SWITCH
Serving Swiss Universities

BEST CURRENT PRACTICES

for operating a SWITCHaai Identity Provider

12. November 2009

Version 1.0

SWITCHaai <aai@switch.ch>

Table of Contents

1. Introduction

1.1. Purpose of this document

This document describes best current practices for operating an Identity Provider (IdP) within the SWITCHaai federation. It is meant to cover identity management related aspects of the organization, its processes and the technical infrastructure for successfully operating an IdP.

These best current practices can also be used as a checklist to determine compliance with the AAI Policy [AAIPol].

1.2. Target audience

Readers of this document are supposed to be operators of an identity provider or IT managers responsible for identity management at an organization that is part of the SWITCHaai federation.

The audience includes staff from outsourcing partners, where some of the IdP related services are operated by third parties.

1.3. Organization of the document

The document is divided into four main parts:

- Identity management
- Service management
- Operation
- Infrastructure

Each main part contains sub parts, which are explained in a common way. For each sub part there are one or more *requirements* and/or *suggestions*, formatted like this:

R-###

This is an example requirement.

Future revisions of the AAI Policy [AAIPol] are expected to require compliance with these requirements for IdPs.

S-###

This is an example suggestion.

Suggestions reflect best common practices. Depending on the specific local environment, their implementation can be considered optional.

The identifiers are chosen in a serial order.

2. Identity Management

Identity management (IdM) is a concept that combines business processes, policies and technologies that enable organizations to:

- identify persons
- provide secure access to resources
- efficiently control this access
- respond faster and more consistently to changing information related to affiliates
- protect confidential information from unauthorized users

Identity management is the core topic of this document and is therefore addressed first and at a detailed level.

2.1. Roles and responsibilities

This section describes which roles are involved in the whole identity management process.

S-001

Staff each role by at least two persons, a main contact and a deputy.

2.1.1. Human resources and student administration (Matriculation department)

The human resources department and student administration are responsible for an organizational view of identity management. They assure general quality about all identities within the organization. Notice that all requirements and recommendations in these chapters concern AAI-enabled accounts. Other types of accounts might be managed in a different way.

The main intentions of these processes are:

- Creation of student/staff user information
- Maintenance of student/staff user information
- Removal of student/staff user information

Generally, it is required that the above processes are well implemented.

R-002

Identify students and staff with an AAI-enabled account by a photo from an official identity card or passport.

S-003

Verify basic personal information based on an official identity card or passport by the human resources department.

R-004

Update student/staff user information within two weeks of being notified of the change.

S-005

Set an expiration date for time limited accounts (e.g., course attendees).

R-006

Perform a clean-up process regularly in order to find expired or unused accounts (e.g., guest accounts).

R-007

Disable the user accounts for student/staff no later than 6 months after the person has left.

R-008

Keep student/staff user information for identifying a person (firstname, lastname, birthdate and last known address) as long as the burden of proof for a specific delict (criminally liable). If there are any questions about it consult with your organization's legal counsel.

R-009

Perform initial credential (i.e., username and password) distribution on a separate channel. For instance, sent by postal mail to the verified home postal address.

2.1.2. IdM service manager

The service manager is responsible for the identity management service in the view of information technology and in charge of its operation. Some of the main processes are:

- Setup of support
- Availability assurance
- Reporting

The duties of this role are:

R-010

Design and implement support and operation processes. See Section 3, “Service Management” and Section 4, “Operation”.

S-011

Develop a continuous improvement process (CIP) for the identity management service.

R-012

Ensure the availability of the identity management service. See Section 3.1, “Availability”.

S-013

Provide monthly reports about availability, incidents, usage and changes to the identity management service. See Section 3.4, “Reporting”.

2.1.3. System administrator

The system administrator runs and operates the IdP system. The main duties are:

- Hard- and software setup & maintenance
- Configuration and changes
- Monitoring
- Backup/Restore
- Security

R-014

Implement and document configuration changes. See Section 4.7, “Documentation”.

