SWITCHslcs CA

Certificate Policy and Certification Practice Statement

Status: Released
Version: 1.1

Table of Contents

Document history

V0.9 (Nov 4, 2006)	First draft version to be submitted to EUGRIDPMA
V0.9.5 (Jan 11, 2007)	Revised version with comments from reviewers (Mike Helm and Jens Jensen)
V1.0 (Jan 24, 2007)	Revised version with comments from meeting in Abingdon
V1.0 (Feb 8, 2007)	Minor changes after comments by W.Weisz
V1.1 (Mar 9, 2009)	Amendments when introducing a CRL for the SWITCHslcs CA

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), called SWITCHaai, which is to simplify inter-organizational access to networked services. The framework of the SWITCHaai federation, formed by the participating institutions, gives the organisational and legal basis of this service (see http://www.switch.ch/aai/join/members.html for details). The software implementation is based on Shibboleth, a product developed by the Internet2 initiative.

SWITCH joined the EU funded project EGEE-II (“Enabling Grid for E-sciencE Phase 2) in order to implement interoperability between Shibboleth and gLite, the EGEE middleware stack. As part of this work a short-lived credential service (SLCS) was developed, which issues X.509 certificates with a lifetime of less than one million seconds (roughly 11.5 days) to members of the SWITCHaai federation.

This short-lived credential service, called SWITCHslcs, is a web-based application, where a user can request and obtain a short-lived certificate if and only if

- the user has received permission from an RA authority, located at his Identity Provider, to access the service
- the user has successfully authenticated at his SWITCHaai Identity Provider every time he requests a new certificate

This document is the combined Certificate Policy and Certification Practice Statement (CP/CPS) of the SWITCH Short-lived Credential Service CA, further referred to as “SWITCHslcs CA” or “this CA” or “this CA and its subsidiary CAs". 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.

Note that

- this CA is a Subject CA of the SWITCHgrid Root CA, whose CP/CPS is described in the document “SWITCH Root CA Certificate Policy and Certification Practice Statement”, OID 2.16.756.1.2.6.3
- this service and its underlying CA are independent of the SWITCHpki service as described by in the document “SWITCH Certificate Policy and Certification Practice Statement”, OID 2.16.756.1.2.6.1.*.
- this CA implements the short-lived credential service profile of the IGTF.

1.2 Document name and identification

This document is named SWITCH Short-lived Credential Service Certificate Policy and Certification Practice Statement.

The version is 1.1, dated March 9th, 2009.

The following ASN.1 Object Identifier (OID) has been assigned to this document (where the OID components starting at position 8 reflect the version number):

2.16.756.1.2.6.4.1.1

1.3 PKI participants

1.3.1 Certification authorities

SWITCHslcs CA is an online Subject CA of the SWITCHgrid Root CA. SWITCHslcs CA issues only short-lived certificates to users of the SWITCHaai federation (see glossary for federation specific terminology).

1.3.2 Registration authorities

SWITCHslcs CA will automatically issue short-lived user certificates to registered users after a successful authentication at an Identity Provider of the SWITCHaai federation.

Users are registered at the SWITCHslcs service through registration authorities operated by its participating members (participants). These registration authorities are located at the organization operating the SWITCHaai Identity Providers and solely enable the access to the SWITCHslcs service. The certificates will subsequently be issued by the SWITCHslcs CA automatically upon a successful authentication at an Identity Provider.

1.3.3 Subscribers

In the context of this CP/CPS the term “Subscribers” encompasses all end users with a valid SWITCHaai account who have obtained a SWITCHslcs 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.

Certificates issued by SWITCHslcs CA are intended to be used primarily by individuals in the grid and e-Science environment. Other uses are not supported.

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.

1.5 Policy administration

1.5.1 Organization administering the document

SWITCH – Teleinformatikdienste für Lehre und Forschung
SWITCHpki Policy Management Authority (PMA)
P. O. Box
CH-8021 Zürich
Switzerland
Tel: +41 44 268 15 15
www.switch.ch

1.5.2 Contact person

Alessandro Usai
pki@switch.ch
Tel: +41 44 268 15 15

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 short-lived credential service profile of the International Grid Trust Federation (IGTF)
- RFC 3647

