SwissSign Silver CP/CPS

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

Document Type: Certificate Policy and Certification Practice Statement
OID: 2.16.756.1.89.1.3.1.7
Author: Michael Doujak / Cornelia Enke
Classification: C1 (public)
Applicability: Global
Owner: CEO
Issue Date: October 16th, 2017
Version: 3.4.3
Obsoletes: Version 3.4.2, September 15th, 2017
Storage: SwissSign Document Repository
Distribution: Global
Status: Released
Review: This document is reviewed periodically at least once per calendar year.
The owner is responsible for this review.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Comment</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.03.2004</td>
<td>0.0.0</td>
<td>Pre-certification version</td>
<td>Joseph A. Doekbrijder</td>
</tr>
<tr>
<td>25.07.2006</td>
<td>2.0.0</td>
<td>Revision</td>
<td>Melanie Raemy</td>
</tr>
<tr>
<td>16.08.2006</td>
<td>2.0.1</td>
<td>Review</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>19.10.2006</td>
<td>2.0.2</td>
<td>Review, Minor changes</td>
<td>Björn Kanebog</td>
</tr>
<tr>
<td>18.12.2006</td>
<td>2.0.3</td>
<td>Revision</td>
<td>Melanie Raemy</td>
</tr>
<tr>
<td>21.12.2006</td>
<td>3.0.0</td>
<td>Insert SWITCH CA</td>
<td>Melanie Raemy</td>
</tr>
<tr>
<td>14.05.2007</td>
<td>3.0.1</td>
<td>Review, Minor changes</td>
<td>Björn Kanebog</td>
</tr>
<tr>
<td>27.06.2007</td>
<td>3.0.2</td>
<td>Extensions: domain validation</td>
<td>Melanie Raemy</td>
</tr>
<tr>
<td>15.04.2008</td>
<td>3.1.0</td>
<td>New layout; Review; added changes about life cycle management</td>
<td>Björn Kanebog</td>
</tr>
<tr>
<td>17.04.2008</td>
<td>3.1.1</td>
<td>Review</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>19.11.2008</td>
<td>3.1.2</td>
<td>Update for flexible pseudonym identifiers.</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>02.11.2009</td>
<td>3.1.3</td>
<td>Allow domain validation, 7*24 availability,</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>19.07.2010</td>
<td>3.2.0</td>
<td>Added G3 CA certificates</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>27.06.2011</td>
<td>3.2.1</td>
<td>Allow Nicknames, E-mail validated only, OCSP Responder</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>26.03.2012</td>
<td>3.2.2</td>
<td>prohibit MITM and traffic management</td>
<td>Michael Doujak</td>
</tr>
<tr>
<td>26.06.2012</td>
<td>2.3.3</td>
<td>Adjustments to the CA/Browser Forum Baseline Requirements</td>
<td>Christoph Stalder</td>
</tr>
<tr>
<td>30.09.2014</td>
<td>2.4.0</td>
<td>Added G22 Issuing CA Certificates</td>
<td>Cornelia Enke</td>
</tr>
<tr>
<td>13.10.2014</td>
<td>2.4.1</td>
<td>Deleted SWITCH CA</td>
<td>Cornelia Enke</td>
</tr>
<tr>
<td>13.09.2017</td>
<td>2.4.2</td>
<td>Implement CAA</td>
<td>Cornelia Enke</td>
</tr>
<tr>
<td>06.10.2017</td>
<td>2.4.2.1</td>
<td>adjust layout</td>
<td>Cornelia Enke</td>
</tr>
<tr>
<td>16.10.2017</td>
<td>2.4.3</td>
<td>adjust after auditor review</td>
<td>Cornelia Enke</td>
</tr>
</tbody>
</table>
# Authorization

<table>
<thead>
<tr>
<th>Date</th>
<th>Approved by</th>
<th>Approved by</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>21.12.2006</td>
<td>Michael Doujak</td>
<td>Melanie Raemy</td>
<td>2.0.0 / OID=1</td>
</tr>
<tr>
<td>26.07.2007</td>
<td>Michael Doujak</td>
<td>Melanie Raemy</td>
<td>3.0.2 / OID=2</td>
</tr>
<tr>
<td>28.04.2008</td>
<td>Adrian Humbel</td>
<td>Björn Kanebog</td>
<td>3.1.1 / OID=3</td>
</tr>
<tr>
<td>19.11.2008</td>
<td>Freddy Kaiser</td>
<td>Michael Doujak</td>
<td>3.1.2 / OID=3</td>
</tr>
<tr>
<td>02.11.2009</td>
<td>Adrian Humbel</td>
<td>Michael Doujak</td>
<td>3.1.4 / OID=4</td>
</tr>
<tr>
<td>29.07.2010</td>
<td>Adrian Humbel</td>
<td>Michael Doujak</td>
<td>3.2.0 / OID=5</td>
</tr>
<tr>
<td>29.06.2011</td>
<td>Adrian Humbel</td>
<td>Michael Doujak</td>
<td>3.2.1 / OID=5</td>
</tr>
<tr>
<td>20.04.2012</td>
<td>Uwe Fischer</td>
<td>Reinhard Dietrich</td>
<td>3.2.2 / OID=5</td>
</tr>
<tr>
<td>28.06.2012</td>
<td>Uwe Fischer</td>
<td>Reinhard Dietrich</td>
<td>2.3.3 / OID=5</td>
</tr>
<tr>
<td>30.09.2014</td>
<td>Uwe Fischer</td>
<td>Reinhard Dietrich</td>
<td>2.4.0 / OID=6</td>
</tr>
<tr>
<td>13.10.2014</td>
<td>Uwe Fischer</td>
<td>Reinhard Dietrich</td>
<td>2.4.1 / OID=6</td>
</tr>
<tr>
<td>15.09.2017</td>
<td>Reinhard Dietrich</td>
<td>Markus Naef</td>
<td>2.4.2 / OID=7</td>
</tr>
<tr>
<td>16.10.2017</td>
<td>Reinhard Dietrich</td>
<td>Markus Naef</td>
<td>2.4.3 / OID=8</td>
</tr>
</tbody>
</table>

© SwissSign AG, 16.10.2017
# Table of Contents

1. **Introduction** ................................................................. 6
   1.1 Overview ........................................................................... 7
   1.2 Document name and identification .................................. 8
   1.3 PKI participants .............................................................. 8
   1.4 Certificate usage ........................................................... 10
   1.5 Policy administration ...................................................... 11
   1.6 Definitions and acronyms ............................................... 11

2. **Publication and Repository Responsibilities** ..................... 18
   2.1 Repositories ...................................................................... 18
   2.2 Time or frequency of publication .................................... 18
   2.4 Access controls on repositories ....................................... 19

3. **Identification and Authentication** .................................... 20
   3.1 Naming ............................................................................. 20
   3.2 Initial identity validation .................................................. 22
   3.3 Identification and authentication for re-key requests .......... 23
   3.4 Identification and authentication for revocation request ...... 24

4. **Certificate Life-Cycle Operational Requirements** ............... 25
   4.1 Certificate application .................................................... 25
   4.2 Certificate application processing ................................... 25
   4.3 Certificate issuance ......................................................... 26
   4.4 Certificate acceptance ..................................................... 26
   4.5 Key pair and certificate usage ........................................ 26
   4.6 Certificate renewal .......................................................... 27
   4.7 Certificate re-key ............................................................. 27
   4.8 Certificate modification .................................................. 28
   4.9 Certificate revocation and suspension ......................... 29
   4.10 Certificate status services ............................................. 31
   4.11 End of subscription ....................................................... 32
   4.12 Key escrow and recovery .............................................. 32

5. **Facility, Management, and Operations Controls** ............... 33
   5.1 Physical controls ............................................................ 33
   5.2 Procedural controls ......................................................... 34
   5.3 Personnel controls ........................................................ 35
   5.4 Audit logging procedures ............................................... 36
   5.5 Records archival ............................................................ 38
   5.6 Key changeover .............................................................. 39
   5.7 Compromise and disaster recovery ............................... 39

6. **Technical Security Controls** ....................................... 41
   6.1 Key pair generation and installation ............................... 41
   6.2 Private Key Protection and Cryptographic Module Engineering Controls .......................................................... 42
   6.3 Other aspects of key pair management ......................... 44
   6.4 Activation data .............................................................. 44
   6.5 Computer security controls ......................................... 45
   6.6 Life cycle technical controls ......................................... 45
   6.7 Network security controls ............................................. 46
   6.8 Time-stamping .............................................................. 46

7. **Certificate, CRL and OCSP Profiles** ........................... 47
   7.1 Certificate profile .......................................................... 47
   7.2 CRL profile ................................................................. 53
   7.3 OCSP profile .............................................................. 53
8 Compliance Audit and Other Assessments

8.1 Frequency or circumstances of assessment

8.2 Identity/qualifications of assessor

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

8.5 Actions taken as a result of deficiency

8.6 Communication of results

9 Other Business and Legal Matters

9.1 Fees

9.2 Financial responsibility

9.3 Confidentiality of business information

9.4 Privacy of personal information

9.5 Intellectual property rights

9.6 Representations and warranties

9.7 Disclaimers of warranties

9.8 Indemnities

9.9 Term and termination

9.10 Individual notices and communications with participants

9.11 Amendments

9.12 Dispute resolution provisions

9.13 Governing law and place of jurisdiction

9.14 Compliance with applicable law

9.15 Miscellaneous provisions

9.16 Other provisions
1 Introduction

The “SwissSign Silver CA” is a root certification authority operated by SwissSign AG.