S-015

Set up a monitoring system for the IdP. See Section 4.1, “Monitoring”.

R-016

Implement a backup, backup verification and restoration process. See Section 4.4, “Backup & Restore”.

R-017

Ensure technical security of the IdP. See Section 4.5, “Security”.

2.2. Data sources

Data sources are the place where student/staff user information is stored. In the context of IdM this information consists of the student/staff attributes which might be released to resources.

S-018

Store user information in a single source (directory, database etc.).

R-019

Ensure consistent, perpetual aggregation (same keys on the different sources) if user data is merged from different sources.

2.3. Policies

This section focuses on policies regarding the IdM, such as recommendations about the password security, level of authentitcation (strong authentication) and data protection issues.

2.3.1. Password policy

When username and password credentials are used for authentication:

R-020

Publish a password policy that describes the requirements and usage of the password.

R-021

Require passwords to be at least 6 characters.

S-022

Require passwords to be at least 8 characters.

S-023

Require passwords to be a mix of lower and upper case characters, digits and punctuation characters of the ASCII character set.

S-024

Disallow passwords composed of common dictionary words.

S-025

Require passwords to be changed at least once a year.

S-026

Disallow reuse of a password for at least 5 years.

S-027

Detect and mitigate possible brute-force attacks (against login and password changes) by requiring a five minute time delay after three failed attempts.

2.3.2. Level of authentication

R-028

Transmit username/password by means of an encrypted channel (e.g., HTTPS).

Strong authentication

For some applications (e.g., those containing sensitive data like grades, financial or personal information) a higher level of authentication should be supported by the IdP.

S-029

Use at least two-factor authentication (e.g., X.509 user certificates, RSA Secure ID etc.) for applications that require strong authentication.

2.4. Regulations & Compliance

This section refers to some general regulations concerning privacy and data protection. The organization may also have its own compliance standards and processes. Every organization has to obey federal and/or cantonal data protection regulations.

R-030

Follow all (federal, cantonal and organizational) applicable privacy and data protection regulations. If there are any questions about these regulations consult with your organization's legal counsel.

The guidelines published by The Federal Data Protection and Information Commissioner [FDPIC] may be considered helpful.

2.4.1. Privacy & data protection

R-031

Store and transmit only that information, which is required to fulfill services for users.

Attribute release and filter policy

R-032

Maintain attribute release and filter policy information within the SWITCHaai resource registry [AAIRR] and validate it at least twice a year.

User consent

R-033

Ensure that the user is informed of, and consents to, the release of personal information to a resource.

S-034

Use [uApprove] to implement user consent.

3. Service Management

The Service Management chapter contains requirements and recommendations about running the Identity Managament service. Its focus is to support availability, emergency processes and reporting.

3.1. Availability

In the context of availability, a distinction is made between planned and unplanned downtimes.

S-035

Ensure that planned downtimes only occur during defined maintenance windows.

S-036

Document a service level description (SLD) which includes the:

- Maximum number of planned downtimes per year (e.g., at most 12 planned downtimes).
- Maximum cumulative downtime per year (e.g., will not exceed 72 hours per year).
- Method for communicating location and lead time for downtime announcements.
- Method for communicating location for unplanned downtime announcements.

S-037

Define the maximum tolerable downtime (MTD) to be equal to the MTD for the organization's other business-critical systems (e.g., at most 2h during standard office hours).

3.1.1. Maintenance

The section about maintenance summarizes some practices about maintenance windows. When they should occur and how they should be announced.

Maintenance windows

S-038

Define fixed recurring maintenance windows (for standard system updates, such as the installation of patches or new software releases). Define the maximum length per maintenance window, too.

S-039

Ensure users are aware of the maintenance windows and their consequences. Announce (irregular) maintenance windows at least 48h in advance (e.g., on the IdP login page).

