	~~Matthias Bartholdi~~	~~Markus Naef~~	~~2.7.0 / OID=11~~
25.11.2019	Nathalie Weiler	Markus Naef	2.8.0 / OID=12

Markus Naef (Qualified Signature)

Digital unterschrieben von Markus Naef (Qualified Signature)
Datum: 2019.11.25 13:04:39 +01'00'

digital signature

Nathalie Weiler (Qualified Signature)

Digitally signed by Nathalie Weiler (Qualified Signature)
Date: 2019.11.25 10:38:04 +01'00'

digital signature

Table of Contents

© SwissSign AG, 25.11.2019

© SwissSign AG, 25.11.2019

1. Introduction

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

This Trust Service Provider (TSP) document describes the Certificate Policy / Certification Practice Statement CP/CPS of the trust services provided by SwissSign AG. The structure of this document corresponds to RFC3647. Under this CP/CPS the TSP operates all Trust Services published under the root "SwissSign Gold CA G2".

This Root Certificate Authorities are operated by SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Switzerland and only issue certificates to its subordinated issuing CA.

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, shall remain responsible for compliance with the procedures for the purposes of this document or any legal or certification requirements to the TSP.

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

For the issuance of SSL certificates for extended validation (EV) and organization validation (OV), SwissSign fully complies with the rules and regulations published by the CA/Browser Forum, using the currently valid versions (http://www.cabforum.org):

- BR Guidelines: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"
- EV Guidelines: „Guidelines for the Issuance and Management of Extended Validation Certificates"
- ETSI EN 319 401 (2018): General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI TS 119 312 (2019): Cryptographic Suites
- IETF RFC 6960 (2013): Online Certificate Status Protocol - OCSP
- IETF RFC 3647 (2003): Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- IETF RFC 5280 (May 2008): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The TSP issues under this roots certificates that meet the stipulations of :

- NCP
- NCP+
- EVCP
- CAB-EV
- OVCP
- CAB-OV-o

In this CP/CPS, "this CA" refers to the "SwissSign Gold CA G2" and all its subordinated issuing CAs, unless stated differently.

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

1.1 Overview

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

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

© SwissSign AG, 25.11.2019

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

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

The TSP provides a detailed product overview on the website (swisssign.com) for Gold Certificates and for other services.

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

1.2 Document name and identification

This document is named ”SwissSign Gold CP/CPS - Certificate Policy and Certification Practice Statement of the SwissSign Gold CA and its subordinated issuing CAs“ as indicated on the cover page of this document.

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

The Object Identification Number (OID) for this and only this document is 2.16.756.1.89.1.2.1.12

According to the requirements for **EV certificates**, SwissSign uses the following OIDs to identify its EV certificates:

SwissSign OID:	2.16.756.1.89.1.2.1.1
CA/B Guidelines for EV:	2.23.140.1.1
ETSI EN 319 411-1:	0.4.0.2042.1.4

The last position of the OID represents the document version.

1.3 PKI Participants

1.3.1 Certification Authorities

The TSP operates a Public Key Infrastructure, consisting of a “SwissSign Gold CA” and its subordinated issuing CAs. The issuing CAs listed in chapter 7.1.2.1 are the only public CAs operated by the TSP that issue certificates under this CP/CPS.

1.3.2 Registration Authorities

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

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

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

- The RA must have a contractual agreement with the TSP which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities.
- The registration process must meet the stipulations of EU Regulation No 910/2014 ,Swiss Digital Signature Law, the BR and EV Guideline. It must be documented, published, and distributed to all parties involved in the RA process.
- Other 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 CP/CPS 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.

© SwissSign AG, 25.11.2019

- The information collected during the RA process is subject to applicable data protection regulations. Compliance with these provisions must be demonstrated (Chapters 9.3 and 9.4).

1.3.3 Subscribers

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

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

Subscribers and Requesters are responsible for:

- having a basic understanding of the proper use of public key cryptography and certificates,
- providing only correct information without errors, omissions or misrepresentations,
- substantiating information by providing a properly completed registration form as specified in chapter 3.2,
- supplementing such information with a proof of identity and the provision of the information as specified in chapter 3.1 and 3.2,
- using a secure, and cryptographically sound key pair,
- 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 CP/CPS, other relevant regulations and agreements,
- reading and agreeing to the general terms and conditions of the requested product,
- the maintenance of their certificates using the tools provided by the 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,
- 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,

© SwissSign AG, 25.11.2019

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

1.3.4 Relying Parties

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

Relying Parties can also be Subscribers within this CA.

1.3.5 Other participants

Not applicable

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The following certificates are issued under this CA:

(NCP) E-Mail ID Gold Certificates are issued with the following key usage bits set: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment and keyAgreement. The extended key usage is set with ClientAuthentication, emailProtection, Microsoft Encrypted File System (msEFS), Microsoft Smart Card Logon (msSCL).

(NCP+) Code Signing Certificates are currently not issued since 1.1.2019.

(OVCP) SSL Gold Certificates are issued with the following key usage bits set: digitalSignature and keyEncipherment. The extended key usage is set with ServerAuthentication and ClientAuthentication.

(EVCP) EV Gold Certificates are issued with the following key usage bits set: digitalSignature and keyEncipherment. The extended key usage is set with ServerAuthentication and ClientAuthentication.

1.4.2 Prohibited certificate uses

Any other use than defined in chapter 1.4.1 is prohibited.

The key usage bit digitalSignature of E-Mail ID Gold, SSL Gold or EV Gold Certificates does not allow the certificate to be used for qualified digital signatures mentioned in Article 14 para. 2bis OR (Swiss Code of Obligations).

© SwissSign AG, 25.11.2019

1.5 Policy administration

1.5.1 Organization administering the document

The SwissSign Gold CP/CPS is written and updated by SwissSign AG.

SwissSign AG

Sägereistrasse 25
8152 Glattbrugg
Switzerland
Tel.: +41 848 77 66 55
Mail: info@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

CEO

Sägereistrasse 25
8152 Glattbrugg
Switzerland
Tel.: +41 848 77 66 55
Mail: info@swisssign.com
Web: https://swisssign.com

Business hours are business days (excluding public holidays) from 08:00 to 12:00, 13:00 to 17:00 CET/CEST.

1.5.3 Person determining CPS suitability for the policy

The Board of Directors of SwissSign AG determines the suitability of this CP/CPS document.

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

1.5.4 CP/CPS approval procedures

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

© SwissSign AG, 25.11.2019

1.6 Definitions and acronyms

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.
Certification Authority Authorization	CAA	RFC 6844 defines a Certification Authority Authorization DNS Resource Record (CAA). A CAA allows a DNS domain name holder to specify the CAs authorized to issue certificates for that domain. Publication of the CAA gives domain holders additional controls to reduce the risk of unintended certificate misissuance.
CA Operator	CAO	A person responsible for CA operation, including establishment of certificate parameters for RA and RAO in accordance with certificate policy.
Certificate		Information issued by a trusted third party, often published in a directory with public access. The certificate contains at least a subject, a unique serial number, an issuer and a validity period.
Certification Authority	CA	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certificate Extension		Optional fields in a certificate.
Certificate Policy	CP	A set of rules that a request must comply with in order for the RA to approve the request or a CA to issue the certificate.
Certificate Revocation List	CRL	List of certificates that have been declared invalid. This list is issued by the CA at regular intervals and is used by applications to verify the validity of a certificate.
Certification Practice Statement	CPS	Document that regulates the rights and responsibilities of all involved parties (RA, CA, directory service, end entity, Relying Party).
Certification Service Provider	CSP	Individual or corporation that issues certificates to individual or corporate third parties.
Cipher		A cryptographic algorithm used to encrypt and decrypt files and messages.
Cipher Text		Data that has been encrypted. Cipher text is unreadable unless it is converted into plain text (decrypted) with a key.
Chief Security Officer	CISO	the senior-level executive within the TSP responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