1.6 Definitions and acronyms

Attribute Authority (AA)	(Shibboleth term.) The AA is the portion of the Identity Provider responsible for issuing attributes on behalf of an organization.
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. 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.
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
Distinguished Name	⇒ Subject
DN	⇒ Distinguished Name
Extension	Optional fields in a X509 Certificate.
Identity Provider (IdP)	(Shibboleth term.) Authority responsible for generating and asserting authentication, authorization, and identity information about their users in a security domain. This means the Identity Provider • registers its users and stores information about them • is able to authenticate their users
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
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
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.
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	Processes and technologies used to issue and manage digital identities

Infrastructure	for the use of third parties to authenticate individuals. Abbrev. PKI.
RDN	⇒ Relative Distinguished Name
Relative Distinguished Name	⇒ Subject
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.
Service Provider (SP)	(Shibboleth term.) A collection of Resources. However, since most Service Providers contain only one Resource, the term Service Provider is often used as synonym for Resource, although more in a technical sense.
Shibboleth	Federated identity management solution from Internet2/MACE (Middleware Architecture Committee for Education), which is the name of the architecture but also the name of its open source implementation.
Signature	Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document.
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). The DN is composed of several fields, called relative distinguished names (RDN), which have the structure *variable_abbreviation=value*. Examples: DC=ch,DC=switch, DC=slcs, O=Switch - Teleinformatikdienste fuer Lehre und Forschung, CN=Valery Tschopp Possible variables and their abbreviation of the subject are: Common Name /CN Organization /O Organizational Unit /OU Domain Component /DC Country Name /C
SWITCHaai	The SWITCHaai Federation is a group of organizations (universities, hospitals, libraries, etc.) that agree to cooperate in the area of inter-organizational authentication and authorization and, for this purpose, operate an AAI infrastructure. The participants page lists all the Federation Members and Federation Partners of the SWITCHaai Federation. Web site: http://www.switch.ch/aai

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CA 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. The website can be reached at the following address:
http://www.switch.ch/pki/grid

2.2 Publication of certification information

SWITCH operates a secure online repository that contains all past and current versions of the CP/CPS for this CA

2.3 Time or frequency of publication

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

2.4 Access controls on repositories

CP/CPS of this CA are available to the public as read-only information from the SWITCH web site.

Modification of CP/CPS 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 for the first time registration of the user of SWITCHslcs (see 3.2). The organization hosting the RA must have signed the SWITCHaai federation member agreement. In addition, SWITCH acts as RA of the virtual home organisation of the SWITCHaai federation, which allows enabling access to resources for individuals, whose institute does not provide SWITCHaai credentials to its users.

Using this procedure the RA must ensure that

- the individual has a valid SWITCHaai account
- the identity of the individual is substantial enough for the transactions as intended in this CP/CPS

3.1.1 Types of names

The subject name in certificates issued by this CA is an X.500 distinguished name, which is constructed based on the user's attributes as provided by the requester's SWITCHaai Identity Provider.

For the distinguished name the following relative distinguished names (RDN) are required:

DC, CN and either O or OU.

The distinguished name shall start with the following RDNs: /DC=ch/DC=switch/DC=slcs.

The organization RDN (O) contains the name of the institution operating the Identity Provider as registered in the Commercial Registry Office or used in an official document, such as cantonal law, e.g. 'Switch - Teleinformatikdienste fuer Lehre und Forschung'.

If the identity provider of the requester is the virtual home organization, the O RDN is not present and the OU RDN is set to 'SWITCHaai Virtual Home Organization'.

The common name (CN) is constructed based on the attributes of the user as provided by his/her Identity Provider: CN='givenname surname uniqueInt'.

Givenname and surname are the corresponding attributes of the user. The attribute definitions of SWITCHaai are derived from the eduPerson schema and are described in the attribute specification document available at http://www.switch.ch/aai/documents.

The uniqueInt is an immutable unique integer in hexadecimal format, generated out of the requester's attributes as provided by the Identity Provider. The uniqueness of the uniqueInt, and therefore of the DN, is guaranteed by the SWITCHaai attribute UniqueID, which identifies an individual uniquely within the SWITCHaai federation.

If the optional subjectAltName extension is present, then it must contain an rfc822Name entry carrying the "e-mail" attribute of the user as provided by his/her Identity Provider.

3.1.2 Need for names to be meaningful

The Subject and Issuer name are meaningful in the sense that they are obtained from the user's attributes "givenname" and "surname" and the name of the organisation hosting the Identity Provider.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity are not supported.

