SwissSign Qualified Platinum CP/CPS

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

Document Type:	Certificate Policy and Certification Practice Statement
OID:	2.16.756.1.89.1.1.1.2.1
Author:	Michael Doujak, CEO
Classification:	C1 (public)
Applicability:	Global
Owner:	CEO
Issue Date:	July 19th, 2007
Version:	2.0.2
Obsoletes:	Version 2.0.1, Mai 7th, 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 Qualified Platinum CA operating under this CPS and issuing certificates under this CP is in connection with the SwissSign 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
27.02.2007	2.0.0	CP/CPS split	M. Raemy, M. Doujak, B. Öchslin
07.05.2007	2.0.1	Review, Minor Changes	Björn Kanebog
19.07.2007	2.0.2	Authorization for organizations without entry in commercial register	Melanie Raemy

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~~
19.07.2007	Michael Doujak	Melanie Raemy	2.0.2

Michael Doujak
Digitally signed by Michael Doujak
DN: cn=Michael Doujak, c=CH, o=SwissSign AG, email=michael.doujak@swisssign.com
Reason: I am approving this document
Date: 2007.07.20 16:25:49 +02'00'

digital signature

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: 2007.07.20 14:07:10 +02'00'

digital signature

Table of Contents

1 Introduction

The "SwissSign Qualified Platinum CA" is an issuing CA operating under the "SwissSign Platinum CA". The "SwissSign Platinum CA" is a root certification authority operating according to the stipulations of the Swiss Digital Signature Law. For the certificate policy and certification practice statement of the Root CA, the "SwissSign Platinum CP/CPS" is authoritative.

The "SwissSign Qualified Platinum CA" issues qualified certificates that meet the stipulations of 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)

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

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

1.1 Overview

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

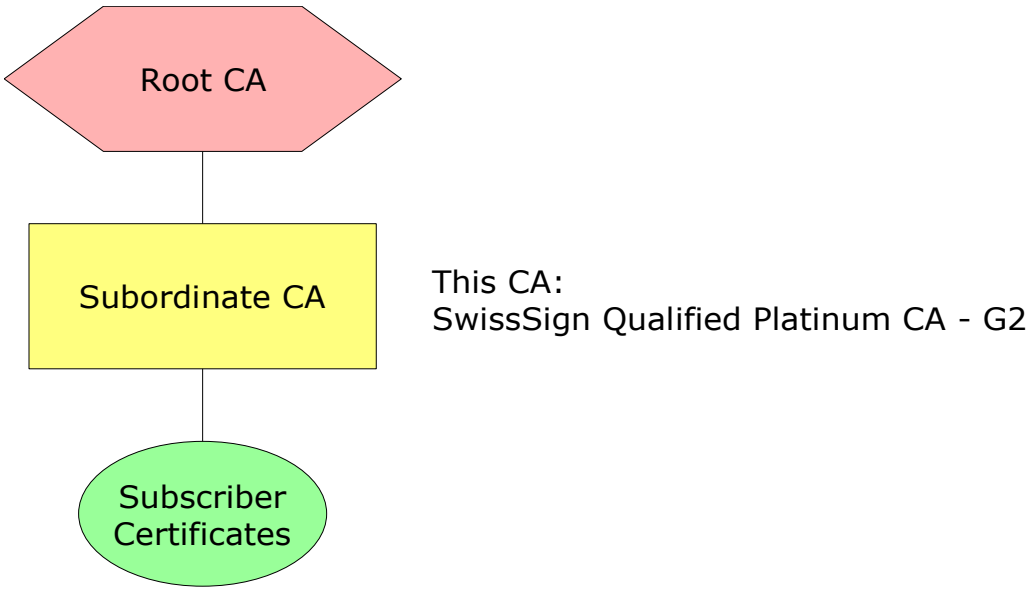

Illustration 1: Platinum CA Hierarchy

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

This Certificate Policy and Certification Practice Statement (CP/CPS) only applies to the SwissSign Qualified Platinum Certificates. The "SwissSign Qualified Platinum CA" is an issuing CA, which is signed by the SwissSign Platinum CA (Root CA).

