SWITCH
Serving Swiss Universities

BEST CURRENT PRACTICES

for operating a SWITCHaai Service Provider

11. August 2010

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 a Service Provider (SP) within the SWITCHaai federation in production use. It is meant to cover service management and operational related aspects as well as the technical infrastructure for successfully operating an SP.

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 operator of a Service Provider or service manager responsible for the resource that is part of the SWITCHaai federation. This includes federation members as well as federation partners.

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

1.3. Organization of the Document

The document is divided into four main parts:

- Web application 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 SPs.

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. Web Application Management

Web application management describes how to manage responsibilities and business processes around a service provider. In addition this includes integration into the SWITCHaai federation as well as authorization guidelines and attribute usage.

2.1. Roles and Responsibilities

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

☞ **R-001**

Staff each role by at least two persons, a main contact and a deputy contact. A person can staff multiple roles.

2.1.1. Business Responsible

The business responsible is in charge of the overall service and its content. The duties of this role are:

☞ **R-002**

Assure that customer and business needs are addressed and tracked.

☞ **R-003**

Verify compliance with privacy and data protection. See Section 2.2, “Regulations & Compliance”.

☞ **R-004**

Verify that the service management is well implemented. See Section 3, “Service Management”.

☞ **R-005**

Specify authorization rules and access control. See Section 2.3, “Authentication & Authorization”.

☞ **R-006**

Specify attribute usage. See Section 2.5, “Attribute Usage”.

2.1.2. Service Manager

The service manager is responsible for the 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-007

Design and implement the integration into the SWITCHaai federation.

☞

R-008

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

S-009

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

☞

R-010

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

S-011

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

☞

R-012

Keep administrative, support and technical contacts up to date in the SWITCHaai Resource Registry [AAIRR]. See Section 4.9.6, “Resource Registry”.

2.1.3. System Administrator

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

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

☞

R-013

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

S-014

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

R-015

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

R-016

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

2.2. 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-017

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.

2.2.1. Privacy & Data Protection

R-018

Request only information, which is absolutely required to operate the service for users. See Section 2.5, “Attribute Usage”.

R-019

Store as little user specific information as possible.

2.3. Authentication & Authorization

Authentication is the act of confirming an identity and happens at the IdP. *Authorization* is the function of defining access rights.

2.3.1. Level of Authentication

S-020

Require strong authentication (two-factor authentication) for resources containing confidential and/or sensitive information, if supported by the IdPs of the users.

2.3.2. Access Control

S-021

Use attributes provided by the IdP for access control rules. (E.g., home organization, affiliation, study branch etc.)

S-022

If users cannot be authorized due to a missing common set of attributes, consider the usage of the Group Management Tool or the Virtual Organization service. (Group based access control)

☞

R-023

Define access control rules as restrictive as possible.

☞

R-024

In general do not grant access to VHO users unless the resource is used by a VHO group and then limit the access to this group (using the *eduPersonEntitlement*).

2.3.3. Implementation

Access rules can either be implemented using the SP (for an example refer to Access Rules [accessRules]) or configured within the resource application itself.

For more information about the Group Management Tool refer to the Group Management Tool [GMTool].

2.4. Integration

This section contains some general hints for integrating SWITCHaai support into resource applications, which need to be modified.

In some cases the application was already modified to support SWITCHaai (see Shibboleth Enabled Applications and Services [ShibEnabled]). In those cases the configuration only has to be adapted properly.

2.4.1. User Information Management

In order to integrate SWITCHaai support into an application the following four CRUD operations have to be implemented:

- Create user information
- Read user information
- Update user information
- Delete user information

This applies only if persistent personalization is required by the application.

S-025

Register a new user automatically within the application using the data provided by the IdP.

☞

R-026

Update the attributes stored in the application data store with the ones provided by the IdP if they differ.

☞

R-027

Ensure that deleted/disabled users have no access.

S-028

Use the *persistentID* or the *eduPersonTargetedID* instead of the *swissEduPersonUniqueID* for persistent identification of users.

2.4.2. Non-AAI Users

The resource might be accessible for users who do not have a SWITCHaai account. One possibility is to maintain a local authentication and authorization mechanism in parallel (dual login). Another alternative is to use the VHO Service [VHOservice].