The “SwissSign Silver CA” only issues certificates to its subordinated issuing CAs and special purpose certificates for the operation of the CSP.

The “SwissSign Silver CA” has two subordinate CAs: the “SwissSign Personal Silver CA” and the “SwissSign Server Silver CA”. The “SwissSign Personal Silver CA” issues certificates that support digital signing and/or encryption for individuals. The “SwissSign Server Silver CA” issues certificates for servers.

For the issuance of certificates intended to be used for authenticating servers accessible through the Internet, SwissSign conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

SwissSign AG complies with the following Swiss digital signature laws including the relevant international standards:

- 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)
- BR Guidelines: “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”

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

- The EU Regulation and the Swiss digital signature law refers to the standards listed below and declares them prerequisites for the issuance of qualified certificates:
  - ETSI EN 319 401 (2016): General Policy Requirements for Trust Service Providers
  - ETSI EN 319 411-1 (2016): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
  - ETSI EN 319 411-2 (2016): Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
  - ETSI EN 319 422 (2016): Time-stamping protocol and time-stamp token profiles
  - ETSI TS 119 312 (2016): Cryptographic Suites

The “SwissSign Personal Silver CA” and the “SwissSign Server Silver CA” are issuing CAs for certificates that meet the stipulations of:

- NCP: 0.4.0.2042.1.1
- DVCP: 0.4.0.2042.1.6 / CAB-DV: 2.23.140.1.2.1

Certificates issued by these CAs do not meet the requirements of the Swiss Digital Signature Law and are not governed by the Swiss digital signature laws listed above.

All the certificates issued by the “SwissSign Personal Silver CA” and the “SwissSign Server Silver CA” are levied a fee which is determined by SwissSign AG or its RA.

In this CP/CPS, “this CA” refers to the “SwissSign Silver CA” and all its subordinated CAs, unless stated differently.
1.1 Overview

The following illustration shows the structure of the SwissSign Silver CA and its subsidiaries:

![Silver CA Hierarchy G2](image)

Figure 1: Silver CA Hierarchy G2

The following illustration shows the structure of the SwissSign Silver CA and its subsidiaries:

![Silver CA Hierarchy G22](image)

Figure 2: Silver CA Hierarchy G22

The picture below shows the hierarchy of the SwissSign Silver CA tree for the generation G3:

![Silver CA Hierarchy G3](image)

Figure 3: Silver CA Hierarchy G3

This SwissSign AG certificate policy and certification practice statement (CP/CPS) for the “SwissSign Silver CA” and all its subordinate CAs 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 CP/CPS is applicable to all persons, including, without limitation, all requesters, subscribers, relying parties, registration authorities and any other persons, that have a relationship with SwissSign AG with respect to certificates issued by this CA.

This CP/CPS also provides statements of the rights and obligations of SwissSign AG, authorized registration authorities, requesters, subscribers, relying parties, resellers, co-marketers and any other person, or organization that may use or rely on certificates issued by this CA.

SwissSign AG provides a detailed product overview on their website (swisssign.com) for Silver certificates and for other services.

1.2 Document name and identification

This document is named "SwissSign Silver 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 2.16.756.1.89.1.3.1.8

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

<table>
<thead>
<tr>
<th>Position 1</th>
<th>Position 2</th>
<th>Position 3</th>
<th>Position 4</th>
<th>Position 5</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Joint ISO-CCITT Tree</td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Country</td>
</tr>
<tr>
<td>756</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Switzerland</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RDN</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>89</td>
<td>SwissSign</td>
</tr>
</tbody>
</table>

Position 6 to 8 of the SwissSign OID number represent the document and 9 represents the document version. The version number is omitted from CA certificates to indicate that the version number in the subscriber certificate is binding.

The following structure may be expanded without any problems, as long as already associated OIDs remain untouched.

1.3 PKI participants

1.3.1 Certification authorities

The SwissSign Silver CA and its subsidiary CAs (SwissSign Personal Silver CA, SwissSign Server Silver CA) are the only CAs operated by SwissSign AG that issue certificates under this CP/CPS. SwissSign may under this CP/CPS issue at any time additional subsidiary CAs for private or enterprise purposes.

1.3.2 Registration authorities

SwissSign AG operates a registration authority, called SwissSign RA that registers subscribers of certificates issued by this CA.

Third parties may operate their own registration authority services, if these third parties abide by all the rules and regulations of this CP/CPS 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 of any other RA must be documented and presented to SwissSign AG. The other RA is only allowed to execute their registration process if SwissSign AG has audited and approved the process as meeting the quality requirements of this CP/CPS and therefore being equivalent to the registration process of the SwissSign RA.
- The RA must pass an annual audit. All costs related to this audit are to be paid by the operator of 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 copy of 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;
- 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;
- protecting the private key from unauthorized access;
- using the private key only in secure computing environments that have been provided by trustworthy sources and that are protected by state-of-the-art security measures;
- ensuring complete control over the private key by not sharing private keys and passwords and not using easily guessable passwords;
- notifying the registration authority of any change to any of the information included in the certificate or any change of circumstances that would make the information in the certificate misleading or inaccurate;
- 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 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 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 and applicable policies.

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 Relying Party agrees to observe the following conditions:

- Silver Certificates may only be used in accordance with the rules stipulated in the “SwissSign Silver 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 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.

Other participants can be also subscribers within this CA.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The following certificates are issued under this CA:

- Personal Silver Certificates are issued by the SwissSign Personal Silver CA with the following key usage bits set: digitalSignature, nonrepudiation, keyAgreement, dataEncipherment and keyEncipherment.

The subscriber may choose the key usage of his certificates. SwissSign AG strongly recommends at least dual keying, where two certificates are requested. The first certificate is issued with the digitalSignature, nonrepudiation and keyAgreement key usage bits set. The second certificate is issued with the keyEncipherment and dataEncipherment key usage bits set.

- Server Silver Certificates are issued by the SwissSign Server Silver CA with the digitalSignature and keyEncipherment key usage bits set.

1.4.2 SSL Silver Certificates are issued by the SwissSign Server Silver CA with the digitalSignature and keyEncipherment key usage bits set. The extended key usage is set with ServerAuthentication and ClientAuthenticationProhibited certificate uses

Any other use than defined in chapter 1.4.1 is prohibited.

The Personal Silver and SSL Silver Certificates shall never be used for digital signing according to Article 14 para. 2nd OR (Swiss Code of Obligations).

This specifically includes the prohibition of using subordinate CAs chaining to this CA for MiTM or “traffic management” of domain names or IPs that the certificate holder does not legitimately own or control, regardless of whether it is in a closed and controlled environment or not.
1.5  Policy administration

1.5.1 Organization administering the document

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

SwissSign AG
Sägereistrasse 25
Postfach
8152 Glattbrugg
Switzerland
Tel.: +41 (44) 838 36 00
Mail: info@swisssign.com
Web: http://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 Silver CP/CPS.

The following policies are part of the legal framework of this CA and apply to them:

• PDS – PKI Disclosurer Statement OID: 2.16.756.1.89.1.0.6.0.1
• EUA - End User Agreement / Subscriber Agreement OID: 2.16.756.1.89.1.0.2.0.2
• RPA – Relying Party Agreement OID: 2.16.756.1.89.1.0.5.0.1
• AGB – Terms and Conditions Ausgabe 11. Mai 2017

1.5.2 Contact persons

The following persons are the main contacts for any questions or suggestions regarding the SwissSign Silver CP/CPS.

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.