The usage of Qualified Platinum Certificates is defined in chapter 1.4.1 of this CP/CPS. SwissSign AG provides a detailed product overview on their website (swisssign.net) for Platinum Certificates and for other services.

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.

1.2 Document name and identification

This document is named "SwissSign Qualified Platinum 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 2.16.756.1.89.1.1.1.2.1

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 not shown in the certificate (see chapter 7).

1.3 PKI participants

1.3.1 Certification authorities

The "SwissSign Qualified Platinum CA" is the only CA operated by SwissSign AG that issues certificates under this CP/CPS.

1.3.2 Registration authorities

SwissSign AG operates a registration authority, called SwissSign RA that registers subscribers of certificates issued by the "SwissSign Qualified Platinum CA".

Third parties may operate their own registration authority services, if these third parties abide by all the rules and regulations of this CP/CPS, Swiss digital signature law and the stipulations of standards (see chapter 1).

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

- The RA must have a contractual agreement with SwissSign AG which indicates the authorization for their role as RA and clearly details the minimum requirements, processes and liabilities.
- The registration process must meet the stipulations of Swiss Digital Signature Law. It must be documented, published, and distributed to all parties involved in the RA process.
- The RA must be certified according to Swiss Digital Signature Law and must pass an annual audit. All costs related to this audit are to be paid by the operator of this RA. Failure to pass the annual audit may lead to the revocation of RA privileges.

1.3.3 Subscribers

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

- Requesters are individuals that have requested (but not yet obtained) a certificate.
- Subscribers are individuals 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 and personally signed registration form;
- supplementing such information with a proof of identity and the provision of the information as specified in chapter 3.1 and 3.2;
- generating a new, secure, and cryptographically sound key pair on a SwissSign-approved crypto device while physically present at the RA location;
- reading and agreeing to all terms and conditions of this CP/CPS, other relevant regulations and agreements;
- the maintenance of their certificates using the tools provided by the RA;
- deciding on creation of a certificate whether the respective certificate is to be published in the public directory: directory.swisssign.net;
- using SwissSign certificates exclusively for legal and authorized intended purposes;
- ensuring that SwissSign certificates are exclusively used on behalf of the person specified as the subject of the certificate;
- defining a transaction limit according to the rules stipulated in the registration forms; on calculating the transaction limit, the subscriber must consider all possible monetary consequences, such as, but not limited to, any kinds of damages and other obligations which can result from using the qualified certificate;
- protecting the private key from unauthorized access;
- using the private key only in secure computing environments that have been provided by trustworthy sources and that are protected by state-of-the-art security measures;
- ensuring complete control over the private key by not sharing private keys and passwords and not using easily guessable passwords;
- ensuring complete control over the Secure Signature Creation Device and activation data by not entrusting any other person with the safekeeping of this device and data;
- notifying the registration authority of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate;
- invalidating 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;
- 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.

1.3.4 Relying parties

Relying parties are individuals or organizations that use these certificates to validate the signatures and verify the identity of subscribers and/or to secure communication with this subscriber. 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 their sole responsibility to verify legal validity, transaction limits and applicable policies.

The Relying Party agrees to observe the following conditions:

- Platinum Certificates may only be used in accordance with the rules stipulated in the "SwissSign Platinum Certificate Policy and Certification Practice Statement".
- The Relying Party is obliged to have an appropriate understanding of the proper use of public key cryptography as well as an understanding of the associated risks.
- SwissSign Certificates may be used exclusively in accordance with applicable laws, rules, and regulations and only for authorized intended purposes.
- It is the sole responsibility of the Relying Party to always use the certificate with due diligence and reasonable judgment.
- It is in the sole responsibility of the Relying Party to verify revocation status, legal validity, transaction limits and applicable policies.
- The revocation status can be checked via OCSP or via CRL (Certificate Revocation List). The Relying Party must be aware, that the CRLs are valid 10 days, but updated each day. Therefore the Relying Party shall always check the newest available CRL to have the complete, up to date revocation information.
- Should the situation arise that for technical reasons an updated CRL is not available, it is the relying party's responsibility to decide how long a CRL is to be trusted for revocation checking. This decision may depend on the type of transaction being authorized and the damage potential. Under no circumstances should the trust be extended beyond the maximum life time of the CRL.

