SwissSign

SwissSign Platinum CP/CPS

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

Document Type:	Certificate Policy and Certification Practice Statement
OID:	2.16.756.1.89.1.1.1.1.16
Author:	Information Security and Compliance
Classification:	Attribution-NoDerivs (CC-BY-ND) 4.0
Applicability:	Global
Owner:	CEO
Issue Date:	19 November 2022
Version:	3.13.0
Obsoletes:	Version 3.12.0, 11 November 2022
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released

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.

Compliance: The SwissSign Platinum CA and its subordinated SwissSign Qualified Platinum CA operating under this CP/CPS and issuing certificates under this CP/CPS are fully compliant with ZertES, VZertES and all stipulations therein.

SwissSign

Version Control

Date	Version	Comment	Author
17.08.2005	1.1.4	Initial version	Joseph A. Doekbrijder
04.10.2005 – 19.10.2005	1.1.5 – 1.1.7	Update	J. Doekbrijder with ext. QS, Michael Doujak
24.11.2005 - 15.12.2005	1.2.0 – 1.2.3	KPMG Audit Input	Michael Doujak, J. Doekbrijder
05.03.2006 - 14.03.2006	1.3.0 - 1.3.1	KPMG Audit Input	M. Doujak, M. Raemy
30.04.2006 – 18.10.2006	1.4.0 - 1.4.9	Minor Changes and KPMG Audit Input	M. Raemy, M. Doujak, B. Kanebog, ext. QS
12.01.2007	2.0.0	CP/CPS split	M. Raemy, M. Doujak, B. Oechslin
04.05.2007	2.0.1	Review, Minor Changes	Björn Kanebog
11.04.2008	2.1.0	New layout, Review, added changes about life cycle management	Björn Kanebog
15.04.2008	2.1.1	Review	Michael Doujak
27.06.2009	3.0.0	Merged Root, Qualified, Personal and Swiss Post CP/CPS in one document	Michael Doujak
30.07.2009	3.0.1	Review	B. Oechslin
03.11.2009	3.0.2	KPMG Audit Input: KPMG Klynfeld Peat Marwick Goerdeler SA changed to KPMG AG	Christoph Graf
30.03.2010	3.1.0	Added SuisseID, Renewal, G3 CA, SHA-2	Michael Doujak
26.03.2012	3.1.1	prohibit MitM and traffic management	Michael Doujak
30-09.2014	3.2.0	Added G22 CA – SHA256	Cornelia Enke
13.10.2014	3.2.1	Improving description of Organization validation	Cornelia Enke
25.11.2015	3.2.2	Added new OID for TSA Certificate	Cornelia Enke
17.05.2016	3.3.0	Added Qualified Platinum CA G22 16-1	Reinhard Dietrich
21.11.2016	3.3.1	Added changed Issuer for SID-Auth Cetificate Added new Product	Cornelia Enke
25.06.2018	3.4.0	Improvement in accordance with the requirements of ETSI EN 319 401/411-1/2	Cornelia Enke
18.10.2018	3.5.0	Revised after annual audit	Jürg Eiholzer
17.12.2018	3.6.0	Removal G3 CA hierarchy	Michael Günther
25.11.2019	3.7.0	Improvement CA hierarchy, Removal revoked Issuing CA	Nathalie Weiler
13.12.2019	3.7.1	Correction of Typos	Nathalie Weiler
24.06.2020	3.8.0	Changes of BRG and ETSI reflected	Nathalie Weiler
17.11.2020	3.9.0	Added input from auditors on changed ETSI requirements	Michael Günther
14.06.2021	3.10.0	KPMG Audit Input Amendment of chapter 4.9.12. Key compromise	Michael Günther
15.08.2022	3.11.0	Changes based on the Swiss Signature Law; , update of chapter 5. 6 & 7	Adrian Müller, Michael Günther
11.11.2022	3.12.0	Removing revoked Issuing CAs	Adrian Müller, Michael Günther
19.12.2022	3.13.0	Chapter 3.3 & 4.7: Clarification of re-key procedures Chapter 7: Adding CA profiles	Adrian Müller, Michael Günther

SwissSign

Authorization

Date	Approved by	Approved by	Version
~~19.10.2005~~	~~Michael Doujak~~	~~Joseph A. Doekbrijder~~	~~1.1.7~~
~~15.12.2005~~	~~Michael Doujak~~	~~Joseph A. Doekbrijder~~	~~1.2.3~~
~~01.05.2006~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~1.4.1~~
~~29.08.2006~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~1.4.6~~
~~26.09.2006~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~1.4.8~~
~~18.10.2006~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~1.4.9~~
~~27.02.2007~~	~~Michael Doujak~~	~~Melanie Raemy~~	~~2.0.0~~
~~21.05.2007~~	~~Melanie Raemy~~	~~Björn Kanebog~~	~~2.0.1 / OID=1~~
~~17.04.2008~~	~~Adrian Humbel~~	~~Björn Kanebog~~	~~2.1.1 / OID=2~~
~~01.05.2010~~	~~Adrian Humbel~~	~~Michael Doujak~~	~~3.1.0 / OID=3~~
~~20.04.2012~~	~~Urs Fischer~~	~~Reinhard Dietrich~~	~~3.1.1 / OID=3~~
~~30.09.2014~~	~~Christoph Graf~~	~~Reinhard Dietrich~~	~~3.2.0 / OID=4~~
~~23.10.2014~~	~~Reinhard Dietrich~~	~~Urs Fischer~~	~~3.2.1 / OID=4~~
~~25.10.2015~~	~~Reinhard Dietrich~~	~~Urs Fischer~~	~~3.2.2 / OID=5~~
~~04.10.2016~~	~~Reinhard Dietrich~~	~~Urs Fischer~~	~~3.3.0 / OID=6~~
~~21.11.2016~~	~~Reinhard Dietrich~~	~~Urs Fischer~~	~~3.3.1 / OID=6~~
~~28.06.2018~~	~~Reinhard Dietrich~~	~~Markus Naef~~	~~3.4.0 / OID=7~~
~~22.10.2018~~	~~Matthias Bartholdi~~	~~Markus Naef~~	~~3.5.0 / OID=8~~
~~17.12.2018~~	~~Matthias Bartholdi~~	~~Markus Naef~~	~~3.6.0 / OID=9~~
~~25.11.2019~~	~~Nathalie Weiler~~	~~Markus Naef~~	~~3.7.0 / OID=10~~
~~13.12.2019~~	~~Nathalie Weiler~~	~~Markus Naef~~	~~3.7.1 / OID =10~~
~~30.06.2020~~	~~Michael Günther~~	~~Markus Naef~~	~~3.8.0 / OID =11~~
~~17.11.2020~~	~~Michael Günther~~	~~Markus Naef~~	~~3.9.0 / OID =12~~
~~11.06.2021~~	~~Michael Günther~~	~~Markus Naef~~	~~3.10.0 / OID =13~~
15.08.2022	Michael Günther	Michael Widmer	3.11.0 / OID=14
11.11.2022	Michael Günther	Jürg Graf	3.12.0. / OID=15
19.12.2022	Michael Günther	Michael Widmer	3.13.0. / OID=16

Michael Frank Günther
13. Dezember 2022

Qualified Electronic Signature by SwissID

digital signature

Michael Peter Widmer
15. Dezember 2022

Qualified Electronic Signature by SwissID

digital signature

SwissSign

Table of Contents

SwissSign

1. Introduction

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

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

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

The TSP can outsource partial tasks to partners or external providers. The TSP, represented by the management or its agents, shall remain responsible for compliance with the procedures for the purposes of this document or any legal or certification requirements to the TSP.

