SWITCH Certificate Policy and Certification Practice Statement

Status: Final Version

Version 1.0 Author(s):
J. Doekbrijder, SwissSign AG, Chr. Graf, SWITCH, R. Gartmann, SWITCH

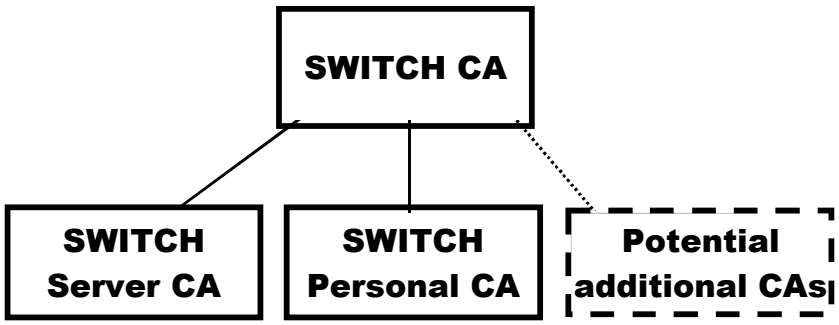
Table of Contents

1. INTRODUCTION

1.1 Overview

"SWITCH - The Swiss Education & Research Network" was established as a foundation by the Swiss Confederation and the university cantons. The Berne-based foundation has as its objective "to create, promote and offer the necessary basis for the effective use of modern methods of tele-computing in teaching and research in Switzerland, to be involved in and to support such methods". It is a non-profit foundation that does not pursue commercial aims.

SWITCH offers a broad variety of different services from domain name registration to network services to the Swiss education and research network. One of these services is the Authentication and Authorization Infrastructure (AAI) which is to simplify inter-organizational access to networked services. In order to provide this and other services SWITCH maintains a public key infrastructure (PKI) that is able to create certificates for: server/services and persons. SWITCH has outsourced the management of the CA infrastructure to SwissSign AG. Organizations that wish to operate their own CA infrastructure under this CP/CPS are to adhere to the minimum requirements described in this document. The following picture shows the current CA hierarchy.



Picture 1: CA hierarchy

This document is the combined Certificate Policy and Certification Practice Statement (CP/CPS) of the SWITCH PKI further referred to as “SWITCH CA” or “this CA” or “this CA and its subsidiary CAs” and includes one or more registration authorities (RA). It describes the set of procedures followed by this CA and is structured according to RFC 3647. No other documentations form part of this document and only the information provided in this document may be relied on.

1.2 Document name and identification

This document is named SWITCH Certificate Policy and Certification Practice Statement.

The version is 1, dated 01. January 2004.

The following ASN.1 Object Identifier (OID) has been assigned to this document: 2.16.756.1.2.6.1.0.3.

1.3 PKI participants

1.3.1 Certification authorities

This CA only issues certificates to subordinate CAs. Subordinate or Subsidiary CAs can be any of the following types:

- SWITCH Server CA: Certificate Authority that issues only server or service related certificates.
- SWITCH Personal CA: Certificate Authority that issues certificates to people.

1.3.2 Registration authorities

Registration for certificates issued by this CA or its subsidiaries is possible through registration authorities operated by SWITCH or its participating members (participants).

Third parties may operate their own registration authorities and authorize the issuance of certificates for the subsidiaries of this CA if they abide by all the rules and regulations of this CP/CPS. Any registration authority may choose to implement a more restrictive CP/CPS.

1.3.3 Subscribers

In the context of this CP/CPS the term “Subscribers” encompasses all end users of certificates issued by this CA or one of its subsidiary CAs:

- Requesters are individuals or organizations that have requested but not obtained a certificate.
- Subscribers are individuals, servers/services or organizations that have obtained a certificate.

1.3.4 Relying parties

Relying parties are individuals or organizations using the certificates to verify the identity of subscribers and to secure communication with this subscriber.

Relying parties may or may not be subscribers within this CA.

1.3.5 Other participants

Other participants are individuals or organizations that are using, or are in some form involved with manufacturing of, the certificates of a subscriber and may or may not wish to secure communication with this subscriber.

Other participants may or may not be subscribers within this CA.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

This CP/CPS is applicable to all the certificates issued by this CA or any of its subsidiaries.

Certificates issued by the “SWITCH Personal CA” are intended to be used by individuals in any application for client authentication, digital signature and data encryption purposes.

Certificates issued by the “SWITCH Server CA” are intended to be used by computer

systems for server authentication and server encryption services.

1.4.2. Prohibited certificate uses

Any certificate use is permissible only, if the limitations in the registration process and therefore the restrictions on the liability are accepted for the intended purpose. Applications should check the validity, purpose and liability of the certificates before accepting them for any transaction. Requesters are made aware and must acknowledge the limitations to use their certificates by signing the “End User Agreement” and the “certificate registration document”.

1.5 Policy administration

1.5.1 Organization administering the document

SWITCH - Teleinformatikdienste für Lehre und Forschung
Limmatquai 138
Policy Management Authority (PMA)
CH-8021 Zürich
Switzerland
Tel: +41 1 268 15 15
info@switch.ch
www.switch.ch

1.5.2 Contact person

Christoph Graf
christoph.graf@switch.ch
Tel: +41 (1) 268 15 37

1.5.3 Person determining CPS suitability for the policy

The PMA of SWITCH is responsible for reviewing and approving this CP/CPS.

1.5.4 CPS approval procedures

The PMA of SWITCH is responsible for reviewing and approving this CP/CPS such that it adheres to:

- the minimum requirements of the SwissSign Silver CA.
- RFC 3647
- Swiss law

1.6 Definitions and acronyms

Algorithm	A process for completing a task. An encryption algorithm is merely the process, usually a mathematical process, to encrypt and decrypt messages.
Authentication	Authentication is the process of identifying a user. Usernames and passwords are the most common method of authentication

Certificate	Information issued by a trusted third party. Often published in a directory with public access. Used to identify an individual or a system. Contains at least a subject, a unique serial number, an issuer and a validity period.
Certificate Authority	An internal entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certificate Extension	Optional fields in a certificate.
Certificate Policy	Rules that a request must comply with for the RA to approve the request or a CA to issue the certificate.
Certificate Revocation List	List of certificates that have been declared invalid. This list is issued by the CA at a regular interval and is used by applications to verify if a certificate is to be trusted.
Certification Practice Statement	Document that regulates rights and responsibilities of all the parties involved (RA, CA, directory service, end entity, relying party)
Certification Service Provider	Individual or corporation that issues certificates to individual or corporate third parties.
Cipher	A cryptographic algorithm used to encrypt and decrypt files and messages.
Cipher Text	Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key
CP	-> Certificate Policy
CPS	-> Certification Practice Statement
Credentials	Evidence or testimonials concerning the user's right to access certain systems (e.g. username, password, etc)
CRL	-> Certificate Revocation List
CSP	-> Certification Service Provider
Decryption	The process of transforming cipher text into readable text.
DES	Data Encryption Standard. A cipher developed by the United States government in the 1970s to be the official encryption algorithm of the U.S.
Digital signature	A system allowing people and organizations to electronically certify such features as their identity, their ability to pay, or the authenticity of an electronic document.
Distinguished Name	-> Subject
DN	-> Distinguished Name
DNS	Domain Name System. The Internet system of holding a distributed register of entity names. For example the domain is the part of the email address to the right of the `@', e.g. `anytown.ac.uk'.
Encryption	Encryption is the process of using a formula, called an encryption algorithm, to translate plain text into an incomprehensible cipher text for transmission.
Extension	Optional fields in a X509 Certificate.
FQDN	Fully Qualified Domain Name.

HTTP	Hyper-Text Transfer Protocol used by the Internet. HTTP defines how data is fetched or transmitted on the Internet and what actions should be taken by web servers and browsers.
HTTPS	Secure Hyper-Text Transfer Protocol using SSL
Key	The secret used as input for cryptographic algorithms during the transformation of a message. -> See Private Key, Public Key
Key password	Password used to encrypt the private key
Key size	Length of private and public key. Regular key sizes are 512, 768, 1024 2048 and 4096 with 1024 the most common key size today.
Key usage	Purpose for which the key is intended to be used. This information is stored in the certificate itself to allow application to verify that the key presented is also intended for this usage..
LDAP	Directory access protocol. Used to retrieve data from a public directory.
LDAPS	LDAP secured with SSL
OCSP	Online Certificate Status Protocol: method to verify in real-time if a certificate is valid.
Participants	Entities like CAs, RAs, and repositories. These can be different legal entities.
PKI	-> Public Key Infrastructure
Plaintext	The original message or file. After a file or message has been encrypted and then decrypted you should end up with the original file or message
PMA	The Policy Management Authority, established by SWITCH, consists of a minimum of three (3) persons responsible for defining the functioning of the SWITCH PKI by means of this CP/CPS
Privacy Level	Used to determine how the certificate is managed in the directory. Private, Public Lookup and Public Download are the available levels.
Private Key	One of two keys used in public key cryptography. The private key is known only to the owner and is used to sign and decrypt messages. The secret key of a public-private key cryptography system. This key is used to “sign” outgoing messages, and is used to decrypt incoming messages.
Profile	End users can optionally create a Profile which functions as a “container” for the end user certificates. The profile contains information, which helps the RA identify the end user in case of forgotten passwords or other service requests. A profile is an alternate method to authenticate end users, when, through the profile, end users access and manage their digital identities and their requests. The Profile is stored inside the CA infrastructure in encrypted form and can only be accessed by the owner and viewed by the appropriate RAO.
Public Key	One of two keys used in public key cryptography. The public key can be known to anyone and is used to verify signatures and encrypt messages. The public key of a public-private key cryptography system. This key is used to confirm “signatures” on incoming messages or to encrypt a file or message so that only the holder of the private key can decrypt the file or message.

