SWITCHaai Interfederation Metadata Signing CA

Certificate Policy and Certification Practice Statement

Version 1.0, OID 2.16.756.1.2.6.8.1.0

July 19, 2011

Table of Contents

V0.9 (June 28, 2011)	First draft version, based on SWITCHaai Metadata Signing CA CP/CPS
V1.0 (July 19, 2011)	Integrated comments from reviews by T. Lenggenhager and L. Hämmerle

1. INTRODUCTION

1.1 Overview

SWITCH 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.

This document is the combined Certificate Policy and Certification Practice Statement (CP/CPS) of the SWITCHaai Interfederation Metadata Signing CA, further referred to as “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 SWITCHaai Root CA, whose CP/CPS is described in the document “SWITCHaai Root CA Certificate Policy and Certification Practice Statement”.

1.2 Document name and identification

This document is named SWITCHaai Interfederation Metadata Signing CA Certificate Policy and Certification Practice Statement. The version is 1.0, dated July 19, 2011.

The ASN.1 object identifier 2.16.756.1.2.6.8.1.0 has been assigned to this document, where the OID components at position 8ff. reflect the version number of this document.

1.3 PKI participants

1.3.1 Certification authorities

The SWITCHaai Interfederation Metadata Signing CA is an online Subject CA of the SWITCHaai Root CA. The SWITCHaai Interfederation Metadata Signing CA is only used to issue end-entity certificates which are used to sign metadata for interfederation use.

1.3.2 Registration authorities

There are no RAs external to the issuing authority. The issuing authority alone is responsible for all approvals and revocations.

1.3.3 Subscribers

In the context of this CP/CPS the term “Subscribers” refers to the persons who are in charge of maintaining the system(s) where certificate(s) signed by the SWITCHaai Interfederation Metadata Signing CA are installed.

1.3.4 Relying parties

Relying parties are individuals or organizations using the certificates to verify the integrity of interfederation metadata. They 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 the SWITCHaai Interfederation Metadata Signing CA are intended to be used for verifying the integrity of interfederation metadata. 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
SWITCHpki Policy Management Authority (PMA)
Werdstrasse 2, P. O. Box
8021 Zürich, Switzerland
http://www.switch.ch

1.5.2 Contact person

SWITCHaai Interfederation Metadata Signing CA Manager
aai@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 RFC 3647.

1.6 Definitions and acronyms

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 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
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
Distinguished Name	→ Subject
DN	→ Distinguished Name
Extension	Optional fields in a X.509 Certificate.
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, which is 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. 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
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 roll over 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.
Signature	Cryptographic element that is used to identify the originator of the document and to verify the integrity of the document
Secure Signature Creation Device	A device for creating digital signature which meets the requirements specified in annex III of the European Directive on a Community framework for electronic signatures (1999/93/EC)
SSCD	→ Secure Signature Creation Device
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).
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 authentication and authorization infrastructure (AAI).

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

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 http://www.switch.ch/pki/aai.

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 documents 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

3.1.1 Types of names

The subject name in certificates issued by this CA is an X.500 distinguished name where the following relative distinguished names (RDN) are mandatory: countryName (C), organizationName (O) and commonName (CN). The distinguished name may include additional RDNs.

For all certificates issued by this CA, C is set to “CH” and O to “SWITCH”.

3.1.2 Need for names to be meaningful

The Subject and Issuer name are meaningful in the sense that they include an accurately validated name of the organization to which the certificate was issued.

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 (if applicable):

- 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 CA makes sure that the subject distinguished name for a particular end-entity in any issued certificate is unique.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

This CA only issues certificates to system entities, not to real persons. For the initial identity validation, the CA verifies that the request is submitted by an authorized operator for that system, and that a proof of possession of the private key is provided (e.g. by a correct digital signature on the CSR).

3.3 Identification and authentication for re-key requests

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

3.4 Identification and authentication for revocation request

Certificates issued by this CA will be revoked in the following cases:

- A revocation request is received which is signed with the private key of the end-entity certificate.
- An authenticated revocation request is submitted by an operator of the system to which the certificate was issued.
- The CA has otherwise determined the need for revocation, e.g. if the responsible system operator does not comply with the requirements on it by this CA.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

Certificate requests can be submitted by operators who are in charge of a system which is used to sign metadata for interfederation use. The operator creating the request must ensure that the key pair is created based on a strong random number generator with adequate entropy. The private key must be stored on a hardware token only.

4.2 Certificate application processing

The CA will process a certificate request as soon as it has determined its correctness and its authenticity (submission by an authorized system operator).

4.3 Certificate issuance

Certificate signing requests (CSR) are manually processed, and all issued certificates are stored in the CA's repository. End-entity certificates may optionally be published on a Web site.

4.4 Certificate acceptance

The operator of the system hosting the certificate shall verify its content. The certificate shall be considered accepted if no objections to its content have been made within five working days.

In case of non-acceptance, the operator shall inform the manager of this CA, describing required amendments. The certificate shall be revoked by the CA, and reissued with the amendments, provided the amended certificate is still compatible with this CP/CPS. Re-issuance may be based on the original request.

4.5 Key pair and certificate usage

The certificates issued by this CA are intended for verifying the integrity of metadata for interfederation use. Other purposes are not supported.

Relying parties shall verify certificates issued by this CA, including use of CRLs, in accordance with the certification path validation procedure as specified in RFC 5280, taking into account any critical extensions, key usage, and approved technical corrigenda as appropriate.