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

These subordinate CA comply with the Swiss Digital Signature Law, i.e.

- ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03)
- VZertES: Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032)
- TAV-BAKOM: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.032.1)
- ETSI EN 319 401 (2018): General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 (2018): Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421 (2016): Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- 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 In this CP/CPS, “this CA” refers to the “SwissSign Platinum CA G2” and all it subordinated issuing CA, unless stated differently.

This CA does not issue new CA or end-user certificates. It solely provides revocation services and revocation status services. For this purpose OCSP responder certificates might be issued under this CA.

The certificates are classified with the following Policy OIDs:

- QCP-l-qscd
- NCP+

Discontinued previous policies (all certificates have expired or have been revoked):

- QCP-n-qscd
- SuisseID QC: 2.16.756.5.26.1.1.1
- SuisseID IAC: 2.16.756.5.26.1.1.2

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

1.1 Overview

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

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

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

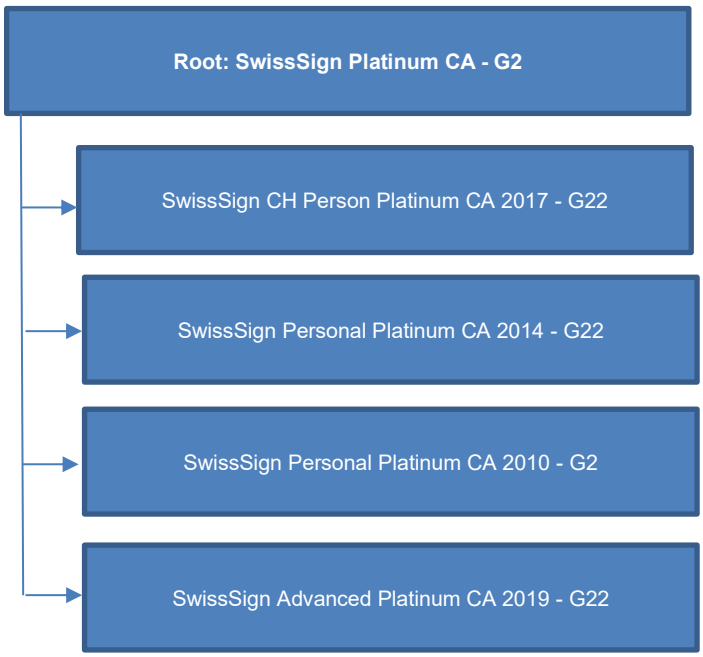
This CP/CPS is applicable to all persons, including, without limitation, all Requesters, Subscribers, Relying Parties, registration authorities and any other persons that have a relationship with SwissSign AG with respect to certificates issued by this CA. This CP/CPS also provides statements of the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

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

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

The certificate hierarchy (Root CA, Issuing CA, enduser) of the active CAs (providing revocation and status services) is as follows:

- Root CA: CN=SwissSign Platinum CA - G2
  - Issuing CA: CN=SwissSign CH Person Platinum CA 2017 - G22
    - Regulated seal certificates according to ZertES (QCP-l-qscd) incl. Timestamping certificates
  - Issuing CA: CN=SwissSign Advanced Platinum CA 2019 - G22
    - Advanced seal certificates (NCP+) incl. Timestamping certificates
  - Issuing CA: CN=SwissSign Personal Platinum CA 2010 - G2
    - Timestamping certificates
  - Issuing CA: CN=SwissSign Personal Platinum CA 2014 - G22
    - Timestamping certificates



Graphic representation of the Platinum CA hierarchy

1.2 Document name and identification

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

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

The Object identification number (OID) for this and only this document is: OID 2.16.756.1.89.1.1.1.1.14

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 Platinum CA” and its subordinated issuing CAs. The issuing CAs listed in chapter 7 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.

SwissSign AG operates a registration authority called “RA UBS” that operates under the trademark “UBS” and registers Subscribers of certificates issued by the “SwissSign Qualified Platinum G22 17-1”.

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 and Swiss Digital Signature Law. It must be documented, published, and distributed to all parties involved in the RA process.
- The RA must be certified according to EU Regulation No 910/2014 and Swiss Digital Signature Law. The RA must pass an annual audit. All costs related to this audit are to be paid by the operator of the RA. Failure to pass the annual audit may lead to the revocation of RA privileges.
- The information collected during the RA process is subject to applicable data protection regulations. Compliance with these provisions must be demonstrated (Chapters 9.3 and 9.4).

1.3.3 Subscribers

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

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

Subscribers and Requesters are responsible for:

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

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

1.3.4 Relying Parties

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

(NCP+, SuisseID IAC) SuisseID Identity and Authentication Certificates are intended for authentication with SuisseID and for Windows Smart Card Logon on properly configured systems. The corresponding private key is required to have been created on an SSCD but may be cloned.

(QCP-n-qscd, SuisseID QC) SuisseID Qualified Certificates and Qualified Signature Certificates are intended for use in Qualified Electronic Signatures according to Swiss Digital Signature law with legal equivalence to handwritten signatures, and may be restricted to usage with certain contracting parties only.

SuisseID certificates are not issued anymore under this CP/CPS.(QCP-l-qscd) Regulated Seal Certificates are intended for use in Regulated Electronic Seals according to Swiss Digital Signature law.

(NCP+) Advanced Seal Certificates are intended to be used to ensure authenticity of electronic documents.

1.4.2 Prohibited certificate uses

Any other use than defined in chapter 1.4.1 is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

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

SwissSign AG

Sägereistrasse 25

8152 Glattbrugg

Switzerland

Tel.: +41 800 55 77 77

Mail: helpdesk@swisssign.com

Web: https://swisssign.com

1.5.2 Contact persons

For all questions or suggestions concerning this document, and to submit Certificate Problem Reports, the following contact options are available:

SwissSign AG

Sägereistrasse 25

8152 Glattbrugg

Switzerland

Tel.: +41 800 55 77 77

Mail: certificatemisuse@swisssign.com

Web: https://swisssign.com

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

1.5.3 Person determining CPS suitability for the policy

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

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

1.5.4 CP/CPS approval procedures

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

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.

