SwissSign Platinum CP/CPS

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

Document Type:	Certificate Policy and Certification Practice Statement
OID:	2.16.756.1.89.1.1.1.1.1
Author:	Michael Doujak, CEO
Classification:	C1 (public)
Applicability:	Global
Owner:	CEO
Issue Date:	Mai 4th, 2007
Version:	2.0.1
Obsoletes:	Version 2.0.0, February 27th, 2007
Storage:	SwissSign Document Repository
Distribution:	Global
Status:	Released
Review:	This document is reviewed periodically at least once per calendar year. The owner is responsible for this review.
Compliance:	The SwissSign Platinum CA operating under this CP/CPS is only in connection with the SwissSign Qualified Platinum CA operating under the respective CP/CPS fully compliant with the rules and regulations of ZertES, VZertES and all stipulations therein.

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

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

Melanie Reinhilde Raemy
Digitally signed by Melanie Reinhilde Raemy
DN: cn=Melanie Reinhilde Raemy, c=CH, o=SwissSign AG, email=melanie.raemy@swisssign.com
Reason: I am approving this document
Date: 2007.05.21 10:03:26 +02'00'
digital signature

Bjoern Alexander Kanebog
Digitally signed by Bjoern Alexander Kanebog
DN: cn=Bjoern Alexander Kanebog, c=CH, o=SwissSign AG, email=bjoern.kanebog@swisssign.com
Reason: I am approving this document
Date: 2007.05.21 10:17:42 +02'00'
digital signature

Table of Contents

1 Introduction

The "SwissSign Platinum CA" is a root certification authority operated by SwissSign AG.

The "SwissSign Platinum CA" only issues certificates to its subordinated issuing CAs and special purpose certificates for the operation of the CSP (e.g. Time Stamping Authority).

The "SwissSign Platinum CA" complies with the following Swiss digital signature laws, 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)

Swiss digital signature law refers to the standards listed below that are prerequisites for the issuance of qualified certificates:

- ETSI TS 101 456 v1.4.1: Electronic Signatures and Infrastructures (ESI) – Certificate Policy and Certification Practices Framework
- ETSI TS 101 861 v1.3.1: Time Stamping Profile
- ETSI TS 101 862 v1.3.3: Qualified Certificate Profile
- IETF RFC 3647 (2003): Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
- IETF RFC 3280 (2002): Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The "SwissSign Platinum CA" has different subordinated issuing CAs, one of those issuing qualified certificates. The Certificate Policies and Certification Practice Statements of all subordinated issuing CAs are not subject of this CP/CPS with exception of certain minimal standards which are stated in this document.

In this CP/CPS "this CA" refers to the "SwissSign Platinum CA" only.

1.1 Overview

The picture below shows the hierarchy of the SwissSign Platinum CA tree:

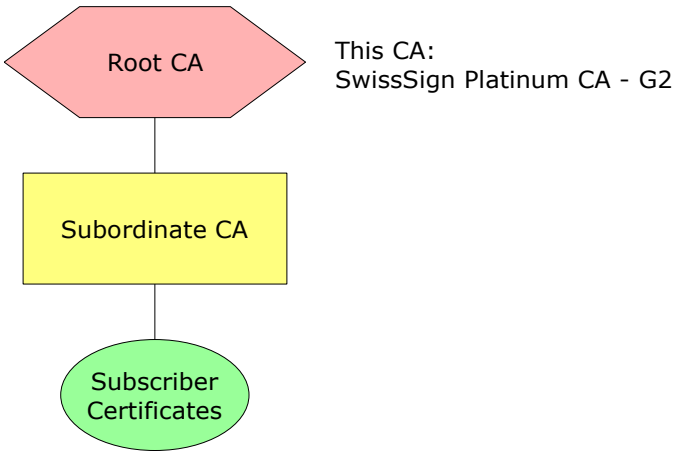

Illustration 1: Platinum CA Hierarchy

This SwissSign AG certificate policy and certification practice statement (CP/CPS) for the "SwissSign Platinum CA" describes:

- The certificate policy of this CA.
- Practices and procedures of this CA.
- Terms and conditions under which this root certificate is made available.

This CP/CPS is applicable to all persons, including, without limitation, all requesters, subscribers, relying parties, registration authorities and any other person, that have a relationship with SwissSign AG with respect to certificates issued by this CA.

1.2 Document name and identification

This document is named "SwissSign Platinum CA Certificate Policy and Certification Practice Statement" as indicated on the cover page of this document.

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

OID 2.16.756.1.89.1.1.1.1.1

The OID of SwissSign AG is based on the RDN issued by the Swiss Federal Office of Communications (OFCOM) and structured as follows:

Position 1	**Position 2**	**Position 3**	**Position 4**	**Position 5**	**Meaning**
2					Joint ISO-CCITT Tree
	16				Country
		756			Switzerland
			1		RDN
				89	SwissSign

Position 6 to 9 of the SwissSign OID number represent the document and 10 represents the document version, which is only shown in subscriber certificates (see chapter 7).

1.3 PKI participants

1.3.1 Certification authorities

SwissSign AG operates a Public Key Infrastructure, consisting of a "SwissSign Platinum CA" and its subordinated issuing CAs. The "SwissSign Platinum CA" is the only CA operated by SwissSign AG that issues root certificates under this CP/CPS.

1.3.2 Registration authorities

The "SwissSign Platinum CA" does not issue subscriber certificates. SwissSign AG does therefore not operate a registration authority for this CA. Registration Authorities and registration processes are specified in the CP/CPS of the respective issuing CA.