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Abbrev.</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Digital Signature</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Algorithm</td>
<td></td>
<td>A process for completing a task. An encryption algorithm is merely the process, usually mathematical, to encrypt and decrypt messages.</td>
</tr>
<tr>
<td>Attribute</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Term</td>
<td>Abbrev.</td>
<td>Explanation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td>The process of identifying a user. User names and passwords are the most commonly used methods of authentication.</td>
</tr>
<tr>
<td>CA Operator</td>
<td>CAO</td>
<td>A person responsible for CA operation, including establishment of certificate parameters for RA and RAO in accordance with certificate policy.</td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Certification Authority</td>
<td>CA</td>
<td>An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.</td>
</tr>
<tr>
<td>Certificate Extension</td>
<td></td>
<td>Optional fields in a certificate.</td>
</tr>
<tr>
<td>Certificate Policy</td>
<td>CP</td>
<td>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.</td>
</tr>
<tr>
<td>Certificate Revocation List</td>
<td>CRL</td>
<td>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.</td>
</tr>
<tr>
<td>Certification Practice Statement</td>
<td>CPS</td>
<td>Document that regulates the rights and responsibilities of all involved parties (RA, CA, directory service, end entity, relying party).</td>
</tr>
<tr>
<td>Certification Service Provider</td>
<td>CSP</td>
<td>Individual or corporation that issues certificates to individual or corporate third parties.</td>
</tr>
<tr>
<td>Cipher</td>
<td></td>
<td>A cryptographic algorithm used to encrypt and decrypt files and messages.</td>
</tr>
<tr>
<td>Cipher Text</td>
<td></td>
<td>Data that has been encrypted. Cipher text is unreadable unless it is converted into plain text (decrypted) with a key.</td>
</tr>
<tr>
<td>Coordinated Universal Time</td>
<td>UTC</td>
<td>Mean solar time at the prime meridian (0°). The time scale is based on seconds as defined in in ETSI EN 319 421. Time scale realized by the laboratory “k” and kept in close agreement with UTC, with the goal to reach ±100 ns.</td>
</tr>
<tr>
<td></td>
<td>UTC(k)</td>
<td></td>
</tr>
<tr>
<td>Credentials</td>
<td></td>
<td>Evidence or testimonials governing the user’s right to access certain systems (e.g. User name, password, etc)</td>
</tr>
<tr>
<td>Certificate Transparency</td>
<td>CT</td>
<td>Is an experimental IETF open standard (RFC 6962) and open source framework for monitoring and auditing digital certificates. Through a system of certificate logs, monitors, and auditors, certificate transparency allows website users and domain owners to identify mistakenly or maliciously issued certificates and to identify certificate authorities (CAs) they issued such certificates.</td>
</tr>
<tr>
<td>Decryption</td>
<td></td>
<td>The process of transforming cipher text into readable plain text.</td>
</tr>
<tr>
<td>DES</td>
<td></td>
<td>Data Encryption Standard. A cipher developed by the United States government in the 1970s as the official encryption algorithm of the U.S.</td>
</tr>
<tr>
<td>Digital signature</td>
<td></td>
<td>A system allowing individuals and organizations to electronically certify features such as their identity or the authenticity of an electronic document.</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>DN</td>
<td>- &gt; Subject</td>
</tr>
<tr>
<td>Term</td>
<td>Abbrev.</td>
<td>Explanation</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DNS</td>
<td></td>
<td>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 <code>@', e.g. </code>anytown.ac.uk'.</td>
</tr>
<tr>
<td>Electronic Signature</td>
<td></td>
<td>- &gt; Digital Signature</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td>Encryption is the process of using a formula, called an encryption algorithm, to transform plain text into an incomprehensible cipher text for transmission.</td>
</tr>
<tr>
<td>End Entity</td>
<td></td>
<td>Used to describe all end users of certificates, i.e. subscribers and relying parties.</td>
</tr>
<tr>
<td>End-User Agreement</td>
<td>EUA</td>
<td>Contractual agreement between seller of certificates and the subscriber.</td>
</tr>
<tr>
<td>Enterprise EV Certificate</td>
<td></td>
<td>An EV certificate that an enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original valid EV certificate issued to the enterprise RA.</td>
</tr>
<tr>
<td>Entropy</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>EV Certificate</td>
<td></td>
<td>A digital certificate that contains information specific in the EV guidelines and that has been validated in accordance with the guidelines.</td>
</tr>
<tr>
<td>Extended Validation</td>
<td>EV</td>
<td>Validation procedures defined by the guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and major browser vendors.</td>
</tr>
<tr>
<td>Extension</td>
<td></td>
<td>- &gt; Certificate Extension</td>
</tr>
<tr>
<td>FIPS 140</td>
<td></td>
<td>FIPS 140 (Federal Information Processing Standards Publication 140) is a United States federal standard that specifies security requirements for cryptography modules.</td>
</tr>
<tr>
<td>FQDN</td>
<td>FQDN</td>
<td>Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>Hardware Security Module</td>
<td>HSM</td>
<td>Hardware Security Module is a device that physically protects key material against unauthorized parties.</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP</td>
<td>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.</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HTTPS</td>
<td>Secure Hyper-Text Transfer Protocol using TLS/SSL</td>
</tr>
<tr>
<td>Key</td>
<td></td>
<td>The secret input for cryptographic algorithms that allows a message to be transformed. - &gt; See Private Key, Public Key</td>
</tr>
<tr>
<td>Key password</td>
<td></td>
<td>Password used to encrypt the private key.</td>
</tr>
<tr>
<td>Key size</td>
<td></td>
<td>Length of private and public key. Regular key sizes are 2048 and 4096. 2048 bit is the recommended key size according to NIST today.</td>
</tr>
<tr>
<td>Key usage</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol</td>
<td>LDAP</td>
<td>LDAP is used to retrieve data from a public directory.</td>
</tr>
<tr>
<td>LDAP Secure</td>
<td>LDAPS</td>
<td>LDAP secured with TLS/SSL</td>
</tr>
<tr>
<td>Term</td>
<td>Abbrev.</td>
<td>Explanation</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Man-in-the-middle</td>
<td>MITM</td>
<td>Active eavesdropping of secure communications in which attacker/third party relays and controls messages between sender and receiver.</td>
</tr>
<tr>
<td>Online Certificate Status Protocol</td>
<td>OCSP</td>
<td>Method to verify the validity of a certificate in real time.</td>
</tr>
<tr>
<td>Participants</td>
<td></td>
<td>Entities like CAs, RAs, and repositories. These can be different legal entities.</td>
</tr>
<tr>
<td>PKCS</td>
<td></td>
<td>PKCS refers to a group of Public Key Cryptography Standards devised and published by RSA Laboratories.</td>
</tr>
<tr>
<td>Plain Text</td>
<td></td>
<td>The original message or file.</td>
</tr>
<tr>
<td>Privacy Level</td>
<td></td>
<td>Used to determine how the certificate can be accessed in the directory. Private, Public Lookup and Public Download are the available levels.</td>
</tr>
<tr>
<td>Private Key</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Profile</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Public Key</td>
<td></td>
<td>One of two keys used in public key cryptography. The public key can be known to anyone and is used to verify signatures or encrypt messages. The public key of a public-private key cryptography system is used to verify the &quot;signatures&quot; 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.</td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td>PKI</td>
<td>Processes and technologies that are used to issue and manage digital identities that may be used by third parties to authenticate individuals or organizations.</td>
</tr>
<tr>
<td>Qualified Certificate</td>
<td>QC</td>
<td>Certificate which meets the requirements of article 8 ZertES.</td>
</tr>
<tr>
<td>Qualified Certificate Policy</td>
<td>QCP</td>
<td>Certificate policy which incorporates the requirements defined in ETSI EN 319-401 and ETSI EN 391 411-2</td>
</tr>
<tr>
<td>Qualified Digital Signature</td>
<td></td>
<td>qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures, as defined in article 3 (12) of the Directive No 910/2014 and in ZertES article 2</td>
</tr>
<tr>
<td>RA Operator</td>
<td>RAO</td>
<td>The person responsible for identifying the requester, collecting the identity substantiating evidence, authorizing the CSR, and forwarding the authorized CSR to the CA.</td>
</tr>
<tr>
<td>Recognition Body</td>
<td></td>
<td>The Recognition Body of Switzerland is accredited by the SAS and conducts the audits prescribed by Swiss Digital Signature Law.</td>
</tr>
<tr>
<td>Recognized Qualified Digital Signature</td>
<td></td>
<td>Qualified digital signature created with a certificate issued by a CA that has successfully been certified by a Swiss recognition body.</td>
</tr>
<tr>
<td>Relying Party</td>
<td></td>
<td>Recipient of a certificate which acts in reliance on that certificate and/or digital signatures verified using that certificate.</td>
</tr>
<tr>
<td>Requester</td>
<td></td>
<td>Requesters are individuals or organization that have requested, but not yet obtained a certificate.</td>
</tr>
<tr>
<td>Revocation</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Term</td>
<td>Abbrev.</td>
<td>Explanation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rollover</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td>A public key encryption algorithm named after its founders: Rivest-Shamir-Adleman.</td>
</tr>
<tr>
<td>S/MIME</td>
<td></td>
<td>Secure / Multipurpose Internet Mail Extensions is a standard for public key encryption and signing of e-mail.</td>
</tr>
<tr>
<td>Secure Signature Creation Device</td>
<td>SSCD</td>
<td>Signature-creation device which meets the requirements specified in article 30 of Directive 910/2014/EC.</td>
</tr>
<tr>
<td>Smart-card</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Signature</td>
<td></td>
<td>Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.</td>
</tr>
<tr>
<td>Signature-creation data</td>
<td></td>
<td>Unique data, such as parameters of signature algorithms or private cryptographic keys, used by the signatory to create an electronic signature.</td>
</tr>
<tr>
<td>Signature-creation device</td>
<td></td>
<td>Configured software or hardware used to implement the signature-creation data</td>
</tr>
<tr>
<td>Signature-verification data</td>
<td></td>
<td>Data, such as parameters of signature algorithms or public cryptographic keys, used for the purpose of verifying an electronic signature.</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td></td>
<td>Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). A protocol that enables secure transactions via the Internet. URLs that require an TLS connection for HTTP start with https: instead of http.</td>
</tr>
<tr>
<td>SSO</td>
<td></td>
<td>Single Sign On: The user only needs to log in once to access various services.</td>
</tr>
<tr>
<td>Term</td>
<td>Abbrev.</td>
<td>Explanation</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subject</td>
<td>DN</td>
<td>Field in the certificate that identifies the owner of the certificate. Also referred to as distinguished name (DN). Examples: /CN=John Doe /Email=<a href="mailto:jd@signdemo.com">jd@signdemo.com</a> /CN=SwissSign AG /Email=<a href="mailto:info@swisssign.com">info@swisssign.com</a> /O=SwissSign AG /C=CH /CN=pseudo: Marketing /Email=<a href="mailto:marketing@signdemo.com">marketing@signdemo.com</a> /CN=John Doe /O=SwissSign AG /OU=DEMO /Email=<a href="mailto:root@signdemo.com">root@signdemo.com</a> /CN=swiss.signdemo.com /OU=DEMO /Email=<a href="mailto:root@signdemo.com">root@signdemo.com</a></td>
</tr>
<tr>
<td>mandatory fields in the subject:</td>
<td>Common Name /CN</td>
<td>Email address /Email</td>
</tr>
<tr>
<td>optional fields in the subject:</td>
<td>Organization /O</td>
<td>Organizational Unit /OU</td>
</tr>
<tr>
<td>Additional fields for EV SSL certificates in the subject:</td>
<td>City or Town of Incorporation</td>
<td>State/Province of Incorporation</td>
</tr>
<tr>
<td>Subscriber</td>
<td></td>
<td>Subscribers are individuals that have obtained a certificate.</td>
</tr>
<tr>
<td>SuisseID</td>
<td></td>
<td>Specification for certificates and services, issued by eCH as eCH-0113. see <a href="http://www.ech.ch">www.ech.ch</a></td>
</tr>
<tr>
<td>Swiss Code of Obligations</td>
<td>OR</td>
<td>Federal Act of 30 March 1911 on the Supplement to the Swiss Civil Code (Fifth Section: Obligatory Law)</td>
</tr>
<tr>
<td>TAV-BAKOM</td>
<td></td>
<td>Amendment to VZertES, technical and administrative directives on the issuance of digital signatures, issued November 23rd, 2016. SR 943.032.1.</td>
</tr>
<tr>
<td>Time-stamping Authority</td>
<td>TSA</td>
<td>Authority which issues time-stamp tokens.</td>
</tr>
<tr>
<td>Time-stamp Policy</td>
<td>TP</td>
<td>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.</td>
</tr>
<tr>
<td>Time-stamp Token</td>
<td>TST</td>
<td>Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.</td>
</tr>
<tr>
<td>Time-stamping Unit</td>
<td></td>
<td>Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.</td>
</tr>
<tr>
<td>Traffic management</td>
<td></td>
<td>Management and surveillance of network traffic with domain names or IPs owned or controlled by third parties.</td>
</tr>
<tr>
<td>TSA Disclosure statement</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>TSA practice statement</td>
<td>TPS</td>
<td>Statement of the practices that a TSA employs in issuing time-stamp tokens.</td>
</tr>
<tr>
<td>Term</td>
<td>Abbrev.</td>
<td>Explanation</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TSA system</td>
<td></td>
<td>Composition of IT products and components organized to support the provision of time-stamping services.</td>
</tr>
<tr>
<td>Transaction Limit</td>
<td></td>
<td>The transaction limit is detailing liability limits of SwissSign AG, the subscriber and relying parties. This limit is published in the respective certificate.</td>
</tr>
<tr>
<td>Triple DES</td>
<td></td>
<td>A method of improving the strength of the DES algorithm by using it three times in sequence with different keys.</td>
</tr>
<tr>
<td>Two-factor authentication</td>
<td></td>
<td>A two-factor authentication is any authentication protocol that requires two independent ways to establish identity and privileges.</td>
</tr>
<tr>
<td>Uniform Resource Locator</td>
<td>URL</td>
<td>The global address of documents and other resources on the WWW, e.g., <a href="http://swisssign.net">http://swisssign.net</a>. The first part indicates the protocol to be used (http) and the second part shows the domain where the document is located.</td>
</tr>
<tr>
<td>USB Token</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>VZertES</td>
<td></td>
<td>Swiss directive for digital signatures, issued November 23th, 2016. SR 943.032.</td>
</tr>
<tr>
<td>ZertES</td>
<td></td>
<td>Swiss Digital Signature Law. Issued March 18, 2016. SR 943.03. Compliance with this law always implies adherence to VZertES and TAV-BAKOM.</td>
</tr>
</tbody>
</table>
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 employees 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.