Term	Abbrev.	Explanation
Baseline Requirements Guidelines	BRG	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CA Operator	CAO	A person responsible for CA operation, including establishment of certificate parameters for RA and RAO in accordance with certificate policy.
Certificate		Information issued by a trusted third party, often published in a directory with public access. The certificate contains at least a subject, a 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 Profile		A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software. Please see clause 7.1 of this Document.
Certification Authority Revocation List	CARL	Revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer
Certificate Revocation List	CRL	List of certificates that have been declared invalid. This list is issued by the CA at regular intervals and is used by applications to verify the validity of a certificate.
Certification Practice Statement	CPS	Document that regulates the rights and responsibilities of all involved parties (RA, CA, directory service, end entity, Relying Party).
Certification Service Provider	CSP	Individual or corporation that issues certificates to individual or corporate third parties.
Cipher		A cryptographic algorithm used to encrypt and decrypt files and messages.
Cipher Text		Data that has been encrypted. Cipher text is unreadable unless it is converted into plain text (decrypted) with a key.
Chief Security Officer	CISO	the senior-level executive within the TSP responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.
Coordinated Universal Time	UTC UTC(k)	Mean solar time at the prime meridian (0°). The time scale is based on seconds as defined in ETSI EN 319 421. Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.
Credentials		Evidence or testimonials governing the user's right to access certain systems (e.g. User name, password, etc.)
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.

Term	Abbrev.	Explanation
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
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		Contractual agreement between seller of certificates and the Subscriber.
Entropy		A numerical measure of the uncertainty of an outcome. The entropy of a system is related to the amount of information it contains. In PKI and mathematics, a cryptographic key contains a certain amount of information and tends to lose a small amount of entropy each time it is used in a mathematical calculation. For this reason, one should not use a key too frequently or for too long a period.
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.
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.
Leaf-certificate		A certificate issued under this CP/CPS that is not a CA Certificate.
Lightweight Directory Access Protocol	LDAP	LDAP is used to retrieve data from a public directory.
LDAP Secure	LDAPS	LDAP secured with TLS/SSL
Man-in-the-middle	MITM	Active eavesdropping of secure communications in which attacker/third party relays and controls messages between sender and receiver.
Online Certificate Status Protocol	OCSP	Method to verify the validity of a certificate in real time.
Participants		Entities like CAs, RAs, and repositories. These can be different legal entities.

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 and article 8 ZertES.
Qualified Certificate Policy	QCP	Certificate policy which incorporates the requirements laid down in annex I and annex II of the Directive 1999/93/EC.
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.
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.
Secure Signature Creation Device	SSCD	Signature-creation device which meets the requirements specified in article 30 of Directive No 910/2014 /EC.

Term	Abbrev.	Explanation
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.
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 --- / GivenName (2.5.4.42) Surname --- /Surname (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.

Term	Abbrev.	Explanation
Time-stamp Policy	TP	Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements.
Time-stamp Token	TST	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time-stamping Unit		Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.
Traffic management		Management and surveillance of network traffic with domain names or IPs owned or controlled by third parties.
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.
Triple DES		A method of improving the strength of the DES algorithm by using it three times in sequence with different keys.
Two-factor authentication		Two-factor authentication (also known as 2FA or 2-Step Verification) is a method of confirming a user's claimed identity by utilizing a combination of two different components.
Unique identification number	UID	The UID is an unique organization number, e.g. the number of the commercial register entry or the VAT number or a number assigned by SwissSign.
Uniform Resource Locator	URL	The global address of documents and other resources on the WWW, e.g. http://swisssign.net. The first part indicates the protocol to be used (http) and the second part shows the domain where the document is located.
USB Token		Secure crypto processor that appears like a common USB memory stick. It has tamper resistant properties and is intended for the secure storage and usage of private keys.
VZertES		Swiss directive for digital signatures, issued November 23th, 2016. SR 943.032.
ZertES		Swiss Digital Signature Law. Issued March 18, 2016. SR 943.03. Compliance with this law always implies adherence to VZertES and TAV-BAKOM.

2. Publication and Repository Responsibilities

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

2.1 Repositories

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

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

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

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

2.2 Publication of certification information

Changes to the policies can be communicated to third parties.

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.
  Please note: No subscriber certificate issued by this CA is published in the directory.
- The certificate revocation list (CRL) for this CA. The CRL may be downloaded from the swisssign.net web site. The exact URL is documented in every certificate that is issued by this CA or its subordinated issuing CA in the field: “CRL Distribution Point”. For details, please refer to chapter 7.

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

2.3 Time or frequency of publication

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

The SwissSign Platinum 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.

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

SwissSign

3. Identification and Authentication

3.1 Naming

3.1.1 Types of names

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

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

To comply with SuisseID specifications, the SuisseID number must be present in the distinguished name. It must be added as serialNumber (OID: 2.5.4.5).

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

- organization names
- given name, middle name and surname,
- pseudonyms

Real names are specified as /CN='given name' optional 'middle name' 'surname' or /CN='organizational name'.

- 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 /CN or in /O must be spelled absolutely identical to the name as it appears in the documentation provided according to chapter 3.2.2.
- If the /CN is an organizational name, then the /O field must also be present and it must be identical to the /CN field.
- If a /O field is present, the /C field must also be present.

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

For CodeSigning Certificates, the common name (/CN) is identical to the Organization field (/O).

The use of names in the /CN and /O fields must be authorized. This means:

- The use of a real name and its identifying information must be authenticated and authorized according to chapter 3.2.3.
- A pseudonym requires that the requester authenticates and authorizes the request containing identifying information according to chapter 3.2.3.
- The use of academic and/or job titles are not allowed in any part of the subject information.

For Regulated Seal certificates, the /OI (organizationIdentifier) field shall be present and the content shall be the UID-Number of the company from the national register accompanied by the prefix NTRCH-UID. E.g. NTRCH-CHE-109.357.012 for SwissSign AG.

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

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

3.1.2 Need for names to be meaningful

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

3.1.3 Anonymity or pseudonymity of Subscribers

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

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

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

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

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

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

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

3.1.4 Rules for interpreting various name forms

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

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

- In general, national characters are represented by their ASCII equivalent, e.g. é, è, à, ç are represented by e, e, a, c.
- The German “Umlaut” characters ä, ö, ü are represented by either ae, oe, ue or a, o , u.

3.1.5 Uniqueness of names

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

- All certificates for individuals with identical subjects must belong to the same individual. This explicitly includes possession of revoked or expired certificates.
- All organizational certificates with identical subjects must belong to the same organization.

3.1.6 Recognition, authentication, and role of trademarks

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

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

3.1.7 Certificates for test purposes

Certificates for test purposes contain the pseudonym with a string “Test” in the Common Name.

3.2 Initial identity validation

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

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

3.2.1 Method to prove possession of private key

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

Advanced Seal:	The key pair is generated in a HSM. Control over the user’s private keys on HSM is granted to the subscriber through authentication means fulfilling the requirements of ETSI EN 319 411-1
RA UBS	The user's private keys are protected using Common Criteria EAL 4+ certified Cryptographic Modules. The sole control of signature keys are secured using a signature activation module (SAM) through which the signature activation data (SAD) is supplied. Both SAP and SAD are in conformance with TS 419

241:2014.Control over the user's private keys are granted to the subscriber in the context of UBS user onboarding processes.

Subscriber: 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. The subscriber must use the Secure Signature Creation device in accordance with the Subscriber Agreement clause 10 and the Swiss Signature Law (ZertES).