1.3.3 Subscribers

The "SwissSign Platinum CA" does not issue subscriber certificates. The role and responsibilities of the subscribers are specified in the CP/CPS of the respective issuing CA. The subscriber obligations must meet the stipulations of chapter 6.2 of ETSI 101 456 v1.4.1.

1.3.4 Relying parties

Relying parties are individuals or organizations, which use certificates of subordinated issuing CAs and use the root CA Certificate to verify the validity of the issuing CA. The role and responsibilities of the relying parties are specified in the CP/CPS of the respective issuing CA. The information of relying parties must meet the stipulations of chapter 6.3 of ETSI 101 456 v1.4.1.

1.3.5 Other participants

Other participants are individuals or organizations that are in some way involved with PKI-related services.

The following participants have very specific roles with regard to the "SwissSign Platinum CA":

BAKOM: BAKOM issues the "Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur" which governs the technical aspects of the CSP operation.

SAS:	SAS, as the accreditation authority, chooses the auditors for the certification of CSPs in Switzerland.
KPMG:	KPMG is the official recognition body for Swiss CSPs and, as such, conducts the audits prescribed by Swiss digital signature law.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The use of the signing key of this CA is limited to sign its own certificate, the certificates of the subordinated issuing CAs, CRLs and the TSA units.

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
Beethovenstrasse 49
8002 Zürich
Switzerland
Tel.: +41 (43) 344 88 11
info@swisssign.com

Current versions of documents may be downloaded from the SwissSign website:

- http://repository.swisssign.com

The current version of this CP/CPS document must be digitally signed by two officers of SwissSign AG and is the only reliable source for the SwissSign Platinum CP/CPS.

1.5.2 Contact persons

The following person is the main contact for any questions or suggestions regarding the SwissSign Platinum CP/CPS.

Michael Doujak
C.E.O of SwissSign AG
csp.feedback@swisssign.com

All feedback, positive or negative, is welcome and should be submitted to the above e-mail address to ensure that it is dealt with appropriately and in due time.

1.5.3 Person determining CPS suitability for the policy

Executive management of SwissSign AG determines the suitability and applicability of this CP/CPS.

Changes or updates of documents describing the "SwissSign Platinum CA" must be made in accordance with the stipulations of Swiss Digital Signature Law and the provisions contained in this CP/CPS and can therefore be subject to an approval by the organization appointed by SAS. Currently, this role is held by:

KPMG Klynfeld Peat Marwick Goerdeler SA
Badenerstrasse 172
8026 Zürich
Switzerland

1.5.4 CP/CPS approval procedures

Executive management of SwissSign AG regularly evaluates documents describing the "SwissSign Platinum CA" so that it adheres to applicable law, such as stipulated in chapter 1 of this CP/CPS.

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.
CA Operator	CAO	A person responsible for CA operation, including establishment of certificate parameters for RA and RAO in accordance with certificate policy.
Certificate		Information issued by a trusted third party, often published in a directory with public access. The certificate contains at least a subject, a unique serial number, an issuer and a validity period.
Certification Authority	CA	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certificate Extension		Optional fields in a certificate.
Certificate Policy	CP	A set of rules that a request must comply with in order for the RA to approve the request or a CA to issue the certificate.
Certificate Revocation List	CRL	List of certificates that have been declared invalid. This list is issued by the CA at regular intervals and is used by applications to verify the validity of a certificate.
Certification Practice Statement	CPS	Document that regulates the rights and responsibilities of all involved parties (RA, CA, directory service, end entity, relying party).
Certification Service Provider	CSP	Individual or corporation that issues certificates to individual or corporate third parties.
Cipher		A cryptographic algorithm used to encrypt and decrypt files and messages.
Cipher Text		Data that has been encrypted. Cipher text is unreadable unless it is converted into plain text (decrypted) with a key.
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 TS 102.023 v1.2.1. 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.

Term	Abbrev.	Explanation
Digital signature		A system allowing individuals and organizations to electronically certify features such as their identity or the authenticity of an electronic document.
Directive 1999/93/EC		European digital signature law: Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures. Compliance with this law always implies compliance with the following standards: ETSI TS 101 456 v1.4.1, ETSI TS 101 861 v1.3.1 and ETSI TS 101 862 v1.3.3
Distinguished Name	DN	-> Subject
DNS		Domain Name System. The Internet system of holding a distributed register of entity names. For example, the domain is the part of the email address to the right of the `@', e.g. `anytown.ac.uk'.
Electronic Signature		-> Digital Signature
Encryption		Encryption is the process of using a formula, called an encryption algorithm, to translate 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.
End-User Agreement	EUA	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.
FQDN	FQDN	Fully Qualified Domain Name.
Hardware Security Module	HSM	Hardware Security Module, used for special protection of encryption keys.
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 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 (1024 is the most common key size today).
Key usage		Key's intended purpose. This information is stored in the certificate itself to allow an application to verify that the key is intended for the specified use.
Lightweight Directory Access Protocol	LDAP	LDAP is used to retrieve data from a public directory.
LDAP Secure	LDAPS	LDAP secured with SSL
Online Certificate Status Protocol	OCSP	Method to verify the validity of a certificate in real-time.