Public Key Infrastructure	Processes and technologies used to issue and manage digital identities for the use of third parties to authenticate individuals. Abbrev. PKI.
Revocation	Invalidation of a certificate. Every CA regularly issues a list of revoked certificates called CRL. This list should be verified by all applications that use certificates from that CA before trusting a certificate.
Rollover	To rollover a certificate means that a new certificate is issued while the old is still valid and usable. This is used to issue a new CA certificate while keeping the old valid and all the certificates that were issued with it.
RSA	Public key encryption algorithm
S/MIME	Secure MIME
Signature	Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
SSL	Secure Sockets Layer. A protocol developed by Netscape that enables secure transactions via the Internet. URLs that require an SSL connection start with https: instead of http:.
SSO	Single Sign On. The user only needs to login once to access various services.
Subject	Field in the Certificate that identifies the owner of the certificate. Also referred to as distinguished name (DN). Examples: /CN=John Doe/O=SwissSign/OU=DEMO/C=CH/Email=john.doe@signdemo.com /CN=swiss.signdemo.com/O=SwissSign/OU=DEMO/C=CH/Email=root @signdemo.com Possible variables of the subject: Common Name --- /CN Email address --- /Email Organization --- /O= Organizational Unit --- /OU= Domain Component --- /DC= Country Name --- /C= Locality Name --- /L= Street Address --- /STREET Given Name --- /G Surname --- /S= Initials --- /I Unique Identifier --- /UID= Serial Number --- /SN= Title --- /T= Description --- /D=
Triple DES	A method of improving the strength of the DES algorithm by using it three times in sequence with different keys.
URL	Uniform Resource Locator. The global address of documents and other resources on the WWW, e.g. http://swisssign.com. The first part indicates the protocol to be used (http) and the second part shows the domain where the document is located.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CA and its subsidiary CAs will make its Certificate(s), CP, CPS, CRL and related documents for this CA publicly available through the SWITCH web site. In addition it will maintain an online accessible repository of certificate revocation information.

2.1 Repositories

A CA related website is maintained by SWITCH. It contains all the information published by this CA and its subsidiary CAs. The website can be reached at the following address: http://www.switch.ch/pki.

2.2 Publication of certification information

SWITCH operates a secure online repository that contains:

- all publicly accessible certificates issued by this CA
- the certificate revocation list (CRL) for this CA and its subsidiary Cas
- all past and current versions of the CP/CPS for this CA and its subsidiaries
- the end user agreement (EUA) for this CA and its subsidiaries
- pricing information for this CA and its subsidiaries

2.3 Time or frequency of publication

Directory services are updated once every hour. Any delay is a result of system and network performance limitations not entirely under the control of SWITCH.

New versions of CP/CPS are published as soon as they have been approved.

CRL of this CA is updated at least every 6 Months.

CRLs of this CA's subsidiary CAs are updated at least every 24 Hours.

2.4 Access controls on repositories

Directory services, CRL, CP, CPS and EUA of this CA and its subsidiary CAs are available to the public as read-only information from the SWITCH web site.

Modification of CRL and LDAP directory is fully automated and under the control of this CA and its subsidiary CAs.

Modification of CP, CPS and EUA is only permissible to SWITCH employees with proper authorization by the Policy Management Authority (PMA).

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

This CA supports multiple registration authorities with different registration processes. All of these registration authorities in order to become an authorized registration authority

must have a contractual agreement with SWITCH binding them to this CP/CPS and ensuring that the particular process of the registration authority meets the minimum requirements specified in this CP/CPS.

Using this procedure the RA ensures that:

- the identity of the individual is substantial enough for the transactions as intended in this CP/CPS
- a valid e-mail address is stored in the certificate
- authorized representatives approve the use of the name of the organization

3.1.1 Types of names

The subject name in certificates issued by this CA or its subsidiary CAs is an X.500 distinguished name.

For the distinguished name the following fields are required: /CN=, /O=, /C= and /Email=.

/OU= fields are optional.

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

- Real names are specified as /CN='Official name indication on the identifying document'
- Pseudonyms are specified as /CN=pseudo: ‘arbitrary string’
- Server names are specified as /CN='FQDN' (fully qualified domain name)

Names in the CN have to be identical to the names as they appear in the documentation provided. Abbreviations or nicknames are prohibited. Names consisting of multiple words are permissible.

A real name must be authorized with identifying information according to chapter 3.2.3.

The use of a pseudonym in the CN requires the name to start with the fixed string ‘pseudo: ‘. A pseudonym requires that the requester authorizes the request with identifying information according to chapter 3.2.3.

A server name must be specified as FQDN (fully qualified domain name, name entry of the server in the DNS system of the Internet). The use of an IP Address to identify a server is prohibited.

A server name must be authorized with identifying information according to chapter 3.2.2.

SubjectAltName is a mandatory field for certificates issued to individuals and contains an exact copy of the Email field of the subject. SubjectAltName is an optional field for servers and may contain a FQDN.

If an optional server name is entered in the SubjectAltName field, this name must be authorized with identifying information according to chapter 3.2.2.

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.

For a host/server certificate, the CN must be the fully qualified domain name registered in DNS.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers can be anonymous or pseudonymous, for this option subscribers have to start the /CN= with the fixed string ‘pseudo: ‘. A subscriber can use any string of characters after the fixed string ‘pseudo: ‘. SWITCH or its RAs reserve the right to reject certificate requests or revoke certificates containing offensive or misleading information. Anonymous or pseudonymous common names are available on a “first come, first served” basis. Chapter 3.1.6 applies.

3.1.4 Rules for interpreting various name forms

Many languages have special characters that are not supported by the ASCII character set used to define the subject in the certificate. To work around this problem local substitution rules can be used:

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

3.1.5 Uniqueness of names

The content of the subject field of valid certificates must be unique within the entire CA tree of the “SwissSign Root CA” and all its subsidiaries. Certificates can have non-unique subjects if there is disjunctive key usage.

A request for a subject that was already issued will be successful if:

- the subscriber with management access to the certificate issues the request. In this case the old certificate will be revoked and a new certificate will be issued.
- a registration authority issues the request. In this case the old certificate will be revoked and a new certificate will be issued.
- the second request has a different key usage than the first (dual keying). This works only with a signing certificate and the subscriber will then receive a separate certificate with key usage set to encryption.

3.1.6 Recognition, authentication, and role of trademarks

Names are being allocated on a “first come, first served” basis.

Should a certificate infringe the rights of a third party, the RA that issued the certificate with the contested content, will, presented with sufficient legal proof, attempt to rectify the situation within this CA and its subsidiaries at its own discretion.

SWITCH will always comply with any court orders issued in accordance with Swiss Law regarding remedies for any infringements of third party rights by certificates issued under this CPS.

3.2 Initial identity validation

The initial registration process with the SWITCH CA for certificates consists of the following steps:

- The requester registers a user account with the SWITCH RA web site.
- The requester requests a registration through the interface provided by the web site.
- The requester fills out the online form with the registration information.
- As supporting documentation the requester creates a high quality copy of a valid, official photo identity (student ID, driver's license, passport or national identity card).
- If the certificate is intended for a system, server or service, a printout of the WHOIS entry for the domain must be included. One of the contacts listed in the WHOIS entry must supply a high quality copy of an official photo identity (Student ID, driver's license, passport or national identity card) and authorize the request with a personal signature in the appropriate place on the registration form.
- The requester signs the registration form and sends the original together with the required supporting documentation by mail to the SWITCH RA.
- The requester provides documentation for the organizational or corporate name that should be included in the /O= field of the certificate (e.g. excerpt from the Federal Commercial Registry Office). The wording of the organizational or corporate name that should be included in the certificate needs to be identical to the wording in the documentation provided.
- If the documentation does not identify the person applying for the organization or corporation as a legal representative for that legal entity, such a legal representative must authorize the request by supplying a high quality copy of an official photo identity (student ID, driver's license, passport or national identity card) and authorize the request with a personal signature in the appropriate place on the registration form.
- If all the documentation is available and correct the SWITCH RA approves the creation of the digital identity and issues the CSR to one of the subsidiaries of this CA.
- The subsidiary CA issues the certificate and uses the e-mail address in the profile to inform the requester that the certificate has been created.
- Using the user account the requester can login and download the certificate
- The initial registration process for Registration Authorities other than the SWITCH RA for certificates must meet the following requirements:
- The RA process must be described and published to the parties involved.
- The identification of the requester must be of at least equal quality to that of the SWICH RA. This specifically includes the situation where the RA has an existing contractual relationship with the requester E.g. the requester is an existing student, customer, supplier or employee of the RA.