© SwissSign AG, 25.11.2019

Term	Abbrev.	Explanation
Coordinated Universal Time	UTC UTC(k)	Mean solar time at the prime meridian (0°). The time scale is based on seconds as defined in ETSI EN 319 421. Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.
Credentials		Evidence or testimonials governing the user's right to access certain systems (e.g. User name, password, etc.)
Certificate Transparency	CT	Is an experimental IETF open standard (RFC 6962) and open source framework for monitoring and auditing digital certificates. Through a system of certificate logs, monitors, and auditors, certificate transparency allows website users and domain owners to identify mistakenly or maliciously issued certificates and to identify certificate authorities (CAs) they issued such certificates.
Decryption		The process of transforming cipher text into readable plain text.
DES		Data Encryption Standard. A cipher developed by the United States government in the 1970s as the official encryption algorithm of the U.S.
Digital signature		A system allowing individuals and organizations to electronically certify features such as their identity or the authenticity of an electronic document.
Directive No 910/2014 /EC		European digital signature law: Directive No 910/2014 /EC of the European Parliament and of the Council of 23 July 2014 on a community framework for electronic signatures. Compliance with this law always implies compliance with the following standards: ETSI EN 319 401, 319 411-1, 319 411-2, policy QCP-n-qscd
Distinguished Name	DN	-> Subject
DNS		Domain Name System. The Internet system of holding a distributed register of entity names. For example, the domain is the part of the email address to the right of the `@', e.g. `anytown.ac.uk'.
Electronic Signature		-> Digital Signature
Encryption		Encryption is the process of using a formula, called an encryption algorithm, to transform plain text into an incomprehensible cipher text for transmission.
End Entity		Used to describe all end users of certificates, i.e. Subscribers and Relying Parties.
Subscriber Agreement	EUA	Contractual agreement between seller of certificates and the Subscriber.
Enterprise EV Certificate		An EV certificate that an enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original valid EV certificate issued to the enterprise RA.
Entropy		A numerical measure of the uncertainty of an outcome. The entropy of a system is related to the amount of information it contains. In PKI and mathematics, a cryptographic key contains a certain amount of information and tends to lose a small amount of entropy each time it is used in a mathematical calculation. For this reason, one should not use a key too frequently or for too long a period.

Term	Abbrev.	Explanation
EV Certificate		A digital certificate that contains information specific in the EV guidelines and that has been validated in accordance with the guidelines.
Extended Validation	EV	Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.
Extension		-> Certificate Extension
FIPS 140		FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules.
FQDN	FQDN	Fully Qualified Domain Name.
FTA	FTA	Federal Tax Administration (Eidgenössische Steuerverwaltung, ESTV)
General Data Protection Regulation	GDPR	The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union.
Hardware Security Module	HSM	Hardware Security Module is a device that physically protects key material against unauthorized parties.
HTTP	HTTP	Hyper-Text Transfer Protocol used by the Internet. HTTP defines how data is retrieved or transmitted via the Internet and what actions should be taken by web servers and browsers.
HTTPS	HTTPS	Secure Hyper-Text Transfer Protocol using TLS/SSL
Key		The secret input for cryptographic algorithms that allows a message to be transformed. -> See Private Key, Public Key
Key password		Password used to encrypt the private key.
Key size		Length of private and public key. Regular key sizes are 512, 768, 1024, 2048 and 4096. 2048 bit is the recommended key size according to NIST today.
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.
Lightweight Directory Access Protocol	LDAP	LDAP is used to retrieve data from a public directory.
LDAP Secure	LDAPS	LDAP secured with TLS/SSL
Man-in-the-middle	MITM	Active eavesdropping of secure communications in which attacker/third party relays and controls messages between sender and receiver.
Online Certificate Status Protocol	OCSP	Method to verify the validity of a certificate in real time.
Participants		Entities like CAs, RAs, and repositories. These can be different legal entities.

© SwissSign AG, 25.11.2019

Term	Abbrev.	Explanation
PKCS		PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Laboratories.
Plain Text		The original message or file.
Privacy Level		Used to determine how the certificate can be accessed in the directory. Private, Public Lookup and Public Download are the available levels.
Private Key		One of two keys used in public key cryptography. The private key is known only to the owner and is used to sign outgoing messages or decrypt incoming messages.
Profile		A user profile is a personal area where end users can access and manage their digital identities and requests directly on the TSP web page. Access to this profile can be granted by means of user name and password.
Public Key		One of two keys used in public key cryptography. The public key can be known to anyone and is used to verify signatures or encrypt messages. The public key of a public-private key cryptography system is used to verify the “signatures” on incoming messages or to encrypt a file or message so that only the holder of the private key can decrypt the file or message.
Public Key Infrastructure	PKI	Processes and technologies that are used to issue and manage digital identities that may be used by third parties to authenticate individuals or organizations.
Qualified Certificate	QC	Certificate which meets the requirements of ETSI EN 319 411-1/2 and article 8 ZertES.
Qualified Certificate Policy	QCP	Certificate policy which incorporates the requirements laid down in ETSI EN 319-401 and ETSI EN 391 411-2.
Qualified Digital Signature		qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures, as defined in article 3 (12) of the Directive No 910/2014 and in ZertES article 2 e
RA Operator	RAO	The person responsible for identifying the requester, collecting the identity substantiating evidence, authorizing the CSR, and forwarding the authorized CSR to the CA.
Recognition Body		The Recognition Body of Switzerland is accredited by the SAS and conducts the audits prescribed by Swiss Digital Signature Law.
Recognized Qualified Digital Signature		Qualified digital signature created with a certificate issued by a CA that has successfully been certified by a Swiss recognition body.
Registration Authority	RA	A registration authority (RA) verifies the identity of entities requesting their digital certificates and tells the Certificate Authority (CA) to issue it.
Relying Party		Recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate.
Requester		Requesters are individuals or organization that have requested, but not yet obtained a certificate.

Term	Abbrev.	Explanation
Revocation		Invalidation of a certificate. Every CA regularly issues a list of revoked certificates called CRL. This list should be verified by all applications using certificates from that CA before trusting a certificate.
Rollover		To rollover a certificate means that a new certificate is issued while the old one is still valid and usable. The rollover is used to issue a new CA certificate while keeping the old one valid along with all the certificates issued with it.
RSA		A public key encryption algorithm named after its founders: Rivest-Shamir-Adleman.
S/MIME		Secure / Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail.
Secure Signature Creation Device	SSCD	Signature-creation device which meets the requirements specified in article 30 of Directive No 910/2014 /EC.
Smart-card		Credit Card or SIM-shaped carrier of a secure crypto processor with tamper-resistant properties intended for the secure storage and usage of private keys.
Signature		Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
Signature-creation data		Unique data, such as parameters of signature algorithms or private cryptographic keys, used by the signatory to create an electronic signature.
Signature-creation device		Configured software or hardware used to implement the signature-creation data
Signature-verification data		Data, such as parameters of signature algorithms or public cryptographic keys, used for the purpose of verifying an electronic signature.
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
SSO		Single Sign On: The user only needs to log in once to access various services.

© SwissSign AG, 25.11.2019

Term	Abbrev.	Explanation
Subject	DN	Field in the certificate that identifies the owner of the certificate. Also referred to as distinguished name (DN). Examples: /CN=John Doe /Email=jd@signdemo.com /CN=pseudo: Marketing /O=SwissSign AG /C=CH /Email=marketing@signdemo.com /CN=John Doe /O=SwissSign AG /OU=DEMO/C=CH /Email=john.doe@signdemo.com /CN=swiss.signdemo.com /O=SwissSign AG /organizationIdentifier = NTRCH-CHE-109.357.012 /OU=DEMO /C=CH /Email=info@swisssign.li mandatory fields in the subject: Common Name --- /CN (2.5.4.3) optional fields in the subject: Email address --- /Email (1.2.840.113549.1.9.1) Organization --- /O (2.5.4.10) organizationIdentifier --- /OID (2.5.4.97) Organizational Unit --- /OU (2.5.4.11) Country Name --- /C (2.5.4.6) Locality Name --- /L (2.5.4.7) Street Address --- /Street (2.5.4.9) Postal Code --- /PostalCode (2.5.4.17) Given Name --- /GN (2.5.4.42) Surname --- /SN (2.5.4.4) Serial Number --- /serialNumber (2.5.4.5) Business Category --- /BC (2.5.4.15) Jurisdiction of Incorporation Locality --- /joiL (1.3.6.1.4.1.311.60.2.1.1) Jurisdiction of Incorporation State --- /joiST (1.3.6.1.4.1.311.60.2.1.2) Jurisdiction of Incorporation Country --- /joiC (1.3.6.1.4.1.311.60.2.1.3)
Subscriber		Subscribers are individuals that have obtained a certificate.
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.
Time-stamp Policy	TP	Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements.
Time-stamp Token	TST	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time-stamping Unit		Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.