S-029

Due to security and usability, do not implement dual login.

S-030

Sign up for a VHO group for your resource if you have to maintain non-SWITCHaai users.

2.4.3. Home Organization Discovery

For integrating the *Home organization discovery service* into the user interface, there are different options:

- Classic DS, aka. Central WAYF
- Embedded WAYF [embeddedWAYF]
- Login Link Composer [composeLoginURL]
- Local DS implementation
- Local login only (single pre-configured IdP)

S-031

Use the Embedded WAYF [embeddedWAYF] as preferred user interface integration.

S-032

Do not use a local DS unless the SP participates in multiple federations.

2.4.4. Attributes

S-033

Define a configurable mapping between the SP attributes (e.g., provided as environment or HTTP header variables) and the application variables.

S-034

Set the directive *ShibUseHeaders On* only if your application is not able to access the web server's environment variables.

2.5. Attribute Usage

Attribute requirements can be configured in the SWITCHaai Resource Registry [AAIRR].

☞ R-035

Only declare attributes as *required*, which are absolutely necessary to provide the service to the user.

☞ R-036

Only declare attributes as *desired*, which add value for the user using the application.

S-037

Provide a description in the SWITCHaai Resource Registry [AAIRR] of why an attribute is required/desired.

2.6. Federation Partner

☞ R-038

Consult the Federation Partner [FedPartner] deployment information.

S-039

Stay in contact with the RRA Operator from the supporting organization (Because of attribute requirement change approval).

3. Service Management

The Service Management chapter contains requirements and recommendations about running the 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-040

Ensure that planned downtimes only occur during defined maintenance windows.

S-041

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-042

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

3.1.1. Maintenance

The section about maintenance summarizes practices regarding maintenance windows, when they should occur and how they should be announced.

Maintenance Windows

S-043

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

S-044

Ensure users are aware of maintenance windows and their consequences. Announce maintenance windows at least 2 working days in advance (e.g., on the SP home page).

S-045

Schedule maintenance windows for off-peak hours (e.g., before 8 am during weekdays)

S-046

Plan maintenance of the SP while the SWITCHaai team is reachable. If critical updates are planned, notify the SWITCHaai team in advance.

S-047

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

S-048

Do not exceed the defined downtime per maintenance window.

3.1.2. Clustering and High Availability

If the web application is an enterprise service, it should be deployed in a manner that ensures scalability and availability. A clustered setup meets this requirement.

S-049

Deploy the web application in a clustered setup. Ensure requests are routed to operational nodes only.

S-050

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

Session and User data Redundancy

S-051

Use one of the supported session synchronization mechanisms of the SP (e.g., memcached, database).

S-052

Ensure that backend systems (e.g., databases) used by the SP as well as the load balancer itself are not a single point of failure.

Load balancing and Failover

S-053

Use a load balancer to distribute workload amongst SP nodes. Session affinity or sticky sessions (requests from the same client always get routed to the same server) should be supported by the load balancer if it is not implemented by the SP (See the section called “Session and User data Redundancy”).

3.2. Support

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

3.2.1. Help Desk

☞

R-054

Maintain a website for end user support and add its URL to the SWITCHaai Resource Registry [AAIRR] so it can be shown to the user on the Central SWITCHaai Help Desk page [AAIHelpdesk].

S-055

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

S-056

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

S-057

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

3.2.2. Problem Management

S-058

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

S-059

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

S-060

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 service.

Disaster Recovery

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

S-061

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 service.

Certificate Revocation

☞ R-062

If a CA issued X.509 certificate is used on the SP host, revoke it following the procedures given by the CA.

☞ R-063

Remove the certificate of the SP from the SWITCHaai Resource Registry [AAIRR] in case of compromise. After recovery, the certificate(s) and private key(s) will have to be regenerated. Add the new certificate to the SP entry in the SWITCHaai Resource Registry [AAIRR].

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-064

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

3.4. Reporting

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

General Usage Statistics

S-065

Collect statistics on total number of logins at the service.

S-066

Collect statistics on total number of logins from internal and external organizations (identity providers).