Relying parties can also be subscribers within this CA.

1.3.5 Other participants

Other participants are individuals or organizations that rely on the certificate of a subscriber, or are in some way involved with certificate manufacturing and may or may not wish to verify the identity of subscribers and/or to secure communication with this subscriber.

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

Switzerland:	On January 1, 2005, Swiss Digital Signature Law (ZertES) was officially put into force.
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.

Other participants can be also subscribers within this CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The use of certificates issued by the "SwissSign Qualified Platinum CA" is limited to digital signing in accordance with Swiss Digital Signature Law, in particular ZertES and Article 14 para. 2bis OR (Swiss Code of Obligations) .

The following certificates are issued under this CP/CPS:

- [QC] A qualified certificate is issued by the "SwissSign Qualified Platinum CA" with nonRepudiation key usage bit set. See also chapter 6.1.7. The corresponding private key is required to have been created on an SSCD and may only exist once. The QC can only be used for digital signing in accordance with Swiss Digital Signature Law, in particular ZertES and Article 14 para. 2bis OR (Swiss Code of Obligations).

1.4.2 Prohibited certificate uses

Any other use than defined in chapter 1.4.1 is prohibited by Swiss Digital Signature Law.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact persons

The following persons are the main contacts for any questions or suggestions regarding the SwissSign Qualified 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 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 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 this CP/CPS and its related documentation 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.

Term	Abbrev.	Explanation
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.
Digital signature		A system allowing people 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 SwissSign and the customer.

Term	Abbrev.	Explanation
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.
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 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 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.

Term	Abbrev.	Explanation
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.
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.

Term	Abbrev.	Explanation
Subject	DN	Field in the certificate that identifies the owner of the certificate. Also referred to as distinguished name (DN). Examples: /CN=John Doe /Email=jd@signdemo.com /CN=pseudo: Marketing /O=SwissSign AG /C=CH /Email=marketing@signdemo.com /CN=John Doe /O=SwissSign AG /OU=DEMO/C=CH /Email=john.doe@signdemo.com /CN=swiss.signdemo.com /O=SwissSign AG /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 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 require emphasis or disclosure to subscribers and relying parties, for example, to meet regulatory requirements.
TSA practice statement	TPS	Statement of the practices that a TSA employs in issuing time-stamp tokens.
TSA system		Composition of IT products and components organized to support the provision of time-stamping services.
Transaction Limit		The transaction limit is detailing liability limits of 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.

Term	Abbrev.	Explanation
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 any of its CAs 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 (request, renew, revoke, download...). 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 certification practice statement (CP/CPS)
- the end-user agreement (EUA) for subscribers
- the end-user agreement (EUA) for relying parties
- pricing information

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

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

SwissSign will publish this information on a regular schedule:

- CRLs for the "SwissSign Qualified Platinum CA" 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.

2.4 Access controls on repositories

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) in a certificate issued by the "SwissSign Qualified Platinum CA" complies with the X.500 standard.

For the distinguished name, a minimum of two fields are required. These fields must be /CN= and /Email= where /Email='Mail address'.

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

Real names are specified as /CN='First Name' optional 'Middle Names' 'Last Name'.

Pseudonyms are specified as /CN=pseudo: 'arbitrary string'.

- First, Middle and Last Name in the CN have to be absolutely identical to the names as they appear in the identifying documentation provided. Special characters are treated according to chapter 3.1.4. Abbreviations or nicknames are prohibited. Names consisting of multiple words are permissible.
- A real name and its identifying information must be authorized according to chapter 3.2.3.
- The use of a pseudonym in the CN requires the name to start with the fixed string 'pseudo: '.
- A pseudonym requires that the requester authorize the request containing identifying information according to chapter 3.2.3.