S-040

Schedule maintenance windows for off-peak times.

S-041

Do not schedule maintenance windows more frequently than once per week.

S-042

Do not exceed the defined downtime per maintenance window.

3.1.2. Clustering and High Availability

The IdP is an enterprise service and should be deployed in a manner that ensures scalability and availability. A clustered setup meets this requirements.

S-043

Deploy the IdP service in a clustered setup. Ensure requests are routed to operational nodes only.

S-044

Ensure a standby system is available for manual failover if a clustered setup is infeasible.

Load balancing and failover

S-045

Use a load balancer to distribute workload amongst IdP nodes. Session affinity or sticky sessions (requests from the same client always get routed back to the same server) should be supported by the load balancer.

Session and user data redundancy

S-046

Enable IdP user session synchronization between clustered IdPs.

S-047

Ensure that the data sources used by the IdP as well as the load balancer itself are not a single point of failure.

3.2. Support

The support section describe requirements and recommendations regarding help desk and problem management processes concerning the IdM service.

3.2.1. Help desk

R-048

Maintain a website for end user support and provide the URL to the SWITCHaai resource registry [AAIRR] for inclusion on the Central SWITCHaai help-desk web page [AAIHelpdesk].

S-049

Use a group phone number and e-mail address (e.g., aai-support@example.org) as the support contact point.

S-050

Be reachable during standard office hours (9-12 and 13-17 on business days).

S-051

Ensure a first response on support requests within 4 business hours.

S-052

Do passwords resets either by personal identification at the helpdesk or postage to the verified home address.

3.2.2. Problem Management

S-053

Use an issue tracking system for end user and IdP operator reported problems.

S-054

Use an knowledge base that help desk personnel can use for diagnosing and solving problems.

S-055

Publish commonly encountered problems and recommended troubleshooting steps at a location typically consulted by users.

3.3. Emergency management

The following section contains some practices concerning disaster recovery and escalation procedures in the case of an unplanned outage of the IdP.

Disaster Recovery

Disaster recovery focuses on the steps required to bring a service back into normal operation in the event of fatal problems.

S-056

Document and test a disaster recovery procedure. The procedure should be tested at least twice a year by the staff in charge of operating the IdP.

IdP revocation

An Identity Provider Emergency Disabling Procedure [IdPRevocation] is available within the SWITCHaai federation.

R-057

Review the Identity Provider Emergency Disabling Procedure [IdPRevocation] at least twice a year with the staff in charge of operating the IdP.

Escalation procedure(s)

Escalation procedures define under what circumstances particular issues are reported to the organization's management. It specifies which persons from the management have to be involved, and which body is in charge of making decision(s) in a given situation.

S-058

Specify an escalation procedure for the IdP service. Review the escalation procedure at least twice a year with the staff in charge of operating the IdP.

3.4. Reporting

Reporting describes the collection and visualization of facts and metrics concerning the quality, scalability etc. of IdM service.

General usage statistics

S-059

Collect statistics on total number of authentications, authentications of distinct users and failed login attempts at the IdP.

S-060

Collect statistics on total number of accessed internal and external resources (service providers).

S-061

Collect statistics about which attributes are released.

S-062

Report collected information on a daily, weekly, monthly and yearly basis. Shorter time scales may allow better analysis of trends (e.g., peak usage).

Availability report

S-063

Generate reports about the availability of the IdP service. Include both the availability (in %) for specific time periods (week/month/year) and the number of downtimes per corresponding period.

4. Operation

This chapter deals with operational issues. It covers aspects like monitoring, alerting, logging, release and configuration management as well as security.

4.1. Monitoring

IdP monitoring is a good practice for pro-active incident and problem management. It helps to keep potential downtimes low and provides an overview about the service availability.

Network

R-064

Ensure that the IdP is monitored in a manner consistent with the user's interaction with the service (e.g., the monitoring system uses a similar network path as the user).