The repository is available 24 hours per day, 7 days per week.

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).
- PKI Disclosurer Statement (PDS).
- The end-user agreement (EUA).
- Relying Party Agreement (RPA).

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 one of the subsidiaries of the SwissSign Silver CA in the field: “CRL Distribution Point”.

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.

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

2.3 Time or frequency of publication

SwissSign will publish this information on a regular schedule:

- CRLs for the SwissSign Silver CA and all its subsidiaries 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 Silver 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 CP/CPS, PDS and EUA information is provided as public information on the repository.swisssign.com web site. These documents are only valid if they are published as a PDF with the digital signatures of two officers of SwissSign AG.

SwissSign provides CRL and OCSP status service. Access to these services is provided through the web site “swisssign.net” and the online LDAP directory “directory.swisssign.net”. The integrity and authenticity of the online status information (OCSP) is protected by a digital signature of the dedicated OCSP responder certificate which is signed from the appropriate issuing CA. The CRL is directly signed by the appropriate issuing CA. Integrity and authenticity of the revocation information is guaranteed by a signature of the CRL or the OCSP response. Revocation information remains in the CRL until the end of the issuing CA validity. Write access to the document repository is controlled through certificate-based two factor authentication.

The LDAP, CRL and OCSP information is managed in an encrypted database system. All management access to the data in this database system is managed through the swisssign.net web interface and protected requires sufficient authorization. The type of authorization required depends on how the process is executed. End-user access either requires user name/password authorization or certificate authentication. Manager access always requires certificate-based two factor authentication.
3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

The distinguished name (DN) in a certificate issued by the "SwissSign Silver CA" or one of its subsidiaries complies with the X.500 standard.

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

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

- real names
- pseudonyms
- fully qualified domain names (FQDN).

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

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.

Registration Authorities other than the SwissSign RA may choose to accept a wide range of identifying documents. Should these documents provide name forms that differ from official documentation, it is the registrations authorities choice whether such name forms are admissible to be used in the CN.

The organizational name in /CN or in /O must be spelled absolutely identical to the name as it appears in the documentation provided according to chapter 3.2.2.

If the CN is a organizational name, then the entries in the /O and /C field must also be inserted. In this case the /CN field must be identical to the /O field.

Pseudonyms are specified as /CN='identifier': 'arbitrary string'. The SwissSign RA requires pseudonym certificates to use the string 'pseudo' as identifier. An example of a correctly formulated pseudonym is: "/CN=pseudo: John Doe". Other registration authorities may use other identifiers.

FQDNs must be well formed according to RFC 1035.

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

- The use of an organizational name must be authorized according to chapter 3.2.5.
- The use of a real name and its identifying information must be authenticated and authorized according to chapter 3.2.3.
- A pseudonym requires that the requester authenticates and authorizes the request providing identifying information according to chapter 3.2.3.
- The use of a FQDN requires authentication and authorization of the domain owner. For individuals the rules in chapter 3.2.3 and for organizations the rules in chapter 3.2.5 apply respectively.
- The use of a FQDN may be authorized through domain validation. Certificates issued in this way must be clearly marked as "domain validated only" certificates. The requirements of chapters 3.2.3 and 3.2.5 do not apply and domain validation must be obtained by one of the following methods:
  - The requester proves control of an administrative mail address in the domain.
  - The requester proves control of the DNS entry.
  - The requester proves control over the web server.

SubjectAltNames in SSL certificates must contain at least the CN of the certificate.

SubjectAltName is a recommended field for personal certificates issued with real names or pseudonyms. If it is present, it contains at least an email address. Additional attributes in the SubjectAltName are permissible and may be supported by the RA at their own discretion: .

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

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 clearly mark the certificate as a pseudonym. To this end the /CN= attribute in the subject must start with the following sequence:

<identifier><colon><space>

• Identifier is a string that clearly indicates the nature oft he CN. The SwissSign RA only allows the string "pseudo"
• The identifier and the content of the /CN= attribute must be separated with a <colon> <space> sequence.
A subscriber can use any string of characters after the 'identifier'.

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.

Other registrations authorities may use different identifiers to identify pseudonym certificates, if they meet the following requirements:
• SwissSign has approved the identifier.
• The identifier and the resulting /CN= values are neither incorrect nor misleading.
• The identifier is alphabetical and can be used with the <identifier><colon><space> formatting.

3.1.4 Rules for interpreting various name forms
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 ä, ö, ü are represented by ae, oe, ue.

3.1.5 Uniqueness of names
The CAs operating under this CP/CPS do enforce the uniqueness of certificate subject fields in such a manner that all valid certificates with identical subject fields must belong to the same individual. The following rules are enforced:
• All actual valid certificates for individuals with identical subjects must belong to the same individual.
• All actual valid organizational certificates with identical subjects must belong to the same organization.
• All actual valid server certificates with identical subjects must belong to the same domain owner.