Term	Abbrev.	Explanation
Participants		Entities like CAs, RAs, and repositories. These can be different legal entities.
PKCS		PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Laboratories.
Plain Text		The original message or file.
Privacy Level		Used to determine how the certificate is managed 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 SwissSign web page. Access to this profile can be granted by means of username 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 confirm 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.
Qualified Certificate	QC	Certificate which meets the requirements of article 7 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		Advanced electronic signature, which is based on a qualified certificate and created by a secure-signature creating device, as defined in article 5.1 of the Directive 1999/93/EC.
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.
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.
S/MIME		Secure / Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail.
Secure Signature Creation Device	SSCD	Signature-creation device which meets the requirements specified in annex III of Directive 1999/93/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 codes 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 codes or public cryptographic keys, used for the purpose of verifying an electronic signature.
SSL		Secure Sockets Layer. A protocol developed by Netscape that enables secure transactions via the Internet. URLs that require an SSL connection for HTTP start with https: instead of http:.
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 /OU=DEMO /C=CH /Email=root@signdemo.com mandatory fields in the subject: Common Name --- /CN Email address --- /Email optional fields in the subject: Organization --- /O Organizational Unit --- /OU Domain Component --- /DC Country Name --- /C Locality Name --- /L Street Address --- /STREET Given Name --- /G Surname --- /S Initials --- /I Unique Identifier --- /UID Serial Number --- /SN Title --- /T Description --- /D
Subscriber		Subscribers are individuals and organizations that have obtained a certificate.
TAV-BAKOM		Swiss addition to VZertES, technical and administrative directives on the issuance of digital signatures, issued December 6, 2004. SR 943.032.1.
Time-stamping Authority	TSA	Authority which issues time-stamp tokens.
Time-stamp Policy	TP	Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements.
Time-stamp Token	TST	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
Time-stamping Unit		Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.
TSA Disclosure statement		Set of statements concerning the policies and practices of a TSA that requires emphasis or disclosure to subscribers and relying parties, for example, to meet regulatory requirements.

Term	Abbrev.	Explanation
TSA practice statement	TPS	Statement of the practices that a TSA employs in issuing time-stamp tokens.
TSA system		Composition of IT products and components organized to support the provision of time-stamping services.
Transaction Limit		The transaction limit is detailing liability limits of SwissSign AG, the subscriber and relying parties. This limit is published in the respective certificate.
Triple DES		A method of improving the strength of the DES algorithm by using it three times in sequence with different keys.
Two-factor authentication		A two-factor authentication is any authentication protocol that requires two independent ways to establish identity and privileges.
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 December 3, 2004. SR 943.032.
ZertES		Swiss Digital Signature Law. Issued December 19, 2003. SR 943.03. Compliance with this law always implies adherence to VZertES and TAV-BAKOM.

2 Publication and Repository Responsibilities

SwissSign AG will make its certificate(s), 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 must be digitally signed. To document the validity period of the document, a version history is included.

2.1 Repositories

SwissSign AG maintains all documentation related to the "SwissSign Platinum CA" on the swisssign.com and swisssign.net web sites. The web sites are cross-linked to enable seamless browsing.

SwissSign AG maintains two web sites to enhance the overall security of the solution:

swisssign.net: This web site is used for all certificate- (CRL, LDAP, ...) and certificate-management-related functions. SwissSign employee access to this web site is strictly regulated (role-based access control) and the coding as secure as possible.

swisssign.com: This web site is used for the distribution of information. Product and corporate information can be found here. Access to this web site by SwissSign employees does not follow the general role model as all important content (documents) consists of digitally signed documents.

http://www.admin.ch/ch/index.de.html	This link points to the official web site of the Swiss government. Relevant documentation to Swiss Digital Signature Law can be found here.
http://www.admin.ch/ch/d/sr/c943_03.html	"Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur"
http://www.admin.ch/ch/d/sr/c943_032.html	"Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur"
http://www.sas.ch/de/pki_isms/pki.html	PKI page of the Swiss accreditation body.
http://pda.etsi.org/pda/queryform.asp	ETSI provides a searchable download area where standards like ETSI 101.456, ETSI, 101.861 and ETSI 101.862 can be found.

2.2 Publication of certification information

SwissSign AG publishes all current documentation pertaining to this CA on the swisssign.com and/or swisssign.net web site. This web site is the only source for up-to-date documentation and SwissSign AG reserves the right to publish newer versions of the documentation without prior notice.

For this CA, SwissSign AG will publish an approved, current and digitally signed version of the certificate policy and practice statement (CP/CPS).

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

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

The data formats used for certificates issued by this CA and for certificate revocation lists in the swisssign.net web site are in accordance with the associated schema definitions as defined in the X.500 series of recommendations.

2.3 Time or frequency of publication

SwissSign will publish this information on a regular schedule:

- CRLs for the "SwissSign Platinum CA" and all its subordinated issuing CAs are published according to the schedule detailed in chapter 4.9.7.
- OCSP Information: Real-time. The OCSP responder will immediately report a certificate that has been revoked. See also chapter 4.9.9.

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

- SwissSign Platinum CP/CPS: This document will be reviewed at least once a year. If no updates are required, no new version will be published.

2.4 Access controls on repositories

The LDAP, CRL and OCSP information is managed in an encrypted 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. Manager access always requires certificate-based two factor authentication.

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. Write access to the document repository is controlled through certificate-based two factor authentication.

3 Identification and Authentication

Identification and authentication processes for this CA and its duties/obligations are defined in non-public documents, reviewed regularly by the recognition body.