- The documentation retained must be of at least equal quality to that of the SWITCH RA. This specifically includes the situation where the RA already maintains up to date electronic data about the existing contractual relationship. E.g. customer/supplier database or human resources information or student database. Such information may be used to automatically generate and approve certificate signing requests.

3.2.1 Method to prove possession of private key

Possession of the private key is verified for certificates issued by this CA or any of its subsidiaries by any of the following methods:

- generating the key pair for the requester
- verifying the digital signature on the CSR (certificate signing request) if the requester has generated the key pair.

3.2.2 Authentication of organization identity

The DN of a certificate issued by one of the subsidiaries of this CA must contain one instance of the organization field. The following rules must be adhered to:

- The use of the organization field makes the use of the country field mandatory.
- The registration process of any registration authority operating under this CPS must contain provisions to determine the identity of an organization and to authorize the use of its name.
- The requester must provide legal documentation about the organization (e.g. excerpt from the Commercial Registry Office).
- The use of the organizations name must be authorized by one or more legal representatives (as indicated on the excerpt) of the organization with personal signatures on the registration form. - The legal representative must provide proof of identity according to chapter 3.2.3

3.2.3 Authentication of individual identity

Various individuals may need to authorize the use of names in different parts of the DN. The registration process of any registration authority operating under this CP/CPS must contain provisions to determine the identity of such individuals. To achieve this goal, the following rules must be adhered to:

- The identity of a person is documented with a high-quality copy of a legal photo ID (student ID, driver’s license, national passport or national identity card).
- The authorization is acceptable if both name and signature on the identifying document match both name and signature on the registration form. The wording in the request has to be identical to the first name and the family name of the requester.
- Documentation must be provided on paper or a high quality scan (for email delivery) and the registration form must carry original, personal signatures only.

3.2.4 Non-verified subscriber information

The information in the OU (Organizational Unit) field and the email address are not necessarily verified.

3.2.5 Validation of authority

The requester provides documentation for the organizational name that should be included in the certificate (e.g. excerpt from the Federal Commercial Registry Office). The wording of the organizational name that should be included in the certificate needs to be identical to the wording in the documentation provided. If the documentation does not identify the person applying for the organization as a legal representative for that legal entity, such a legal representative must authorize the request by supplying a high quality copy of an official photo identity as per chapter 3.2.3 and authorize the request with a personal signature in the appropriate place on the registration form.

3.2.6 Criteria for interoperation

This CA and its subsidiaries support multiple registration authorities (RAs) with different registration processes. SWITCH does not support cross-certification. In order to become an authorized registration authority, the registration authority must sign a contractual agreement with SWITCH binding them to this CP/CPS and ensuring that the registration process of the registration authority meets the minimum requirements specified in this CP/CPS.

The initial registration process of the SWITCH RA consists of the following steps:

- The requester creates a profile on the SWITCH web site or on the web site of any SWITCH RA.
- The requester requests a certificate through the certificate management interface provided by the web site.
- The requester creates copies of the required supporting documentation.
- The requester and all other individuals required to authorize parts of the request sign the registration form in the appropriate places and send it together with the required supporting documentation to the SWITCH RA.
- The requester pays the fee (if applicable).

The initial registration process for Registrations Authorities other than the SWITCH RA must meet the following minimum requirements:

- The RA must have a contractual agreement with SWITCH to be authorized for the role as RA.
- The RA process must be described and published to the parties involved in the RA process.
- The identification of the requester must be of equal quality as the initial registration process of the SWITCH RA or better.
- The documentation retained must be of equal quality or better.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

To renew a certificate issued by a SWITCH RA by re-keying, the subscriber must:

- If a profile was used to request the certificate, login to the profile
- prove ownership of the private key

The renewal by re-keying process of registration authorities other than the SWITCH RA must meet the following requirement:

- subscriber identification and authentication must be the of the same quality as the SWITCH process, or better.

3.3.2 Identification and authentication for re-key after revocation

To renew by re-keying a certificate issued by a SWITCH RA after its revocation, the subscriber must issue a new certificate signing request. To authorize this request, the subscriber must:

- Supply a registration form carrying the original, personal signatures of the same individuals that signed the initial registration form. In this case the identifying documentation is optional.

or, if one or more signatories need to be changed:

- Re-apply for a certificate as if no certificate had ever been issued.

The renewal by re-keying process of registration authorities other than a SWITCH RA must meet the following requirements:

- The process must be of the same quality as a SWITCH RA process, or better.

3.4 Identification and authentication for revocation request

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

- Successful authentication to the profile allows access to the certificate revocation function for all certificates requested with this profile.
- Providing proof of private key possession on the RA web site allows access to the certificate revocation function for this particular private key.
- A process provided on the RA web site.

The revocation process of registration authorities other than the SWITCH RA must meet the following requirements:

- The process must be of the same quality as the SWITCH RA process, or better.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The SWITCH RA's initial registration process is a process open to the Swiss educational and research community and SWITCH's customers. Selected employees and/or students of the educational and research community or the customers may be allowed to register a profile and submit a certificate signing request.

Registrations Authorities other than SWITCH may limit the population of profiles and/or certificate requesters to a certain group. It is up to this RA to publish this to all those concerned. (An example could be, a university registering only its own staff but not its students.)

4.1.2 Enrollment process and responsibilities

Enrollment process used by subscribers and requesters to submit certificate applications:

- The requester creates a profile on the website of the appropriate RA.
- The requester requests a certificate through the certificate management interface provided by the web site.
- The requester creates copies of the required supporting documentation.
- The requester and all other individuals required to authorize parts of the request sign the registration form in the appropriate places and send it together with the required supporting documentation to the appropriate RA.
- The requester pays the fee (if applicable).

Subscribers and requesters responsibilities:

- have a basic understanding of the proper use of public key cryptography and certificates;
- provide to SWITCH and to any third party registration authority only correct information without errors, omissions or misrepresentations;
- substantiate information by providing a copy of the properly filled out and personally signed application form;
- supplementing such information by proving the identity through providing identifying information as specified in the registration process described in chapter 3.1;
- generate a new, secure, and cryptographically sound Key Pair or have one generated by an appropriate method;
- read and agree to all terms and conditions of this CP/CPS;
- maintain their certificates using the tools provided by the RA;
- decide during the creation process of a certificate, whether such certificate will be

published in the public directory;

- use SWITCH certificates exclusively for legal and authorized intended purposes;
- only use a SWITCH certificate on behalf of the person, entity, or organization listed as the Subject of such certificate;
- protect the private key from unauthorized access;
- notify the registration authority of any change to any information included in the certificate or any change in any circumstances that would make the information in the certificate misleading or inaccurate;
- immediately cease to use the certificate if any information included in the certificate or if any change in any circumstances would make the information in the certificate misleading or inaccurate;
- notify the registration authority immediately of any suspected or actual compromise of the private key and request the revocation of the certificate;
- immediately cease to use the certificate upon (a) expiration or revocation of such certificate, or (b) any suspected or actual compromise of the private key corresponding to the public key in such certificate, and remove such certificate from the devices and/or software in which it has been installed;
- refrain from using the subscriber's private key corresponding to the public key certificate to sign other certificates;
- use 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;
- comply 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.

4.2 Certificate application processing

The SWITCH RA will approve a certificate signing request (CSR), if the following criteria are met:

- all documentation has been received and verified successfully
- all authorizations have been received and verified successfully
- payment has been received (if applicable)

Once the CSR has been approved, the proper CA will issue the certificate.

Registration authorities other than the SWITCH RA may have different criteria as long as the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.2.1 Performing identification and authentication functions

The SWITCH RA will identify the requester based upon the identifying documents the requester presents as stipulated in chapter 3.2 of this document.