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

- The registration process must be documented and presented to SwissSign AG.
- The other RA is only allowed to execute their registration process if SwissSign AG has audited and approved the process as equivalent to the registration process of the SwissSign RA.

In conformance with a requirement of the Mozilla Foundation concerning SSL Server certificates, every RA operating under this CP/CPS must ascertain:

- Not to issue certificates for SSL Servers with a lifetime exceeding 39 months or
- For each certificate, issued for a SSL Server and with a lifetime exceeding thirty-nine months, to re-validate all the information (domain name, organization, etc.) contained in the certificate before the initial thirty-nine months usage period has expired and every three years after.
- As of 01 March 2018, only SSL certificates with a 2-year term will be issued in accordance with the CAB Browser Forum.

3.2.1 Method to prove possession of private key

The Certificate Signing Request sent to the CA from the Subscriber is signed with the private key. Therefore the possession of the private key is proven.

3.2.2 Authentication of organization identity

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

- The use of the organization field means that the use of the country field is mandatory.
- The registration process of any registration authority operating under this CP/CPS must contain provisions to determine the identity of an organization and to authorize the use of its name.
- To validate the name 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 12 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 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.
- SwissSign validates that the person enrolling for the certificate has control of the domain by requiring the person to respond to an e-mail hosted at that domain (eg. webmaster@domain, postmaster@domain etc.).
- Additionally, the domain will only be accepted if a printout of the WHOIS entry for the domain is included. The owner of the domain must approve the request with a handwritten personal signature in the appropriate position on the registration form and provide information as to his identity. The RA will creat a high-quality copy or scan of all required supporting documentation.
- /DC= (Domain Components) fields are verified equivalent to domain validation.

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. 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.

A copy of this registration form has to be submitted.

Additionally the requester and only the requester must be identified according to these additional rules:
• The individual must present a copy of a legal, valid photo ID. The RA is to make a high-quality copy or scan of the documentation.
• 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.

Other RA's may implement a different process if they meet the following requirements:
• The registration process must be documented and presented to SwissSign AG.
• The other RA is only allowed to execute their registration process if SwissSign AG has audited and approved the process as equivalent to the registration process of the SwissSign RA.

3.2.4 Non-verified subscriber information
All subscriber information required 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.

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.

Under this CP/CPS email validated only certificates are permissible, if all of the following conditions are met:
• The email address has been validated during the registration process.
• The certificate indicates clearly that this certificate has been issued with only the email address validated.

The SwissSign RA will issue all such certificates with the /OU attribute in the DN showing the string: “Email Validated Only”. Other RAs may choose different methods to mark their certificates.

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 requester identifies and authenticated himself for routine re-keying with the valid certificate and the possession of the corresponding private key through a SSL Authentication. Therefore a resubmission of the registration documents is not necessary.

3.3.2 Identification and authentication for re-key after revocation
The SwissSign RA does not allow re-keying of certificates issued by this CA after revocation.

---

1 For identification purposes SwissSign will accept a national passport or a Swiss identity card or other official documents, like a National drivers license.
3.4 Identification and authentication for revocation request

Revocation of a certificate that is issued by one of the subsidiaries of this CA requires that the subscriber use one of the following methods:

- Successful login to the user profile.
- Providing proof of the possession of the private key on the web site of the registration authority.
- With a personal signature on a revocation form.
- Personal appearance at the registration authority.
- Providing a one-time revocation key on the web site of the registration authority.

Not all registration authorities must support all methods of revocation.

The process how the revocation request can be submitted is described in chapter 4.9.3.
4 Certificate Life-Cycle Operational Requirements

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. The certificate is issued only after successful completion of the registration process. The main steps for a certificate registration are:

(I) 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,

(II) all documents and informations are approved by the SwissSign RA.

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.

Prior to issuance SwissSign validates each server Name FQDN in publicly trusted SSL certificates against the domain CAA records. If a CAA record exists that does not list swisssign.com as an authorized CA, SwissSign will not issue the certificate.

SwissSign:
- caches CAA records for reuse for up to 8 hours
- supports the issue and issuewild CAA tags
- processes but does not act on iodef property tag (i.e., SwissSign does not dis-patch reports of such
- issuance requests to the contact(s) stipulated in the CAA iodef record(s))
- does not support any additional property tags

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:

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

If the requester fails to adhere to any of the above, or in any other way violates the stipulations of this document, the 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

After receiving the registration form as well as the complete, accurate registration documentation, the time to process certificate applications is three working days.
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

4.4.2 Once the Certificate is approved and issued by the CA, the subscriber receives an email with a link to download the certificate. If the subscriber utilizes this link, has downloaded the requested certificate, he has to verify the certificate content immediately. During a time frame of 24 hours after the first download, the subscriber can reject or complain the certificate. After this time frame, he has accepted the certificate.

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:
- Certificates issued by the SwissSign Personal Silver CA or the SwissSign Server Silver CA may only be used in accordance with the key usage declaration contained in the certificate.
- Subscribers may use SwissSign certificates exclusively for intended, legal, and authorized purposes.

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 End-User Agreement;
• 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;
• 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 AG 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 AG does not support renewal.

4.6.2 Who may request renewal
As indicated in chapter 4.6 SwissSign AG does not support renewal.

4.6.3 Processing certificate renewal requests
As indicated in chapter 4.6 SwissSign AG does not support renewal.

4.6.4 Notification of new certificate issuance to subscriber
As indicated in chapter 4.6 SwissSign AG does not support renewal.

4.6.5 Conduct constituting acceptance of a renewal certificate
As indicated in chapter 4.6 SwissSign AG does not support renewal.

4.6.6 Publication of the renewal certificate by the CA
As indicated in chapter 4.6 SwissSign AG does not support renewal.

4.6.7 Notification of certificate issuance by the CA to other entities
As indicated in chapter 4.6 SwissSign AG 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 offer re-keying of Silver Certificates.
Other RAs may choose not to offer re-keying.

4.7.1 Circumstance for certificate re-key
A certificate re-key is possible at any time while the current certificate is valid. A typical reason for a certificate re-key is shortly before its expiration, to extend the usage of the certificate subject with a new key pair and a new validity period.
To successfully request a certificate re-key, the subscriber must proof the key possession of the current private key. No other means of authorization are permissible.

4.7.2 Who may request certification of a new public key
The subscriber may request certification of a new public key.

4.7.3 Processing certificate re-keying requests
The subscriber has to visit the swisssign.net web site. After choosing a certificate re-key, he is asked to proof the possession of the corresponding private key. The CSR (certificate signing request) is sent to the corresponding CA. The SwissSign CA will verify
• the integrity of the request;
• 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.
No additional identification documents must be submitted to the SwissSign RA and no RA Operator needs to approve the CSR.

4.7.4 Notification of new certificate issuance to subscriber
See Chapter 4.3.2 of this CP/CPS.

4.7.5 Conduct constituting acceptance of a re-keyed certificate
See Chapter 4.4.1 of this CP/CPS.

4.7.6 Publication of the re-keyed certificate by the CA
See Chapter 4.4.2 of this CP/CPS.

4.7.7 Notification of certificate issuance by the CA to other entities
See Chapter 4.4.3 of this CP/CPS.

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 AG 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 AG does not support certificate modification.

4.8.2 Who may request certificate modification
As indicated in chapter 4.8 SwissSign AG does not support certificate modification.
4.8.3 Processing certificate modification requests
As indicated in chapter 4.8 SwissSign AG does not support certificate modification.

4.8.4 Notification of new certificate issuance to subscriber
As indicated in chapter 4.8 SwissSign AG does not support certificate modification.

4.8.5 Conduct constituting acceptance of modified certificate
As indicated in chapter 4.8 SwissSign AG does not support certificate modification.

4.8.6 Publication of the modified certificate by the CA
As indicated in chapter 4.8 SwissSign AG 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 AG 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. (e.g. bankruptcy of the organization)
- The certificate /CN= field is no longer valid (e.g. name change due to change in marital status or omission of domain registration renewal).
- The 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
All subsidiaries of 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 a revocation form, 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 as well as proof of identity (as described in chapter 3.2.3).
• The subscriber can personally visit the RA offices and request the revocation of a certificate offline. 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.

All registrations authorities operating under this CP/CPS must adhere to the following stipulations:

Online revocation management services must be available 24 hours per day, 7 days per week. The annual availability of the revocation management services must be guaranteed at no less than 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.

Offline revocation management services must be available and be able to receive revocation requests during business hours. The registration authorities operating under this CP/CPS must guarantee to process a revocation request until end of day of the next business day.

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

After proper authorization has been demonstrated, the SwissSign CA will process revocation requests within two hours after receiving such requests from the 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 5280. Also, any and all critical extensions, key usage, and approved technical corrigenda as appropriate should be taken into account.