3.2.2 Authentication of organization identity (QCP-n-qscd, QCP-l-qscd, ncp+)

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 and ETSI EN 319 411-2.

The DN of a certificate issued by 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.
- Organizations with an entry in a nationally recognized commercial register must supply an attested verifiably current excerpt.
- For organization certificates a copy of a excerpt of the trade registry (example: Federal Directory for public organizations in accordance to SR 641.201.511.1 / appendix).
- Government entities must supply official documentation to prove the existence and the correct spelling of the entities name.
- All other organizations must supply either the certificate of registration with the FTA or a current VAT invoice.
- Registrations authorities operating under this CP/CPS may choose to validate an organization's name directly with the authoritative source instead of having Requesters supply this information.

3.2.3 Authentication of individual identity (QCP-n-qscd, 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 and ETSI EN 319 411-2. The regulations defined in the registration forms may be summarized as follows:

- The registration form must carry original, personal handwritten signatures or it must be supplied electronically and digitally signed using a qualified certificate or digitally as agreed with the Certification Authority
- The information on the identifying document must match the name on the registration form. In case the registration form carries the original, personal handwritten signature, this signature and the signature on the identifying document must also match.
- The wording in the request has to be identical to the given name(s) and the family name of the identifying documents.

Additionally the requester and only the requester must be identified according to these additional rules:

- 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.
  - 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. The requester must prove that he has access to the mailbox and that he can use it to receive mail.

3.2.4 Non-verified subscriber information

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

3.2.5 Validation of authority

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.

In accordance with Swiss Digital Signature Law, 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

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

As no new enduser certificates are issued anymore, no re-key is performed.

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.
- Providing proof of the possession of the private key on the web site of the registration authority.
- With a personal signature or a recognized qualified signature according to ZertES regulation on a revocation form.
- Appearance in person at the registration authority.
- Providing a one-time revocation key on the web site of the registration authority.

Not all registration authorities must support all methods of revocation.

The process how the revocation request can be submitted is described in chapter 4.9.3.

4. Certificate Life-Cycle Operational Requirements

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

4.1 Certificate application

4.1.1 Who can submit a certificate application

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

4.1.2 Enrollment process and responsibilities

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

The RA has a valid contract with the TSP.

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

The RA collects the following during its enrollment process:

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

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

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 is fulfilling these requirements it will be a trusted RA within the TSP.

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

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

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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

4.2.2 Approval or rejection of certificate applications

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

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

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 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 and install the certificate for the first time. This step is considered sufficient, and no further confirmation is required.

4.4.2 Publication of the certificate by the CA

The Requester agrees that SwissSign AG will publish certificate status information in accordance with applicable regulations. 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.

Regulated and qualified certificates according to ZertES (QCP-l-qscd and QCP-n-qscd) are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

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

- Qualified certificates can be used for qualified electronic signatures .
- Subscribers may only use a SwissSign certificate on behalf of the person or the organization listed as the subject of such a certificate.
- Certificates issued based on an enrollment process involving the UBS RA are restricted in usage to contexts involving the bank which performed the identification, in accordance with Swiss Digital Signature Law.

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.

4.6 Certificate renewal

Certificate renewal is not supported.

4.7 Certificate re-key

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

As no new enduser certificates are issued anymore, no re-key is performed

4.7.1 Circumstance for certificate re-key

N/A

4.7.2 Who may request certification of a new public key

N/A

4.7.3 Processing certificate re-keying requests

N/A

4.7.4 Notification of new certificate issuance to Subscriber

N/A

4.7.5 Conduct constituting acceptance of a re-keyed certificate

N/A

4.7.6 Publication of the re-keyed certificate by the CA

N/A

4.7.7 Notification of certificate issuance by the CA to other entities

N/A

4.8 Certificate modification

The TSP does not support certificate modification.

4.9 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 cannot 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 Subscriber's membership of an organization).

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

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

4.9.1 Circumstances for revocation

Subscribers may revoke their certificates at will.

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

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

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

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

- The CA is made aware of a material change in the information contained in the Certificate, e.g.
  - Any part of the certificate subject has changed.
  - The certificate /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.

4.9.2 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.

4.9.3 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.

4.9.3.1 Notification about revocation

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

4.9.4 Revocation request grace period

No stipulations.

4.9.5 Time within which CA must process the revocation request

After the formal requirements as detailed in chapters 4.9.1 and 4.9.2 have been met, the registration authority will process any written revocation requests within 24 hours (Monday throught Friday, except public holidays in the canton of Zurich, Switzerland) and without unnecessary delay. If the subscriber requires the revocation on an appointed date, this will be noted accordingly and the certificate concerned will be revoked at the time required.

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

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

4.9.6 Revocation checking requirement for Relying Parties

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

4.9.7 CRL issuance frequency

CA	Information	Frequency
SwissSign Platinum 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 hour may pass from the time a certificate is revoked until the revocation is reported on the CRL.
	OCSP Information	Real-time. The OCSP responder will report a certificate's revocation immediately respectively 10 minutes after the revocation has been completed.

4.9.8 Maximum latency for CRLs

The CRL of this CA and all its subordinated issuing CAs is issued according to chapter 4.9.7 and published without delay.

4.9.9 On-line revocation/status checking availability

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 Platinum 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.

4.9.10 On-line revocation checking requirements

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

4.9.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.9.12 Special requirements regarding key compromise

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

- immediately cease using the certificate,
- 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.

A party who discovers a key compromise may report it by sending an email to the address keycompromise@swisssign.com. The email must contain:

- Subject: “Key compromise SwissSign certificate”,
- the certificate affected by the key compromise in PEM format.
- a Certificate Signing Request in PEM format
  - signed by the compromised key and
  - containing a Common Name «Key compromise SwissSign certificate”

4.9.13 Circumstances for suspension

Certificates may not be suspended.

4.9.14 Who can request suspension

Certificates may not be suspended.

4.9.15 Procedure for suspension request

Certificates may not be suspended.

4.9.16 Limits on suspension period

Certificates may not be suspended.

4.10 Certificate status services

The TSP provides CRL and OCSP status service. Access to these services is provided through the web site “swisssign.net” and the online LDAP directory “directory.swisssign.net”. The certificate status services provide information on the status of certificates for at least 11 years after the certificate has expired or was revoked. 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.

The CRL includes expired certificates.

Before revoking an Issuing CA certificate, the TSP makes sure that all leaf-certificates in the scope of the CRL are either expired or revoked. Afterwards, a last CRL will be issued and will be available for download at least 11 years after the expiry date of the last leaf-certificate in scope, not only until the end of the Issuing CA validity.A certificate can only be revoked by authorized persons using the required credentials.

The OCSP response and the CRL do not include revocation reasons when a certificate is revoked.

4.10.1 Operational characteristics

Consent to the publication is a condition for the application for certificates. CA and OCSP responder certificates are published after they are issued and are available at least until the end of the year in which they become invalid (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.

4.10.2 Service availability

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

4.10.3 Optional features

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

4.11 End of subscription

End of subscription occurs after:

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

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

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

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

4.12.2 Session key encapsulation and recovery policy and practices

This CA does not support session key encapsulation.