The CP/CPS of every subordinated issuing CA defines in detail the identification and authentication of its subscribers according to RFC 3647 and must be compliant with chapter 7.3 of ETSI 101 456 v1.4.1.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate application

Certificate application for this CA and subordinated issuing CAs are defined in non-public documents, reviewed regularly by the recognition body.

The CP/CPS of every subordinated issuing CA defines in detail Subscriber Certificate application.

4.2 Certificate application processing

Certificate application processes of this CA and subordinated issuing CAs are defined in non-public documents, reviewed regularly by the recognition body.

The CP/CPS of every subordinated issuing CA defines in detail subscriber certificate application process. Requesters have to be identified on the basis of identifying documents as specified by the relevant issuing CA.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon receipt of an approved certificate signing request, all CAs will verify the integrity of the request.

On successful verification, all CAs will then issue the requested certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The requester of a subscriber certificate will be notified in a way specified in the respective CP/CPS.

4.4 Certificate acceptance

The CP/CPS of every subordinated issuing CA defines in detail certificate acceptance by subscribers.

4.5 Key pair and certificate usage

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

The usage of certificates by subscribers is specified in the CP/CPS of the according issuing CA.

4.6 Certificate renewal

Certificate renewal is a process in which a new certificate is issued to a subscriber. The certificate contains new validity information, but retains subject and key information.

The process of certificate renewal shall not be supported.

4.7 Certificate re-key

Details of certificate re-keying are specified in the CP/CPS of the according issuing CA.

4.8 Certificate modification

Certificate modification is the process through which a subscriber requests a certificate with modified subject information. These requests are treated as initial registration requests. The requester is therefore required to start a new certificate request.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Circumstances under which certificates must be revoked are specified in the CP/CPS of the according issuing CA.

4.9.2 Who can request revocation

Details are specified in the CP/CPS of the according issuing CA.

4.9.3 Procedures for revocation request

Details are specified in the CP/CPS of the according issuing CA.

4.9.4 Revocation request grace period

Details are specified in the CP/CPS of the according issuing CA.

4.9.5 Time within which CA must process the revocation request

After proper authorization has been demonstrated, the relevant CA will process revocation requests within two hours after receiving such requests from an RA.

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 3280. 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

The CRL of the "SwissSign Platinum CA" and its subordinated issuing CAs are updated according to the following schedule:

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.
Subordinated issuing CAs	CRL	At least once every 24 hours. At most, 24 hours may pass from the time a certificate is revoked until the revocation is reported on the CRL. CRLs are issued with a life-time of at least 10 days.
	OCSP Information	Real-time. The OCSP responder will report a certificate's revocation immediately 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 Info Access").

4.9.10 On-line revocation checking requirements

The details are specified in the CP/CPS of the according issuing CA.

4.9.11 Other forms of revocation advertisements available

Currently, no other forms of revocation advertisements are available.

4.9.12 Special requirements re key compromise

The details are specified in the CP/CPS of the according issuing CA.

4.9.13 Circumstances for suspension

Certificates suspension is not allowed.

4.10 Certificate status services

4.10.1 Operational characteristics

The certificate status services are CRL and OCSP. The certificate status services provide information on the status of valid certificates. The integrity and authenticity of the status information is protected by a digital signature of the respective CA.

4.10.2 Service availability

SwissSign AG guarantees the annual availability of the certificate status services at 97% for business hours only and a maximum unplanned service interruption duration of 10 days. Outside of business hours the service is available without guarantees.

4.10.3 Optional features

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

4.11 End of subscription

Details of end of subscription are specified in the CP/CPS of the according issuing CA.

4.12 Key escrow and recovery

Details of key escrow and recovery are specified in the CP/CPS of the according issuing CA.

5 Facility, Management, and Operations Controls

All stipulations in this chapter are applicable to this CA only. Subordinated CAs may define different stipulations.

5.1 Physical controls

- Two identical clones of the SwissSign Platinum CA keys are stored off line in Swiss bank safe deposit boxes.
- The SwissSign CA servers are located in a commercial data center that meets the highest security requirements:
  - The data center complies with the IT-Security outsourcing requirements (99/2) of the Swiss banking committee.
  - The data center is a SunTone Certified Member.
  - The data center as well as its operation is annually reviewed by PricewaterhouseCoopers llc.

5.1.1 Site location and construction

Swiss bank:	The Swiss bank safe deposit boxes have been opened with different Banks. One is located in Zurich, the other is located in Bern.
Data center:	The SwissSign electronic data processing center is located in a data center in the greater Zurich area in Switzerland.

5.1.2 Physical access

Swiss bank:	Physical access is only granted to a group of three persons, where one must be a member of the board of directors and one must be a member of the SwissSign executive management. Identification documentation (Passport, ID) and the personal signature of every employee are checked by the personnel of the Swiss Bank. Swiss bank personnel does not have access to the safe deposit box.
Data center:	Physical access is restricted to system administrators and authorized data center personnel. Biometric and electronic badge identification is required to enter the facility in which all movements are recorded by video and access control points.

5.1.3 Power and air-conditioning

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

5.1.4 Water exposure

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

All data relevant to CA services, whether off line or on line in nature, is encrypted and stored.

The disposal of storage media is outsourced to a third party specializing in the destruction of data on storage media.

5.1.7 Waste disposal

The regular operations of the CA services do not create waste in the data center that would require any special action.

5.1.8 Off-site backup

The system periodically generates a backup of all digital information (data, code, configuration, etc.). The backup contains all information relevant for the CA service in encrypted form. A CD or DVD is created and stored off-site in a bank safe deposit box.