S-065

Test no less than every 5 minutes.

S-066

Test reachability and latency.

S-067

Test (port) connectivity.

S-068

Test that the IdP responds to status request (e.g., https://idp.example.org/idp/Status).

S-069

Test that a dedicated test user account is able to log in to the IdP.

Host

R-070

Ensure that time synchronization (i.e., NTP) is running.

S-071

Alert if CPU usage exceeds 60%.

S-072

Alert if memory usage exceeds 80%.

S-073

Alert if disk usage exceeds 75%.

Log files

R-074

Monitor operating system log files (e.g., messages, syslog, secure) for error entries. Suspicious entries should be filtered to detect possible break-in attempts.

S-075

Monitor operating system log files (e.g., messages, syslog, secure) for warning entries.

R-076

Monitor webserver log files (e.g., access.log, error.log) for error conditions. Suspicious entries should be filtered to detect possible break-in attempts or abuse.

R-077

Monitor these log files for ERROR entries:

- Application container log files
- IdP log files
- Data source log files

S-078

Monitor these log files for WARN entries:

- Application container log files
- IdP log files
- Data source log files

Other

S-079

Monitor IdP profile endpoints for expired certificates (i.e., the configured X.509 certificates).

4.2. Alerting

In case of unexpected behavior in the system it is very important to alert people in order to react and fix the problem fast.

R-080

Send e-mail or similar alerts to the IdP operator group in the event of ERROR (i.e., service disrupting) messages in any of the monitored log files.

4.3. Logging

It is not possible to keep all log files forever, therefore log rotation should be used. But it could be necessary to track problems over a time or have access to older logs in case of an audit, responsibility issues or other legal reasons.

R-081

Keep log files as long as the burden of proof for a specific delict (criminally liable) requires it. If there are any questions about it consult with your organization's legal counsel.

S-082

Keep log files for at least 6 months.

R-083

Verify that only permitted staff have access to the log files regularly.

R-084

Keep a log of the access to the personal data (e.g., actions concerning data sources).

S-085

Rotate web server and IdP log files daily.

S-086

Compress log files after being rotated.

S-087

Prevent log files from being overwritten or altered (e.g. by setting appropriate permissions after log rotation).

R-088

Anonymize user identifying data (client IP address, username, ...) when copies of log files leave the organization.

4.3.1. IdP logfiles

The requirements and suggestions in this section are [Shibboleth] IdP specific, analogous steps should be taken if another SAML implementation is used.

idp-process.log

S-089

Use the log level INFO in a production environment.

IdP audit log

S-090

Ensure that IdP generates an audit log with the following information:

- Audit event time
- ID of the relying party
- ID of the response
- Principal name
- Authentication method
- IDs of the released attributes
- Name identifier
- IDs of the assertion
- Request binding
- Response binding

See SWITCHaai IdP deployment information [IdPDeployment] for details.

4.4. Backup & Restore

It is a good practice to have backups of your IdP system. The main objective is to restore a broken service quickly. A backup history makes sense in case the system was compromised.

S-091

Perform a daily incremental backup of the IdP.

R-092

Perform a weekly full backup of the IdP.

S-093

Ensure that backups are stored in an offsite and secure location.

S-094

Use a backup retention built on the *grandfather-father-son* principle with the following generation retention:
Generation: Grandfather
Rotation: Yearly
Retention: 1
Generation: Father
Rotation: Weekly
Retention: 4
Generation: Son
Rotation: Daily
Retention: 7

S-095

Test the restore procedure at least twice a year and ensure it does not exceed 4 hours.

4.5. Security

The next section covers host and network security as well as X.509 certificates.

4.5.1. Host security

Access control

R-096

Use secure and strong authentication methods for logins on the server (i.e, use SSH with public key authentication, one-time passwords, tokens or similar).

R-097

Restrict access to strong authentication methods and/or specific network ranges.