SubjectAltName is a mandatory field for certificates issued to individuals and contains an exact copy of the email field of the subject.

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 RA has proper evidence of the existent association between these names or pseudonyms and the entities to which they belong. To achieve this goal, 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

Subscribers can be anonymous or pseudonymous. For the latter option, subscribers have to begin the "/CN= entry" with the fixed string 'pseudo: '. A subscriber can use any string of characters after the fixed string 'pseudo: '. SwissSign or 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 is not obliged to verify lawful use of such names. SwissSign AG reserves 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.

3.1.4 Rules for interpreting various name forms

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 can 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 may receive special treatment: ä, ö, ü are represented by either ae, oe, ue or a, o , u.

3.1.5 Uniqueness of names

The content of the subject field of valid certificates must be unique, regardless of which of the CAs operating under this CP/CPS issues the certificate. Certificates can have non-unique subjects if there is disjunctive key usage.

See also chapter "1.4.1, Appropriate certificate uses".

3.1.6 Recognition, authentication, and role of trademarks

SwissSign 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. SwissSign AG is not obliged to verify lawful use of names. It is the sole responsibility of the subscriber to ensure lawful use of chosen names.

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

3.2 Initial identity validation

The initial identity validation is part of the Certificate Application process as described in chapter 4.1.

3.2.1 Method to prove possession of private key

The SwissSign RA verifies possession of the private key for certificates issued by this CA by requiring the RA Operator to witness the requester generate the key pair on a SwissSign-approved crypto device.

3.2.2 Authentication of organization identity

Platinum qualified certificates can only be issued to individuals in accordance with Swiss Digital Signature Law. Individuals may use an organization's name with sufficient authorization by the organization.

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 of the organization, the requester must provide official documentation about the organization. Organizations with an entry in the federal commercial register must supply an excerpt, no older than 3 months. All other organizations must supply either the certificate of registration with the ESTV or a current VAT invoice.

- The use of the organization's name and the requested transaction limit must be authorized by one or more legal representatives of the organization, and handwritten personal signatures must be included on the registration form.
- The legal representative must provide proof of identity according to chapter 3.2.3.
- The legal representative must provide proof of authorization according to chapter 3.2.5.

An organization may contractually define that all certificates using the name of the organization in the /O= field may only contain e-mail addresses in the /email= field that are in the domain of the organization. Should such a contract exist, the organization takes full responsibility for the proper management of e-mail accounts. Therefore, the requirement to verify individual e-mail addresses during the registration process is optional.

3.2.3 Authentication of individual identity

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 Swiss Digital Signature Law (ZertES). The regulations defined in the registration forms may be summarized as follows:

- The registration form must carry original, personal handwritten signatures.
- The information on the identifying document must match both the name and signature on the registration form.
- 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 person to be identified must be physically present during the registration at the authenticating RA.
- The individual must present a valid original of a legal, valid photo ID. The RA is to make a high-quality copy or scan of the documentation.

- The photo in the identifying document is compared to the person physically present (facial features, age, gender and size).
- The /email= field must be verified during the registration process. The requester must prove that he has access to the mailbox and that he can use it to receive mail.

3.2.4 Non-verified subscriber information

All subscriber information required by Swiss Digital Signature Law has to be 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 top level 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, which are listed in the excerpt of the Federal 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

The SwissSign RA does not allow re-keying of certificates issued by the “SwissSign Qualified Platinum CA”.

3.3.2 Identification and authentication for re-key after revocation

The SwissSign RA does not allow re-keying of certificates issued by the “SwissSign Qualified Platinum CA”.

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 RA web site.
- With a personal signature on a revocation form.
- Personal appearance at the SwissSign RA.

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

4 Certificate Life-Cycle Operational Requirements

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.