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

5.2 Procedural controls

5.2.1 Trusted roles

In order to guarantee a segregation of duties, the roles within the SwissSign CA software are operated by three separated authorization groups: Access, Operations and Audit. Any person may only be part of one of these authorization groups. Within these authorization groups, multiple roles are defined (see picture below). A person assigned to one of the groups may have one or more roles within the same authorization group.

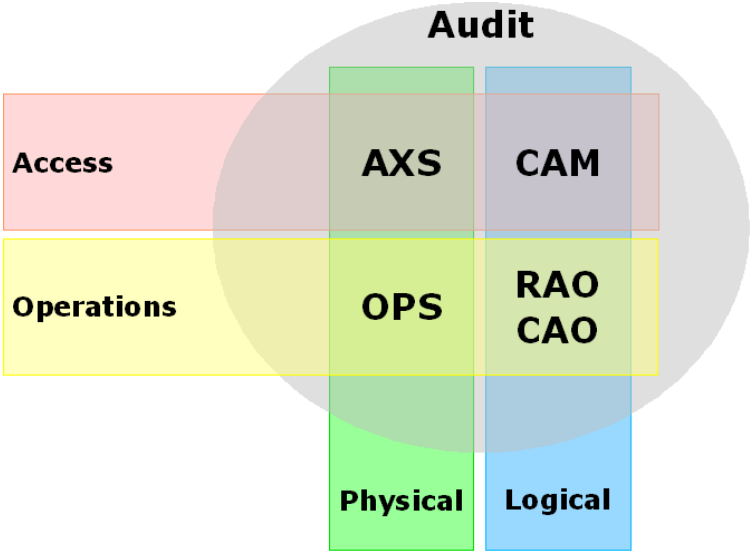

Illustration 2: Segregation of duties

5.2.1.1 Access (AXS & CAM)

Network Administrators (NA) have full control over the network access to all the systems that, when combined, define the SwissSign PKI. The NA has no access to the application software. In other words, an NA neither "sees" the CA software, nor the CA defined in this software, nor the data in the CA.

The CA Manager (CAM) defines, creates, changes, deletes, and thus has full control over one or more of the actual CA and RA systems. The CAM uses the hardware and software provided by the SA.

5.2.1.2 Operations (OPS & RAO/CAO)

System Administrators (SA) have full control of the hardware, operating system and application software (like the CA server), but not of cryptographically relevant information such as the private key of the CA, or the CA itself. The

SA is authorized to install, configure, and maintain the CA's trustworthy systems for registration, certificate generation, subject-device provision and revocation management.

Certification Authority Operators (CAO) can manage all certificates, requests, and profiles as well as a subset of certificate authorities described by the operator access rules. The CAO works with the CA as defined by the CAM and cannot change the definition of the CA. The CAO is responsible for operating the CA's trustworthy systems on a day-to-day basis and is authorized to perform system backup and recovery.

Registration Authority Operators (RAO) can manage a subset of certificates and requests as described by the RA policies and the operator access rules. The RAO works with the RA as defined by the CAM and cannot change the definition of the RA. The RAO is responsible for operating the RA's trustworthy systems on a day-to-day basis and is authorized to perform system backup and recovery.

5.2.1.3 Audit

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

5.2.2 Number of persons required per task

The operation of the "SwissSign Platinum CA" and its subordinated issuing CAs are entirely role-driven and therefore requires at least:

- Access: 2 employees for network access configuration and CA maintenance and management tasks
- Operations: 2 employees for system administration, RA and CA operation
- Audit: 1 auditor

The certificate store and all cryptographically relevant aspects of all CAs (signing operations) can only be accessed by two persons working together (four-eye-principle).

5.2.3 Identification and authentication for each role

Within the CA Software, identification and authentication for all roles is achieved using SwissSign certificates.

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

SwissSign AG has very high standards with regards to the skills of employees.

To be assigned the role "Access", an employee must prove that he has expert knowledge of TCP/IP networking, Unix operating systems, and PKI technology, concepts and applications.

To be assigned the role "Operations", an employee must prove that he has expert knowledge of PKI technology and applications that use PKI. Also, he must have strong people skills and a good understanding of PKI processes.

To be assigned the role "Audit", an employee must prove that he has expert knowledge of TCP/IP networking, Unix operating systems, PKI technology and applications using PKI, as well as a good understanding of PKI processes and strong people skills.

To be assigned the role "RAO", an employee must be trained to have a good understanding of security in general and the PKI processes relevant for this role.

All SwissSign employees must demonstrate understanding of security in general and expert knowledge of IT security in particular. SwissSign personnel shall be formally appointed to trusted roles by senior management members responsible for security.

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

5.3.2 Background check procedures

With regard to this CA, SwissSign AG verifies the background of its employees and ensures that employees do not have a criminal record.

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

5.3.3 Training requirements

Employees of SwissSign AG must provide evidence that they have obtained the skills required for their position. Shortcomings will be addressed and alleviated by appropriate training.

During the year, there will be at least one meeting with the Chief Security Officer, the Human Resource Officer, and staff. The meeting will be similar in structure to the one on the first working day. Topics to be covered are information-security issues and the roles of employees.

5.3.4 Retraining frequency and requirements

Retraining of employees is done as necessity arises, depending on the needs of the organization or the needs of the individual.

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

SwissSign AG reserves the right to prosecute unauthorized actions to the fullest extent of applicable Swiss law.