Registration authorities other than the SWITCH RA may have different criteria as long as the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.2.2 Approval or rejection of certificate applications

The SWITCH RA will approve a certificate signing request (CSR), if the following criteria are met:

- all documentation has been received and verified successfully
- all authorizations have been received and verified successfully
- payment has been received (if applicable)

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

Registration authorities other than the SWITCH RA may have different criteria as long as the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.2.3 Time to process certificate applications

The SWITCH RA will approve a certificate signing request (CSR) without delay as soon as:

- all documentation has been received and verified successfully
- all authorizations have been received and verified successfully
- payment has been received (if applicable)

A request remains active as stipulated per RA. If the requester fails to submit the supporting documents to the RA within this time frame, the certificate request may be cancelled or rejected.

Registration authorities other than the SWITCH RA may have different criteria as long as the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate signing requests (CSR) are made by an RA to the CA on behalf of the requester. The CA verifies the RA signature to determine validity, authority and possible RA dependent other factors and then generate the requested certificate. All steps of this process are logged according to applicable laws.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA may notify the requester in different ways.

- e-mail the certificate directly to the subscriber

- e-mail the certificate directly to the requesting RA
- e-mail information permitting the subscriber to download the certificate from a web site or repository
- e-mail information permitting the RA to download the certificate from a web site or repository
- The CA may perform another action allowing the subscriber or the RA access to the certificate under the condition that this process is described by the RA and made available to those parties involved.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The CA uses the e-mail address specified in the profile to inform the requester about the successful issuance of the certificate. The requester accepts the certificate by:

- downloading the certificate and
- using a SWITCH certificate exclusively for legal and authorized intended purposes.

Other RAs must use certificate distribution mechanisms, where the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.4.2 Publication of the certificate by the CA

If the requester decides, during the creation process of a certificate, that such certificate may be published in the public directory, the SWITCH CA will do so and additionally publish the certificate on the SWITCH website.

4.4.3 Notification of certificate issuance by the CA to other entities

The CA will notify the requester and may notify the RA as well that the certificate has been issued.

Other RAs may implement other certificate issuance notification processes, where the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers and requesters shall:

- be held responsible to have a basic understanding of the proper use of public key cryptography and certificates;
- provide to SWITCH and to any third party registration authority only correct information without errors, omissions or misrepresentations;
- substantiate information by providing a copy of the properly filled out and personally signed application form;

- supplementing such information by proving the identity through providing identifying information as specified in the registration process described in chapter 3.1;
- generate a new, secure, and cryptographically sound Key Pair or have one generated by an appropriate method;
- read and agree to all terms and conditions of this CP/CPS;
- maintain their certificates using the tools provided by the RA;
- decide during the creation process of a certificate, whether such certificate will be published in the public directory;
- use SWITCH certificates exclusively for intended, legal and authorized purposes;
- only use a SWITCH certificate on behalf of the person, entity, or organization listed as the Subject of such a certificate;
- protect the private key from unauthorized access;
- notify the registration authority of any change to any information included in the certificate or any change in any circumstances that would make the information in the certificate misleading or inaccurate;
- immediately cease to use the certificate if any information included in the certificate or if any change in any circumstances would make the information in the certificate misleading or inaccurate;
- notify the registration authority immediately of any suspected or actual compromise of the private key and request the revocation of the certificate;
- immediately cease to use the certificate upon (a) expiration or revocation of such certificate, or (b) any suspected or actual compromise of the private key corresponding to the public key in such certificate, and remove such certificate from the devices and/or software in which it has been installed;
- refrain from using the subscriber's private key corresponding to the public key certificate to sign other certificates;
- use 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;
- comply 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.

4.5.2 Relying party public key and certificate usage

Relying parties shall:

- be held responsible to understand the proper use of public key cryptography and certificates;

- read and agree to all terms and conditions of this CP/CPS;
- verify certificates issued by this CA, including use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:1997 | ISO/IEC 9594-8 (1997), taking into account any critical extensions, key usage, and approved technical corrigenda as appropriate;
- trust and make use of a certificate issued by this CA only if such certificate has not expired, been suspended or been revoked and if a proper chain of trust can be established to a trustworthy issuing party;
- make their own judgment and rely on a certificate issued by this CA only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a certificate issued by this CA and the value of any transaction that may involve the use of the aforementioned certificates;
- 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 means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate. Due to loss of entropy while using the key, SWITCH strongly advices against this practise and thus does not support it.

4.6.1 Circumstance for certificate renewal

SWITCH does not support renewal as defined in chapter 4.6.

4.6.2 Who may request renewal

SWITCH does not support renewal as defined in chapter 4.6.

4.6.3 Processing certificate renewal requests

SWITCH does not support renewal as defined in chapter 4.6.

4.6.4 Notification of new certificate issuance to subscriber

SWITCH does not support renewal as defined in chapter 4.6.

4.6.5 Conduct constituting acceptance of a renewal certificate

SWITCH does not support renewal as defined in chapter 4.6.

4.6.6 Publication of the renewal certificate by the CA

SWITCH does not support renewal as defined in chapter 4.6.

4.6.7 Notification of certificate issuance by the CA to other entities

SWITCH does not support renewal as defined in chapter 4.6.

4.7 Certificate re-key

Re-keying a certificate is the process where a subscriber or other participant generates a new key pair and applies for the issuance of a new certificate that certifies the new public key. SWITCH may refer to this process as “renew by re-keying” or “renewing by re-keying”.

4.7.1 Circumstance for certificate re-key

To re-key a certificate issued by the SWITCH RA, the subscriber must

- If a profile was used to request the certificate, login to the profile
- prove ownership of the private key

The re-keying process of registration authorities other than the SWITCH RA must meet the following requirement:

- subscriber identification and authentication must be the of the same quality as the SWITCH process, or better.

4.7.2 Who may request certification of a new public key

Certificate renewal by re-keying is permitted to anyone who can

- If a profile was used to request the certificate, login to the profile
- prove ownership of the private key

4.7.3 Processing certificate re-keying requests

The processing of re-keying requests is similar to the initial certificate issuance. The main exception is: documentation which is valid and present at the RA (for the former certificate) does not need to be represented when requesting a new certificate through re-keying.

4.7.4 Notification of new certificate issuance to subscriber

The CA may notify the requester in different ways.

- e-mail the certificate directly to the subscriber and/or the requesting RA
- e-mail information permitting the subscriber and/or the requesting RA to download the certificate from a web site or repository
- The CA may perform another action allowing the subscriber or the RA access to the certificate under the condition that this process is described by the RA and made available to those parties involved.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The CA uses the e-mail address specified in the profile to inform the requester about the successful issuance of the certificate. The requester accepts the certificate by:

- downloading the certificate and
- using a SWITCH certificate exclusively for legal and authorized intended purposes.

Other RAs use certificate distribution mechanisms, where the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.7.6 Publication of the re-keyed certificate by the CA

If the requester decides, during the creation process of a certificate, that such certificate may be published in the public directory, the SWITCH CA will do so and additionally publish the certificate on the SWITCH website.

4.7.7 Notification of certificate issuance by the CA to other entities

The CA may notify the RA as well as the requester that the certificate has been issued

Other RAs may implement other certificate issuance notification processes, where the quality of the process is the same as, or better than, the process for the SWITCH RA.

4.8 Certificate modification

Certificate modification is the process where a subscriber or other participant generates a new key pair and applies for the issuance of a new certificate using a certificate signing request which includes new information that certifies this new public key. Thus, this is a new certificate request.

See Chapter 4.1

4.8.1 Circumstance for certificate modification

See Chapter 4.1

4.8.2 Who may request certificate modification

See Chapter 4.1

4.8.3 Processing certificate modification requests

See Chapter 4.1

4.8.4 Notification of new certificate issuance to subscriber

See Chapter 4.1

4.8.5 Conduct constituting acceptance of modified certificate

See Chapter 4.1

4.8.6 Publication of the modified certificate by the CA

See Chapter 4.1

4.8.7 Notification of certificate issuance by the CA to other entities

See Chapter 4.1

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A subscriber may revoke a certificate issued by this CA or any of its subsidiaries at will.

The SWITCH RA or an authorized RA shall revoke a subscriber's certificate if one of the following conditions is met:

- The private key of the CA or any of its superior CAs has been compromised.
- The private key store (= cryptographic token) is lost.
- The certificate subject is no longer valid (ex: name change, employer change)
- The subscriber does not comply with the terms and conditions of this CP/CPS.
- The certificate was not issued in compliance with the terms and conditions of this CP/CPS.

Registration authorities other then the SWITCH RA may specify additional reasons for certificate revocation, if they are properly documented.

4.9.2 Who can request revocation

All subsidiaries of this CA will accept certificate revocation requests from the following

- the owner of the profile that was used to issue the initial registration request
- the owner of the private key
- a properly authorized registration authority
- a CA operator

4.9.3 Procedure for revocation request

Using the profile that was used to issue the initial registration request, the subscriber can use the ID management functions to revoke an active certificate.

The private key owner can use an SSL session with strong authentication to instantly revoke a certificate.

Properly authorized registration authorities can revoke certificates according to their documented processes.

4.9.4 Revocation request grace period

All revocation requests shall be processed and executed without delay.