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

© SwissSign AG, 25.11.2019

2. Publication and Repository Responsibilities

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

2.1 Repositories

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

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

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

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

2.2 Publication of certification information

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

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

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

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

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

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

2.3 Time or frequency of publication

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

The TSP publishes this information on a regular schedule:

- CRLs are published according to the schedule detailed in chapter 4.9.7.
- OCSP Information: Real-time. The OCSP responder immediately reports a certificate that has been revoked. See also chapter 4.9.9.

2.4 Access controls on repositories

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

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

Management access always requires two factor authentication.

2.5 Additional testing

Demo pages are offered for all web server certificate types.

SSL Gold and EV Gold Certficates:

Status	SSL Gold Certificates (OV)	EV Gold Certificates (EV)
Valid	https://gold-g2-valid-cert-demo.swisssign.net	https://ev-g2-valid-cert-demo.swisssign.net
Expired	https://gold-g2-expired-cert-demo.swisssign.net	https://ev-g2-expired-cert-demo.swisssign.net
Revoked	https://gold-g2-revoked-cert-demo.swisssign.net	https://ev-g2-revoked-cert-demo.swisssign.net

E-Mail ID Gold Certificates

https://repository.swisssign.com/reference_certs/

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) in a certificate issued by this CA complies with the X.500 standard and with RFC 5280.

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

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

- given name, middle name and surname,
- pseudonyms
- fully qualified domain names (FQDN).

Real names are specified as /CN='given name' optional 'middle name' 'surname' or /CN='organizational name'.
Underscore characters are not allowed in a any part of the subject information.

- Given name, middle name and surname in the CN have to be identical to the names as they appear in the identifying documentation provided. Characters are encoded according to chapter 3.1.4. Abbreviations or nicknames without substantiating identifying documentation are prohibited. Names consisting of multiple words are permissible.
- The organizational name in /O must be spelled absolutely identical to the name as it appears in the documentation provided according to chapter 3.2.2.
- If a /O field is present, the /C field must also be present.

FQDNs must be well formed according to RFC 1035. The permitted methods are described in chapter 3.2.2.

SubjectAltName is an optional field for E-Mail ID Gold Certificates issued with real names or pseudonyms. If present, it contains at least an email address.

SubjectAltNames in EV and OV SSL certificates contain at least the CN of the certificate.

Additional attributes in the SubjectAltName are permissible in any certificate and may be supported by the RA at their own discretion:

- otherName: content to be verified by the RA.
- rfc822Name: e-mail address according to RFC 5322
- dNSName: FQDN, fully qualified domain name according to RFC 1035
- x400Address: content to be verified by the RA
- directoryName: content to be verified by the RA
- ediPartyName: content to be verified by the RA
- uniformResourceIdentifier: URI according to RFC 3986
- iPAddress: IP v4 or IP v6 address, that is not in the private address space according to RFC 1918
- registeredID: OID, content to be verified by the RA

Prohibited IPv4 or IPv6 addresses are these, that the IANA has marked as reserved:

- http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
- http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

For Extended Validation Certificates the following, additional rules apply:

- The certificate subject must conform to the EV guidelines
- Wildcard certificates are not allowed

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of Subscribers

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

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

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

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

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

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

- The TSP has approved the identifier.
- The identifier and the resulting /CN= values are neither incorrect nor misleading.
- The identifier is alphabetical and can be used with the <identifier><colon><space> formatting.

3.1.4 Rules for interpreting various name forms

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

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

- In general, national characters are represented by their ASCII equivalent, e.g. é, è, à, ç are represented by e, e, a, c.
- The German "Umlaut" characters ä, ö, ü are represented by either ae, oe, ue or a, o, u.
- SwissSign follows RFC 3490 (to_ascii, to_unicode), RFC 3491 (nameprep) and RFC 3492 (punycode) guidelines to internationalize domain names.

3.1.5 Uniqueness of names

All CAs issued under this CP/CPS enforce the uniqueness of certificate subject fields in such a manner that all certificates with identical subject fields must belong to the same individual or organization. The following rules are enforced:

- All actual valid certificates for individuals with identical subjects must belong to the same individual.
- All actual valid organizational certificates with identical subjects must belong to the same organization.
- All actual valid server certificates with identical subjects must belong to the same domain owner.

© SwissSign AG, 25.11.2019

3.1.6 Recognition, authentication, and role of trademarks

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

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

3.2 Initial identity validation

The initial identity validation is part of the Certificate Application process as described in chapter 4.1. Existing evidences can be re-used to validate the identity depending on whether the validity of the evidence. These evidences must not be older than 13 months (EV products) resp. 825 days (OV products).

The TSP has implemented procedures that identify certain certificate requests they will require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval. Each certificate request that is categorized as High Risk Certificate Request is reviewed separately by a member of the compliance department of the TSP.

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

3.2.1 Method to prove possession of private key

The Certificate Signing Request sent to the CA from the Subscriber is signed with the private key. The requester must present a PKCS#10 formated request.

3.2.2 Authentication of organization identity (ncp+, OVCP, EVCP)

Individuals may use a legal entity's name as.organization name with sufficient authorization by the legal entity. The TSP follows the requirements of ETSI EN 319 411-1.

The DN of a certificate issued by one of the subsidiaries of this CA may contain one instance of the organization field. Should the requester decide to make the organization field part of the DN, the following rules must be adhered to:

- The use of the organization field means that the use of the country field is mandatory.
- The registration process of any registration authority operating under this CP/CPS must contain provisions to determine the identity of an organization and to authorize the use of its name.
- To validate the name and location of the organization, the requester must provide official documentation about the organization provided by a government agency in the jurisdiction of the organization's legal creation, existence, or recognition or by any other official source.
- Organizations with an entry in the federal or a nationally recognized commercial register must supply verifiably current excerpt. All other organizations must supply either the certificate of registration with the FTA or a current VAT invoice.
- Government entities must supply official documentation to prove the existence and the correct spelling of the entities name. RAs operating under this CP/CPS may choose to validate an organization's name directly with the authoritative source instead of the organization, and handwritten personal signatures must be included on the registration form number (UID) of the organization. The number of the commercial register entry as well as the VAT number or a number assigned by SwissSign can be entered.
- The use of a domain name in an FQDN must be authorized.The TSP only accepts the automated SwissSign-check procedure as proof of domain ownership. In this automated procedure, the applicant must prove control of the domain according to the methods for domain validation permitted in chapter 3.2.2.4 of the CA Browser Forum Baseline Requirements (BR). To check access to the domains, the random value generated by the TSP must be stored at one of the following three locations on the domain owners Website. Internal domain names that cannot be accessed through public DNS are not accepted by the TSP, in particular domain names containing a gTLD which is not yet

resolvable. The system checks for 30 days whether the random value was stored at one of the three places mentioned below. Only after a successful check is control of the domain ownership completed.

  - BR 3.2.2.4.4 Constructed Email to Domain Contact
  - BR 3.2.2.4.6 Agreed-Upon Change to Website
  - BR 3.2.2.4.7 DNS Change
- An organization may contractually define that all certificates using the name of the organization in the /O= field may only contain e-mail addresses in the /email= field that are in the domain of the organization. Should such a contract exist, the organization takes full responsibility for the proper management of e-mail accounts. Therefore, the requirement to verify individual e-mail addresses during the registration process is optional.

EV Certificates will only be issued in accordance with the EV Guidelines to the following types of organizations:

- Private Organizations
- Government Entities
- Business Entities
- Non-commercial Entities

Any RA operating under this CP/CPS must implement a registration process that meets the requirements of the EV Guidelines and that authenticates the organization identity in accordance with these guidelines.

For Organizations acting as Business Entity a Face to Face Identification is required.

3.2.3 Authentication of individual identity (ncp)

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

- The requester must be present in person or in an equivalent procedure according to ETSI EN 319 411-1 6.2.2. This step may be conducted by:
  - the registration authority processing the certificate request,
  - an accredited notary,
  - a trained and contracted partner for the identification service.
- The individual must present a valid original of an official identification document as recognized by ETSI EN 319 411-1. The identifying agent is to make a high-quality copy, scan or photograph of the identifying document and to confirm proper execution of the identification in writing or electronically as agreed with the TSP.
- The photo in the identifying document is compared to as has to match (facial features, age, gender and size) the person present as described above.
- If the /Email= field is used, the e-mail address must be verified during the registration process, the requester must prove that he has access to the mailbox and that he can use it to receive mail.
- Only address information verified in context of legal identity may be included in certificate requests.