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 are 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 uniqueness of the subject field of valid certificates is guaranteed by the presence of an integer, which is derived from the requester's attributes, among them the uniqueID attribute of the SWITCHaai federation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

The initial identity validation consists of the following steps:

- the requester contacts the RA of his Identity Provider in order to obtain permission to access the SWITCHslcs service
- the RA enables access to the SWITCHslcs service for the requester upon confirmation that the following two requirements are fulfilled:
  a) the individual has a valid SWITCHaai account
  b) the account creation was dependent on a process which had one of the following properties:
     1) Issuance of an identity card, which gives its holder monetary benefits
     2) the account has a direct relation to human resources data, which is used for salary payments
     3) a registration process with the RA, which included submission of a copy of a passport or other official identity card.
- The requester can access the SWITCHslcs website and obtain his/her short-lived certificate upon successful authentication at his/her Identity Provider.

The RAs devise their own registration process in order to ensure the two requirements a) and b) as stated above are fulfilled.

The SWITCHslcs service allows the RA to allow as well as prohibit access to the SWITCHslcs service for its users.

3.2.1 Method to prove possession of private key

Possession of the private key is verified for certificates issued by this CA through the verification of the digital signature on the CSR (certificate signing request) as the requester always generates the key pair.

3.2.2 Authentication of organization identity

The DN of a certificate issued by this CA must contain either one instance of the organization RDN or one instance of the organizational unit RDN. The following rules must be adhered to:

- The organization must be a member of the SWITCHaai federation and operate a SWITCHaai Identity Provider.
- If the organization RDN of the DN is set, then it must be set to the legal name of the organization (as registered in the Commercial Registry Office or used in an official document, such as cantonal law or official code reference thereof).

3.2.3 Authentication of individual identity

The user identity will be authenticated through successful logon at the Identity Provider using a secure transaction.

3.2.4 Non-verified subscriber information

The information in the email address field is optional and as supplied by the Identity Provider.

3.2.5 Validation of authority

Identity Providers must have procedures in place that guarantee the requirements as stated in 3.2. The wording of the organizational name (or organizational unit in case of the virtual home organization) that is included in the certificate is determined by the Identity Provider, which asserts the successful authentication of the user at the time of requesting the certificate.

3.2.6 Criteria for interoperation

None.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Certificates issued by this CA are not re-keyed. Thus every certificate request is treated as an initial request.

3.3.2 Identification and authentication for re-key after revocation

Every certificate request is treated as an initial request.

3.4 Identification and authentication for revocation request

This section explains the circumstances under which a certificate should be revoked. Once a certificate has been revoked, it must not be renewed or extended. Suspension of certificates is not supported.

3.4.1 Circumstances for revocation of a certificate

A valid certificate shall be revoked if its key material or the key material of a proxy certificate, directly or indirectly derived at any level from the certificate, is compromised.

A valid certificate shall also be revoked if the AAI account of the user or its password are compromised in any possible way: in the occurrence of such an event the SWITCHslcs service RA shall request the suspension of the affected organization's Identity Provider from the SWITCHslcs service until the affected Identity Provider and corresponding Identity Management System are secured.

Subscribers are obliged to immediately notify their SWITCHslcs service RA or directly the SWITCHslcs service personnel of such events as described above, so as to initiate revocation of the certificate.
SLCS RAs are required to notify the SWITCHslcs service personnel of any event that requires the revocation of a certificate.

3.4.2 Revocation requests vetting

Subscribers may at their discretion require that their certificates be revoked: the requests should be sent directly to the SWITCHslcs service personnel, who will process the requests accordingly.
Acceptance of a revocation of a certificate is subject to the successful identification and authentication of the subscriber.
Additionally SLCS RAs may also request the revocation of certificates that were issued using the Identity Providers of their organizations.

Others may request the revocation of a certificate provided they can prove that this one and/or its derived proxy certificate, or the corresponding AAI account of the user are compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Anybody who has a SWITCHaai account and who has been given access to the SWITCHslcs by the RA tied to his Identity Provider can submit a certificate request.

4.1.2 Enrolment process and responsibilities

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

- The requester must have a valid SWITCHaai account
- The requester must have been given access to the SWITCHslcs by the RA tied to his Identity Provider as described in 3.2.3.