5. Facility, Management, and Operations Controls

5.1 Physical controls

Refer to clause 5.1 of SwissSign TSPS.

5.1.1 Site location and construction

Refer to clause 5.1.1 of SwissSign TSPS.

UBS RA	The UBS RA fulfils the requirements of Swiss Digital Signature Law.

5.1.2 Physical access

Refer to clause 5.1.2 of SwissSign TSPS.

UBS RA	The UBS RA fulfils the requirements of Swiss Digital Signature Law.

5.1.3 Power and air-conditioning

Refer to clause 5.1.3 of SwissSign TSPS.

5.1.4 Water exposure

Refer to clause 5.1.4 of SwissSign TSPS.

5.1.5 Fire prevention and protection

Refer to clause 5.1.5 of SwissSign TSPS.

5.1.6 Media storage

Refer to clause 5.1.6 of SwissSign TSPS.

5.1.7 Waste disposal

Refer to clause 5.1.7 of SwissSign TSPS.

5.1.8 Off-site backup

Refer to clause 5.1.8 of SwissSign TSPS.

5.2 Procedural controls

Refer to clause 5.2 of SwissSign TSPS.

5.3 Personnel controls

Refer to clause 5.3 of SwissSign TSPS.

5.4 Audit logging procedures

Refer to clause 5.4 of SwissSign TSPS.

5.5 Records archival

Refer to clause 5.5 of SwissSign TSPS.

5.6 Key changeover

Refer to clause 5.6 of SwissSign TSPS.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Refer to clause 5.7.1 of SwissSign TSPS.

5.7.2 Computing resources, software and/or data are corrupted

Refer to clause 5.7.2 of SwissSign TSPS.

5.7.3 Entity private key compromise procedures

Refer to clause 5.7.3 of SwissSign TSPS.

If the private key of a “timestamping certificate is suspected to be compromised, executive management of the TSP must be informed immediately. The following steps will be taken:

- The certificate of the TSA Unit will be revoked.
- All registered TSA Subscribers will be informed by e-mail as soon as possible.
- New CRLs will be issued.
- The cause of the key compromise will be determined and the situation rectified.

Please note: No timestamping certificate is in active use anymore and the according private keys have been securely destroyed.

5.7.4 Business continuity capabilities after a disaster

Refer to clause 5.7.4 of SwissSign TSPS.

5.8 CA or RA termination

Refer to clause 5.8 of SwissSign TSPS.

6. Technical Security Controls

Refer to clause 6 of SwissSign TSPS.

6.1 Key pair generation and installation

Refer to clause 6.1 of SwissSign TSPS.

6.1.1 Key pair generation

Following the TSP's documented procedures, the key pair for the "SwissSign Platinum CA" (Root CA Key) has been created in an offline HSM that meets the requirements 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 and ETSI EN 319 411-2.

Following the TSP's documented procedures, the key pairs for the subordinated issuing CA of the SwissSign Platinum 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 were documented and stored in accordance with the requirements of ETSI EN 319 411-1 and ETSI 319 411-2. During the operation of the issuing CA, the role 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

QCP-n-qscd: Subscriber keys were generated by the TSP using an HSM or on a qualified signature creation device (SSCD) in the secure environment of the TSP. In both cases the requirements of EN 319 411-2 were met.

QCP-l-qscd, NCP+: Subscriber keys were generated by the TSP using an HSM or on a qualified signature creation device (SSCD) in the secure environment of the TSP. In both cases, requirements of EN 319 411-2 were met.

QCP-l-qscd: If the key pairs were produced under the responsibility of the Subscriber, they had to use a qualified signature creation device (HSM) that meets the requirements of ETSI EN 319 411-2 and ETSI EN 119 312. This had to be proven to the TSP. By transmitting a PKCS # 10 request to the TSP, the subscriber proves the possession of the private key.

TSA/TSU: Keys were generated using an HSM and this is done only by personnel in trusted roles using, at least, dual control in a physically secured environment.

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

The TSP uses only eligible secure signature creation device (SSCD). The SSCD are initialized in the secure environment of the TSP, during which each SSCD is checked for its authenticity. During the initialization process, the key pairs are generated on the SSCD and the TIN and PUK information is generated.

The TSP stores the SSCD and the TIN and PUK information separately within the secure premises of the TSP. After a certificate application has been successfully checked, the SSCD associated with the applicants data is sent to the applicant by postal mail. The TIN and PUK letters are sent separately and with a dedicated delay.

Private keys generated by the subscriber do not need to be delivered.

NCP+, Advanced Seal: Private keys were not delivered as they are maintained by the TSP on behalf of the TSP.

QCP-n-qscd (UBS) is a remote service and the keys are managed on behalf.

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	

The “SwissSign Platinum CA” uses a 4096 bit RSA key.

The subordinate 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 and which are divisible by 8.

6.1.6 Public key parameters generation and quality checking

Key pairs are generated on SwissSign-approved secure crypto devices and parameters have been specified to meet all certification and security requirements.

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

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

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

6.1.7.1 TSA Platinum CA Certificate

Key usage:

- keyCertSign, cRLSign

Extended key usage:

- TimeStamping

6.1.7.2 Regulated Seal Certificate (qcp-l-qscd)

Key usage:

- digital Signature

Extended key usage:

- DocumentSigning
- AuthenticDocumentsTrust

6.1.7.3 Advanced Seal Certificate (ncp+)

Key usage:

- digitalSignature
- nonRepudiation (optional)

Extended key usage:

- DocumentSigning
- AuthenticDocumentsTrust

6.1.7.4 SuisseID Qualified Certificate and Qualified Signature Certificate (UBS) (qcp-n-qscd)

Key usage:

- nonRepudiation

6.1.7.5 SuisseID Identity and Authentication Certificate (ncp+)

Key usage:

- digitalSignature

Extended key usage:

- clientAuth
- emailProtection
- Microsoft Smart Card Logon (msSCL)

6.1.7.6 UBS qualified signature certificates (QCP-n-qscd)

Key usage:

- NonRepudation

Extended key usage:

- DocumentSigning,
- AuthenticDocumentsTrust

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.
TSA keys	The HSM used for TSA 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.
IAC / QC / Reg. Seal	Subscriber keys for qualified and regulated certificates must be generated and stored on a secure signature-creation devices (SSCD) or an HSM that meets the applicable security and certification requirements. The TSP has implemented organizational monitoring procedures to ensure that the device is certified as a QSCD regarding to Regulation (EU) N° 910/2014 as well as that it fulfills the requirements of ZertES/VZertES and TAV during the whole certificate life cycle. The number of PIN entries is not greater than 4 attempts. The minimal PIN length is at least 6 characters. The subscriber must document the steps for generating and activating the private key if he manages the QSCD himself.
Advanced Seal	The HSM used for must meets at least FIPS 140-2 level 3 requirements or equivalent.

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.
TSA keys	Management access to these keys is only possible using '4-eye' principle (2 out of m). Once the TSA is operable, signing operations are fully automated.
IAC / QC / Reg. Seal / Advanced Seal	The registration process ensures that the Subscriber is the only person with access to the keys on the Subscriber SSCD.