Other RA's may implement a different process if they meet the following requirements:

- The registration process must be documented and presented to the TSP.
- The other RA is only allowed to execute their registration process if the TSP has audited and approved the process as equivalent to the registration process of the SwissSign RA.
- RA’s other than the SwissSign RA may choose to accept different identifying documents or information sources. Such documents or information sources may contain name forms that differ from official identity documents.

- Any RA operating under this CP/CPS must implement a registration process that meets the requirements of the BR and EV Guidelines and that authenticates the individual identity in accordance with these guidelines.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

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

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

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

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

3.2.6 Criteria for interoperation

(ncp) This CA supports multiple registration authorities. In order to become an authorized registration authority, the respective authority must sign a contractual agreement with SwissSign binding them to this CP/CPS and ensuring that all the processes and procedures of the authority meet the minimum requirements specified in this CP/CPS.

The requirements to be met by the authority must include but are not limited to:

- signing a contractual agreement with SwissSign,
- being compliant with the stipulations of this CP/CPS,
- having passed and keeping current a WebTrust or ETSI audit,
- publishing its own CPS (certification practice statement).

SwissSign does not support cross-certification.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The requester is identified by the SwisSign RAO using the contact information from the original request.

The validity period for the data included in an EV certificate is limited to 13 months. After this period, the data provided in the certificate must be validated again.

The validity period for the data included in an OVCP certificate is limited to 27 months (<825 days). After this period, the data provided in the certificate must be validated again.

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

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

- successful login to the user profile on the website of the RA,
- providing proof of the possession of the private key on the web site of the registration authority,
- with a personal signature on a revocation form,
- appearance in person at the registration authority,
- providing a one-time revocation key on the web site of the registration authority.

Not all registration authorities must support all methods of revocation.

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

© SwissSign AG, 25.11.2019

4. Certificate Life-Cycle Operational Requirements

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

4.1 Certificate application

4.1.1 Who can submit a certificate application

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

4.1.2 Enrollment process and responsibilities

The registration authority must establish an enrollment process that meets the requirements of ETSI EN 319 411-1, the CA Browser Forum Baseline Requirements and EV Guidelines.

The RA has a valid contract with the TSP.

The RA is only allowed to execute their registration process if the TSP has audited and approved the process as equivalent to the registration process of the SwissSign RA.

The RA collects the following during its enrollment process:

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

The RA collects and verifies all the required documentation according to chapter 3.

The RA personalizes and disseminates an SSCD in a secure manner to the requester and ensure that the activation data is only known to the requester.

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

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

- Valid identification documentation is provided and complete registration forms have been signed, and the CP/CPS and End-User Agreement have been accepted by the subscriber,
- all documents and informations are approved by the SwissSign RA.

© SwissSign AG, 25.11.2019

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

Prior to issuance SwissSign validates each server Name FQDN in publicly trusted SSL certificates against the domain CAA records. If a CAA record exists that does not list swisssign.com as an authorized CA, SwissSign will not issue the certificate. If the verification of the CAA entry fails or is not possible for technical reasons, no certificate will be issued.

SwissSign:

- caches CAA records for reuse for up to 8 hours,
- supports the issue and issuewild CAA tags,
- processes but does not act on iodef property tag (i.e., SwissSignSign does not dispatch reports of such, issuance requests to the contact(s) stipulated in the CAA iodef record(s)),
- does not support any additional property tags,
- if a CAA check cannot be executed for any reason, no certificate will be issued.

Before issuing an EV certificate, SwissSign ensures that all subject organisation information in the EV certificate conforms to the requirements of, and has been verified in accordance with, the EV Guidelines and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended accomplish the following:

Verify the organization's existence and identity, including:

- the organization's legal existence and identity (as established with an incorporating agency),
- the organization's physical existence (business presence at a physical address),
- the organization's operational existence (business activity),
- that the organization (or a corporate parent/subsidiary) is a registered holder or has exclusive control of the domain name to be included in the EV certificate.

Verify the requester's authorization for the EV certificate, including:

- the name, title, and authority of the certificate requester,
- that the certificate requester signed the registration form,
- the authority to approve the EV certificate request („certificate approver" role according to CA Browserforum),
- the authority to approve the Terms and Conditions („contract signer" role according to CA Browserforum).

The TSP has implemented technical contraints that determines that the wildcard character does not occur in the first label position to the left of a "registry-controlled" label or "public suffix".

4.2.2 Approval or rejection of certificate applications

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

- the requester has presented the identifying documentation according to chapter 3.2.3,
- all documentation has been received and verified successfully,
- all authorizations have been received and verified successfully,
- the information provided in the registration form is deemed adequate and complete,
- the verification of the Uniqueness of Names according to chapter 3.1.5 has not revealed any collisions.
- for EV certificates that all stipulations of the EV Guidelines have been met.

© SwissSign AG, 25.11.2019

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

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

4.2.3 Time to process certificate applications

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

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

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

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

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

4.3.2 Notification to Subscriber by the CA of issuance of certificate

The CA may notify the requester in different ways:

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

The CA may:

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

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

© SwissSign AG, 25.11.2019

4.4.2 Publication of the certificate by the CA

The Requester agrees that The TSP will publish certificate status information in accordance with applicable regulations. The Requester decides during the registration process whether or not the certificate will be published in a public directory service and is thus available for retrieval. If the subject is a device or system, the consent of the natural or legal person responsible for the operating of the device or system needs to be obtained, instead of the subjects consent.

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.4.4 Certificate Transparency

SwissSign is supporting Certificate Transparency for EV and OV certificates using OCSP. During the issuing of a SSL certificate SwissSign provides the SSL certificate to the required amount of CT log servers. For OV and EV SSL certificates SwissSign returns the SCT within the OCSP status answer to the client. This method requires the server operator to enable OCSP stapling on the server who is hosting the SSL certificate. Information on Certificate Transparency may be found in IETF RFC 6962. For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, will not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under this CP/CPS.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The use of certificates by Subscribers must adhere to the obligations stipulated in chapter 1.3.3, summarized as follows:

- Certificates issued under this CP/CPS may only be used in accordance with the key usage declaration contained in the certificate.
- Subscribers may only use SwissSign certificates for intended, legal, and authorized purposes.
- Subscribers may only use a SwissSign certificate on behalf of the person or the organization listed as the subject of such a certificate.
- Subscribers must read and agree to the General Terms and Conditions and the applicable End-User Agreement,

4.5.2 Relying Party public key and certificate usage

Relying Parties shall:

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

© SwissSign AG, 25.11.2019

4.6 Certificate renewal

Certificate renewal is not supported.

4.7 Certificate reissuance

Certificate reissuance is a process in which a new certificate is issued to a Subscriber based on an existing valid certificate. The new certificate contains new key information, but retains subject information and end of validity of the existing valid certificate.

4.7.1 Circumstance for certificate reissuance

The Subscriber may choose to renew a certificate if the following conditions are met:

- The Subscriber owns a currently valid certificate from this CA.
- All information in the certificate is still correct.
- The verification of the identity is still within the time period allowed by legal and regulatory requirements governing this type of certificate.
- The cryptographic material used meets the requirements of ETSI EN 119 312 and ETSI EN 319 411-1.

4.7.2 Who may request reissuance

Reissuance may be requested by the Subscriber only.

4.7.3 Processing certificate reissuance requests

The process of the application for reissuance request will be conducted as follows:

- The applicant can request the reissuance of a valid certificate either by telephone or via SwissSign Support.
- The SwissSign RAO sends an e-mail to the contact person named in the original request or, if an account exists, to the e-mail address named in the account. The confirmation of the application for certificate reissuance must be made by replying to this e-mail.
- After successful email validation, the new certificate is issued.

4.7.4 Notification of new certificate issuance to Subscriber

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

4.7.5 Conduct constituting acceptance of a reissuance certificate

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

4.7.6 Publication of the reissuance certificate by the CA

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

4.7.7 Notification of certificate issuance by the CA to other entities

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

© SwissSign AG, 25.11.2019

4.8 Certificate re-key

Certificate re-keying is a process where a Subscriber requests a certificate, using a new keypair. The resulting certificate contains new validity information and a new public key, but retains the same subject information.