R-098

Do not permit remote root logins.

S-099

Change the root password regularly.

S-100

Set up and use a host intrusion detection system (IDS).

User accounts

S-101

Review host login accounts and permissions (separation of duties) regularly. That means users have only the rights needed for doing their work.

4.5.2. Network security

Firewall

R-102

Protect the IdP with a firewall or a packet filter.

S-103

Ensure that the front and back channel HTTPS ports (usually 443 and 8443) are the only ports accessible from the external network.

Domain names

S-104

Use an FQDN that is part of the organizations primary domain (e.g., aai-logon.example.org).

HTTPS certificates

S-105

Use an extended validation (EV) certificate from a browser trusted CA for front channel connections (e.g., the login page).

4.5.3. X.509 keys and certificates

R-106

Ensure private keys are only readable by the IdP process.

R-107

Create a new key pair after at most 3 years.

R-108

Discontinue the use of private keys that have been compromised or were on a compromised host. Certificates issued by a public CA have to be revoked. Self-

signed certificates used for the IdP metadata have to be removed from the metadata immediately.

R-109

Configure key revocation checking (e.g., CRL).

4.6. Releases and updates

In order to keep a service in good running condition it is important to apply updates in a timely fashion.

Operating system updates

R-110

Apply critical updates within two weeks of their release.

S-111

Apply all updates within a month of their release.

IdP updates

R-112

Apply critical updates within two weeks of their release.

S-113

Apply all updates within a month of their release.

4.7. Documentation

The objective of documentation is to preserve knowledge and to ensure that the setup is understandable for others. Keep in mind that documentation is only useful if it is up to date.

Data sources

S-114

Document the data source, authoritative source and data steward for each attribute resolved by the IdP.

Setup

R-115

Document the following aspects of the IdP setup:

- Operating system, kernel version and installed package versions
- Network addresses, host names, accessible ports
- Running services and their configuration location, cron jobs, log location and rotation schedule

Startup and shutdown

S-116

Document commands for starting and stopping the IdP.

S-117

Document some tests that can be used to verify that the service is started correctly.

Changelog

S-118

Document all host and IdP configuration changes.

4.8. Education & Training

S-119

Educate and train the staff to operate the IdP.

4.9. IdP Configuration

This section contains requirements and recommendations about IdP configuration such as metadata loading, ID management, attribute resolving and attribute filtering. See SWITCHaai IdP deployment information [IdPDeployment] for details.

The requirements and suggestions in this section are [Shibboleth] IdP specific, analogous steps should be taken if another SAML implementation is used.

4.9.1. ID management

R-120

Ensure that the IdP's *entityID* is in the form of *https://idp.example.org/idp/shibboleth*.

S-121

Do not make the *entityID* a component of the persistent ID value.

R-122

Do not reassign a *swissEduPersonUniqueID* to another identity.

4.9.2. Metadata (SAML)

The SWITCHaai federation metadata establishes trust on the technical level between federation participants. Therefore its authenticity has to be checked and it has to be kept up-to-date. The metadata is signed with a certificate that chains up to the the SWITCHaai trust root (SWITCHaai Root CA).

R-123

Use the SWITCHaai federation metadata as published by SWITCH.

S-124

Update Metadata on an hourly basis.

R-125

Update Metadata on an daily basis.

R-126

Install the SWITCHaai trust root after the certificate fingerprint have been verified with SWITCH.

R-127

Verify the signature of the metadata against the SWITCHaai Metadata Signing [MDS] certificate after each download.

S-128

Check the SWITCHaai Metadata Signing [MDS] certificate and its chain against the CRL.

4.9.3. Certificates

The IdP needs at least one certificate to sign SAML assertions.

S-129

Use a self-signed certificate for signing SAML assertions.

R-130

Meet the Requirements for SAML2 Metadata embedded certificates [EmbdCerts] guidelines for certificates used by the IdP.