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.
IAC / QC / Reg. Seal	Private key escrow is not allowed for qualified and regulated certificates.
Advanced Seal	Private key escrow is not supported for advanced seal certificates.

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.
TSA keys	The TSA 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.
IAC / QC / Reg. Seal	All keys are generated on the SSCD and cannot be put into backup.
Advanced Seal	Private key are managed by the TSP within secure HSM and cannot be extracted decrypted.

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.
TSA keys	The TSA keys are not archived.
IAC / QC / Reg. Seal	All keys are generated on the SSCD and cannot be extracted.
Advanced Seal	Private key are managed by the TSP within secure HSM and cannot be extracted decrypted.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Root CA keys	Root CA keys have been backed up onto an HSM so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 6 persons be present in order to gain physical and logical access. At least one of these persons must be a member of the Board of Directors of the TSP.
Issuing CA keys	The Issuing CA keys are cloned in the same manner as Root keys.
TSA keys	The TSA keys are generated and managed in the SSCD. They are not transferred..
IAC / QC / Reg. Seal	Subscriber keys that have been generated on the SSCD cannot be cloned.
Advanced Seal	Private key are managed by the TSP within secure HSM and cannot be extracted decrypted.

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.
TSA keys	The TSA keys are stored on cryptographic modules so that they can be used only if properly activated.
IAC / QC / Reg. Seal	Subscriber keys are stored on cryptographic modules so that they can be used only if properly activated.
Advanced Seal	Private key are managed by the TSP within secure HSM and cannot be extracted decrypted.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

Root CA keys	The Root CA keys are activated with a user key (physical), a user pin (knowledge) and 3 authentication keys (physical).
Issuing CA keys	The Issuing CA keys are activated with role-based access control requiring at least two persons and an SSCD PIN.
TSA keys	The TSA keys are activated with role-based access control requiring at least two persons and an SSCD PIN.
IAC / QC / Reg. Seal	Subscriber keys are activated with a token PIN and, in the case of the recognized qualified certificate, a secondary authentication PIN for the EAL 4+ certified key store. The PIN letter is deliverd to the subscriber. The PIN letter will be handeld securely and seperatd from the SSCD.
Advanced Seal	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.
TSA keys	The TSA keys are deactivated by terminating the key daemon process, by shutting down the CA server processes or by shutting down the server.
QC	Subscriber keys are deactivated by removing the SSCD from the computer or by terminating the application that had access to the SSCD. In the case of the recognized qualified certificate, the key is automatically deactivated with every use.
Advanced Seal	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.
TSA keys	The TSA keys are destroyed by initializing the partition on the HSM.
QC	Subscriber keys can only be destroyed by destroying the SSCD.
Advanced Seal	Private key are managed by the TSP within secure HSM and cannot be extracted decrypted.

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

6.4 Activation data

6.4.1 Activation data generation and installation

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 six 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.
TSA keys	The TSA keys are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.
QC/NCP+	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

Refer to clause 6.5 of SwissSign TSPS.

6.5.1 Specific computer security technical requirements

Refer to clause 6.5.1 of SwissSign TSPS.

6.5.2 Computer Security rating

Refer to clause 6.5.2 of SwissSign TSPS.

6.6 Life cycle technical controls

6.6.1 System development controls

Refer to clause 6.6.1 of SwissSign TSPS.

6.6.2 Security management controls

Refer to clause 6.6.2 of SwissSign TSPS.

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

6.6.3 Life cycle security controls

Refer to clause 6.6.3 of SwissSign TSPS.

6.7 Network security controls

Refer to clause 6.7 of SwissSign TSPS.

6.8 Time-stamping

Please note: No timestamping service operating according to this CP/CPS (or with a certificate issued under the Platinum G2 root) is issuing timestamps anymore.

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 service that can be used to create a timestamp for arbitrary documents. This service is implemented in accordance with ETSI EN 319 421.

SwissSign AG has established procedures to ensure that hardware security modules for non-repudiation services are not tampered with during shipment and storage.

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 Platinum CA”.

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.

For this PKI no additional ICA or end-user certificates will be issued.

7.1 Certificate profile

The TSP issues X.509 Version 3 certificates in accordance with ITU-T X.509, IETF RFC5280 and the regulations of ETSI EN 319 412-1 to ETSI EN 319 412-5. 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 Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key	See Chapter 7.1.3
Extensions	X509V3 Extensions	See Chapter 7.1.2
Signature	Certificate Signature	See Chapter 7.1.3

7.1.1 Version number(s)

Version of X.509 certificates: version 3.

7.1.2 Certificate Extensions

7.1.2.1 SwissSign Platinum CA Certificates for Generation 2

CA Type	Subject	Issuer
Root CA (CRL & OCSP only)	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH
Issuing CA (CRL & OCSP only)	CN = SwissSign Personal Platinum CA 2010 - G2 O = SwissSign AG C = CH	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH
Issuing CA (CRL & OCSP only)	CN=SwissSign Personal Platinum CA 2014 – G22 O=SwissSign AG C=CH	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH
Issuing CA (CRL & OCSP only)	CN=SwissSign CH Person Platinum CA 2017 - G22 O=SwissSign AG C=CH organizationIdentifier=NTRCH-CHE-109.357.012	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH
Issuing CA (CRL & OCSP only)	CN = SwissSign Advanced Platinum CA 2019 - G22 O = SwissSign AG C = CH organizationIdentifier=NTRCH-CHE-109.357.012	CN=SwissSign Platinum CA - G2 O=SwissSign AG C=CH

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

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 4096 bit length	
Basic Constraints	CA: TRUE	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	
Authority Key Identifier	50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.1 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 CH Person Platinum CA 2017 - G22

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 4096 bit length	
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	1EC8046DFB72625160A273246FBEF25F4D3492FC	
Authority Key Identifier	50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.1.7 CPS: http://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC ldap://directory.swisssign.net/CN=50AFCC078715476F38C5B465D1DE95AAE9DF9CCC,O=SwissSign,C=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC http://ocsp.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA256withRSAEncryption	

7.1.2.1.2.2 SwissSign Advanced Platinum CA 2019 - G22

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 4096 bit length	
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 4096 bit length	
Subject Key Identifier	32A57E31D842DBBA2CB2FEE669099DB7DA90D210	
Authority Key Identifier	50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.1.10 CPS: http://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC ldap://directory.swisssign.net/CN=50AFCC078715476F38C5B465D1DE95AAE9DF9CCC,O=SwissSign,C=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC http://ocsp.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA256withRSAEncryption	

7.1.2.1.2.3 SwissSign Personal Platinum CA 2010 - G2

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 2048 bit length	
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical
Subject Key Identifier	4ad43b86ef10538eafe44c77594782fd00117688	
Authority Key Identifier	50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	
Certificate Policies	Policy: 2.5.29.32.0 (anyPolicy) CPS: http://repository.swisssign.com/SwissSign-Platinum-CP-CPS-R3.pdf	
CRL Distribution Points	http://crl.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC ldap://directory.swisssign.net/CN=50AFCC078715476F38C5B465D1DE95AAE9DF9CCC,O=SwissSign,C=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC http://ocsp.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA1withRSAEncryption	