Requester's responsibilities:

- provide to SWITCH and to any third party RA only correct information without errors, omissions or misrepresentations;
- supplementing any information required by the RA tied to his Identity Provider
- read and agree to all terms and conditions of this CP/CPS;
- use SWITCHslcs certificates exclusively for legal and authorized intended purposes;
- only use a SWITCHslcs certificate on behalf of the person, entity, or organization listed as the Subject of such certificate;
- 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 RA immediately of any suspected or actual compromise of the SWITCHaai account that is used to authenticate against the SWITCHslcs
- immediately cease to use the certificate upon (a) expiration 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, with the exception of proxy certificates as described in RFC 3820;
- 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

4.2.1 Performing identification and authentication functions

The SWITCHslcs service will identify the requester based on the successful SWITCHaai login.

4.2.2 Approval or rejection of certificate applications

SWITCHslcs will approve a certificate signing request (CSR) automatically if the following criteria are met

- the requester has been granted access to the SWITCHslcs after successful authentication at an Identity Provider
- the requester has been added to the list of authorized users of the SWITCHslcs by the RA tied to this Identity Provider.

If the requester fails to adhere to any of the above, or in any other way violates the stipulations of this document, the RA will reject the access request to SWITCHslcs.

4.2.3 Time to process certificate applications

Certificate requests are processed automatically and in real time.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate signing requests (CSR) are processed automatically by SWITCHslcs if the user has authenticated himself successfully at his/her Identity Provider. All steps of this process are logged in real time.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The user receives the certificates through the application they are using to request them.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The user accepts the certificate by invoking the application, which requests it in first place.

4.4.2 Publication of the certificate by the CA

SWITCHslcs certificates are not published.

4.4.3 Notification of certificate issuance by the CA to other entities

SWITCHslcs will not perform any notifications.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers may use their certificates as they wish but shall:

- use SWITCHslcs certificates exclusively for legal and authorized intended purposes;
- only use a SWITCHslcs certificate on behalf of the person, entity, or organization listed as the Subject of such a certificate – the Subject is the only legitimate user of the certificate;
- refrain from using the subscriber's private key corresponding to the public key certificate to sign other certificates, with the exception of proxy certificates as described in RFC 3820

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 as specified in RFC 3280, 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 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;

4.6 Certificate renewal

SWITCHslcs does not support certificate renewal. The subscriber requests a new certificate instead.

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.

SWITCHslcs does not explicitly re-key certificates. The subscriber requests a new certificate instead.

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

4.9 Certificate revocation and suspension

Revocation requests are handled by the SWITCHslcs service personnel, which will proceed to issue a Certificate Revocation List within one working day after having received the request.
Suspension of certificates is not supported.

4.10 Certificate status services

4.10.1 Operational characteristics

The SWITCHslcs certificate service can be reached 24x7 through the Internet.

4.10.2 Service availability

SWITCH provides all services (registration, certification, directory) as 24x7 services with minimal 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

No stipulation.

4.12 Key escrow and recovery

This CA does not support private key escrow.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

The SWITCHslcs CA server is located in Zurich, with access control by SWITCH.

5.1.1 Site location and construction

The sites are located in a data center in Zurich, 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

No stipulation.

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

No stipulation.

5.2 Procedural controls

All persons with access to the systems hosting the SWITCHslcs will be permanently employed SWITCH personnel, which are either trained system administrators or members of the SWITCH security department.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Operators of the SWITCHslcs will be qualified system administrators or members of the SWITCH security department.

5.3.2 Background check procedures

No stipulation.

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

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

SWITCH reserves the rights to prosecute unauthorized actions to the fullest extent of applicable Swiss laws.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No special requirements apply.

5.4 Audit logging procedures

All major events in this CA 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
- CA rollover

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 CA Operator of this CA and to authorized audit personnel.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

Depending on the severity of the log entry, SWITCH 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 is monitored and attempts to gain unauthorized access are logged. SWITCH 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 produced

5.5.2 Retention period for archive

Archived information is kept at least 1 year.

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 centre.

5.5.5 Requirements for time-stamping of records

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

5.5.6 Archive collection system (internal or external)

Internal.

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

SWITCH will change the keys of this CA at least every 5 years. The CA certificate is available for download on the SWITCH website and is signed by the long-living trust anchor of the SWITCHgrid Root CA.

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 Root CA will sign a new certificate for this CA. When the CA certificate is revoked, all certificates signed directly or indirectly are invalid.

5.7.2 Computing resources, software, and/or data are corrupted

The master server of this CA is part of a daily backup process.