S-067

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

Availability Report

S-068

Generate reports about the availability of the service. Include both the availability (in %) for specific time periods (day/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

SP 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-069

Ensure that the SP 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-070

Test no less than every 5 minutes.

S-071

Test reachability and latency.

S-072

Test (port) connectivity.

S-073

Test that the SP responds on the status URL e.g., https://sp.example.org/Shibboleth.sso/Status.

S-074

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

Host

☞

R-075

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

S-076

Alert if CPU usage exceeds 60% during normal operations.

S-077

Alert if memory usage exceeds 80%.

S-078

Alert if disk usage exceeds 75%.

Log Files

☞

R-079

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-080

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

☞

R-081

Monitor web server 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-082

Monitor these log files for ERROR entries:

- Application log files
- SP log files
- Data source log files

S-083

Monitor these log files for WARN entries:

- Application log files
- SP log files
- Data source log files

Other

S-084

Monitor SP HTTPS ports for expired certificates (i.e., the configured X.509 certificates).

4.2. Alerting

In case the system behaves unexpectedly it is very important to alert staff in order to react and quickly fix the problem.

☞ R-085

Send e-mail or similar alerts to the SP 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. However it still has to be possible to track problems over a longer period or have access to older logs in case of an audit, responsibility issue or other legal reasons.

☞ R-086

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

S-087

Keep log files for at least 6 months.

☞ R-088

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

S-089

Rotate web server and SP log files daily.

S-090

Compress log files after rotation.

S-091

Prevent log files from being overwritten or manipulated (e.g. by setting appropriate permissions after log rotation, copying files to another server or using secure remote logging).

☞ R-092

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

4.3.1. SP Log Files

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

shibd.log

S-093

Use the log level INFO in a production environment.

native.log

S-094

Use the log level INFO in a production environment.

transaction.log

S-095

Use the log level INFO in a production environment.

S-096

Use the transaction.log as audit log.

4.3.2. Resource Log Files

S-097

Log resource transactions (e.g., administrative tasks, operations etc.).

4.4. Backup & Restore

The main objective having backups of your SP system is to restore a broken service quickly. A backup history makes sense in case the system was compromised.

☞

R-098

Perform full backups of the SP regularly (e.g., at least monthly).

S-099

Perform a daily incremental backup of the SP.

S-100

Ensure that backups are stored in an off-site and secure location.

S-101

Use a backup retention built on the *grandfather-father-son* principle with the following generation retention:
Generation: Grandfather
Rotation: Monthly
Retention: 12
Generation: Father
Rotation: Weekly
Retention: 4
Generation: Son
Rotation: Daily
Retention: 7

S-102

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-103

Use secure and strong authentication methods for logins on the server (i.e., use SSH2 with public key authentication, one-time passwords, tokens or similar).

☞ R-104

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

☞ R-105

Do not permit remote root logins.

S-106

Change the root password regularly.

S-107

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

User Accounts

S-108

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

S-109

Set up an unprivileged user account for running the SP daemon (e.g., shibd).

S-110

Assure that files reloaded from external resources (e.g., metadata) are writable by the SP process.

4.5.2. Network Security

Firewall

☞

R-111

Protect the SP with a firewall or a packet filter.

S-112

Ensure that the HTTPS port (usually 443) and HTTP (usually 80) are the only ports accessible from the external network.

HTTPS

S-113

Redirect HTTP to HTTPS.

S-114

Use an extended validation (EV) certificate from a browser trusted CA.

S-115

Use TLS v1.0 or higher with strong ciphers.

4.5.3. X.509 Keys and Certificates

☞

R-116

Ensure private keys are only readable by the SP (e.g., shibd) process.

☞

R-117

Create a new key pair after at most 3 years.

☞

R-118

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 SP metadata have to be removed from the metadata immediately.

☞

R-119

Configure key revocation checking (e.g., CRL), where feasible (e.g., metadata signature).

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-120

Apply critical updates within two weeks after their release.

S-121

Apply relevant updates within a month after their release.

SP Updates

☞

R-122

Apply critical updates within two weeks after their release.

S-123

Apply relevant updates within a month after their release.