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

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

5.4.1 Types of events recorded

The following events are recorded in the CA log:

- new certificate requests
- rejected certificate requests
- account violations
- certificate signing

- certificate revocation
- user account logon
- CRL signing
- CA rollover
- certificate expiration
- certificate downloads/installation

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

5.4.2 Frequency of processing log

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

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

5.4.3 Retention period for audit log

The journal information in the "SwissSign Platinum CA" database is never deleted.

5.4.4 Protection of audit log

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

- Auditor
- RAO
- CAO
- CAM

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

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

5.4.8 Vulnerability assessments

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

5.5 Records archival

5.5.1 Types of records archived

The following records are archived:

- a daily backup of any information that this CA and its subordinated issuing CAs produce
- journal
- registration information of end entities

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

Protection of the archive is as follows:

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

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

The system time of all servers is synchronized with the time source of the SwissSign Time-Stamping Authority or another official time source.

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

5.5.6 Archive collection system (internal or external)

This CA and all its subordinated issuing CAs use a SwissSign-internal archiving system.

5.5.7 Procedures to obtain and verify archived information

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

5.6 Key changeover

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

To manage all operational processes, SwissSign has adopted the ITIL best practices model:

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

To manage a crisis or catastrophe, SwissSign has a Business Continuity Management plan. Once this plan goes into action, the Task Force Business Continuity (TFBC) assumes managerial duties of SwissSign until the crisis is dealt with and the TFBC is disbanded.

The TFBC has a charted course of action for the following events:

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

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

5.7.2 Computing resources, software and/or data are corrupted

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

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

5.7.3 Entity private key compromise procedures

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

- The CA certificate will be revoked.
- SwissSign AG will inform Swiss authorities of any trust-anchor compromise.
- All subscribers with certificates issued by either the revoked CA or one of its subordinated issuing CA will be informed by e-mail as soon as possible.
- All subscriber certificates will be revoked and new CRLs will be issued.
- The cause of the key compromise will be determined and the situation rectified.
- The revoked CA will generate a new key pair and the resulting certificate request will be signed by the superior CA.
- The new CA certificate will be published on the swisssign.com or the swisssign.net web site.
- New CRLs will be issued.

If the private key of a "SwissSign Time-Stamp Unit" is suspected to be compromised, executive management of SwissSign AG 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.
- A new key pair will be generated and the according certificate request will be signed by the SwissSign Platinum CA.
- The new certificate will be published on the swisssign.com or the swisssign.net web site.

5.7.4 Business continuity capabilities after a disaster

In case of a disaster, Executive Management and the Board of Directors of SwissSign AG will assess the situation and take all decisions necessary to establish a new, fully redundant server location for the SwissSign CA servers.

A new server location will be chosen based on its ability to support the security requirements of SwissSign with reference to the requirements as stipulated in this document. The off-site backups will be used to restore the CA, its data and its processes.

5.8 CA or RA termination

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

- SwissSign AG will report, without delay, any threat of bankruptcy to the Swiss SAS, the Swiss Recognition Body and any other governmental control agency or legal quality control organization.
- When the decision to discontinue certification services has been taken, SwissSign AG will inform, without delay, all its subscribers, relying parties and if applicable to other registration authorities and other CAs with which there are agreements or any other form of established relations. SwissSign AG endeavors to give at least 30 days advance notice before revoking any certificates.
  This explicitly includes the Swiss SAS, the Swiss Recognition Body and any other governmental control agency or legal quality control organization.
- SwissSign AG will immediately stop all registration services and if applicable will enforce this cessation of services for all other registration authorities.
- SwissSign AG will immediately cancel all current and valid contracts. The cancellation is to be effective after the entire business termination process has been concluded. SwissSign AG will also immediately revoke all rights of contracted parties to act on behalf of SwissSign AG.

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

- SwissSign AG will revoke all subscriber certificates. SwissSign AG will issue a CRL. SwissSign AG will revoke all root certificates.
- SwissSign AG will transfer obligations for maintaining registration information, certificate status information, and event log archives that cover the respective time to the appropriate organization.
- SwissSign AG will destroy all backup copies and escrow copies of the private signing keys of the SwissSign Platinum CA, such that the private keys cannot be retrieved, retained, or put back into use.
- All copies of documents which are required to be saved according to the stipulations of any applicable law will be stored under the conditions and for the duration as stipulated in this CP/CPS.

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

6 Technical Security Controls

This Chapter defines the technical security controls of the "SwissSign Platinum CA" (Root CA), all its subordinated issuing CAs and the SwissSign Platinum TSA Units. The Technical security controls of the subscriber keys are defined in the CP/CPS of the according issuing CA.

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for the "SwissSign Platinum CA" (Root CA Key) has been created in an off line SSCD that meets at least FIPS 140-1 level 3 requirements.

The key pairs for the subordinated issuing CAs of the SwissSign Platinum CA (Issuing CA Keys) have been generated in an off line SSCD that meets at least FIPS 140-1 level 3 requirements. Subsequently, the Issuing CA keys have been cloned into an on line SSCD meeting at least FIPS 140-1 level 4 requirements.

TSA key pairs are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

6.1.2 Private key delivery to subscriber

No subscriber certificates are issued from the "SwissSign Platinum CA".

6.1.3 Public key delivery to certificate issuer

No subscriber certificates are issued from the "SwissSign Platinum CA".

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 "SwissSign Platinum CA" uses a 4096 bit RSA key.

All issuing CAs use 2048 bit RSA key.

6.1.6 Public key parameters generation and quality checking

No subscriber certificates are issued from the "SwissSign Platinum CA".