7.1.2.1.2.4 SwissSign Personal Platinum CA 2014 - G22

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 2048 bit length	
Basic Constraints	CA: TRUE, pathlen: 0	Critical
Key Usage	keyCertSign, cRLSign	Critical

Extension Attribute	Values	Comment
Subject Public Key Info	Public Key algorithm: RSAEncryption, Subject Public Key of 2048 bit length	
Subject Key Identifier	59b0d9bf3dc137b6dc0614a7e199e34218da9641	
Authority Key Identifier	50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	
Certificate Policies	Policy: 2.5.29.32.0 (anyPolicy) CPS: http://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf	
CRL Distribution Points	http://crl.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC ldap://directory.swisssign.net/CN=50AFCC078715476F38C5B465D1DE95AAE9DF9CCC,O=SwissSign,C=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC http://ocsp.swisssign.net/50AFCC078715476F38C5B465D1DE95AAE9DF9CCC	URL to OCSP responder and URL to root certificate
SignatureAlgorithm	SHA256withRSAEncryption	

7.1.2.1.3 Fields and extensions of Leaf Certificates

For the following profiles, the certificates shall not contain any information regarding the power of attorney or the right to sign on behalf of a company or another individual.

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

7.1.2.1.3.1 Regulated Seal Certificates issued by SwissSign CH Person Platinum CA 2017 – G22 (QCP-L-QSCD)

No certificates are being issued under this product/profile anymore.

Extension Attribute	Values	Comment
Subject	/CN=/O (mandatory) /organizationIdentifier (mandatory) /OU (optional) /O (mandatory) /L (optional) /ST (optional) /C (mandatory)	See Definitions in Chapter 1.6
Valid from/to	3 years	Maximum validity in years of a certificate issued under this profiled. Certificates issued under this profile can have also a validity period shorter than the maximum validity period stated here.
Issuer Name	/ CN=SwissSign CH Person Platinum CA 2017 - G22 / organizationIdentifier=NTRCH-CHE-109.357.012 / O=SwissSign AG / C=CH	DN of the issuing CA
Authority Key Identifier	1EC8046DFB72625160A273246FBEF25F4D3492FC	
CRL Distribution Points	http://crl.swisssign.net/1EC8046DFB72625160A273246FBEF25F4D3492FC ldap://directory.swisssign.com/CN=1EC8046DFB72625160A273246FBEF25F4D3492FC,O=SwissSign AG,C=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.1.1 CPS: https://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf Policy: 0.4.0.194112.1.3 (qcp-l-qscd)	

Extension Attribute	Values	Comment
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/1EC8046DFB72625160A273246FBEF25F4D3492FC http://platinum-suisseid-g2.ocsp.swisssign.net/1EC8046DFB72625160A273246FBEF25F4D3492FC	URL to OCSP responder and optional URL to CA issuer certificate
QC Statements	0.4.0.1862.1.7 QcCClegislation (CountryName = CH) 0.4.0.1862.1.4 Secure Signature Creation Device Qualified Certificate 0.4.0.1862.1.5 PDS=https://repository.swisssign.com/SwissSign-PDS.pdf 0.4.0.1862.1.6 QC Type=0.4.0.1862.1.6.2 (Certificate for electronic seals)	
Key Usage	digitalSignature	
Extended Key Usage	DocumentSigning, AuthenticDocumentsTrust	see chapter 6.1.7 for additional values
SignatureAlgorithm	SHA256withRSAEncryption	

7.1.2.1.3.2 Advanced Seal Certificates issued by SwissSign Advanced Platinum CA 2019 - G22 (NCP+)

Extension Attribute	Values	Comment
Subject	/CN=/O (mandatory) /organizationIdentifier (mandatory) /O (mandatory) /OU (optional) /L (optional) /ST (optional) /C (mandatory)	See Definitions in Chapter 1.6
Valid from/to	3 years	Maximum validity in years of a certificate issued under this profiled. Certificates issued under this profile can have also a validity period shorter than the maximum validity period stated here.
Issuer Name	/ CN=SwissSign Advanced Platinum CA 2019 - G22 / organizationIdentifier=NTRCH-CHE-109.357.012 / O=SwissSign AG / C=CH	DN of the issuing CA
Authority Key Identifier	32A57E31D842DBBA2CB2FEE669099DB7DA90D210	
CRL Distribution Points	http://crl.swisssign.net/32A57E31D842DBBA2CB2FEE669099DB7DA90D210 ldap://directory.swisssign.net/CN=32A57E31D842DBBA2CB2FEE669099DB7DA90D210%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy:2.16.756.1.89.1.1.1.1.1 CPS: https://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf Policy: 0.4.0.2042.1.2 (NCP+)	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/32A57E31D842DBBA2CB2FEE669099DB7DA90D210 http://ocsp.swisssign.net/32A57E31D842DBBA2CB2FEE669099DB7DA90D210	URL to OCSP responder and optional URL to CA issuer certificate
Key Usage	digitalSignature, nonRepudiation	nonRepudiation optional

Extension Attribute	Values	Comment
Extended Key Usage	DocumentSigning, AuthenticDocumentsTrust	see chapter 6.1.7 for additional values
SignatureAlgorithm	SHA256withRSAEncryption	

7.1.2.1.3.3 Timestamping certificates issued by SwissSign Personal Platinum CA 2010 - G2

Extension Attribute	Values	Comment
Subject	/CN=Time Stamping Authority: PostFinance AG /OU (optional) /O=*PostFinance AG* OR *Die Schweizerische Post* /L=Bern /ST=Bern /C=CH	See Definitions in Chapter 1.6
Valid from/to	11 years	Maximum validity in years of a certificate issued under this profiled. Certificates issued under this profile can have also a validity period shorter than the maximum validity period stated here.
Issuer Name	/CN=SwissSign Personal Platinum CA 2010 - G2/O=SwissSign AG/C=CH	DN of the issuing CA
Authority Key Identifier	4AD43B86EF10538EAFE44C77594782FD00117688	
CRL Distribution Points	http://crl.swisssign.net/4AD43B86EF10538EAFE44C77594782FD00117688 ldap://directory.swisssign.net/CN=4AD43B86EF10538EAFE44C77594782FD00117688%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.1 CPS: http://repository.swisssign.com/SwissSign-Platinum-CP-CPS-R3.pdf	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/4AD43B86EF10538EAFE44C77594782FD00117688 http://ocsp.swisssign.net/4AD43B86EF10538EAFE44C77594782FD00117688	URL to OCSP responder and optional URL to CA issuer certificate
Key Usage	digitalSignature, nonRepudiation	
Extended Key Usage	• timeStamping	
SignatureAlgorithm	SHA1withRSAEncryption	