4.9.4. Attribute resolving

R-131

Comply with the latest AAI Attribute Specification [AttrSpec] published by SWITCH.

Other attributes may be used with service providers, as agreed upon with them.

Data source connection

R-132

Use a secured connection (e.g., TLS/SSL) to the data source (LDAP, RDBMS) except on local host.

S-133

Use a dedicated service user for connecting to data sources.

R-134

Do not allow the IdP to add, update or delete information from a data source unless the IdP is authoritative for that information.

4.9.5. Attribute filtering & release

R-135

Ensure that the default attribute filter policy is to deny the release of information.

S-136

Use the customized `attribute-filter.xml` as provided by the *SWITCHaai resource registry [AAIRR]*.

S-137

Maintain local or custom attribute filtering rules in a separate file.

S-138

Release only those attributes explicitly requested by the service provider.

S-139

Use persistent name identifiers with services that support identification of returning users (i.e., *targetedID* instead of *swissEduPersonUniqueID*).

4.9.6. Configuration & Change management

S-140

Use a version control system to track changes to the IdP's configuration files.

The [Shibboleth] IdP supports configuration loading from a subversion repository.

Test system

S-141

Operate a test system (staging system) which is equivalent to the productive system.

S-142

Apply and verify each change within the test system before applying it to the production system.

4.9.7. Resource Registry

To run an IdP within the SWITCHaai federation the IdP has to be registered in the SWITCHaai resource registry [AAIRR], the central federation management system.

R-143

Keep the information about the identity provider in the SWITCHaai resource registry [AAIRR] up to date (e.g. service locations, certificates, contacts etc.).

R-144

Verify the IdP information in the SWITCHaai resource registry [AAIRR] at least twice a year.

5. Infrastructure requirements

5.1. Environment

The environment section contains recommendations about the server room. Generally, the IdP server should meet the same requirements for physical security as other business critical servers.

Server room access control

R-145

Ensure that only entitled staff members have access to the server room.

S-146

Log entries to the server room. This may be done by an electronical access control system.

Arrangement against force majeure

R-147

Place server hardware, including peripheral equipment, at least 1 meter above the floor.

S-148

Use a server rack.

S-149

Ensure that the server room have fire-safe walls, windows and doors.

S-150

Monitor the room temperature and humidity. Alarm and react if abnormal numbers are measured.

R-151

Connect the server(s) to an uninterruptible power supply (UPS) which can operate server(s) for at least 1 hour.

5.2. Network

This section contains information about network connectivity.

S-152

Ensure that the server(s) are connected to more than one LAN switch for redundancy.

Consider whether the external network connection (LAN to WAN) should be redundant (i.e., the LAN is connected in two different paths or using more than one provider).

S-153

Use 100Mbit/s links at minimum.

5.3. Server hardware

The server may be real hardware or a virtual machine. For specific hardware requirements (e.g., CPU, Memory, Disk etc.) take a look at the SWITCHaai IdP deployment information [IdPDeployment].

Vendor & Supplier

The vendor of your hardware should be well known and established.

R-154

Ensure that you have sufficient spare hardware or an on-site support contract for all hardware in production.

S-155

Use support contracts with a maximum supplier reaction time of 1 working day or have an identical configured IdP as stand-by.

5.4. Software

For specific software requirements (e.g., web server, application container, Java runtime environment, libraries etc.) take a look at the SWITCHaai IdP deployment information [IdPDeployment].

5.4.1. Operating system

S-156

Use an operating system for which security patches are provided through the vendor. For Linux operating system, a distribution with long-term support (5 years) should be chosen.

Time synchronization

R-157

Ensure that the maximum clock drift does not exceed 1 minute from the reference time. Use of NTP is recommended.