4.9.7 CRL issuance frequency (if applicable)

The CRL of the SwissSign Silver CA and its subsidiaries are updated according to the following schedule:

<table>
<thead>
<tr>
<th>CA</th>
<th>Information</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>SwissSign Personal Silver CA</td>
<td>CRL</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>OCSP Information</td>
<td>Real-time. The OCSP responder will report a certificate’s revocation immediately after the revocation has been completed.</td>
</tr>
<tr>
<td>SwissSign Server Silver CA</td>
<td>CRL</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>OCSP Information</td>
<td>Real-time. The OCSP responder will report a certificate’s revocation immediately after the revocation has been completed.</td>
</tr>
<tr>
<td>SwissSign Silver CA</td>
<td>CRL</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>OCSP Information</td>
<td>Real-time. The OCSP responder will report a certificate’s revocation immediately after the revocation has been completed.</td>
</tr>
</tbody>
</table>
4.9.8 Maximum latency for CRLs (if applicable)

The CRL of this CA and all its subsidiaries 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 subsidiaries optionally support the OCSP protocol for on-line revocation checking. The OCSP responder URL is stored in every certificate issued by one of the subsidiaries of the SwissSign Silver CA (field “authorityInformationAccess”).

4.9.10 On-line revocation checking requirements

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

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

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

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

4.9.13 Circumstances for suspension

Certificates may not be suspended.

4.9.14 Who can request suspension

Certificates may not be suspended.

4.9.15 Procedure for suspension request

Certificates may not be suspended.

4.9.16 Limits on suspension period

Certificates may not be suspended.

4.10 Certificate status services

4.10.1 Operational characteristics

The SwissSign certificate status services for this CA 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 service provides 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
Certificate status services are available 24 hours per day, 7 days per week.
SwissSign RA provides customers with pre-filled revocation request forms during the registration process. SwissSign RA guarantees timely processing of revocation requests without undue delay if these forms are sent through registered mail and if all required signatures are present.

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
SwissSign RA does offer key escrow for certificates through the profile of the certificate holder, if in the registration process the subscriber has chosen an online key generation. For keys generated in a SSCD, a key escrow is not possible.
SwissSign RA does not offer key recovery for Silver certificates, but other RAs may offer key recovery.

4.12.2 Session key encapsulation and recovery policy and practices
This CA and its subsidiaries do not support session key encapsulation.
5 Facility, Management, and Operations Controls

5.1 Physical controls

Two identical clones of the SwissSign Silver 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 does 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 backup media 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 SwissSign CA and RA are operated by three separated authorization groups, Access, Operations and Audit. Any one employee may only be part of one of these authorization groups. Within these authorization groups, multiple roles are defined (see picture below). An employee assigned to one of the groups may have one or more roles within the same authorization group.

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 Silver CA and all its subsidiaries is 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 the CA (signing operations) can only be accessed by two persons working together (four-eye-principle).

5.2.3 Identification and authentication for each role
Identification and authentication for all roles is achieved using SwissSign certificates. Access to data facilities (including bank safe deposit box) requires national passport and/or biometric identification.

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.

5.2.5 Security and Compliance
The TSP has an ISMS management system. This ensures that a defined security policy exists and is active. This policy is reviewed at least once a year and released by management. The TSP ensures that all employees and partners are made aware of security relevant requirements and/or behavioral rules. The TSP is responsible for adhering to the requirements set out in the policies, even if individual tasks are provided by partners.

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

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.

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
SwissSign AG verifies the background of its employees and ensures that employees do not have a criminal record. SwissSign will not appoint any person who is known to have been convicted of a serious crime or other offense which could effect 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,
- sign 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 Silver 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 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 subsidiaries 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 subsidiaries produce
- 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 SwissSign 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 deletion: The RA archive (physical documents) is stored in a safe deposit box of a major Swiss bank and can only be accessed by authorized SwissSign employees as detailed in the role model presented in 5.2.
- 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 safe deposit boxes at a major Swiss bank.

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. 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 subsidiaries 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 intermediate CAs on a regular basis. All certificates of such intermediate 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 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 subsidiaries 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 subsidiaries is part of a daily backup process.

5.7.3 Entity private key compromise procedures
If the private key of the “SwissSign Silver CA” or one of its subsidiaries 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 subsidiaries 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.

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 Silver CSP terminates its services, the following actions will be executed:

- SwissSign AG will report, without delay, any threat of bankruptcy to the Swiss METAS/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 METAS/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 Silver CA, SwissSign Personal Silver CA and SwissSign Server Silver 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 SwissSign Silver CP/CPS.

Any RA other than the SwissSign RA that decides to terminate its RA operation, must give at least 180 days notice. During this period the RA must work with SwissSign AG to find a suitable solution that meets all contractual and legal obligations concerning the subscribers and relying parties.

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for the SwissSign Silver 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 subsidiaries of the SwissSign Silver 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.

6.1.2 Private key delivery to subscriber

Subscribers of the SwissSign RA have the choice, where the keys will be generated. SwissSign AG recommends to generate the keys for a signing certificate on a secure crypto device and the keys for an encryption certificate on the SwissSign website.

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

The delivery of private keys generated on the SwissSign website will be delivered through a passphrase-protected download mechanism (PKCS#12).

Other RAs may manage the key generation and the delivery differently.

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

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

ETSI: ETSI TS 119 312 http://www.etsi.org/standards-search
NIST: SP 800-57 http://csrc.nist.gov

The "SwissSign Platinum CA" uses a 4096 bit RSA key.
The subordinate CAs use a 2048 bit RSA key.

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

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)

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

Subscribers can obtain certificates that may have one or more of the following key usage bits included:

- digitalSignature
- nonRepudiation
- keyAgreement
- keyEncipherment
- DataEncipherment

Subscribers can obtain certificates issued by this CA with the following extended key usages included:

- Server Authentication
- Client Authentication
- Code Signing
- Email Protection
- Time Stamping
- Microsoft Individual Code Signing (msICS)
- Microsoft Commercial Code Signing (msCCS)
- Microsoft Trust List Signing (msTLS)
- Microsoft Encrypted Files System (msEFS)
- Microsoft Smart Card Logon (msSCL)
- IPSec End System
- IPSec Tunnel
- IPSec User

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

- **Root CA keys**: The 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.
- **Subscriber keys**: The subscriber is fully responsible for the evaluation, implementation and protection of the cryptographic module, where the subscriber keys are generated and stored. SwissSign AG recommends that the subscriber uses a SSCD.

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

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

- **Root CA keys**: Root CA keys can only be accessed on the physical and on the logical level by adhering to ‘3 out of 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.
- **Subscriber keys**: The subscriber has single-person control of the subscriber keys.

6.2.3 Private key escrow

The following list shows how private key escrow is implemented:

- **Root CA keys**: Root CA keys are not in escrow.
- **Issuing CA keys**: The issuing CA keys are not in escrow.
- **Subscriber keys**: Private key escrow is not offered by the SwissSign RA. Other RAs may offer Private key escrow.
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.

Subscriber keys  Private key backup is offered by the SwissSign RA for key pairs generated on the SwissSign web site. The key pair is stored in the database and protected with a subscriber-chosen password. All keys generated on the SSCD cannot be put into backup.

Other RAs may offer private key backup differently.

6.2.5 Private key archival

The following list shows how private key archival is implemented:

Root CA keys  The Root CA keys are not archived.

Issuing CA keys  The Issuing CA keys are not archived.

Subscriber keys  SwissSign RA offers subscribers the option of downloading their keys generated on the SwissSign Web Site in the form of a PKCS#12 file. Subscribers may wish to archive this file.

Other RAs may offer private key archival differently.

6.2.6 Private key transfer into or from a cryptographic module

The following list shows how private key transfers are implemented:

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

Issuing CA keys  The Issuing CA keys are cloned in the same manner as Root keys.

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

Other RAs may assist subscribers with the transfer.

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

6.2.7 Private key storage on cryptographic module

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

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

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

Subscriber keys  Subscribers of the SwissSign RA are solely responsible for the key storage on cryptographic module and may choose not to store his private keys on a cryptographic module.

Other RAs may manage this differently.

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.

Subscriber keys  The subscriber of the SwissSign RA is solely responsible for the method of activating private keys.

Other RAs may define a method of activating private keys for their subscribers.
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.

- **Subscriber keys**
  - The subscriber is solely responsible for the deactivation of private key.

6.2.10 **Method of destroying private key**

The following list shows how private keys are destroyed:

- **Root CA keys**
  - The Root CA keys are destroyed by initializing the SSCD.

- **Issuing CA keys**
  - The Issuing CA keys are destroyed by initializing the SSCD.

- **Subscriber keys**
  - The subscriber is solely responsible for the destroying of his subscriber keys.

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 Silver CA” as well as all trust-anchor certificates are valid approximately 30 years. Key changeover is performed every 15 years.
- Issuing CA certificates are issued for a maximum lifetime of 15 years.
- The Rollover of CA certificates will be done manually and is after at most two thirds of the lifetime of the certificate.
- Enduser certificates can have a lifetime of up to the maximum remaining lifetime of the issuing CA certificate minus 10 days.

6.4 **Activation data**

6.4.1 **Activation data generation and installation**

The subscriber of the SwissSign RA is solely responsible to generate and install activation data.

Other RAs may manage the generation and installation of activation data for subscriber keys differently.

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 control access.

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

6.4.3 Other aspects of activation data

Not applicable.