4.1.2 Enrollment process and responsibilities

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

- Valid identification documentation is provided and complete registration forms have been signed, and the CP/CPS and End-User Agreement have been accepted by the subscriber,
- all documents and informations are approved by the SwissSign RA,
- private keys are securely generated and the SwissSign RA provides an SSCD that meets the security requirements as stipulated in Swiss Digital Signature Law.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The SwissSign RA identifies the requester on the basis of the identifying documents that the requester presents, as stipulated in chapter 3.2 of this document. The requester must present all documentation in person.

4.2.2 Approval or rejection of certificate applications

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

- the requester has presented the identifying documentation in person,
- 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.

If the requester fails to adhere to any of the above, or in any other way violates the stipulations of this document, the SwissSign RA must reject the certificate signing request. SwissSign reserves the right to decline certificate requests without giving reasons.

4.2.3 Time to process certificate applications

The SwissSign registration process specifies that verification of identity and processing of the application be carried out during a personal visit of the requester.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

- the integrity of the request;
- the authenticity and authority of the RA operator;
- verify the contents of the certificate requests for compliance with the technical specification as outlined in chapter 7.1.2.

On successful verification, the SwissSign CA will then issue the requested certificate.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA may notify the requester in different ways:

- If the certificate is presented to the subscriber immediately, special notification may not be necessary.
- The CA may:
  - email the certificate to the subscriber
  - email 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

The subscriber will receive all certificates during the personal visit with the SwissSign RA. No further confirmation of certificate acceptance 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 in the course of the registration process whether or not the certificate will be published.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA will not notify the SwissSign RA of the certificate issuance, since the certificate was issued immediately after authorization by the SwissSign RA operator.

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 issued by the "SwissSign Qualified Platinum CA" may be used only for qualified electronic signatures in accordance with ZertES. Use for other purposes is not permissible.
- Subscribers may use SwissSign certificates exclusively for intended, legal, and authorized purposes;
- Subscribers may only use a SwissSign certificate on behalf of the person listed as the subject of such a certificate.

4.5.2 Relying party public key and certificate usage

Relying parties shall:

- be held responsible for the understanding of:
  - the proper use of public key cryptography and certificates
  - the related risks;
- read and agree to all terms and conditions of this CP/CPS and the End-User Agreement for relying parties;
- verify certificates issued by this CA, including use of CRLs, in accordance with the certification path validation procedure, taking into account any critical certificate extensions;
- use their best judgment when relying on a certificate issued by this CA and assess if such reliance is reasonable under the circumstances:
  - determine whether such reliance is reasonable given the extent of the security and trust provided by a certificate issued by this CA;
- verify the transaction limit provided in the aforementioned certificate;

- comply with all laws and regulations applicable to a relying party's right to export, import, and/or use a certificate issued by this CA and/or related information. Relying parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of a certificate issued by this CA and/or related information.

4.6 Certificate renewal

Certificate renewal is 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 is not supported by the SwissSign RA. SwissSign RA limits the validity period of certificates to ensure that keys are used only during a stipulated period of time.

SwissSign will also not allow other Registration Authorities to implement a process for certificate renewal.

4.6.1 Circumstance for certificate renewal

As indicated in chapter 4.6 SwissSign does not support renewal.

4.6.2 Who may request renewal

As indicated in chapter 4.6 SwissSign does not support renewal.

4.6.3 Processing certificate renewal requests

As indicated in chapter 4.6 SwissSign does not support renewal.

4.6.4 Notification of new certificate issuance to subscriber

As indicated in chapter 4.6 SwissSign does not support renewal.

4.6.5 Conduct constituting acceptance of a renewal certificate

As indicated in chapter 4.6 SwissSign does not support renewal.

4.6.6 Publication of the renewal certificate by the CA

As indicated in chapter 4.6 SwissSign does not support renewal.

4.6.7 Notification of certificate issuance by the CA to other entities

As indicated in chapter 4.6 SwissSign does not support renewal.