4.8.1 Circumstance for certificate re-key

The Subscriber may choose to re-key a certificate within the process of renewal, therefore the stipulations from **Fehler! Verweisquelle konnte nicht gefunden werden.** apply.

4.8.2 Who may request certification of a new public key

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

4.8.3 Processing certificate re-keying requests

- The subscriber can apply for the re-key either by telephone or via SwissSiign Support. The subscriber must provide either the FQDN, CN or the serial number of the certificate to be re-keyed.
- The SwissSign RAO sends an e-mail to the contact e-mail address specified in the original request or, if an account ("swisssign.net account") exists, to the e-mail address specified in the account.
- Confirmation of the application for certificate reissuance with re-key must follow by replying to this e-mail.
- After receipt of the confirmation, the certificate can be reissued with a new key, whereby the applicant can choose whether with:
    - sending a new CSR

4.8.4 Notification of new certificate issuance to Subscriber

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

4.8.5 Conduct constituting acceptance of a re-keyed certificate

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

4.8.6 Publication of the re-keyed certificate by the CA

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

4.8.7 Notification of certificate issuance by the CA to other entities

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

4.9 Certificate modification

The TSP does not support certificate modification.

4.10 Certificate revocation and suspension

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

Subscribers or Relying Parties are requested to apply for certificate revocation immediately if there is a suspicion that private keys have been compromised or the content of the certificate is no longer correct (e.g. the abolition of the certificate holder's membership of an organization).

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

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

4.10.1 Circumstances for revocation

Subscribers may revoke their certificates at will.

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

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

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

- The certificate issued does not comply with the terms and conditions of this CP/CPS.
- The CA obtains evidence that the Certificate was misused
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use and/or other applicable laws, rules and regulations. In addition, The TSP may investigate any such incidents and take legal action if required.
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name)
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name
- The CA is made aware of a material change in the information contained in the Certificate, e.g.
    - Any part of the certificate subject has changed.
    - The certificate /O= field is no longer valid. (e.g. bankruptcy of the organization)
    - The certificate /CN= field is no longer valid (e.g. name change due to change in marital status or omission of domain registration renewal).
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement
- The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository
- Revocation is required by this CP/CPS
- The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key, or if there is clear evidence that the specific method used to generate the Private Key was flawed.

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

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

4.10.2 Who can request revocation

This CA accepts certificate revocation requests from the following sources:

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

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

4.10.3 Procedures for revocation request

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

- The Subscriber can use the online revocation functions in the profile that issued the initial registration request.
- By using the provided revocation passphrase at the end of the registration process, the Subscriber can revoke the certificate.
- The Subscriber can personally visit the RA offices and request the revocation of a certificate off line. The Subscriber must present either a valid passport or Swiss identity card.
- The RAO of an delegated RA can revoke certificates belonging to this dedicated RA.
- The Subscriber can submit an offline revocation form and send it to the TSP. After checking the validity of the revocation request, the TSP revokes the certificate.

4.10.3.1 Notification about revocation

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

4.10.4 Revocation request grace period

No stipulations.

4.10.5 Time within which CA must process the revocation request

After the formal requirements as detailed in chapters 4.10.1 and 4.10.2 have been met, the registration authority will process written revocation requests and Certificate Problem Reports within 24 hours. If the subscriber requires the revocation on an appointed date, this will be noted accordingly and the certificate concerned will be revoked at the time required.

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

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

4.10.6 Revocation checking requirement for Relying Parties

Relying Parties must, when working with certificates issued by this CA, verify these certificates at all times. This includes the use of CRLs, in accordance with the certification path validation procedure specified in RFC 5280. Also, any and all critical extensions, key usage, and approved technical corrigenda as appropriate should be taken into account.

4.10.7 CRL issuance frequency

CA	Information	Frequency
SwissSign Gold CA (Root CA)	CRL	At least once every 365 days and within 24 hours for every revocation. At most 24 hours may pass from the time a certificate is revoked until it is reported on the CRL.
	OCSP Information	Real-time. The OCSP responder will report a certificate's revocation immediately after the revocation has been completed.
Subordinated issuing CAs	CRL	At least once every 24 hours. At most, one hours may pass from the time a certificate is revoked until the revocation is reported on the CRL.
	OCSP Information	Real-time. The OCSP responder will report a certificate's revocation immediately respectively 10 minutes after the revocation has been completed.

4.10.8 Maximum latency for CRLs

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

4.10.9 On-line revocation/status checking availability

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

© SwissSign AG, 25.11.2019

4.10.10 On-line revocation checking requirements

Relying parties must, when working with certificates issued by this CA, at all times verify the certificates issued by this CA. This includes the use of CRLs in accordance with the certification path validation procedure specified in RFC 5280 and/or RFC 6960 for OCSP.

4.10.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.10.12 Special requirements regarding key compromise

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

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

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

4.10.13 Circumstances for suspension

Certificates may not be suspended.

4.10.14 Who can request suspension

Certificates may not be suspended.

4.10.15 Procedure for suspension request

Certificates may not be suspended.

4.10.16 Limits on suspension period

Certificates may not be suspended.

4.11 Certificate status services

The TSP provides CRL and OCSP status service. Access to these services is provided through the web site “swisssign.net” and the online LDAP directory “directory.swisssign.net”. The certificate status services provide information on the status of certificates. The integrity and authenticity of the online status information (OCSP) is protected by a digital signature of the dedicated OCSP responder certificate which is signed from the appropriate issuing CA. The CRL is directly signed by the appropriate issuing CA. Integrity and authenticity of the revocation information is guaranteed by a signature of the CRL or the OCSP response. Revocation information remains in the CRL until the end of the issuing CA validity.

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

© SwissSign AG, 25.11.2019

4.11.1 Operational characteristics

Consent to the publication is a condition for the application for certificates. CA and OCSP responder certificates are published after they are issued and are available at least until the end of the year in which they become invalid (QCP-n-qscd, QCP-l-qscd, QCP-n, QCP-l). CRL are issued regularly and until the end of the validity of the issuing CA. If a certificate is revoked a new CRL will be created and published within one hour.

4.11.2 Service availability

The TSP has ensured through technical measures that the certificate status services are available 24 hours per day, 7 days per week. The availability of this service is indicated in the form of an URL in the certificates.

4.11.3 Optional features

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

4.12 End of subscription

End of subscription occurs after:

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

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

4.13 Key escrow and recovery

4.13.1 Key escrow and recovery policy and practices

Private key escrow is done by the SwissSign RA only for E-Mail ID Gold Certificate key pairs generated by the TSP. In these cases, the p12 file containing the key pair and protected with a subscriber-chosen password is available for download for the validity period of the requested certificate.

4.13.2 Session key encapsulation and recovery policy and practices

This CA does not support session key encapsulation.

5. Facility, Management, and Operations Controls

5.1 Physical controls

Two identical clones of the SwissSign Gold CA 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. One is located in Zurich, the other is located in Bern.
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

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 loged 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

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

5.1.7 Waste disposal

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

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

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, the roles within the SwissSign TSPare operated by four separated authorization groups: Security Officer, System Administrators, System Operators and System Auditors. Access to any of the systems in the TSP requires 2-factor authentication. Any person may only be part of one of these authorization groups with the exception of the Security Officer and System Auditors. Within these authorization groups, multiple roles are defined (see picture below). 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)

5.2.1.2.1 Infrastructure Engineer (Infra Eng)

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

5.2.1.2.2 Application Engineer (App Eng)

Application Engineers (App Eng) have full control of TSP application software (i.e. all application level systems of the TSP above the operation system), but not of cryptographically relevant information such as the private keys of any of the TSP components. The App Eng is authorized to install, configure, and maintain the TSP's trustworthy systems for registration (of all identity data for certificate issuance), certificate generation, subject-device provision and revocation management. The App Eng is responsible for operating the trustworthy systems on a day-to-day basisand supports system backup and recovery. Regular recovery tests are carried out, the results are recorded and evaluated.

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

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.