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 subsidiaries of the SwissSign Platinum CA.
7 Certificate, CRL and OCSP Profiles

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

7.1 Certificate profile

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

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

7.1.1 Version number(s)

Version of X.509 certificates: version 3

7.1.2 Certificate Extensions

The Authority information Access extension is optional and it is derived from the CA as follows:
- CA Issuers - URI:http://swisssign.net/cgi-bin/authority/download/<keyid of the CA>
- OCSP - URI:http://<ocsp server>/<keyid of the CA>

The server address depends on the CA and the following OCSP Responder addresses are supported:
- ocsp.swisssign.net
- silver-root-g2.ocsp.swisssign.net
- silver-server-g2.ocsp.swisssign.net
- silver-personal-g2.ocsp.swisssign.net
- silver-root-g3.ocsp.swisssign.net
- silver-server-g3.ocsp.swisssign.net
- silver-personal-g3.ocsp.swisssign.net

The Subject Alternative Name extension is optional. It is added in accordance with rfc 5280 and the content depends on the information provided by the subscriber.
7.1.2.1 SwissSign Silver CA Certificates for Generation 2 (G2)

The generation 2 certificates of SwissSign are characterized by a self-signed root certificate with the SHA-1 hash algorithm.

**Subject of the SwissSign Silver CA certificates for Generation 2**

<table>
<thead>
<tr>
<th>CA Type</th>
<th>Subject</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root CA</td>
<td>/CN=SwissSign Silver CA - G2</td>
<td>/CN=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>/CN=SwissSign Personal Silver CA 2008 – G2</td>
<td>/CN=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>/CN=SwissSign Server Silver CA 2008 – G2</td>
<td>/CN=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
</tbody>
</table>

**Common extensions of the SwissSign Silver CA certificates for Generation 2**

<table>
<thead>
<tr>
<th>Extension</th>
<th>Root CA</th>
<th>Issuing CA</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic Constraints</td>
<td>CA: TRUE</td>
<td>CA:TRUE, pathlen: 0</td>
<td>Y</td>
</tr>
<tr>
<td>key Usage</td>
<td>Certificate Sign, CRL Sign</td>
<td>Certificate Sign, CRL Sign</td>
<td>Y</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>17:A0:CD:C1:E4:41:B6:3A:5B:3B:CB:45:9D:BD:1C:C2:98:FA:86:58</td>
<td>individual per CA</td>
<td></td>
</tr>
<tr>
<td>Identifier</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Policies</td>
<td>Policy: 2.16.756.1.89.1.3.1.1</td>
<td>Policy: 2.16.756.1.89.1.3.1.3</td>
<td></td>
</tr>
<tr>
<td>CRL Distribution</td>
<td>not included in Root CA certificate</td>
<td><a href="http://crl.swisssign.net/">http://crl.swisssign.net/</a>&lt;keyid&gt;</td>
<td></td>
</tr>
<tr>
<td>Points</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Extension of the Root Certificate: SwissSign Silver CA – G2**

no exceptions

**Extensions of the Issuing CA: SwissSign Personal Silver CA 2008 – G2**

no exceptions

**Extensions of the Issuing CA: SwissSign Server Silver CA 2008 – G2**

no exceptions

7.1.2.2 SwissSign Silver Special Certificates for Generation 2 (G2)

There are no special certificates issued from this CA.
7.1.2.3 SwissSign Silver End User User Certificates for Generation 2 (G2)

Certificate issued by any of the Issuing CAs

<table>
<thead>
<tr>
<th>Extension Attribute</th>
<th>Values</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Data of Subscriber</td>
<td>See Definitions in Chapter 1.6</td>
</tr>
<tr>
<td>Issuer Name</td>
<td>DN of the issuing CA</td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>&lt;key identifier of the issuing CA's public key&gt;</td>
<td></td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td><a href="http://crl.swisssign.net/">http://crl.swisssign.net/</a>&lt;keyid&gt;</td>
<td>URLs of the CRL Distribution points (LDAP and/or HTTP)</td>
</tr>
<tr>
<td>Certificate Policies</td>
<td>Policy: 2.16.756.1.89.1.3.1.5 CPS: <a href="http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R5.pdf">http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R5.pdf</a></td>
<td></td>
</tr>
<tr>
<td>Authority Information Access</td>
<td></td>
<td>Optional URL to OCSP responder and optional URL to CA issuer certificate</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td></td>
<td>Alternative name of the subscriber: email address</td>
</tr>
<tr>
<td>Key Usage</td>
<td>nonRepudiation, digitalSignature, keyEncipherement, keyAgreement, dataEncipherment</td>
<td>Critical extension, any combination of these key usages is permissible</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td></td>
<td>see chapter 6.1.7 for additional values</td>
</tr>
<tr>
<td>NsComment</td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Microsoft Certificate Template v1 / v2</td>
<td>(OID 1.3.6.1.4.1.311.20.2) (OID 1.3.6.1.4.1.311.21.7)</td>
<td>Optional</td>
</tr>
</tbody>
</table>

7.1.2.4 SwissSign Silver CA Certificates for Generation 22 (G22)

The generation 2 certificates of SwissSign are characterized by a self-signed root certificate with the SHA-1 hash algorithm and subordinated Issuing CAs with SHA-256 hash algorithm.

Subject of the SwissSign Silver CA certificates for Generation 2

<table>
<thead>
<tr>
<th>CA Type</th>
<th>Subject</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root CA</td>
<td>/CN=SwissSign Silver CA - G2</td>
<td>/CN=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>/CN=SwissSign Personal Silver CA 2014 – G22</td>
<td>/CN=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/C=CH</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>/CN=SwissSign Server Silver CA 2014 – G22</td>
<td>/CN=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign Silver CA - G2</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/C=CH</td>
</tr>
</tbody>
</table>

Common extensions of the SwissSign Silver CA certificates for Generation 22

<table>
<thead>
<tr>
<th>Extension</th>
<th>Root CA</th>
<th>Issuing CA</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic Constraints</td>
<td>CA: TRUE</td>
<td>CA:TRUE, pathlen: 0</td>
<td>Y</td>
</tr>
<tr>
<td>key Usage</td>
<td>Certificate Sign, CRL Sign</td>
<td>Certificate Sign, CRL Sign</td>
<td>Y</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>17:A0:CD:C1:E4:41:B6:3A:5B:3B:CB:45:9D:BD:1C:C2:98:FA:86:58</td>
<td>individual per CA</td>
<td></td>
</tr>
</tbody>
</table>
### Authority Key Identifier


### Certificate Policies

| Policy: 2.16.756.1.89.1.3.1.1 | Policy: 2.16.756.1.89.1.3.1.6 |
| CPS: [http://repository.swisssign.com/](http://repository.swisssign.com/) | CPS: [http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf](http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf) |

### CRL Distribution Points

| not included in Root CA certificate | [http://crl.swisssign.net/<keyid>](http://crl.swisssign.net/<keyid>) |

---

**Extension of the Root Certificate: SwissSign Silver CA – G22**

no exceptions

**Extensions of the Issuing CA: SwissSign Personal Silver CA 2014 – G22**

no exceptions

**Extensions of the Issuing CA: SwissSign Server Silver CA 2014 – G22**

no exceptions

7.1.2.5 SwissSign Silver Special Certificates for Generation 22 (G22)

There are no special certificates issued from this CA.

7.1.2.6 SwissSign Silver End User Certificates for Generation 22 (G22)

**Certificate issued by any of the Issuing CAs**

<table>
<thead>
<tr>
<th>Extension Attribute</th>
<th>Values</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Data of Subscriber</td>
<td>See Definitions in Chapter 1.6</td>
</tr>
<tr>
<td>Issuer Name</td>
<td>DN of the issuing CA</td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>&lt;key identifier of the issuing CA's public key&gt;</td>
<td></td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td><a href="http://crl.swisssign.net/%3Ckeyid%3E">http://crl.swisssign.net/&lt;keyid&gt;</a></td>
<td>URLs of the CRL Distribution points (LDAP and/or HTTP)</td>
</tr>
<tr>
<td>Certificate Policies</td>
<td>Policy: 2.16.756.1.89.1.3.1.6</td>
<td><a href="http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf">http://repository.swisssign.com/SwissSign-Silver-CP-CPS.pdf</a></td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>Optional URL to OCSP responder and optional URL to CA issuer certificate</td>
<td></td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>Alternative name of the subscriber: email address</td>
<td></td>
</tr>
<tr>
<td>Key Usage</td>
<td>nonRepudiation, digitalSignature, keyEncipherement, keyAgreement, dataEncipherment</td>
<td>Critical extension, any combination of these key usages is permissible</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td>see chapter 6.1.7 for additional values</td>
<td></td>
</tr>
<tr>
<td>NsComment</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Microsoft Certificate Template</td>
<td>(OID 1.3.6.1.4.1.311.21.7)</td>
<td>Optional</td>
</tr>
</tbody>
</table>
7.1.2.7 SwissSign Silver CA Certificates for Generation 3 (G3)

The generation 3 certificates of SwissSign are characterized by a self-signed root certificate with the SHA-2 hash algorithm.