4.9.5 Time within which CA must process the revocation request

The SWITCH RA will process a certificate revocation request without delay.

4.9.6 Revocation checking requirement for relying parties

Relying parties must, when working with certificates issued by this CA, at all times verify these certificates. This includes the use of CRLs, in accordance with the certification path

validation procedure specified in ITU-T Rec. X.509:1997 | ISO/IEC 9594-8 (1997) and includes taking into account any and all critical extensions, key usage, and approved technical corrigenda as appropriate.

Relying parties must make their own judgment and rely on a certificate issued by this CA only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a certificate issued by this CA and the value of any transaction that may involve the use of the aforementioned certificates.

Relying parties must 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.

4.9.7 CRL issuance frequency (if applicable)

The CRL of this CA and of every subsidiary CA is updated at least every 24 hours.

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

The CRL may be searched by subject and downloaded from the online directory.

Additionally, the status of public certificates may be checked through the SWITCH website.

4.9.10 On-line revocation checking requirements

This CA and all its subsidiaries do not yet support the OCSP protocol for on-line revocation checking but may do so in the future.

Relying parties must, when working with certificates issued by this CA, at all times verify certificates issued by this CA. This includes the use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:1997 | ISO/IEC 9594-8 (1997) and may include OCSP in the future.

4.9.11 Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

4.9.12 Special requirements re key compromise

If a subscriber knows or suspects the compromise of the private key for his certificate, the subscriber shall:

- immediately stop using the certificate
- immediately initiate the 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

A subscriber can not suspend a certificate issued by this CA or any of its subsidiaries.

The SwissSign RA or an authorized RA may suspend a subscriber's certificate if one of the following conditions is met:

- The subscriber does not comply with the terms and conditions of this CP/CPS.
- The certificate is not in compliance with the terms and conditions of this CP/CPS.

Registration authorities other then the SWITCH RA may specify additional reasons for certificate suspension, if they are properly documented.

4.9.14 Who can request suspension

This CA or any of its subsidiaries will accept certificate suspension requests only from the CAO or the RAO.

4.9.15 Procedure for suspension request

Properly authorized registration authorities can suspend certificates using the RA management interface.

4.9.16 Limits on suspension period

Certificates may remain suspended for an unlimited period of time.

4.10 Certificate status services

4.10.1 Operational characteristics

The SWITCH certificate services can be reached 24x7 through the SWITCH web site and the online directory.

The status of public certificates may be checked through the SWITCH website by means of the CRL.

4.10.2 Service availability

SWITCH provides all services (registration, certification, directory) as 24x7 services without scheduled interruption. Due to the nature of the internet, SWITCH is in no position to guarantee such services and customers acknowledge that unscheduled interruptions are possible due to circumstances not under the control of SWITCH.

4.10.3 Optional features

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

4.11 End of subscription

End of subscription occurs 10 Years after:

- The successful revocation of the last certificate of a subscriber
- The expiration of the last certificate of the subscriber

For legal compliance reasons, the SWITCH CA and SWITCH, or other, RAs keep all subscriber data and documentation for a period of at least 10 years.

4.12 Key escrow and recovery

This CA and its subsidiaries do not support private key escrow.

An RA may wish to implement key escrow and recovery functionality.

4.12.1 Key escrow and recovery policy and practices

This CA and its subsidiaries do not support private key escrow.

An RA may wish to implement key escrow and recovery functionality.

4.12.2 Session key encapsulation and recovery policy and practices

This CA and its subsidiaries do not support private key escrow.

An RA may wish to implement key escrow and recovery functionality.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

SWITCH is responsible for registration services as described in this CP/CPS.

All other PKI related services are outsourced to SwissSign AG. The requirements SWITCH has of the quality of these services are described in this CP/CPS.

5.1 Physical controls

The SWITCH CA key is stored off-line in a Swiss bank safety deposit.

The SWITCH CA subsidiary servers are located in private data centers with access control by SwissSign AG.

5.1.1 Site location and construction

The sites are located in data centers in the greater Zurich area in Switzerland.

5.1.2 Physical access

Physical access is only granted to system administrators and restricted data center personnel.

5.1.3 Power and air conditioning

Data centers are properly air-conditioned. Power relies on the local power supplier.

5.1.4 Water exposures

No special exposures.

5.1.5 Fire prevention and protection

No special actions taken.

5.1.6 Media storage

This CA and its subsidiaries have been designed as distributed systems over multiple locations to make the requirement for traditional off-site media storage obsolete.

5.1.7 Waste disposal

Defective hardware and/or documentation to be disposed of are destroyed according to common privacy and IT security practices.

5.1.8 Off-site backup

This CA and its subsidiaries have been designed as distributed systems over multiple locations to make the requirement for traditional off-site backup obsolete.

5.2 Procedural controls

5.2.1 Trusted roles

CA System Administrators (SA) have full control over the CA server and software, but not over the cryptographic relevant information like the private key of the CA.

Certificate authority operators (CAO) can manage all certificates, request, profiles and a subset of certificate authorities described by the operator access rules.

Network Administrators (NA) have full control over the network access to all the server systems of this CA.

Auditors have read-only access to all components of the PKI to verify that the operation complies with the rules and regulations of this CP/CPS.

Registration authority operators (RAO) can manage a subset of certificates and requests described by the RA policies and the operator access rules.

5.2.2 Number of persons required per task

The operation of this CA and it subsidiaries requires at least:

- Two SA due to the high availability requirements
- Three CAO due to the high availability requirements and to implement dual controls for the access to the cryptographic secrets.
- Two NA due to the high availability requirements
- No RAO

If the personnel situation does not allow roles to be segregated properly, it is permissible to use dual controls on the roles of SA or NA for two individuals that already have a trusted role in the organization. Similarly it is permissible to have one person as CAO together with one other person (CEO, CTO, CIO, CSO) who knows, or has access to, the cryptographic secrets to guarantee the separation of duties.

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 safety deposit) requires national pass and facial identification.

5.2.4 Roles requiring separation of duties

CA System Administrators (SA) have full control over the CA server and software, but not over the cryptographic relevant information like the private key of the CA. An SA may not be an CAO, NA, or auditor.

Certificate authority operators (CAO) can manage all certificates, request, profiles and a subset of certificate authorities described by the operator access rules but may not configure the CA or be an SA.

Network Administrators (NA) have full control over the network access to all the server systems of the PKI and may not be SA, CAO or auditor.

Auditors have read-only access to all components of the PKI to verify that the operation complies with the rules and regulations of this CP/CPS. An auditor may not be an SA, CAO or NA.

Registration authority operators (RAO) can manage a subset of certificates and requests described by the RA policies and the operator access rules. An RAO may not be an SA, CAO or NA.

5.3 Personnel controls

SWITCH requirements to the quality of:

- roles not performed or under the control of SWITCH are described in subchapters of 5.3
- RAO roles are described in subchapters of 5.3

5.3.1 Qualifications, experience, and clearance requirements

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

To fill the role of SA an employee must proof a very good understanding of the Unix operating system, TCP/IP networking and relational databases.

To fill the role of CAO an employee must proof a very good understanding of PKI technology and applications using PKI.

To fill the role of NA an employee must proof a very good understanding of TCP/IP networking and of the Unix operating system.

To fill the role of RAO an employee must proof very good people skills and a good understanding of PKI processes.

All SwissSign AG employees must show a very good understanding of security in general and IT security in particular.

5.3.2 Background check procedures

SwissSign AG verifies the background of its employees and ensures that no criminal record exists.

RAs verify the background of their RAOs and ensure that no criminal record exists.

5.3.3 Training requirements

Employees must provide proof that they have obtained the skills required for their position within the PKI. Any lack or shortcoming will be addressed and alleviated though proper training.

5.3.4 Retraining frequency and requirements

Retraining of employees is done case by case depending on need of the organization or need of the individual.

5.3.5 Job rotation frequency and sequence

Job rotation of employees is done case by case depending on a need of the organization or the request of the individual employee.

5.3.6 Sanctions for unauthorized actions

SwissSign AG and SWITCH reserve the rights to prosecute unauthorized actions to the fullest extent of applicable Swiss laws.

5.3.7 Independent contractor requirements

Above and beyond regular documentation, contractors must:

- Sign a non-disclosure agreement protecting any and all information of users of this CA and all its subsidiaries.
- Proof that no criminal record exist.

5.3.8 Documentation supplied to personnel

No Special requirements apply.

5.4 Audit logging procedures

All major events in this CA or any of its subsidiaries are being logged and are available for audit.

5.4.1 Types of events recorded

The following, non conclusive, list of events are recorded in the CA log:

- New certificate requests
- Rejected certificate requests
- Account Violations
- Key Upload/Download
- Certificate Signing
- Certificate Revocation
- User account logon

- CRL signing
- CA rollover
- Certificate Expiration
- Certificate Downloads/Installation

The above list of logging activity is limited to events that are directly related to certificate management functions.