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

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

5.2.2 Number of persons required per task

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

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

System Operator: 2 employees for system administration, TSPoperation

System Auditor: 1 auditor

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

5.2.3 Identification and authentication for each role

Security roles and responsibilities, as specified in the role concept, are documented in job descriptions or in documents available to all concerned personnel. Trusted roles, on which the security of the TSP's operation is dependent, are clearly identified. Personnel dedicated to trusted roles is named and accepted by the management and the person to fulfil the role. The requirements of the information security policy apply. Access to systems always requires 2-factor authentication

© SwissSign AG, 25.11.2019

5.2.4 Roles requiring separation of duties

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

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

Illustration 1: Segregation of duties

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

		System Administrator		System Operator			System Auditor	Sec Of
		Infra Eng	App Eng	CAM	RAO	CAO	System Auditor	Sec Of
System Administrator	Infra Eng	-						
	App Eng		-					
System Operator	CAM			-				
	RAO				-			
	CAO					-		
System Auditor	System Auditor						-	
Sec Of	Sec Of							-

Illustration 2: Permitted combinations of roles

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

Illustration 3: Data Access

5.3 Personnel controls

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

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

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

5.3.1 Qualifications, experience, and clearance requirements

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

With regard to this CA, 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.

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

On their first day of work, all SwissSign employees receive an employee handbook and access to the SwissSign security policy, security concept, personal workspace security, and risk management documentation. Every employee is expected to read and understand all of this documentation during the first week of employment with 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. The TSP is responsible for adhering to the requirements set out in the policies, even if individual tasks are provided by partners.

5.4 Audit logging procedures

The SwissSign CA software is built to journal all events that occur in the SwissSign Gold CA. The journal is stored in the SwissSign CA database and is accessible through the SwissSign CA Web Interface.

5.4.1 Types of events recorded

The following events are recorded in the CA log:

- key generation
- certificate requests (also for renewal, rekey)
- rejected certificate requests
- account violations
- certificate signing (also for renewal, rekey)
- certificate revocation
- user account logon
- CRL signing
- CA rollover
- certificate expiration
- certificate downloads/installation
- CAA Check

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

5.4.2 Frequency of processing log

Logs are processed continuously and audited on a monthly basis by the Chief Information Security Officer (CISO). The audit report covers the following aspects:

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

5.4.3 Retention period for audit log

The journal information in the “SwissSign Gold CA” database is never deleted. The journal entries can be viewed via the RA GUI with the role Auditor. A corresponding request for information can be made via the contact given in this CP/CPS. The TSP then checks the authorization and provides the required information.

5.4.4 Protection of audit log

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

- System Auditor
- RAO
- CAO
- CAM

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

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

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

5.5.1 Types of records archived

The following records are archived:

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

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

Protection of the archive is as follows:

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

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

All records that are created manually through the scanning of documents are time-stamped using the SwissSign TSA service.

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.

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.

© SwissSign AG, 25.11.2019

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.

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 corruption.

5.7.2 Computing resources, software and/or data are corrupted

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

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

5.7.3 Entity private key compromise procedures

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

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

- The CA certificate will be revoked.
- 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 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.
- All Subscriber certificates will be revoked and new CRLs will be issued.
- 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.
- New CRLs will be issued.

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.

© SwissSign AG, 25.11.2019

5.8 CA or RA termination

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

- 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.
- When the decision to discontinue certification services has been taken, the TSP will inform, without delay, all its Subscribers, Relying Parties and if applicable the other registration authorities and other CAs with which there are agreements or any other form of established relations. 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.
- 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 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 immediately cancel all current and valid contracts. The cancellation is to be effective after the entire business termination process has been concluded. The TSP will also immediately revoke all rights of contracted parties to act on behalf of the TSP.

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

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

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

© SwissSign AG, 25.11.2019

6. Technical Security Controls

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

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

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

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

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

6.1 Key pair generation and installation

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

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

6.1.1 Key pair generation

The key pair for the “SwissSign Gold CA” (Root CA Key) has been created in an offline HSM that meets the requierements of ETSI EN 119 312. The HSM is located in the high-security area of the TSP. The HSM is operated in FIPS mode, which guarantees that the private keys can never leave the HSM. In the case of key generation, the implementation of the role concept and the principle of double control are enforced. An independent auditor always is either present at the generation of CA Root keys or he satisfies himself after the key generation by means of a video recording of the proper sequence of the key generation. Furthermore, the creation of CA keys is documented in accordance with ETSI EN 319 411-1.

The key pairs for the subordinated issuing CA of the SwissSign Gold CA (Issuing CA Keys) have been generated in an online HSM that meets 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. The key generation activities are documented and stored in accordance with the requirements of ETSI EN 319 411-1. During the operation of the issuing CA, the rule concept and the principle of double control are enforced.

The TSP generates 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. This report will be signed:

- For root CA: by the (CISO) and a trustworthy person independent of the TSP's management (Notary or auditor) as witness that the report correctly records the key management ceremony as carried out.
- For subordinate CAs: by the CISO and the engaged key share holders

OVCP, EVCP: If the key pairs are produced under the responsibility of the subscriber, they must not use weak debian and should use secure keys.

OVCP, EVCP: By transmitting a PKCS # 10 request to the TSP, the subscriber proves the possession of the private key.

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

6.1.2 Private key delivery to Subscriber

If the subscribers of the SwissSign RA have the choice, where the keys will be generated. The TSP recommends to generate the keys for a signing certificate on a secure crypto device and the keys for an encryption certificate on the SwissSign web site.

Private keys generated by the subscriber do not need to be delivered, which is the case for all SSL-certificates.

The delivery of private keys generated by the TSP will be done through a passphrase-protected download mechanism (PKCS#12).

6.1.3 Public key delivery to certificate issuer

The requester presents the public key as a PKCS#10-formatted certificate signing request to the signing CA using a secure SSL-encrypted communication channel.

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.

6.1.5 Key sizes

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

ETSI:	ETSI TS 119 312	http://www.etsi.org/standards-search
NIST:	SP 800-57	mailto:info@swisssign.com

The Root CA uses a 4096 bit RSA key.

The Issuing CAs use a 2048 bit RSA key.

All Issuing CAs allow Subscribers to use RSA keys with a size of at least 2048 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

Key pairs are generated on approved secure crypto devices and parameters have been specified to meet all certification and security requirements. The TSP rejects certificate requests when the submitted Public Key does not meet the requirements of Sections 6.1.5 and 6.1.6 of the CA Browser Forum Baseline Requirements or when the submitted Public Key has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

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

The signing key of this CA and its subordinated issuing CAs are the only keys permitted for signing certificates and CRLs and have the keyCertSign and CRLSign key usage bit set.

Subscribers can obtain certificates issued by this CA with the following key usage bit included, depending on the type of product selected.

6.1.7.1 SSL Gold Certificates (OVCP) and EV Gold Certificates (EVCP)

Key usage:

- digitalSignature
- keyEnchipherment

Extended key usage:

- serverAuth
- clientAuth

6.1.7.2 E-Mail ID Gold Certificates (NCP)

Key usage:

- digitalSignature
- nonRepudiation
- keyEncipherment
- keyAgreement
- dataEncipherment

Extended key Usage

- clientAuth
- emailProtection
- Microsoft Encrypted Files System (msEFS)
- Microsoft Smart Card Logon (msSCL)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

Root CA keys	The HSM used for CA keys is kept offline at all times and meets at least FIPS 140-2 level 3 requirements.
Issuing CA keys	The HSM used for CA keys meets at least FIPS 140-2 level 3 requirements. These keys are online and access is strictly controlled by using the '4-eye' principle.
Subscriber keys	The subscriber is fully responsible for the evaluation, implementation and protection of the cryptographic module, where the subscriber keys are generated and stored. The TSP recommends that the subscriber uses a SSCD.

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.
TSA keys	The TSA keys are not in escrow.

Subscriber keys	Private key escrow is done by the SwissSign RA only for E-Mail ID Gold Certificate key pairs generated by the TSP. In these cases, the p12 file containing the key pair and protected with a subscriber-chosen password is available for download for the validity period of the requested certificate.

6.2.4 Private key backup

The following list shows how private key backup is implemented:

Root CA keys	Root CA keys have been backed up onto an HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access. At least one of these persons must be a member of the Board of Directors of the TSP.
Issuing CA keys	The Issuing CA keys have been put into backup HSM, so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 2 persons are present in order to gain physical and logical access.
Subscriber keys	Subscribers are solely responsible for the backup of subscriber keys .

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	Subscribers are solely responsible for the archival of subscriber keys.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Root CA keys	The Root CA keys can be cloned from the master SSCD to other SSCDs. This is achieved in a cloning ceremony. To protect the private key during the transport, the destination SSCD provides the public key of a key pair it has generated. The master SSCD encrypts the key to be cloned with this public key. Only the destination SSCD is therefore able to successfully decrypt the key pair from the master SSCD.
Issuing CA keys	The Issuing CA keys are cloned in the same manner as Root keys.
Subscriber keys	Subscribers are solely responsible for the transfer of subscriber keys into or from a cryptographic module.