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.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The controls regarding the subscriber keys are specified in the CP/CPS of the corresponding issuing CA.

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 SSCD used for CA keys is kept off line at all times and meets at least FIPS 140-1 level 3 requirements.

Issuing CA keys	The SSCD used for CA keys meets at least FIPS 140-1 level 3 requirements. These keys are on line and access is strictly controlled by using the '4-eye' principle.
TSA keys	The TSA keys are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

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 5' control, meaning that 3 of the 5 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	The TSA keys are generated and managed in the same SSCD as the issuing CA keys. The same rules apply.

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 generated and managed in the same SSCD as the issuing CA keys. The same rules apply.

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 SSCD so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 5 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 SwissSign AG.
Issuing CA keys	The Issuing CA keys have been put into backup SSCD, so that they can be recovered if a major catastrophe destroys the productive set of keys. The recovery requires that 3 out of 5 persons be present in order to gain physical and logical access.
TSA keys	The TSA keys are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

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 generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Root CA keys	The Root CA keys can be cloned from the master SSCD to other SSCDs. This is achieved in a cloning ceremony. To protect the private key during the transport, the destination SSCD provides the public key of a key pair it has generated. The master SSCD encrypts the key to be cloned with this public key. Only the destination SSCD is therefore able to successfully decrypt the key pair from the master SSCD.
Issuing CA keys	The Issuing CA keys are cloned in the same manner as Root keys.
TSA keys	The TSA keys are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

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 generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

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 generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

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 SSCD, by terminating the session with the SSCD, 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 generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

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 SSCD.
Issuing CA keys	The Issuing CA keys are destroyed by initializing the SSCD.
TSA keys	The TSA keys are generated and managed in the same SSCD as the Issuing CA keys. The same rules apply.

6.2.11 Cryptographic Module Rating

Minimum standards for cryptographic modules have been specified in chapter 6.2.1.

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 encrypted daily backup is copied onto a backup server and kept available on line for one year.

A weekly full dump is copied onto write-once media and stored in a bank deposit for archiving purposes. 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.
- The certificates of the subordinated issuing CAs of this CA are valid between 762 days (2 years + 1 month) to a maximum of 12 years. Key changeover is performed every year.
- The usage periods of subscriber certificates are specified in the CP/CPS of the according issuing CA.

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.

Regarding the subscriber keys, this chapter is specified in the according issuing CA.

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 SwissSign AG. 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.

Regarding the subscriber keys, this chapter is specified in the according issuing CA.

6.4.3 Other aspects of activation data

This Chapter is specified in the CP/CPS of the according issuing CA.

6.5 Computer security controls

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

6.5.1 Specific computer security technical requirements

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

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

6.5.2 Computer security rating

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

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

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

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

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

6.6.2 Security management controls

Continuous monitoring is used to ensure that systems and networks are operated in compliance with the specified security policy. All processes are logged and audited according to applicable law and normative requirements.

6.6.3 Life cycle security controls

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

6.7 Network security controls

Network security is based on a multi-level zoning concept using multiple redundant firewalls.

6.8 Time-stamping

SwissSign AG operates an internal time service using various sources from the Internet and a GPS receiver.

Based on this internal time service, SwissSign AG offers a time-stamping service that can be used to create a time-stamp for arbitrary documents. This service is implemented in accordance with Article 12 of the Swiss Digital Signature Law (ZertES).

SwissSign may charge a fee for this service. The keys used for the creation of time-stamping 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.

The Certificate profile for the "SwissSign Platinum CA" and the certificate Profile of the SwissSign Platinum TSA Units are described in this chapter. The Certificate profiles of the all subordinated issuing CAs of the "SwissSign Platinum CA" and the issued subscriber certificates are described in the CP/CPS of the according issuing CA.

7.1 Certificate profile

The subordinated issuing CAs of this CA issue X.509 Version 3 certificates in accordance with PKIX. The structure of such a certificate is:

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

7.1.1 Version number(s)

Version of X.509 certificates: version 3.

7.1.2 Certificate Extensions

7.1.2.1 Extensions of SwissSign Platinum CA Certificate

Extension Attribute	**Values**	**Comment**
Subject	/CN=SwissSign Platinum CA - G2 /O=SwissSign AG/C=CH	
Issuer Name	/CN=SwissSign Platinum CA - G2 /O=SwissSign AG/C=CH	
Key Usage	Certificate Sign, CRL Sign	Critical extension
Basic Constraints	CA:TRUE	Critical extension
Subject Key Identifier	<key identifier of this CA's public key>	See Chapter 7.1.3 Both key identifiers are the same (self signed certificate)
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	
CRL Distribution Points	http://swisssign.net/cgi-bin/authority/crl	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-R1.pdf	

7.1.2.2 Extensions of SwissSign Platinum TSA Units

Extension Attribute	Values	Comment
Subject	/CN=SwissSign Platinum TSA -Unit 1 /O=SwissSign AG /C=CH	Every Unit has a unique Common name. The Units are numbered: Unit 1, Unit 2 etc.
Issuer Name	/CN=SwissSign Platinum CA - G2 /O=SwissSign AG /C=CH	
Key Usage	DigitalSignature, NonRepudiation	Critical extension
Extended Key Usage	Time Stamping	Critical extension
Subject Key Identifier	<key identifier of this CA's public key>	See Chapter 7.1.3
Authority Key Identifier	keyid: <key identifier of the issuing CA's public key>	See Chapter 7.1.3
CRL Distribution Points	http://swisssign.net/cgi-bin/authority/crl	URLs of the CRL Distribution points (LDAP and/or HTTP)
Certificate Policies	Policy: 2.16.756.1.89.1.1.3.1 http://repository.swisssign.com/SwissSign-Platinum-TSA-R1.pdf	

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
rsaEncryption	1.2.840.113549.1.1.4

7.1.4 Name forms

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

7.1.5 Name constraints

Not implemented.