5.7.3 Entity private key compromise procedures

Any compromise of the private key will be handled by SWITCH on a case-by-case basis. A reasonable attempt will be made to contact affected parties, taking the remaining lifetime of any issued certificates into account.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

All participating Identity Providers will be informed and information of its termination will be made widely available if this CA ceases operation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for this CA has been generated in and is stored in an HSM module meeting at least FIPS 140-2 Level 2 requirements.

The subscriber key pair generation is not performed by this CA, but only by an application under the sole control of the subscriber, or a certificate storage device (e.g. smart card, USB token).

6.1.2 Private key delivery to subscriber

No private key delivery to subscriber is required.

6.1.3 Public key delivery to certificate issuer

The requester (or more precisely the application invoked by the requester) presents the public key as a PKCS#10 formatted request to the signing CA using a secure communication channel.

6.1.4 CA public key delivery to relying parties

Relying parties can download the issuing CA certificate from the website in both raw X.509 (DER) and Base64 encoded format (PEM).

6.1.5 Key sizes

This CA uses a 2048 bit RSA key.

6.1.6 Public key parameters generation and quality checking

The key pairs of this CA have been created using an HSM meeting at least FIPS 140-2

Level 2 requirements.

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 keys for the certificates of the end-entity may be used for authentication and signing proxy certificates. Other usage such as non-repudiation, data and key encryption, message integrity etc. is not supported.

The keys for the CA certificate are used for the certificate signing.

(See also 7.1.2).

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 140-2 level 2 requirements.

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

No stipulation.

6.2.3 Private key escrow

This CA does not support private key escrow.

6.2.4 Private key backup

A copy of private key of this CA is stored on the host file system in encrypted form and is backed up on a daily basis. The wrapping key used for encrypting the private key is protected by secure key tokens (smartcards). The key tokens are stored in a safe with strict access control (limited to SWITCH CA staff).

6.2.5 Private key archival

The CA Key is not archived.

The CA database is archived at regular intervals.

6.2.6 Private key transfer into or from a cryptographic module

The private key of this CA has been generated in the cryptographic module.

6.2.7 Private key storage on cryptographic module

See 6.2.6

6.2.8 Method of activating private key

The private key of this CA is activated during the start-up process of the CA application. The availability of the CA service is supposed to be high for signing certificate requests with only few and short downtimes.

6.2.9 Method of deactivating private key

The private key of this CA is deactivated during the shutdown process of the CA

application when the connection to the HSM is closed.

6.2.10 Method of destroying private key

The private key of this CA is deleted by initializing the HSM.

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 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:

- This CA's certificate is valid for 5 years.
- End entity certificates are valid up to one million seconds.

6.4 Activation data

6.4.1 Activation data generation and installation

The secure key tokens required for activation of the private key of this CA are generated and installed according to the procedures recommended by the HSM vendor.

6.4.2 Public key archival

If not connected to the HSM for operational use, the secure key tokens are stored in a safe with strict access control (limited to SWITCH CA staff).

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

The CA Server includes the following functionality:

- It is connected to a dedicated network carrying only traffic required for the CA service
- Only software needed for the proper functioning of the CA service is installed on the system.
- The operating system has been hardened according to manufacturer's recommendations, and recommended and applicable security patches are applied in a timely fashion.
- Monitoring is done to detect unauthorized software changes.

6.5.1 Specific computer security technical requirements

No stipulation.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

This CA uses SWITCH and commercial software. To ensure quality and availability of the SWITCH software, the SWITCH development team adheres to the following principles:

- All software is stored in a version control system to keep track of software versions.
- The software archive is put onto backup regularly and a copy is stored externally.
- The new version of the CA and Shibboleth software is always first installed in a test-bed before installing it on the production system.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

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 time stamped.

7. CERTIFICATE, CRL, AND OCSP PROFILES

This section contains the rules and guidelines followed by this CA for populating X.509 end-entity certificates.

7.1 Certificate profile

7.1.1 Version number(s)

Version of X.509 certificates: version 3 (i.e., version number is set to 2)

7.1.2 Certificate extensions

The SWITCHslcs CA certificate includes the following extensions:

- basicConstraints: critical; CA=true
- keyUsage: critical; theKeyCertSign and cRLSign bits are set (any others are unset)
- authorityKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the SWITCHgrid Root CA certificate

- subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the SWITCHslcs CA certificate
- cRLDistributionPoints: not critical; includes an HTTP URI for retrieving the CRL of the issuing CA
- authorityInfoAccess: not critical; includes an entry (of syntax id-ad-caIssuers) with a URL for retrieving the issuing CA's certificate.
- certificatePolicies: not critical; contains the anyPolicy OID (2.5.29.32.0)