4.6 Certificate renewal

This CA does not support certificate renewal.

4.7 Certificate re-key

This CA does not support re-keying. Every certificate request is treated as an initial request.

4.8 Certificate modification

Certificate modification is only supported in case of non-acceptance (cf. section 4.4).

4.9 Certificate revocation and suspension

A certificate issued by this CA shall be revoked if

- the operator of the system hosting the certificate is seen to consistently and wilfully violate this CP/CPS;
- the operator is seen to violate the requirements imposed by the policy and practices of this CA;
- it can be shown that the private key has been compromised.

4.10 Certificate status services

This CA issues a CRL which is published on the SWITCH Web site.

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 system hosting the SWITCHaai Interfederation Metadata Signing CA is located in a data center in Zurich, Switzerland. Physical access is only granted to system administrators and a limited number of data center personnel.

5.2 Procedural controls

All persons with access to the systems hosting the SWITCHaai Interfederation Metadata Signing CA are permanently employed SWITCH personnel, which are either trained system administrators or members of the SWITCHaai project team.

5.3 Personnel controls

Operators of the SWITCHaai Interfederation Metadata Signing CA are qualified system administrators or members of the SWITCH middleware group and must provide proof that they have obtained the skills required for their position. Any lack or shortcoming will be addressed and alleviated through proper training.

5.4 Audit logging procedures

All major events on the system hosting this CA (such as bootup, shutdown or operator logins) are logged through the basic logging facilities provided by the operating system. Certificate signing operations are separately logged.

5.5 Records archival

Any information produced by this CA is backed up daily. Archived information is kept at least one year.

5.6 Key changeover

The keys of this CA will be changed 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 SWITCHaai Root CA.

5.7 Compromise and disaster recovery

In case of a CA key compromise, the CA certificate will be revoked and a new key pair will be generated. The SWITCHaai Root CA will then sign a new certificate for this CA.

A reasonable attempt will be made to contact affected parties, taking the remaining lifetime of any issued certificates into account.

5.8 CA or RA termination

All affected parties 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

The key pair for this CA has been generated in and is stored on an SSCD which has been evaluated against the Common Criteria under EAL4+.

This CA uses a 2048-bit RSA key. End-entity certificates signed by this CA use RSA keys with at least 2048 bit.

6.2 Private key protection and cryptographic module engineering controls

The private key of this CA is only stored on one secure signature creation device. Access to the key is protected by a passphrase with a length of at least 11 characters.

6.3 Other aspects of key pair management

All certificates are kept throughout the lifetime of the CA, and a period of no less than one year after the termination of the CA. 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 the CA.

End-entity certificates signed by this CA have a lifetime which does not exceed 1096 days (three years).

6.4 Activation data

The private key of this CA is activated by supplying a passphrase. Three unsuccessful activation attempts will render the private key temporarily inaccessible, after which access can only be re-established supplying the appropriate personal unblocking key (PUK). The PUK is stored offline and only available to authorized CA managers.

6.5 Computer security controls

The system hosting this CA is located on a protected network with limited access from external systems. Only software needed for operating this CA and signing SWITCHaai and interfederation metadata is installed on the system. User accounts are restricted to persons requiring access for maintaining the system.

6.6 Life cycle technical controls

No stipulation.

6.7 Network security controls

Network security is provided by firewalls 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

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

This CA's certificate includes the following extensions:

- basicConstraints: critical; CA=true
- keyUsage: critical; the keyCertSign 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 SWITCHaai Root CA certificate
- subjectKeyIdentifier: not critical; value is set to the SHA-1 hash of the BIT STRING subjectPublicKey of the SWITCHaai Interfederation Metadata Signing 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; two policy information entries: one with the anyPolicy OID (2.5.29.32.0), one with OID 2.16.756.1.2.6.8

End-entity certificates signed by this CA include the following extensions (non-exhaustive list):

- keyUsage: critical; by default, only the digitalSignature bit is set
- 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
- authorityInfoAccess: not critical; includes an entry (of syntax id-ad-caIssuers) with a URI for retrieving the issuing CA's certificate
- certificatePolicies: not critical; one policy information entry with OID 2.16.756.1.2.6.8

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 this CA is C=CH, O=SWITCH, CN=SWITCHaai Interfederation Metadata Signing CA.

7.1.5 Name constraints

All certificates issued by this CA have a subject distinguished name starting with C=CH, O=SWITCH.

7.1.6 Certificate policy object identifier

No stipulation.

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

As long as end-entity certificates signed by this CA are in active use, CRLs are issued at least every 24 hours, or immediately upon revocation of a certificate. The time delta between the thisUpdate and nextUpdate fields is 5 days.

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 SSCD and the protection of its passphrase.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fee is charged for the services provided by this CA.

9.2 Financial responsibility

No financial responsibility is accepted.

9.3 Confidentiality of business information

No stipulation.

9.4 Privacy of personal information

This CA does not process any personal data.

9.5 Intellectual property rights

The SWITCHaai Interfederation Metadata Signing 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 warrants that the information in the certificate issued by this CA is true to the best of the CA's knowledge, based on performing identity vetting 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, and remains available for at least one year after this date.

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

This CA will communicate amendments by publishing an updated CP/CPS on the SWITCH web site.

9.13 Dispute resolution provisions

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 Switzerland shall govern all aspects of this CA.

9.15 Compliance with applicable law

This certification practice statement and its stipulations comply with applicable Swiss law.

9.16 Miscellaneous provisions

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.

Events, compromising the SWITCHaai 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.