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	Subscribers are solely responsible for the transfer of subscriber keys into or from a cryptographic module.

The controls on these processes are explained in chapter 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	Subscribers are solely responsible for the method of activating private keys.

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

Root CA keys	The Root CA keys are deactivated either by logging out of the HSM, by terminating the session with the HSM, by removing the CA token from the computer or by powering down the system.
Issuing CA keys	The Issuing CA keys are deactivated by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.
Subscriber keys	Subscribers are solely responsible for the deactivation of private key.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

Root CA keys	The Root CA keys are destroyed by initializing the partition on the HSM.
Issuing CA keys	The Issuing CA keys are destroyed by initializing the partition on the HSM.
Subscriber keys	Subscribers are solely responsible for destroying the private key.

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 chapter 6.1.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All certificates, and therefore the public keys of all Subscribers and all CAs, are stored 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 on line for 4 weeks.

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

6.3.2 Certificate operational periods and key pair usage periods

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

- The “SwissSign Gold CA” as well as all trust-anchor certificates are valid 30 years. Key changeover is performed every 15 years.
- Issuing CA certificates are issued for a maximum lifetime of 15 years.
- The rollover of CA certificates will be done manually and is after at most two thirds of the lifetime of the most recent CA certificate.

© SwissSign AG, 25.11.2019

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

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.

6.4 Activation data

6.4.1 Activation data generation and installation

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

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

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

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

6.4.3 Other aspects of activation data

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

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. SA access to the system is granted only over secure and restricted protocols using strong public-key authentication.

6.5.1 Specific computer security technical requirements

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

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

- Monitoring and auditing of all activities

6.5.2 Computer security rating

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

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

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

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

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

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

6.6.2 Security management controls

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

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 CSP has implemented a network concept, which ensures that the sensitive CA systems are operated in dedicated secure network zones. For the network concept, a separate documentation is available, which can be viewed on the premises of the TSP in the relevant parts if there is justified interest. To protect the processes of the TSP, among others, firewalls and intrusion detection mechanisms are used, which only allow

explicitly permitted connections. The TSP operates network segments in differentiated severity levels, thereby separating workstation networks from server networks.

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

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

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

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

6.8 Time-stamping

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

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

SwissSign may charge a fee for this service. The keys used for the creation of timestamping signatures are treated in exactly the same fashion as the keys of the subordinated issuing CAs of the “SwissSign Gold CA”.

© SwissSign AG, 25.11.2019

7. Certificate, CRL and OCSP Profiles

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

7.1 Certificate profile

The TSP issues X.509 Version 3 certificates in accordance with **ITU-T X.509** and the regulations of ETSI EN 319 412-1-5. The structure of such a certificate is:

Certificate Field	Value	Comment
Version	X.509 Version 3	See Chapter 7.1.1
Serial number	Unique number	Will be used in CRL
Signature algorithm identifier	OID	See Chapter 7.1.3
Validity period	Start date, expiration date	
Subject	According to X.500	See Definitions in Chapter 1.6
Subject Public Key Info	Public Key algorithm, Subject Public Key	See Chapter 7.1.3
Extensions	X509V3 Extensions	See Chapter 7.1.2
Signature	Certificate Signature	See Chapter 7.1.3

In conformance with a requirement of the Mozilla Foundation and the CAB Forum concerning SSL Server certificates, the TSP will not issue certificates for SSL Servers with a life time exceeding 24 months.

For EV certificates the following fields must be included in the subject:

- Common Name (FQDN): /CN
- Organization: /O
- Locality: /L
- State or Province: /ST
- Country: /C
- Registration Number: 2.5.4.5
- Business Category 2.5.4.15

For EV certificates the following fields may be included in the subject:

- Street and Number: /STREET
- Postal Code: /PostalCode

For EV certificates the following fields must be added for the Jurisdiction of Incorporation or Registration - if they are applicable:

- Country: 1.3.6.1.4.1.311.60.2.1.3 (must be applicable)
- State or Province: 1.3.6.1.4.1.311.60.2.1.2 (may be applicable)
- Locality: 1.3.6.1.4.1.311.60.2.1.1 (may be applicable)

For EV certificates the Field businessCategory (OID 2.5.4.15) must be added. This field MUST contain one of the following strings: „Private Organization“, „Government Entity“, „Business Entity“, or „Non-Commercial Entity“ depending upon whether the Subject qualifies under the terms of Section 8.5 of the EV Guidelines, respectively.

Other fields may be added to the subject.

7.1.1 Version number(s)

Version of X.509 certificates: version 3.

7.1.2 Certificate Extensions

7.1.2.1 SwissSign Gold CA Certificates for Generation 2

CA Type	Subject	Issuer
Root CA	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH
Issuing CA (CRL & OCSP only)	CN=SwissSign Server Gold CA 2008 - G2 O=SwissSign AG C=CH	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH
Issuing CA (CRL & OCSP only)	CN=SwissSign Personal Gold CA 2008 - G2 O=SwissSign AG C=CH	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH
Issuing CA	CN=SwissSign Server Gold CA 2014 - G22 O=SwissSign AG C=CH	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH
Issuing CA	CN=SwissSign Personal Gold CA 2014 - G22 O=SwissSign AG C=CH	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH
Issuing CA	CN=SwissSign EV Gold CA 2014 - G22 O=SwissSign AG C=CH	CN=SwissSign Gold CA - G2 O=SwissSign AG C=CH

7.1.2.1.1 Extension of the Root CA Certificate: SwissSign Gold CA – G2

Extension Attribute	Values	Comment
Basic Constraints	CA: TRUE	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Certificate Policies	Policy: 2.16.756.1.89.1.2.1.1 CPS: http://repository.swisssign.com/	
CRL Distribution Points	not included in Root CA certificate	
SignatureAlgorithm	SHA1RSA	

7.1.2.1.2 Extensions of the Issuing CA Certificates

7.1.2.1.2.1 SwissSign Server Gold CA 2014 – G22

Extension Attribute	Values	Comment
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Certificate Policies	Policy: 2.16.756.1.89.1.2.1.6 CPS: https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE http://ocsp.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA256RSA	

7.1.2.1.2.2 SwissSign Personal Gold CA 2014 – G22

Extension Attribute	Values	Comment
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	DA32F949F851CC9871660CD9CEB6DB923F094BEF	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	
Certificate Policies	Policy: 2.16.756.1.89.1.2.1.6 CPS: https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE http://ocsp.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA256RSA	

7.1.2.1.2.3 SwissSign EV Gold CA 2014 – G22

Extension Attribute	Values	Comment
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642	
Authority Key Identifier	5B257B96A465517EB839F3C078665EE83AE7F0EE	

Extension Attribute	Values	Comment
Certificate Policies	Policy: 2.5.29.32.0 CPS: https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf	The EV standard allows the use of „any policy".
CRL Distribution Points	http://crl.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/5B257B96A465517EB839F3C078665EE83AE7F0EE http://gold-ev-g2.ocsp.swisssign.net/5B257B96A465517EB839F3C078665EE83AE7F0EE	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA256RSA	

7.1.2.1.3 Extensions of Leaf Certificates

7.1.2.1.3.1 SSL Gold Certificate issued by SwissSign Server Gold CA 2014 – G22 (OVCP)

Extension Attribute	Values	Comment
Subject	/CN=FQDN (mandatory) /OU (optional) /O (mandatory) /L (optional) /ST (optional) **/C (mandatory)**	See Definitions in Chapter 1.6
Issuer Name	/CN=SwissSign Server Gold CA 2014 - G22 /O=SwissSign AG /C=CH	DN of the issuing CA
Authority Key Identifier	E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE	
CRL Distribution Points	http://crl.swisssign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.2.1.12 CPS: https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf Policy: 0.4.0.2042.1.7 (OVCP) Policy: 2.23.140.1.2.2 (CAB-OV)	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE http://ocsp.swisssign.net/E7F1E7FD2E53AD11E5811A57A4738F127D98C8AE	URL to OCSP responder and optional URL to CA issuer certificate
Subject Alternative Name	Up to 200 FQDN, at least the FQDN stated in Subject CN of certificate	1 to 200 Alternative DNS names. Wildcard defined as *.FQDN
Key Usage	digitalSignature, keyEncipherment	
Extended Key Usage	serverAuth, clientAuth	see chapter 6.1.7 for additional values