4.7 Certificate re-key

Certificate re-keying is a process where a subscriber automatically obtains a new certificate if proof of key possession of the old certificate can be provided. The resulting certificate contains new validity information, a new key pair but retains the same subject.

The SwissSign RA does not allow re-keying for Qualified Platinum Certificates.

4.7.1 Circumstance for certificate re-key

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.7.2 Who may request certification of a new public key

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.7.3 Processing certificate re-keying requests

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.7.4 Notification of new certificate issuance to subscriber

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.7.6 Publication of the re-keyed certificate by the CA

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.7.7 Notification of certificate issuance by the CA to other entities

As indicated in chapter 4.7, the SwissSign RA does not allow re-keying of certificates issued by the "SwissSign Qualified Platinum CA".

4.8 Certificate modification

Certificate modification is the process through which a subscriber requests a certificate with modified subject information. The SwissSign RA treats these requests as initial registration requests. The requester is therefore required to start a new certificate request.

SwissSign will also not allow other registration authorities to implement a process for certificate modification.

4.8.1 Circumstance for certificate modification

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.8.2 Who may request certificate modification

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.8.3 Processing certificate modification requests

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.8.4 Notification of new certificate issuance to subscriber

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.8.5 Conduct constituting acceptance of modified certificate

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.8.6 Publication of the modified certificate by the CA

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.8.7 Notification of certificate issuance by the CA to other entities

As indicated in chapter 4.8 SwissSign does not support certificate modification.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Subscribers may revoke their certificates at will.

The SwissSign RA will revoke a subscriber's certificate if one of the following conditions is met:

- The private key of the issuing CA or any of its superior CAs has been compromised.
- The subscriber's private key store (= cryptographic token) is lost.
- Any part of the certificate subject has changed.
- The certificate /O= field is no longer valid.
- The certificate issued does not comply with the terms and conditions of this CP/CPS. A SwissSign private key in the trust chain of the customer's certificate has been compromised,
- The subscriber does not comply with the agreed conditions and/or other applicable laws, rules and regulations. In addition, SwissSign AG may investigate any such incidents and take legal action if required.

4.9.2 Who can request revocation

This CA accept certificate revocation requests from the following:

- 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 ID management functions in the profile that issued the initial registration request.
- The owner of the private key can use an SSL session with strong authentication to revoke this certificate on line.
- By using the pre-filled revocation form, handed out at the end of the registration process, the subscriber can issue an off line revocation request in writing. Such a request, in order to be authorized, must carry the personal signature of the original requester of the certificate, proof of identity (as described in chapter 3.2.3) and must be sent through registered mail.
- 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.

Off line revocation methods are typically several days slower than on line revocations. The subscriber must take full responsibility for any and all delays that result from the chosen revocation method.

4.9.4 Revocation request grace period

After the formal requirements as detailed in chapters 4.9.1 and 4.9.2 have been fulfilled, SwissSign RA will process revocation requests as soon as practicable and without unnecessary delay.

4.9.5 Time within which CA must process the revocation request

The time within which the CA must process the revocation request is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

Should the on line revocation method be unavailable, the subscriber must use the off line method. SwissSign RA guarantees processing of off line revocation requests within due time 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 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 (if applicable)

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

4.9.8 Maximum latency for CRLs (if applicable)

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

4.9.9 On-line revocation/status checking availability

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

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 3280 and/or RFC 2560 or OCSP.

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

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

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

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

4.9.13 Circumstances for suspension

According to Swiss Digital Signature Law, certificates may not be suspended.

4.9.14 Who can request suspension

According to Swiss Digital Signature Law, certificates may not be suspended.

4.9.15 Procedure for suspension request

According to Swiss Digital Signature Law, certificates may not be suspended.

4.9.16 Limits on suspension period

According to Swiss Digital Signature Law, certificates may not be suspended.

4.10 Certificate status services

4.10.1 Operational characteristics

The SwissSign certificate status services are CRL and OCSP. Access to these services is through the web site "swisssign.net" and the on line directory "directory.swisssign.net". 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. Service interruptions for maintenance will be announced on the swisssign.com web site at least one week in advance.