5.4.2 Frequency of processing log

Logs must be processed on a monthly basis.

5.4.3 Retention period for audit log

Audit logs must be kept for at least 12 months.

5.4.4 Protection of audit log

Audit logs are only accessible to the CAO of this CA or any of its subsidiaries and to authorized audit personnel.

5.4.5 Audit log backup procedures

Audit logs are being stored at multiple locations under the control of SwissSign AG.

5.4.6 Audit collection system (internal vs. external)

No stipulations

5.4.7 Notification to event-causing subject

Depending on the severity of the log entry, SwissSign 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 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 this CA and its subsidiaries produced
- registration information of end entities

5.5.2 Retention period for archive

Archived information is kept at least 10 years.

5.5.3 Protection of archive

Archived information is only accessible to the appropriate administrators of this PKI.

5.5.4 Archive backup procedures

Archived information is not stored in the data center.

5.5.5 Requirements for time-stamping of records

All certificates and certificate related entries in the CA database are timestamped.

5.5.6 Archive collection system (internal or external)

This CA and all its subsidiaries use a SwissSign internal archiving system.

RAs are to archive their data according to applicable Swiss law.

5.5.7 Procedures to obtain and verify archive information

In case 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 by the court the high quality copy is destroyed. This process is logged.

5.6 Key changeover

Not applicable for this CA and its subsidiaries. SWITCH CAs roll over their keys/certificates with overlapping validities to ensure that no subscriber certificate re-key is needed.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In case of a CA key compromise, the CA certificate will be revoked and a new key pair will be generated. The superior CA will sign a new certificate for this CA. When the CA certificate is revoked, all certificates signed directly or indirectly are invalid.

This CA and its subsidiaries are implemented using multiple CA servers concurrently, which are kept synchronous online. If one system fails, the remaining server takes over the full functionality.

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 all functionality.

SwissSign AG is the owner of the source code of the SWITCH CA with the exception of some freely available code. Any errors in the source code will be addressed and fixed immediately.

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

5.7.3 Entity private key compromise procedures

If the private key of the “SwissSign Root CA” or one of its subsidiaries (including the SWITCH CA) is suspected to be compromised, the executive board of SwissSign AG must be informed immediately. The following steps will be taken:

- revoke the CA certificate
- All subscribers with certificates issued by either the revoked CA or one of its subsidiaries will be informed through E-mail as soon as possible.
- All subscriber certificates will be revoked and new CRLs will be issued.
- determine the cause of the key compromise and correct the situation
- replace all newly revoked certificates
- The revoked CA will generate a new key pair and have the resulting certificate request signed by the superior CA.
- The new CA certificate will be published on the appropriate web site.
- issue new CRL’s

Using their profile subscribers can login to the appropriate RA and request new certificates for existing subjects without resubmitting registration information if such information is available and valid at the RA.

5.7.4 Business continuity capabilities after a disaster

In the case of a disaster whereby the SWITCH CA installation is physically damaged and all copies of the CA signature keys are destroyed as a result, the PMA will inform SwissSign AG and take whatever action it deems appropriate in cooperation with SwissSign AG.

In case of a disaster in the SwissSign data centers, the executive board 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. In the meantime, the service will continue to be provided by the fully redundant equipment in the remaining locations.

5.8 CA or RA termination

If this CA or its subsidiary CAs cease operation, all the certificates issued will be revoked immediately.

RA termination will be subject to negotiations with other equivalent RAs. Another RA may offer the subscribers of the terminating RA to take over the RA function.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The “SWITCH CA” private key is stored in an off-line HSM with a different PIN and was used to sign the subsidiary CA key pairs.

The key pair for the subsidiaries of this CA have been created by the respective CA and are stored in a HSM module that meets at least FIPS 140-1 level 3 requirements.

The subscriber key pair generation is optionally performed by this CA, an application under the sole control of the subscriber, or a certificate storage device (ex. Smart Card, USB Token).

6.1.2 Private key delivery to subscriber

If the private key is generated by the CA, the CA notifies the subscriber by email that the certificate (as well as the private key) is available in the subscriber profile for download in PKCS#12 format. In the case of browser, server or certificate storage device generated key pairs or if the key pair is imported from an external source, no delivery mechanism is required.

A non-SWITCH RA may stipulate a different private key delivery process, where the quality of this process is equal or better than the SWITCH process.

6.1.3 Public key delivery to certificate issuer

The RA presents the public key of the requester as a PKCS#10 formatted request to the signing CA using a communication channel which is secured using SSL encryption with strong authentication of the RAO.

If online generated keys are used, 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 website using the PKCS#7 format.

The issuing CA public key is delivered as a PKCS#12 or PKCS#7 file with the complete chain of certificates that include the public keys thus providing the trust validation tree.

6.1.5 Key sizes

This CA uses a 2048 bit RSA key.

This CA’s subsidiary CAs use 2048 bit RSA keys.

6.1.6 Public key parameters generation and quality checking

The key pairs of this CA's subsidiaries have been created using at least a FIPS140-1 level 3 certified HSM.

For online generated keys, any SWITCH CA uses standard parameters.

No stipulations can be made about the quality of the parameters for other key pairs.

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 bits set.

Subscribers can obtain, through the RA web site, certificates that may have one or more of the following key usage bits included:

- digitalSignature
- nonRepudiation
- keyAgreement
- keyEncipherment
- DataEncipherment

Extended Key Usage may include:

- secureEmail
- clientAuthentication
- codeSigning
- Microsoft Smart Card Logon

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The HSM used for CA keys meets at least FIPS 140-1 level 3 requirements.

Access to the SwissSign and SWITCH CA cryptographic modules is possible only with certificates that have to be generated on the smart card or token.

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

This CA and its subsidiaries do not yet support private key (n out of m) multi person control.

6.2.3 Private key escrow

This CA and its subsidiaries do not support private key escrow.

An RA may wish to implement key escrow and recovery functionality.

6.2.4 Private key backup

The private keys of this CA and all its subsidiaries are stored in the HSM module and cannot be exported from the module. In case of key corruption, the private key/certificate is rolled over with new keying material.

Subscribers that chose online generated keys always have a backup copy of their key stored in the CA database. This key can be downloaded using profile authentication as a “pass phrase protected” PKCS#12 file.

The SwissSign CA database is part of the daily backup schedule.

6.2.5 Private key archival

The CA Key is not archived.

Subscribers may have a backup copy of their key stored in the CA database. Using profile authentication this key can be downloaded as a “pass phrase protected” PKCS#12 file.

The SwissSign CA database is archived at regular intervals.

6.2.6 Private key transfer into or from a cryptographic module

The private keys of this CA and all its subsidiaries have been generated in the cryptographic module and can not be transferred into or from a cryptographic module.

6.2.7 Private key storage on cryptographic module

The private keys of this CA and all its subsidiaries have been generated in the cryptographic module.

6.2.8 Method of activating private key

The private key of this CA is activated at startup to be available at any time if a particular action requires access to this key.

The private keys of the subsidiaries of this CA are activated during the startup process of the CA application. A CA Operator must enter the PIN code of the HSM to establish a successful connection to the HSM.

6.2.9 Method of deactivating private key

The private keys of the subsidiaries of this CA are deactivated during the shutdown process of the CA application when the connection to the HSM module is closed by the SA.

6.2.10 Method of destroying private key

The private keys of this CA and all its subsidiaries are deleted by initializing the key storage slot in the HSM by the CAO.

6.2.11 Cryptographic Module Rating

The HSM used for subsidiary CA keys meets at least FIPS 140-1 level 3 requirements.

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 online, distributed to all servers in the CA cluster and backed up with the normal data backup of each CA.

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 Root CA” certificate is valid for 30 years and is renewed every 15 years.

- This CA's certificate is valid between 762 days (2 years + 1 month) to a maximum of 12 years and goes through a rollover every two years.
- The certificates of the subsidiaries of this CA are valid between 762 days (2 years + 1 month) to a maximum of 12 years and goes through a rollover every year.
- End entity certificates are valid between 365 - 397 days (1 year to 1 year + 1 month)

6.4 Activation data

Starting the HSM requires the entry of a PIN which is under the control of the SwissSign CAO.

6.4.1 Activation data generation and installation

Not applicable

6.4.2 Activation data protection

Not applicable

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 all traffic except the essential. Additionally the CA systems themselves are hardened and have a high security operating system installed. Access to the system for system administrators is granted only over secure and restricted protocols using public key authentication.

6.5.1 Specific computer security technical requirements

Not applicable

6.5.2 Computer security rating

Not applicable

6.6 Life cycle technical controls

6.6.1 System development controls

The SWITCH CA uses SwissSign software. To ensure quality and availability of the SwissSign AG software, the SwissSign 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 is in place with separate Development, Test and

Production environments.