7.1.2.1.3.2 EV Gold Certificate issued by SwissSign EV Gold CA 2014 – G22 (EVCP)

Extension Attribute	**Values**	**Comment**
Subject	/CN=FQDN (mandatory) /serialNumber=Registration Number (mandatory) /OU (optional) /O (mandatory) /Street (optional) /L (mandatory) /ST (optional) /C (mandatory) /PostalCode (optional) /BC (mandatory) /joiL (optional) /joiST (optional) /joiC (mandatory)	See Definitions in Chapter 1.6
Issuer Name	/CN=SwissSign EV Gold CA 2014 - G22 /O=SwissSign AG /C=CH	DN of the issuing CA
Authority Key Identifier	EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642	
CRL Distribution Points	http://crl.swisssign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.2.1.1 CPS: https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf Policy: 0.4.0.2042.1.4 (EVCP) Policy: 2.23.140.1.1 (CAB-EV)	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642 http://ocsp.swisssign.net/EEFD46CAF7275E91BC5AB6E787CD0AFA550A2642	URL to OCSP responder and optional URL to CA issuer certificate
Subject Alternative Name	At least subject FQDN	1 to 200 Alternative DNS names.
Key Usage	digitalSignature, keyEncipherment	
Extended Key Usage	serverAuth, clientAuth	see chapter 6.1.7 for additional values

7.1.2.1.3.3 E-Mail ID Gold Certificate issued by SwissSign Personal Gold CA 2014 – G22 (NCP)

Extension Attribute	**Values**	**Comment**
Subject	/CN=(/GN /SN) or pseudo: Pseudonym (mandatory) /GN (optional) /SN (optional) /Pseudonym (optional) /serialNumber (optional) /Email (optional) /L (optional) /ST (optional) /C (mandatory) /Street (optional) /PostalCode (optional)	See Definitions in Chapter 1.6
Issuer Name	/CN=SwissSign Personal Gold CA 2014 - G22 /O=SwissSign AG /C=CH	DN of the issuing CA
Authority Key Identifier	DA32F949F851CC9871660CD9CEB6DB923F094BEF	
CRL Distribution Points	http://crl.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF	URLs of the CRL Distribution points (LDAP and/or HTTP)

Extension Attribute	Values	Comment
Certificate Policies	Policy: 2.16.756.1.89.1.2.1.12 CPS: https://repository.swisssign.com/SwissSign-Gold-CP-CPS.pdf Policy: 0.4.0.2042.1.1 (NCP)	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/DA32F949F851CC9871660CD9CEB6DB923F094BEF http://ocsp.swisssign.net/DA32F949F851CC9871660CD9CEB6DB923F094BEF	URL to OCSP responder and optional URL to CA issuer certificate
Subject Alternative Name	E-mail address of the subject	
Key Usage	digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement	Critical extension, any combination of these key usages is permissible
Extended Key Usage	emailProtection, clientAuth, msEFS, msSCL	compare chapter 6.1.7, any combination of the listed EKU-OIDs is possible.
Microsoft Certificate Template v1 / v2	(OID 1.3.6.1.4.1.311.20.2) (OID 1.3.6.1.4.1.311.21.7)	Optional

7.1.3 Algorithm object identifiers

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

Algorithm	Object Identifier
SHA1WithRSAEncryption	1.2.840.113549.1.1.5 (phase out)
SHA256withRSAEncryption	1.2.840.113549.1.1.11

7.1.4 Name forms

Certificates issued by the subordinated issuing CAs of this CA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 Name constraints

Issuing CA are not technically constrained. The SwissSign Issuing CA are publicly disclosed within the Mozilla CCADB.

7.1.6 Certificate policy object identifier

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

For information see chapter 7.1.2 of this document.

7.1.7 Usage of Policy Constraints extension

Not implemented.

7.1.8 Policy qualifiers syntax and semantics

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

7.1.9 Processing semantics for the critical Certificate Policies extension

PKI client applications must process extensions marked as critical.

7.2 CRL profile

This CA and its subordinated issuing CAs issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280.

Extension Attribute	Values	Comment
Version Number	V2	Indicates the version of the CRL and thus the permitted content.
Revokation List Number	Number	sequential number
Signature Algorithm	SHA256	hash method and the signature algorithm used to sign the CRL
Issuer	DN of the Issuer	Contains the name of the issuer of the CRL as Distinguished Name
This Update	Date and Time	Defines the date on which this CRL was published
Next Update	Date and Time	Defines the date until this CRL is valid
revoked Certificates:	serial	List of revoked Certificate serial numbers

7.2.1 Version number(s)

The CRL version is v2.

7.2.2 CRL and CRL entry extensions

Version 2 CRL, and CRL extensions and their current status are specified below:

- CRLNumber: Populated by the CA application
- reasonCode: not populated
- authorityKeyIdentifier: Populated by CA application contains key id (SHA1) of issuer public key

7.3 OCSP profile

The SwissSign OCSP functionality is built according to RFC 6960.

© SwissSign AG, 25.11.2019

The OCSP response is according to RFC 6960:

- Good – for valid certificates
- Revoked - for cetificates they have been revoked or
- Unknown – for certificates they are not published or not known by the TSP

7.3.1 Version number(s)

The OCSP version is set to v1.

7.3.2 OCSP extensions

The OCSP extensions used are specified below:

- Nonce
- ServiceLocator

8. Compliance Audit and Other Assessments

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

- The SwissSign Gold CA and its subsidaries
- All registration authorities that process requests for issuance by the subordinate CA

8.1 Frequency or circumstances of assessment

The compliance audit is conducted annually.

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 Guidelines. The scope of the audit and reporting will be fully in line with the rules set out before.

8.3 Assessor's relationship to assessed entity

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

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

8.4 Topics covered by assessment

The auditor will choose the control objectives that are to be covered by the assessment in accordance with ETSI Regulations ETSI EN 319 401 and ETSI EN 319 411-1, BR and EV Guidelines.

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.

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

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

8.7 Risk assessment

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

© SwissSign AG, 25.11.2019

9. Other Business and Legal Matters

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

The TSP may charge a fee according to 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 may establish a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

With regard to the certificates issued pursuant to this CP/CPS document according to ZertES the 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 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.

© SwissSign AG, 25.11.2019

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

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

9.4 Privacy of personal information

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

9.4.1 Privacy Plan

The stipulations of chapter 9.3 and 9.4 apply.

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

© SwissSign AG, 25.11.2019

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 CP/CPS, Swiss Digital Signature Law (as far as qualified certificates are concerned), and related regulations and rules.

9.6.2 RA representations and warranties

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

9.6.3 Subscriber representations and warranties

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

9.6.4 Relying Party representations and warranties

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

9.6.5 Representations and warranties of other participants

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

9.7 Disclaimers of warranties

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

© SwissSign AG, 25.11.2019

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 CP/CPS 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 Certificate Holder

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

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of termination and survival

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

9.11 Individual notices and communications with participants

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

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

© SwissSign AG, 25.11.2019

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

9.12 Amendments

9.12.1 Procedure for amendment

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

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

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

9.12.2 Notification mechanism and period

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

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

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

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

Complaints regarding compliance with or implementation of these CP/CPS must be submitted in writing to the TSP. In case of any dispute or controversy in connection with the performance, execution or interpretation of this agreement that can not be resolved within a period of four weeks after submission of the complaint, the parties are free to file action with the courts pursuant to clause 9.140.

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 CAB Browser Forum, SwissSign will react to a notification of a failure or miss-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 CP/CPS and rights or obligations related hereto are in accordance with the relevant provisions of the EU Regulation No 910/2014 and of the other applicable laws. Compliance with the laws and regulations are verified within the annual external audit. The audits are carried out by an independent qualified auditor.

© SwissSign AG, 25.11.2019

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 (Subscriber):

- the CP/CPS, as indicated in the certificate
- 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 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 these Requirements implemented by the TSP will be described in this chapter of the CP/CPS.

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

© SwissSign AG, 25.11.2019

9.17 Other provisions

9.17.1 Language

If this CP/CPS is provided in additional languages to English, the English version will prevail.

9.17.2 Delegated or outsourced Services

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

© SwissSign AG, 25.11.2019