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 subordinated issuing CAs of this CA do not currently issue certificates with policy qualifiers.

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 3280

7.2.1 Version number(s)

The CRL version is v2.

7.2.2 CRL and CRL entry extensions

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

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

7.3 OCSP profile

The SwissSign OCSP functionality is built according to RFC 2560.

7.3.1 Version number(s)

The OCSP version is set to v1.

7.3.2 OCSP extensions

The OCSP extensions used are specified below:

- Nonce
- ServiceLocator

8 Compliance Audit and Other Assessments

Compliance Audits and other assessments defined in this chapter are exclusively applicable to the "SwissSign Platinum CA".

The CP/CPS of each subordinated issuing CA shall define compliance audits and other assessments for the relevant CA.

8.1 Frequency or circumstances of assessment

The compliance audit will be 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

KPMG is the auditor chosen by SAS and the audits (scope, reporting) will be fully ZertES-compliant.

8.3 Assessor's relationship to assessed entity

KPMG is an independent auditor and will conduct the compliance audits according to the stipulations of ZertES.

KPMG will conduct an initial assessment of SwissSign AG. Once SwissSign AG has achieved certification, KPMG will continue with annual assessments.

KPMG has the right to withdraw the certification of SwissSign AG if a compliance audit reveals a severe deficiency in the operation of SwissSign AG.

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

8.4 Topics covered by assessment

KPMG 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 KPMG.

8.5 Actions taken as a result of deficiency

SwissSign AG implements the ITIL best practices model and the results of a compliance audit are handled within this framework. Depending on severity and urgency, all issues will be entered into the ITIL system either as incidents or as problems and tracked accordingly.

Through the use of a supporting tool, SwissSign AG 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, SwissSign AG 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, SwissSign AG will publish a summarized result of the compliance audit on the SwissSign web site.

9 Other Business and Legal Matters

9.1 Fees

This chapter is specified in the CP/CPS of the according issuing CA.

9.2 Financial responsibility

9.2.1 Insurance coverage

SwissSign AG is a Swiss corporation 100% owned by Swiss Post (Die Schweizerische Post). As far as qualified certificates are concerned Swiss Post contractually guarantees to cover liability claims against SwissSign AG, limited to the minimum amounts stipulated in Art. 16 ZertES and Art. 2 VZertES.

This guarantee expires on the date an insurance according to Art. 2 para. 1 VZertES is concluded, to the extent permitted by applicable law.

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.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Any information or data SwissSign AG 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.

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 SwissSign AG 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).

9.3.3 Responsibility to protect confidential information

SwissSign AG is responsible to take all required measures to comply with the Swiss Data Protection Law.

9.4 Privacy of personal information

SwissSign AG fully complies with the Swiss Data Protection Law. Information and data can be used where needed for professional handling of the services provided herein. Subscribers and other third parties have to comply with the privacy standards of SwissSign AG.

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

SwissSign AG 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

SwissSign AG will release or disclose private information on judicial or other authoritative order.

9.4.7 Other information disclosure circumstances

SwissSign AG 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 SwissSign AG in accordance with applicable license provisions.

9.6 Representations and warranties

SwissSign AG warrants full compliance of the "SwissSign Platinum CA" with all the provisions stated in this CP/CPS. As far as qualified certificates are concerned SwissSign AG warrants full compliance with Swiss Digital Signature Law and related rules and regulations.

9.7 Disclaimers of warranties

Except for the warranties stated herein including related agreements for this CA and to the extent permitted by applicable law, SwissSign AG 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

This chapter is specified in the CP/CPS of the according issuing CA.

As far as qualified certificates are concerned SwissSign AG is liable for damages which are the result of SwissSign's failure to comply with Swiss Digital Signature Law (Article 16 ZertES). SwissSign AG must supply evidence that they have adhered to applicable laws, rules and regulations.

SwissSign AG 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 laws. SwissSign AG shall not be liable for any damages resulting from infringements by the Certificate Holder or the Relying Party on the applicable terms and conditions including the exceeding of the transaction limit.

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

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

SwissSign AG 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

SwissSign AG will implement changes with little or no impact for subscribers and relying parties to this Certificate Policy and Certification Practice Statement upon the approval of the executive board of SwissSign AG.

Changes with material impact will be first submitted to the Swiss Recognition 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 SwissSign AG executive board can decide to amend this CP/CPS without notification for amendments that are non-material (with little or no impact).

The SwissSign AG executive board, at its sole discretion, decides whether amendments have any impact on subscribers and/or relying parties.

All changes to the CP/CPS will be published according to chapter 2. of this CP/CPS.

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

In case of any dispute or controversy in connection with the performance, execution or interpretation of this agreement, the parties will endeavor to reach amicable settlement.

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 Certificate Policy & Certification Practice Statement and rights or obligations related hereto are in accordance with Swiss Digital Signature Law and other applicable regulations.

9.16 Miscellaneous provisions

The provisions of the CP/CPS of the respective issuing CA will apply.

9.17 Other provisions

9.17.1 Language

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