Terms and definitions

AAI	Authentication and Authorization Infrastructure
ASCII	American Standard Code for Information Interchange
back channel connection	System initiated web-service connection to the IdP
BCP	Best Current Practices
CA	Certification authority
CIP	Continuous Improvement Process
CPU	Central processing unit
CRL	Certificate revocation list
FQDN	Fully Qualified Domain Name
front channel connection	User initiated browser connection to the IdP
HTTPS	Hypertext Transfer Protocol Secure
IdM	Identity Management
IdP	Identity Provider. This term is also known as Home Organization, like mentioned in the AAI Policy [AAIPol].
IDS	Host Intrusion Detection
IP	Internet Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MTD	Maximum Tolerable Downtime
NTP	Network Time Protocol
PKI	Public key infrastructure
RDBMS	Relational database management system
SAML	Security Assertion Markup Language
SLD	Service Level Description
SSH	Secure Shell
SSL	Secure Socket Layer

student/staff user information	Student/Staff user information means user account data (e.g., username, password) as well as attributes (e.g., firstname, lastname, address, phone, birth date, study level, affiliation, exmatriculation, etc.)
SWITCHaai	The SWITCH AAI federation
TLS/SSL	Transport Layer Security / Secure Socket Layer
two-factor authentication	Two-factor authentication (T-FA) is a system wherein two different factors are used in conjunction to authenticate. Authentication factors can be human factors ("something you are"), personal factors ("something you know") and technical factors ("something you have").
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
WAN	Wide Area Network

References

[AAIPol] *AAI Policy [AAIPol]*. SWITCH. 7.2004. http://www.switch.ch/aai/docs/AAI_Policy.pdf [http://www.switch.ch/aai/docs/AAI_Policy.pdf] .

[AAIRR] *SWITCHaai resource registry [AAIRR]*. https://rr.aai.switch.ch/ [https://rr.aai.switch.ch/].

[AttrSpec] *AAI Attribute Specification [AttrSpec]*. SWITCH. 9.2007. http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf [http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf] .

[EmbdCerts] *Requirements for SAML2 Metadata embedded certificates [EmbdCerts]*. SWITCH. 9.2008. http://www.switch.ch/aai/support/embeddedcerts-requirements.html [http://www.switch.ch/aai/support/embeddedcerts-requirements.html].

[FDPIC] *The Federal Data Protection and Information Commissioner [FDPIC]*. The Federal Authorities of the Swiss Confederation. http://www.edoeb.admin.ch/ [http://www.edoeb.admin.ch/].

[IdPRevocation] *Identity Provider Emergency Disabling Procedure [IdPRevocation]*. SWITCH. 08.2009. http://www.switch.ch/aai/support/emergency [http://www.switch.ch/aai/support/emergency].

[AAIHelpdesk] *Central SWITCHaai help-desk web page [AAIHelpdesk]*. SWITCH. 08.2009. http://www.switch.ch/aai/help [http://www.switch.ch/aai/help].

[IdPDeployment] *SWITCHaai IdP deployment information [IdPDeployment]*. SWITCH. 09.2009. http://www.switch.ch/aai/support/identityproviders/ [http://www.switch.ch/aai/support/identityproviders/].

[MDS] *SWITCHaai Metadata Signing [MDS]*. SWITCH. 10.2008. https://www.switch.ch/pki/aai/ [https://www.switch.ch/pki/aai/].

[Shibboleth] *[Shibboleth]*. Internet2. http://shibboleth.internet2.edu/ [http://shibboleth.internet2.edu/].

[uApprove] *[uApprove]*. http://www.switch.ch/aai/uapprove [http://www.switch.ch/aai/uapprove].

A. Change log

Revision History

Revision 1.0 12.11.2009

Final Version. Reviewed by the SWITCHaai team. Acknowledgment to Michael Hausherr (FHNW), Alexandre Roy and Etienne Dysli (UNIL), Roberto Mazzoni and Luzian Scherrer (UZH), Matthias Hutter (BFH) and Damiano Bianchi (TI-EDU) for community feedback.