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 certificate of a subscriber.

For reasons of legal compliance, the SwissSign CA and SwissSign RA 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

Swiss Digital Signature law does not allow key escrow for qualified certificates.

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

All stipulations of chapter 5 of the "SwissSign Platinum CP/CPS" are applicable for this CA.

6 Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Subscriber key pairs for qualified and signing certificates are generated on SwissSign-approved crypto devices (ex. Smart Card, USB Token). SwissSign approved crypto-devices are listed on http://swisssign.com.

6.1.2 Private key delivery to subscriber

Private keys generated on a SwissSign-approved secure crypto device do not need to be delivered.

The delivery of the private key for the encryption certificate depends on how the key pair is generated. SwissSign recommends the generation of the key pair on the SwissSign web site and offers delivery of the private key through a passphrase-protected download mechanism.

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.

If keys are generated on line, no public key delivery method is required.

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

All subscribers use 2048 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

Parameters can be selected by requesters, but are verified by the RA and the CA.

For keys generated on line, all SwissSign CAs use standard parameters.

No stipulations can be made for browser-generated key pairs or for key pairs imported from external sources.

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

Subscribers can obtain certificates issued by this CA with the following key usage bit included:

- nonRepudiation (qualified certificate)

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:

Subscriber keys	Subscriber keys for certificates issued by the "SwissSign Qualified Platinum CA" must be generated and stored on an SSCD that meets EAL 4+ certification in accordance with Swiss Digital Signature Law.

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

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

Subscriber keys	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:

Subscriber keys	Private key escrow is not offered by the SwissSign RA.

6.2.4 Private key backup

The following list shows how private key backup is implemented:

Subscriber keys	All keys are generated on the SSCD and cannot be put into backup.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

Subscriber keys	All keys are generated on the SSCD and cannot be extracted.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

Subscriber keys	Subscriber keys that have been generated on the SSCD cannot be cloned.

6.2.7 Private key storage on cryptographic module

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

Subscriber keys	Subscriber keys are stored on cryptographic modules so that they can be used only if properly activated.

6.2.8 Method of activating private key

The following list shows how private keys are activated:

Subscriber keys	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.

6.2.9 Method of deactivating private key

The following list shows how private keys are deactivated:

Subscriber keys	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.

6.2.10 Method of destroying private key

The following list shows how private keys are destroyed:

Subscriber keys	Subscriber keys can only be destroyed by destroying the SSCD.

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

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

6.3.2 Certificate operational periods and key pair usage periods

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

- Subscriber certificates are valid between 365 and 397 days (1 year to 1 year + 1 month)

6.4 Activation data

6.4.1 Activation data generation and installation

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
- have alphabetic and numerical characters
- not contain many occurrences of the same character
- not contain a long substring of the user's name or other guessable words

6.4.2 Activation data protection

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

6.4.3 Other aspects of activation data

SwissSign-approved crypto devices and their product specifications are listed on http://swisssign.com.

6.5 Computer security controls

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

6.6 Life cycle technical controls

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

6.7 Network security controls

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

6.8 Time-stamping

This Chapter is specified in the CP/CPS of the Root CA "SwissSign Platinum CP/CPS".

7 Certificate, CRL and OCSP Profiles

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

7.1 Certificate profile

This CA issues 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 Qualified Platinum CA Certificate

Extension Attribute	**Values**	**Comment**
Subject	/CN=SwissSign Qualified Platinum CA – G2 /O=SwissSign AG /C=CH	
Issuer Name	/CN=SwissSign Platinum CA - G2 /O=SwissSign AG /C=CH	
Issuer Alternative Name	DirName:/C=CH/O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA	
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
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: 2.16.756.1.89.1.1.1.2.1 CPS: http://repository.swisssign.com/SwissSign-Qualified-Platinum-CP-CPS-R1.pdf	