6.6.2 Security management controls

The PK infrastructure checks itself constantly to ensure that the operational systems and networks adhere to the configured security using several tools.

6.6.3 Life cycle security controls

Not applicable

6.7 Network security controls

Network security is ensured using firewalls, virus scanners and intrusion detection systems.

6.8 Time-stamping

All certificates and certificate related entries in the CA database are timestamped based on the network time of several time servers available through the internet.

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 Part 1.

7.1.1 Version number(s)

Version of X.509 certificates: version 3

7.1.2 Certificate extensions

- authorityKeyIdentifier: Contains the key identifier of the issuing CA's public key (SHA1).
- subjectKeyIdentifier: Used for CA certificates only
- KeyUsage*: As specified in the section 6.1.7 "Key usage purposes (as per X.509 v3 key usage field)"
- certificatePolicies: Certificate policy OID = OID
- subjectAlternativeName: Alternative name of the same subject
- BasicConstraints*: Used for CA certificates only
- CRL Distribution Points: URI to CRL distribution point (LDAP and/or HTTP)

- ExtendedKeyUsage: is an optional field
- nsComment: is an optional field
- microsoft certificate template (OID 1.3.6.1.4.1.311.20.2): is an optional field

*Indicates critical extensions

7.1.3 Algorithm object identifiers

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

- Algorithm --- Object Identifier
- Sha1WithRSAEncryption --- 1.2.840.113549.1.1.5
- Md5WithRSAEncryption --- 1.2.840.113549.1.1.4
- rsaEncryption --- 1.2.840.113549.1.1.4

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

The subsidiaries of this CA currently support one digital signature and one confidentiality certificate policy. Each certificate may reference a policy OID, and may contain several as long as none of the policy constraints conflict.

7.1.7 Usage of Policy Constraints extension

Not implemented

7.1.8 Policy qualifiers syntax and semantics

The subsidiaries of this CA do not currently issue certificates with policy qualifiers.

7.1.9 Processing semantics for the critical Certificate Policies extension

The PKI client applications must process extensions marked as critical in accordance with PKIX Part 1.

7.2 CRL profile

This CA and its subsidiaries issue X.509 Version 2 CRLs in accordance with IETF PKIX RFC 3280.

7.2.1 Version number(s)

The CRL version is set to 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: Populated by the CA application as specified by operator. May contain (0) Unspecified, (1) Key compromise, (3) Affiliation change, (4) Superseded, (5) Cessation of operation
- authorityKeyIdentifier: Populated by CA application contains key id (SHA1) of issuer public key

7.3 OCSP profile

This CA and all its subsidiaries currently do not support the Online Certificate Status Protocol (OCSP).

7.3.1 Version number(s)

This CA and all its subsidiaries currently do not support the Online Certificate Status Protocol (OCSP).

7.3.2 OCSP extensions

This CA and all its subsidiaries currently do not support the Online Certificate Status Protocol (OCSP).

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The terms and conditions of this CP/CPS will be used to conduct audits for:

- The SWITCH CA and its subsidiaries
- The registration authority operated by SWITCH and its participants
- All authorized SWITCH registration authorities operated by independent third parties

8.1 Frequency or circumstances of assessment

One audit may be conducted per calendar year and is not free of charge.

More than one audit per calendar 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

The chief security officer of SwissSign AG shall be responsible for conducting the audit.

The auditor must meet the following criteria:

- The auditor must not have access rights to the SWITCH CA or any of its subsidiaries beyond the ability to view data.
- The auditor must proof a solid understanding of cryptography, Unix, TCP/IP networking, relational databases and web server technology.
- The auditor must proof a solid understanding of policies, procedures and general security practices for IT systems and for PKI implementations.

8.3 Assessor's relationship to assessed entity

The chief security officer of SwissSign AG is an employee of SwissSign AG and as such has the responsibility to conduct the annual audit.

It is possible for the chief security officer to outsource the conduct of the audit.

It is possible that SWITCH audits (as outsourcing party) the subordinate RAs.

8.4 Topics covered by assessment

The chief security officer shall propose the topics of the audit in accordance with the applicable CP/CPS.

The topics will be proposed to the SwissSign Executive Board for approval.

Upon approval the audit topics will be presented to the SWITCH PMA.

8.5 Actions taken as a result of deficiency

The results of an audit will be handled as follows:

- The chief security officer will document any deficiency found during the audit.
- The chief security officer will prioritize the deficiencies according to severity.
- The SwissSign Executive Board will review the recommendations of the chief security officer and will present these findings to the SWITCH PMA.
- SwissSign, together with the PMA will assign resources to work on the deficiencies.

8.6 Communication of results

The results of an audit shall be communicated within one month after the results have been presented to the SwissSign Executive Board.

The results of the audit and any actions taken may be made publicly available through the swisssign.com and/or SWITCH web site if both involved parties agree to this.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

SWITCH charges fees for the services provided by this CA in accordance with its current pricing process and procedures. For more information, please contact your SWITCH customer representative.

Authorized registration authorities for this CA may publish their own pricing schedules.

9.1.1 Certificate issuance or renewal fees

All certificates issued or renewed by re-keying by this CA and its subsidiaries are free of charge.

Authorized registration authorities for this CA may charge for their services.

9.1.2 Certificate access fees

Accessing certificates issued or renewed by re-keying by this CA and its subsidiaries is free of charge.

9.1.3 Revocation or status information access fees

Revocation of certificates issued or renewed by re-keying by this CA and its subsidiaries is free of charge.

Requesting status information of certificates issued or renewed by re-keying by this CA and its subsidiaries is free of charge.

Authorized registration authorities for this CA may charge for revocation and/or status information services.

9.1.4 Fees for other services

The registration of a distinguished name (DN) is charged by SWITCH in accordance with its current pricing process and procedures. For more information, please contact your SWITCH customer representative.

Authorized registration authorities for this CA may publish their own pricing schedules.

9.1.5 Refund policy

Not applicable

9.2 Financial responsibility

SwissSign AG is a privately held Swiss corporation that aims to share its shares with Swiss organisations which make a strategic investment (not a financial investment) in the public key infrastructure of Switzerland. This broadens the financial base, and thus the longevity, of the company without creating reliance on stock market fluctuations.

SWITCH is a foundation established 1987 by the Swiss Confederation and the 8 cantons hosting universities.

9.2.1 Insurance coverage

SwissSign and SWITCH maintain appropriate insurance coverage for their liabilities to other participants.

9.2.2 Other assets

Not applicable

9.2.3 Insurance or warranty coverage for end-entities

SWITCH maintains appropriate insurance coverage for their liabilities to end entities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Any information about subscribers and requesters that is not made public through the certificates issued by this CA, the CRL or the directory's content is considered confidential information and SWITCH will not disclose it to any other parties. This includes, business plans, sales information, trade secrets, organizational name, SWITCH Profile information, registration information, etcetera.

The relationship with RAs other than SWITCH's own RAs are governed by contracts where a non disclosure agreement (NDA) may be included or specifically added to.

9.3.2 Information not within the scope of confidential information

Any and all information made public in a certificate issued by this CA or its CRL shall not be considered confidential.

The serial numbers of all revoked certificates of this CA or its subsidiaries will be included in the CRL of the signing CA.

Other subsidiaries of this CA may have different definitions of the confidentiality clause. Such definitions will be subject to the contractual agreement with the owner of the subsidiary CA in question.

9.3.3 Responsibility to protect confidential information

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

SWITCH will comply with Swiss Laws and Regulations and will release information to the Swiss authorities in accordance with such laws.

SWITCH will work with its contractual partners to release relevant information about registration information provided and certificates issued under this contract.

9.4 Privacy of personal information

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 SWITCH. Further, all stipulations of 9.3.1 apply.

9.4.2 Information treated as private

Any information about subscribers or requesters that is not made public through the certificates issued by this CA, the CRL or the 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 shall not be considered private.

The serial numbers of all revoked certificates of this CA or its subsidiaries will be included in the CRL of the signing CA.

Other subsidiaries of this CA may have different definitions of the confidentiality and/or privacy clause. Such definitions will be subject to the contractual agreement with the

owner of the subsidiary CA in question.

9.4.4 Responsibility to protect private information

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

Participants that receive private information will comply with Swiss Laws and Regulations and will release information to the Swiss authorities in accordance with such laws.

9.4.5 Notice and consent to use private information

No Stipulation

9.4.6 Disclosure pursuant to judicial or administrative process

SWITCH, participants, subscribers and relying parties will comply with applicable Laws and Regulations and will release information to the appropriate authorities in accordance with such laws.

9.4.7 Other information disclosure circumstances

SWITCH, participants, subscribers and relying parties will comply with applicable Laws and Regulations and will release information to the appropriate authorities in accordance with such laws.

SWITCH will work with its contractual partners to release relevant information about registration information provided and certificates issued according to the stipulations of this document.