End-entity certificates include the following extensions:

- keyUsage: critical; by default, only the digitalSignature and keyEncipherment bits are set
- extendedKeyUsage: not critical; by default, contains the OID for TLS client authentication (id-kp-clientAuth, 1.3.6.1.5.5.7.3.2); may contain other OIDs
- authorityKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the issuing CA's certificate
- subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the end-entity's certificate
- certificatePolicies: not critical; contains at least the OID of this document (as defined in section 1.2) as the policyIdentifier; may contain additional OIDs
- subjectAlternativeName: not critical; for user certificates, includes an rfc822Name entry with the e-mail address of the end-entity
- authorityInfoAccess: not critical; includes an entry (of syntax id-ad-caIssuers) with a URI for retrieving the issuing CA's certificate
- cRLDistributionPoints: not critical; includes an HTTP URI for retrieving the CRL of the issuing CA

7.1.3 Algorithm object identifiers

The algorithms with OIDs supported by this CA are:

- rsaEncryption (1.2.840.113549.1.1.4)
- sha1WithRSAEncryption (1.2.840.113549.1.1.5)

7.1.4 Name forms

All certificates issued by this CA use X.500 distinguished names as described in 3.1.1.

The subject name of the SWITCHslcs CA certificate is C=CH, O=Switch - Teleinformatikdienste fuer Lehre und Forschung, CN=SWITCHslcs CA

7.1.5 Name constraints

All certificates issued by this CA have a subject distinguished name starting with /DC=ch/DC=switch/DC=slcs.

7.1.6 Certificate policy object identifier

Certificates issued by this CA include a certificatePolicies extension containing at least the OID of this document (as defined in section 1.2) as the policyIdentifier OID. Certificates may contain additional policyIdentifier OIDs.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

This CA issues version 2 CRLs, using the sha1WithRSAEncryption signature algorithm (1.2.840.113549.1.1.5). The validity of the CRL (time delta between thisUpdate and nextUpdate) is 10 days; the CRL is issued at least once per day.

7.3 OCSP profile

This CA does not support the Online Certificate Status Protocol (OCSP).

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PMA of SWITCH shall carry out a compliance audit of the operators once every year. The audit shall inspect the logs, and check the security of the activation data and the copies of the encrypted private key.

In addition, the SWITCHslcs CA will accept at least one external compliance audit per year when requested by a relying party or a peer. The entire cost of such an audit must be covered by the requestor.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

SWITCH may charge a fee for the services provided by this CA in accordance with its current pricing process and procedures. For more information, please contact the SWITCHslcs CA Manager.

9.2 Financial responsibility

No financial responsibility is accepted.

9.3 Confidentiality of business information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

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 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 shall not be considered private.

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

The source code of the SWITCHslcs CA has been developed as part of the EU funded project EGEE-II and is licensed according to the regulations of the EGEE-II project.

The SWITCHslcs CA does not claim any intellectual property rights on certificates which it has issued.

9.6 Representations and warranties

No stipulation.

9.7 Disclaimers of warranties

SWITCH acknowledges the fact that this CA has 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 for such purposes.

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

9.8 Limitations of liability

SWITCH denies any liabilities for damages that occurred to relying parties or subscribers of its certificates.

9.9 Indemnities

This CA declines any payments of indemnities for damages occurring from the use of its certificates.

9.10 Term and termination

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.

This document remains available for at least 1 year 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 can provide notices by email, postal mail, fax or on web pages unless otherwise specified in this CP/CPS.

9.12 Amendments

9.12.1 Procedure for amendment

SWITCH will implement changes with little or no impact for subscribers and relying parties to this document upon the approval of the SWITCH PMA.

Changes of the CP/CPS that may affect security (e.g. changes to the requirements for verifying requests, key sizes) or changes in the policy (e.g. changes to the namespace or introduction of subordinate CA's) will be announced at least 15 days in advance on the website and appropriate mailing lists.

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

9.12.2 Notification mechanism and period

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. This CA will inform its subscribers and all relying parties it knows of by means of an e-mail.

9.12.3 Circumstances under which OID must be changed

Changes of this CP/CPS that do affect subscribers and/or relying parties do require the OID of this CP/CPS to be updated.

9.13 Dispute resolution provisions

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

No stipulation.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

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)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other provisions

No stipulation.