Extension Attribute	Values	Comment
	User Notice: Explicit Text: This is a certification authority that issues qualified certificates according to Swiss Digital Signature Law.	
qcStatements	OID: 0.4.0.1862.1.1 (QcCompliance)	This certificate is issued as a qualified certificate

7.1.2.2 Extensions of SwissSign Qualified Platinum Subscriber Certificate

Extension Attribute	Values	Comment
Subject	Data of Subscriber	See Definitions in Chapter 1.6
Issuer Name	/CN=SwissSign Qualified Platinum CA – G2 /O=SwissSign AG/C=CH	
Issuer Alternative Name	DirName:/C=CH/O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA	
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: 2.16.756.1.89.1.1.1.2.1 CPS: http://repository.swisssign.com/SwissSign-Qualified-Platinum-CP-CPS-R1.pdf User Notice: Explicit Text: This is a qualified certificate according to Swiss Digital Signature Law.	
Authority Information Access		URI to OCSP responder and optional URI to CA issuer certificate
qcStatements	OID: 0.4.0.1862.1.1 (QcCompliance)	This certificate is issued as a qualified certificate
	OID: 0.4.0.1862.1.2 (QcLimitValue)	Transaction limit in CHF ("user defined")
	OID: 0.4.0.1862.1.4 (QcSSCD)	Claim that the private key related to the certified public key resides in a Secure Signature Creation Device (SSCD)
Subject Alternative Name		Alternative name of the subscriber: email address
Key Usage	Non Repudiation	Critical extension

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA 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 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

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 issues 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

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

- The SwissSign Qualified Platinum CA
- The SwissSign RA

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 for the SwissSign Qualified Platinum CSP.

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, 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

SwissSign AG provides a price list for certification and registration services on the website swisssign.com.

9.1.1 Certificate issuance or renewal fees

SwissSign AG 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

SwissSign AG 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

SwissSign AG 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

SwissSign AG may establish a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

SwissSign AG is a Swiss corporation 100% owned by Swiss Post (Die Schweizerische Post). Concerning the certificates issued under this CP/CPS 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, according to Swiss Digital Signature Law.

Upon request, SwissSign AG 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 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

9.6.1 CA representations and warranties

SwissSign AG warrants full compliance with all provisions stated in this CP/CPS, Swiss Digital Signature Law, and related regulations and rules.

9.6.2 RA representations and warranties

SwissSign RA warrants full compliance with all provisions stated in this CP/CPS, related agreements and documents, Swiss Digital Signature Law, 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 and documentation, 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, 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

9.8.1 Liability of SwissSign AG

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

SwissSign AG shall not in any event be liable for damages that result from force majeur events as detailed in chapter 9.16.5. 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.

9.8.2 Liability of the Certificate Holder

The Certificate Holder is liable to SwissSign AG and 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 Certificate Holder and Relying Parties are fully liable for any damages resulting from the exceeding of the transaction limit specified in the certificate (Article 7 para. 2 ZertES and Article 16 para. 3 ZertES). The Certificate Holder is also liable according to Article 59a OR (Swiss Code of Obligations).

All certificates issued by this CA contain a statement declaring the maximum value of a transaction signed with this certificate, according to the stipulations of applicable laws.

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 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

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

9.16.1 Entire agreement

This CP/CPS, the SwissSign Platinum CP/CPS and the End-User-Agreement of SwissSign AG state the agreement between SwissSign AG and the Certificate Holder.

9.16.2 Assignment

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

SwissSign AG can fully or partially assign this agreement and/or its rights or obligations hereunder.

9.16.3 Severability

Invalidity or 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 Majeur

SwissSign AG shall not be in default and the customer cannot hold SwissSign AG 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.

SwissSign AG shall take commercially reasonable measures to mitigate the effects of force majeur in due time.

9.17 Other provisions

9.17.1 Language

If legal documents like this CP/CPS, the End-User-Agreement of SwissSign AG, or registration forms are provided in additional languages to English, the English version of these documents will prevail.