9.5 Intellectual property rights

SwissSign retains all rights, titles, interest and all intellectual property rights, in, to and under all certificates issued by this CA and the technology processes and know-how connected herewith, except for any information that is supplied by a requester or a subscriber. “SwissSign”, the “SwissSign” logo and all related logos are exclusive trademarks of SwissSign AG. The “SwissSign” software and all related documentation are exclusive copyrighted property of SwissSign AG.

SwissSign AG is the owner of the source code of the SwissSign CA. Any errors in the source code will be addressed and fixed immediately. This code includes 3rd party libraries/products developed by:

- the OpenSSL Project for use in the OpenSSL Toolkit (see openssl.org for more information)
- the Apache Software Foundation (see apache.org for more information).
- Ralf S. Engelschall for use in the mod_ssl project (see modssl.org for more information).

9.6 Representations and warranties

9.6.1 CA representations and warranties

This CA and its subsidiaries warrant that the information in the certificate is true to the best of the CA's knowledge based on the RA performing certain identity authentication

procedures with due diligence.

The CA warrants the correct, timely, issuance of documentation and lists as described in this CP/CPS

9.6.2 RA representations and warranties

This CA and its subsidiaries utilize (through the RA) a subscriber agreement, this subscriber agreement must contain a warranty by the RA that information in the certificate is accurate. In addition an RA must be able to present a registration document when requested by an authorized authority (e.g. auditor, court of law).

The RA is responsible for keeping the registration process stipulations.

9.6.3 Subscriber representations and warranties

This CA and its subsidiaries utilize (through the RA) a subscriber agreement, this subscriber agreement must contain a warranty by the subscriber (through signature of the registration document) that information in the certificate is accurate.

The subscriber is responsible for keeping the stipulations of this document.

9.6.4 Relying party representations and warranties

Relying parties use the certificates issued by this CA and its subsidiaries. The relying party should fulfil all requirements as described in this document. SWITCH, however, can not guarantee that a relying party does so and can thus also not held liable for damages arising from the failure of the relying party to verify certificates.

9.6.5 Representations and warranties of other participants

Products offered by participants that are to be used in a PKI should warrant functionality to the subscribers. These products are not necessarily checked by, or under the control of, SWITCH. Therefore, SWITCH cannot guarantee that a participant's products are conformant to particular regulations and thus can also not be held liable for damages arising from the use of these products.

9.7 Disclaimers of warranties

SWITCH acknowledges the fact, that this CA and its subsidiary CAs have been implemented using best practices for commercial products with high availability requirements. However, this does not imply that they meet high availability requirements or that they are suitable for high-risk applications or hazardous activities. Under no circumstances will SWITCH condone the use of certificates signed by this CA or one of its subsidiaries for such purposes.

SWITCH warrants that the information in the certificate issued by this CA and its subsidiaries is true to the best of the CA's knowledge based on the RA performing certain identity authentication procedures with due diligence.

Nothing contained in this document shall:

- create any fiduciary relationship between either SwissSign AG, SWITCH or any authorized registration authority and any end entity for any purpose whatsoever.
- confer on any end entity any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of SwissSign AG, SWITCH or any authorized registration authority.

9.8 Limitations of liability

Requesters or subscribers living/domiciled in jurisdictions that do not allow the exclusion or limitation of liability for consequential or incidental damages are not allowed to apply for certificates issued by this CA.

Under the terms and conditions of this CP/CPS SwissSign AG and SWITCH do NOT provide:

- Cryptographic Algorithms
- Software or Applications
- Communication infrastructure

SWITCH denies liability for any damages that may occur to any party through applications that:

- fail to properly verify certificates issued under this CP/CPS;
- fail to refuse expired, revoked or suspended certificates;
- fail to limit the financial value of their transaction to the limit given in section titled: “Limitations of Liability”;
- fail to adhere to the rules and regulations set in this CP/CPS, in contractual agreements with SWITCH or authorized registration authorities or other applicable law.

SWITCH acknowledges the fact, that this CA and its subsidiary CAs have been implemented using best practices for commercial products with high availability requirements. However this does not imply that they meet high availability requirements or that they are suitable for high-risk applications or hazardous activities. Under no circumstances will SWITCH condone the use of certificates signed by this CA or one of its subsidiaries for such purposes.

Under no circumstances will the total cumulative liability of SWITCH exceed CHF 1’000.

Registration authorities for this CA do NOT provide the following services under the terms and conditions of this CPS:

- Cryptographic Algorithms
- Software or Applications
- Communication infrastructure

and therefore do not make any claim as to the reliability or availability of these services and refuse to take any responsibility for their failure to comply with the expectations of users of certificates issued by this CA.

Processes at the registration authorities for this CA have been implemented using best practices for commercial products.

Under no circumstances will the total cumulative liability of an authorized registration authority for any actions of omissions in connection with this CA or its subsidiaries exceed CHF 1'000.

Products offered by participants that are to be used in a PKI are not necessarily checked by, or under the control of, SWITCH. Therefore SWITCH cannot guarantee that a

participant's products are conformant to particular regulations and thus can also not be held liable for damages arising from the use of these products.

9.9 Indemnities

This CA and its subsidiaries require that subscriber agreements contain a term under which a subscriber is held responsible for losses arising out of a subscriber's fraudulent misrepresentation on the certificate application under which the CA issued the subscriber an inaccurate certificate.

This CA and its subsidiaries require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate.

End entities shall indemnify and hold harmless SWITCH and all authorized registration authorities operating under this CP/CPS against all liabilities, losses, costs, expenses, damages, claims and settlement amounts arising out of or relating to any illegal, incorrect and unintended use of certificates issued by this CA or any of its subsidiaries.

End entities that:

- fail to properly verify certificates issued under this CP/CPS;
- fail to refuse expired, revoked or suspended certificates;
- fail to limit the financial value of their transaction to the limit given in section 9.8 titled: “Limitations of liability”;
- fail to adhere to the rules and regulations set in this CP/CPS, in contractual agreements with SWITCH or authorized registration authorities or other applicable law;
  shall take full responsibility for their actions.

9.10 Term and termination

This document remains in force until:

- no more valid certificates, issued under this CP/CPS, exist.
- it is replaced by a new version.

This document remains available for at least 10 years after no more valid certificates, issued under this CP/CPS, exist.

SWITCH reserves the right to change this document at any time.

Through publication on the SWITCH web site SWITCH notifies all participating parties of a new CP/CPS.

9.10.1 Term

This document becomes effective by publication on the SWITCH web site.

9.10.2 Termination

This CP/CPS remains in force until:

- no more valid certificates, issued under this CP/CPS, exist.

- it is replaced by a new version;

This document remains available for at least 10 years after no more valid certificates, issued under this CP/CPS, exist.

9.10.3 Effect of termination and survival

Upon termination of this document the acknowledgements of intellectual property rights and confidentiality provisions remain in force.

9.11 Individual notices and communications with participants

SWITCH reserves the right to make arbitrary decisions regarding severability, survival, merger and notice.

Any participant has to communicate, in an appropriate way, to all those concerned, any changes in its status as participant of the SWITCH PKI which may reasonably effect any or all those concerned.

9.12 Amendments

9.12.1 Procedure for amendment

This CP/CPS is subject to change without notice given the approval of the PMA.

Amendments become final and effective by publication on the SWITCH web site.

9.12.2 Notification mechanism and period

SWITCH does not implement any specific notification mechanism. This document is subject to change without notice given the approval of the PMA and becomes final and effective by publication on the SWITCH web site.

9.12.3 Circumstances under which OID must be changed

The circumstances under which amendments to the CP or CPS will require a change in CP OID or CPS pointer are decided on, on a case by case basis, by the PMA.

9.13 Dispute resolution provisions

The laws of Zurich, Switzerland shall govern all aspects of this CA. Sole place of venue for any dispute in connection with this CP/CPS or arising in connection with the usage of a SWITCH certificate shall be the commercial court of Zurich (Zürcher Handelsgericht).

9.14 Governing law

The laws of Zurich, Switzerland shall govern all aspects of this CA. Sole place of venue for any dispute in connection with this CP/CPS or arising in connection with the usage of a SWITCH certificate shall be the commercial court of Zurich (Zürcher Handelsgericht).

9.15 Compliance with applicable law

The laws of Switzerland shall govern all aspects of this CA.

9.16 Miscellaneous provisions

Not applicable

9.16.1 Entire agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

In the event that a court or other tribunal determines that a clause within this CP/CPS is, for some reason, invalid or unenforceable the remainder of the document remains in force.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Not applicable

9.16.5 Force Majeure

Events, compromising the SWITCH services, that are outside the reasonable control of SwissSign and/or SWITCH (i.e. “Force Majeure”) will be dealt with immediately by the PMA.

9.17 Other provisions

Not applicable