7.1.2.1.3.4 Timestamping certificates issued by SwissSign Personal Platinum CA 2014 - G22/O=SwissSign AG

Extension Attribute	Values	Comment
Subject	/CN=Time Stamping Authority: PostFinance AG /OU (optional) /O=PostFinance AG /L=Bern /ST=Bern /C=CH	See Definitions in Chapter 1.6
Valid from/to	11 years	Maximum validity in years of a certificate issued under this profiled. Certificates issued under this profile can have also a validity period shorter than the maximum validity period stated here.
Issuer Name	CN=SwissSign Personal Platinum CA 2014 - G22, O=SwissSign AG, C=CH	DN of the issuing CA
Authority Key Identifier	59B0D9BF3DC137B6DC0614A7E199E34218DA9641	
CRL Distribution Points	http://crl.swisssign.net/59B0D9BF3DC137B6DC0614A7E199E34218DA9641 ldap://directory.swisssign.net/CN=59B0D9BF3DC137B6DC0614A7E199E34218DA9641%2CO=SwissSign%2CC=CH?certificateRevocationList?base?objectClass=cRLDistributionPoint	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.1.1 CPS: https://repository.swisssign.com/SwissSign-Platinum-CP-CPS.pdf	
Authority Information Access	http://swisssign.net/cgi-bin/authority/download/59B0D9BF3DC137B6DC0614A7E199E34218DA9641 http://platinum-personal-g2.ocsp.swisssign.net/59B0D9BF3DC137B6DC0614A7E199E34218DA9641	URL to OCSP responder and optional URL to CA issuer certificate
Key Usage	digitalSignature, nonRepudiation	
Extended Key Usage	• timestamping	see chapter 6.1.7 for additional values
SignatureAlgorithm	SHA256withRSAEncryption	

7.1.2.2 User Notices

The following certificates issued respectivly have an according User Notice:

- Under “Person CH Platinum G22” and “TSA Platinum G22”, the User Notice “regulated certificate”

7.1.3 Algorithm object identifiers

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

Algorithm	Object Identifier
Sha1WithRSAEncryption	1.2.840.113549.1.1.5 (phase out)
SHA256withRSAEncryption	1.2.840.113549.1.1.11
RSAEncryption	1.2.840.113549.1.1.1

7.1.4 Name forms

Certificates issued by the subordinated issuing CAs of this CA contain the full X.509 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string. The Subject DN field of the Issuing CA is byte-for-byte identical with the Issuer DN field among all leaf-certificates.

7.1.5 Name constraints

No Issuing CA is technically constrained. The SwissSign Issuing CA are publicly disclosed within the 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	
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 Maximum validity for CARL of the Root CA is 1 year after issuance of the CARL by the Issuing CA (nextUpdate is set to 1 year) If it is the last CRL issued for those certificates in the scope of this CRL, the nextUpdate field in the CRL will be set to "99991231235959Z" as required by IETF RFC 5280.
revoked Certificates:	serial	List of revoked Certificate serial numbers
reasonCode		For CARL issued by the Root CA - reasonCode extension is present and not marked critical - possible reason codes in CARL: - cACompromise (2), or - cessationOfOperation (5)

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
- ExpiredCertsOnCRL: Populated as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 if there are expired certficates on the CRL that have been revoked.

7.3 OCSP profile

The SwissSign OCSP functionality is built according to RFC 6960.

OCSP response Field	Values	Comment
Version Number	V1	Indicates the version
CertStatus	Good, revoked unknown	Indicates the response for certificate status
Validity		The difference in time between the thisUpdate and nextUpdate field. For leaf-certificates: The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate. For Root and Issuing CA: The OCSP response is valid for 3 days. The information provided is updated at least 8 hours prior to the nextUpdate.

The OCSP respons is according to RFC 6960:

- Good - for valid certificates
- Revoked - for certificates that have been revoked or
- Unknown - for certificates that 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

The OCSP extension ArchiveCutOff is not set.

Reasoning: After revocation or expiration of the last leaf certificate issued under a CA a “lastCRL” is issued that contains the serial numbers of all revoked certificates, then the Issuing CA itself is revoked. Therefore, status information is provided via the lastCRL and the continuation of the OCSP service under a revoked CA would not provide an added value.

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 and EN 319 411-2. The terms and conditions of this CP/CPS, Swiss Digital Signature Law and all dependent rules and regulations will be used to conduct compliance audits for:

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

8.1 Frequency or circumstances of assessment

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

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

8.2 Identity/qualifications of assessor

An independent qualified auditor will conduct the compliance audits according to the stipulations of corresponding law, 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 ZertES.

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

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

8.4 Topics covered by assessment

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

8.5 Actions taken as a result of deficiency

The TSP has implemented 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 and the ZertES Recognition Body a plan how the issues are going to be addressed.

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

8.7 Risk assessment

The TSP carries out a regular risk analysis which comprehensively analyzes the threat to the company as well as requirements and countermeasures. A residual risk analysis is carried out and documented in which the legibility of the residual risk is identified and, where appropriate, accepted. The relevant assets are adequately recorded and changes to these assets are reviewed at least yearly or, if applicable, released by the management team. The TSP maintains an inventory of all information assets, assigns a classification

consistent with the risk assessment and ensures an appropriate level of protection of the assets. The risk analysis is carried out annually, based on the requirements of the ISO 27001:2013 standard and released by SwissSign management body.

9. Other Business and Legal Matters

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

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

9.1.2 Certificate access fees

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

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

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

It is in the sole responsibility of Subscribers and Relying Parties to ensure an adequate insurance, to cover risks using the certificate or rendering respective services, according to Swiss Digital Signature Law.

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

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

9.3.2 Information not within the scope of confidential information

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

9.3.3 Responsibility to protect confidential information

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

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

9.4 Privacy of personal information

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

9.4.1 Privacy Plan

The stipulations of chapter 9.3 and 9.4 apply.

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

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

9.4.6 Disclosure pursuant to judicial or administrative process

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

9.4.7 Other information disclosure circumstances

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

9.5 Intellectual property rights

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

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

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

9.6.2 RA representations and warranties

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

9.6.3 Subscriber representations and warranties

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

9.6.4 Relying Party representations and warranties

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

9.6.5 Representations and warranties of other participants

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

9.7 Disclaimers of warranties

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

9.8 Liability

9.8.1 Liability of the TSP

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

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

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

9.8.2 Liability of the Subscriber

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

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

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This Certificate Policy and Certification Practice Statement and respective amendments become effective as they are published on the SwissSign website at “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.

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 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 competent courts at the place of jurisdiction pursuant to clause 9.14.

9.14 Governing law and place of jurisdiction

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

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

9.15 Compliance with applicable law

This CP/CPS and rights or obligations related hereto are in accordance with the relevant provisions of the EU Regulation No 910/2014 and of the other applicable laws. Compliance with the laws and regulations are verified within the annual external audit. The audits are carried out by an independent qualified auditor.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The following documents and the Subscriber-Agreement of SwissSign AG state the agreement between the TSP and the Subscriber:

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

9.16.2 Assignment

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

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

9.16.3 Severability

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

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

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

The TSP will communicate an appropriate change within 90 days.

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable.

9.16.5 Force Majeure

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

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

9.17 Other provisions

9.17.1 Language

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

9.17.2 Delegated or outsourced Services

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