Subject of the SwissSign Silver CA certificates for Generation 3

<table>
<thead>
<tr>
<th>CA Type</th>
<th>Subject</th>
<th>Issuer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root CA</td>
<td>/CN=SwissSign Silver Root CA – G3</td>
<td>/CN=SwissSign Silver Root CA – G3</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>/CN=SwissSign Silver Personal CA 2010 – G3</td>
<td>/CN=SwissSign Silver Root CA – G3</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
<tr>
<td>Issuing CA</td>
<td>/CN=SwissSign Silver Server CA 2010 – G3</td>
<td>/CN=SwissSign Silver Root CA – G3</td>
</tr>
<tr>
<td></td>
<td>/O=SwissSign AG</td>
<td>/O=SwissSign AG</td>
</tr>
<tr>
<td></td>
<td>/C=CH</td>
<td>/C=CH</td>
</tr>
</tbody>
</table>

Common extensions of the SwissSign Silver CA certificates for Generation 3

<table>
<thead>
<tr>
<th>Extension</th>
<th>Root CA</th>
<th>Issuing CA</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic Constraints</td>
<td>CA: TRUE</td>
<td>CA:TRUE, pathlen: 0</td>
<td>Y</td>
</tr>
<tr>
<td>key Usage</td>
<td>Certificate Sign, CRL Sign</td>
<td>Certificate Sign, CRL Sign</td>
<td>Y</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>A1:8C:45:93:0A:12:63:0B:A7:57:</td>
<td>individual per CA</td>
<td></td>
</tr>
<tr>
<td>Certificate Policies</td>
<td>Policy: 2.5.29.32.0 CPS:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R5.pdf">http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R5.pdf</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>not included in Root CA certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="http://crl.swisssign.net/">http://crl.swisssign.net/</a>&lt;keyid&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Extension of the Root Certificate: SwissSign Silver Root CA – G3

no exceptions

Extensions of the Issuing CA: SwissSign Silver Personal CA 2010 – G3

no exceptions

Extensions of the Issuing CA: SwissSign Silver Server CA 2010 – G3

no exceptions
7.1.2.8 SwissSign Silver End User Certificates for Generation 3 (G3)

End User Certificate issued by Issuing CAs

<table>
<thead>
<tr>
<th>Extension Attribute</th>
<th>Values</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Data of Subscriber</td>
<td>See Definitions in Chapter 1.6</td>
</tr>
<tr>
<td>Issuer Name</td>
<td>DN of the Issuing CA</td>
<td></td>
</tr>
<tr>
<td>Authority Key Identifier</td>
<td>&lt;key identifier of the issuing CA's public key&gt;</td>
<td></td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td><a href="http://crl.swisssign.net/">http://crl.swisssign.net/</a>&lt;keyid&gt;</td>
<td>URLs of the CRL Distribution points (LDAP and/or HTTP)</td>
</tr>
<tr>
<td>Certificate Policies</td>
<td>Policy: 2.16.756.1.89.1.3.1.5 CPS: <a href="http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R5.pdf">http://repository.swisssign.com/SwissSign-Silver-CP-CPS-R5.pdf</a></td>
<td></td>
</tr>
<tr>
<td>Authority Information Access</td>
<td></td>
<td>Optional URL to OCSP responder and optional URL to CA issuer certificate</td>
</tr>
<tr>
<td>Subject Alternative Name</td>
<td>Alternative name of the subscriber: email address</td>
<td></td>
</tr>
<tr>
<td>Key Usage</td>
<td>nonRepudiation, digitalSignature, keyEncipherement, keyAgreement, dataEncipherment</td>
<td>Critical extension, any combination of these key usages is permissible</td>
</tr>
<tr>
<td>Extended Key Usage</td>
<td></td>
<td>Optional, see chapter 6.1.7 for possible values</td>
</tr>
<tr>
<td>NsComment</td>
<td></td>
<td>Optional</td>
</tr>
<tr>
<td>Microsoft Certificate Template</td>
<td>(OID 1.3.6.1.4.1.311.217)</td>
<td>Optional</td>
</tr>
</tbody>
</table>

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA and its subsidiaries are:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Object Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sha1WithRSAEncryption</td>
<td>1.2.840.113549.1.1.5</td>
</tr>
<tr>
<td>SHA2WithRSAEncryption</td>
<td>1.2.840.113549.1.1.13</td>
</tr>
<tr>
<td>rsaEncryption</td>
<td>1.2.840.113549.1.1</td>
</tr>
</tbody>
</table>

7.1.4 Name forms

Certificates issued by the subsidiaries 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
In the extension field “Certificate Policies”, the OID and the URI of the according policy are declared.

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 subsidiaries issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 5280

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. Version number(s)
The OCSP version is set to v1.

7.3.1 OCSP extensions
The OCSP extensions used are specified below:
- Nonce
- ServiceLocator
8 Compliance Audit and Other Assessments

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

- The SwissSign Gold CA and its subsidiaries

8.1 All registration authorities that process requests for issuance by the subordinate CA
Frequency or circumstances of assessment

The compliance audit will be conducted annually.

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

8.2 Identity/qualifications of assessor

An independent qualified auditor will conduct the compliance audits according to the stipulations of corresponding law and CA Browser Forum.

TÜV-IT and KPMG are the chosen auditors. The audits (scope, reporting) will be fully ETSI-compliant.

8.3 Assessor's relationship to assessed entity

The qualified auditors have 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 TÜV-IT for the annual assessment.

8.4 Topics covered by assessment

8.5 The auditor will choose the control objectives that are to be covered by the assessment in accordance with ETSI Regulations ETSI EN 319 401 and ETSI EN 319 411-1, BR Guidelines. Actions taken as a result of deficiency

SwissSign AG has implemented the ITIL best practices model ISO27001 System 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 ISMS system either as incidents or as problems, risks, 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.
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

With regard to the qualified certificates issued pursuant to this CP/CPS document according to EU Regulation No 910/2014, SwissSign Switzerland has concluded an insurance for liability claims against SwissSign.

The amount of insurance coverage meets the requirements of Article 24 (2) (c) of EIDAS and EV Guidelines.

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

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

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

Upon request, 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 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 and any other relevant regulations.

9.4 Privacy of personal information
SwissSign AG fully complies with the Swiss Federal Act on Data Protection and other applicable legislation. 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
SwissSign AG has a non disclosure agreement (NDA) which is a contractual obligation and is signed between SwissSign AG and participants. Further, all stipulations of 9.3.1 apply.

9.4.2 Information treated as private
Any information about subscribers and requesters that is not made public through 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 and all information made public 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 are to 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 only 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 Federal Act on Data Protection on judicial or other authoritative order.
9.5 Intellectual property rights

All SwissSign AG intellectual property rights including all trademarks and copyrights of all SwissSign AG documents 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.

9.6.2 RA representations and warranties
SwissSign RA warrants full compliance with all provisions stated in this CP/CPS, related agreements and documents.

9.6.3 Subscriber representations and warranties
Subscribers warrant full compliance with all provisions stated in this CP/CPS and other related agreements and documentation.

9.6.4 Relying party representations and warranties
Relying parties warrant full compliance with the provisions of this CP/CPS and related agreements.

9.6.5 Representations and warranties of other participants
Any other participant warrants full compliance with the provisions set forth in this CP/CPS and related agreements.

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 this CP/CPS and which were provoked deliberately or wantonly negligent.

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.

SwissSign AG shall not in any event be liable for damages that result from force majeur events as detailed in chapter 9.16.4. 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.
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**

After termination, the certificate may no longer be used. However, 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 & Certification Practice Statement upon the approval of the executive board of SwissSign AG.

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**

Complaints regarding compliance with or implementation of these CP/CPS must be submitted in writing to the TSP. In case of any dispute or controversy in connection with the performance, execution or interpretation of this agreement that can not be resolved within a period of four weeks after submission of the complaint, the parties are free to file action with the competent courts at the place of jurisdiction pursuant to clause 9.14.
Complaints regarding the content or format of a certificate must be submitted in writing or over the contact form on the SwissSign home page. According to the requirements of the CAB Browser Forum, SwissSign will react to a notification of a failure or miss-issuance of a certificate within 24 hours.

9.14 Governing law and place of jurisdiction

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

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

9.15 Compliance with applicable law

This Certificate Policy & Certification Practice Statement and rights or obligations related hereto are in accordance with Swiss Law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS may not be the only document which comprises the agreement between the parties involved. Any other agreements may further restrict this CP/CPS, but no document or agreement may lessen the rules and stipulations of this CP/CPS. Any document which serves as an annex to this CP/CPS must be made available to all parties involved. The relationship between the documents must be documented and communicated.

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 Clause

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

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

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

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

The TSP will communicate an appropriate change within 90 days.

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

9.16.4 Enforcement (attorneys’ fees and waiver of rights)

Not applicable.
9.16.5 Force 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 the CP/CPS, the End-User-Agreement, or registration forms are provided in additional languages to English, the English version of these documents will prevail.

9.17.2 Delegated or outsourced Services

The TSP has a documented agreement and contractual relationship in place where the provision of services involves subcontracting, outsourcing or other third party arrangements. The TSP may require compliance with applicable policies to be verified by an approved auditor.