Web Application Updates

☞

R-124

Apply critical updates within two weeks after their release.

S-125

Apply relevant updates within a month after 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.

Backend Systems

S-126

Document data flow to and from backend systems.

Setup

☞

R-127

Document the following aspects of the SP 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-128

Document commands for starting and stopping the SP.

S-129

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

Change Log

S-130

Document all host and SP configuration changes.

4.8. Education & Training

S-131

Educate and train the staff to operate the SP.

4.9. SP Configuration

This section contains requirements and recommendations about SP configuration such as metadata loading, session initiating, attribute mapping and filter policy etc. See SWITCHaai SP Deployment Information [SPDeployment] for details.

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

4.9.1. ID Management

☞

R-132

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

S-133

Provide metadata access on the URL in the SP *entityID*.

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 SWITCHaai trust root (SWITCHaai Root CA).

☞

R-134

Use the SWITCHaai federation metadata as published by SWITCH.

S-135

Update metadata on an hourly basis.

☞

R-136

Update metadata on a daily basis.

☞

R-137

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

☞

R-138

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

☞

R-139

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

4.9.3. Certificates

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

S-140

Use a self-signed certificate for signing SAML assertions.

S-141

Use a second self-signed certificate for rollover/emergency issues.

☞

R-142

For certificates used by the SP comply with the Requirements for SAML2 Metadata Embedded Certificates [EmbdCerts] guidelines.

4.9.4. Attributes

☞

R-143

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

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

Attribute Filter Policy

☞

R-144

Use the attribute filter policy published by SWITCH.

S-145

Maintain local or custom attribute filter policies in a separate file.

Attribute Map

☞

R-146

Use the attribute map published by SWITCH.

S-147

Uncomment local attributes if necessary.

4.9.5. Configuration & Change Management

S-148

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

S-149

Check integrity of files reloaded from external resources (e.g., metadata) before replacing the local configuration (e.g., file signature, trusted TLS/SSL download etc.)

Test System

S-150

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

S-151

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

4.9.6. Resource Registry

To run an SP within the SWITCHaai federation the SP has to be registered in the SWITCHaai Resource Registry [AAIRR], the central federation management system.

R-152

Provide the mandatory basic resource information. Choose *default* as Relying Party. Choose SAML 1 Attribute Push Relying Party [AttributePush] or SAML 2 Attribute Pull Relying Party [AttributePull] only if a there is a special reason for it.

R-153

Provide administrative, technical and support contacts.

R-154

Review *attributes requirements* as well as *intended audience* if they are accurate.

R-155

Keep the information about the Service Provider in the SWITCHaai Resource Registry [AAIRR] up to date (e.g. service locations, certificates, contacts etc.).

R-156

Verify the SP's resource description information in the SWITCHaai Resource Registry [AAIRR] at least twice a year.

4.9.7. Session Initiation

S-157

Configure the DS session initiator favoring SAML2 over SAML1.

S-158

Configure a local session initiator favoring SAML2 over SAML1 using the home organizations IdP.

4.9.8. Bilateral Configuration

S-159

Follow the Bilateral Configuration [bilateralConfiguration] instructions if the SP interoperates with non SWITCHaai IdPs.

4.9.9. Multiple Applications

S-160

Use different application identifier if the application needs different settings.

☞

R-161

Choose another *entityID* and add a separate resource description in the SWITCHaai Resource Registry [AAIRR], if the SP hosts multiple applications with differing attribute requirements.

5. Infrastructure Requirements

5.1. Environment

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

Server Room Access Control

☞

R-162

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

S-163

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

Arrangement against Force Majeure

S-164

Place server hardware, including peripheral equipment above the floor (e.g., 1 meter) to be protected against flooding.

S-165

Use a server rack.

S-166

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

S-167

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

S-168

Connect the server(s) to an uninterruptible power supply (UPS) which can supply server(s) for at least 1 hour with electricity after a power outage.

5.2. Network

This section contains information about network connectivity.

S-169

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-170

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.) consult your service software distributor.

Vendor & Supplier

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

☞ R-171

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

S-172

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

S-173

Choose a vendor which supports an hardware monitoring solution.

5.4. Software

For specific software requirements (e.g., web server, libraries etc.) take a look at the SWITCHaai SP Deployment Information [SPDeployment].

5.4.1. Operating System

S-174

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-175

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
BCP	Best Current Practices
CA	Certification authority
CIP	Continuous Improvement Process
CPU	Central processing unit
CRL	Certificate revocation list
CRUD	Create, Read, Update, Delete
DS	Discovery service, also known as WAYF
FQDN	Fully Qualified Domain Name
Group Management Tool	Group Management Tool
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IdP	Identity Provider
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
RRA	Resource registration authority
SAML	Security Assertion Markup Language
SLD	Service Level Description
SP	Shibboleth Service Provider. This term is also known as Resource, like mentioned in the AAI Policy [AAIPol].

SSH	Secure Shell
SSL	Secure Socket Layer
SWITCHaai	The SWITCHaai federation
TLS	Transport Layer Security
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
user information	Student/Staff user information means user account data (e.g., username) as well as attributes (e.g., first name, last name, address, phone, birth date, study level, affiliation, exmatriculation, etc.)
VHO	Virtual Home Organization
Virtual Organization	Virtual Organization
WAN	Wide Area Network
WAYF	Where Are You From

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/].

[AAIHelpdesk] *Central SWITCHaai Help Desk page [AAIHelpdesk]*. SWITCH. 08.2009. http://www.switch.ch/aai/help [http://www.switch.ch/aai/help].

[SPDeployment] *SWITCHaai SP Deployment Information [SPDeployment]*. SWITCH. 03.2010. http://www.switch.ch/aai/support/serviceproviders/ [http://www.switch.ch/aai/support/serviceproviders/].

[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/].

[embeddedWAYF] *Embedded WAYF [embeddedWAYF]*. SWITCH. http://www.switch.ch/aai/support/serviceproviders/sp-embedded-wayf.html [http://www.switch.ch/aai/support/serviceproviders/sp-embedded-wayf.html].

[composeLoginURL] *Login Link Composer [composeLoginURL]*. SWITCH. http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html [http://www.switch.ch/aai/support/serviceproviders/sp-compose-login-url.html].

[accessRules] *Access Rules [accessRules]*. SWITCH. http://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html [http://www.switch.ch/aai/support/serviceproviders/sp-access-rules.html].

[bilateralConfiguration] *Bilateral Configuration [bilateralConfiguration]*. SWITCH. http://www.switch.ch/aai/support/serviceproviders/bilateral-configuration.html [http://www.switch.ch/aai/support/serviceproviders/bilateral-configuration.html].

[GMTool] *Group Management Tool [GMTool]*. SWITCH. http://www.switch.ch/aai/support/tools/gmt.html [http://www.switch.ch/aai/support/tools/gmt.html].

[VHOservice] *VHO Service [VHOservice]*. SWITCH. http://www.switch.ch/aai/join/vho.html [http://www.switch.ch/aai/join/vho.html].

[AttributePush] *SAML 1 Attribute Push Relying Party [AttributePush]*. SWITCH. https://www.switch.ch/aai/SAML1/Attribute-Push [https://www.switch.ch/aai/SAML1/Attribute-Push].

[AttributePull] *SAML 2 Attribute Pull Relying Party [AttributePull]*. SWITCH. https://www.switch.ch/aai/SAML2/Attribute-Pull [https://www.switch.ch/aai/SAML2/Attribute-Pull].

[FedPartner] *Federation Partner [FedPartner]*. SWITCH. http://www.switch.ch/aai/join/partners.html [http://switch.ch/aai/join/partners.html].

[ShibEnabled] *Shibboleth Enabled Applications and Services [ShibEnabled]*. Internet2. https://spaces.internet2.edu/display/SHIB2/ShibEnabled [https://spaces.internet2.edu/display/SHIB2/ShibEnabled].

A. Change Log

Revision History

Revision 1.0 11.08.2010

Final Version. Reviewed by the SWITCHaai team. Acknowledgment to Beat Müller (ETHZ), Bruno Vuillemin (UniFR), Philipp Tobler (UniBE), Etienne Dysli (UniL) and Tobias Marquart (UniBas) for community feedback.