SWITCH

The Swiss Education & Research Network

AAI – Authentication and Authorization Infrastructure

AAI Services

Document management

Version/status:	1.0 / final	
Date:	15-JAN-04	
Author(s):	Christoph Graf	SWITCH
	Thomas Lenggenhager	SWITCH
	Daniela Isch	at rete ag
	André Redard	at rete ag
File name:	AAI_Services_v10.doc	
Replacing:	0.6 / 10-NOV-03	
Approved by:		

Table of Content

1. Introduction

Besides the roles of Home Organization and Resource Owner, the setup of the AAI also includes the role of an AAI Service Provider. This Service Provider is to offer a number of services that complement the activities of the other organizations involved. Given the tasks to be fulfilled, it became evident that SWITCH was the best choice for this role since these tasks were in keeping with SWITCH's charter.

The document at hand gives an overview of the services offered by SWITCH, including rough descriptions, and is also meant to serve as guidance for make or buy decisions of Home Organizations and Resource Owners.

2. Service Overview

As Figure 1 shows, SWITCH provides different AAI services, some of which are optional. The Security Service RA/CA is – although mandatory for members of the Federation – not exclusively intended for AAI purposes and therefore labeled "AAI-related".

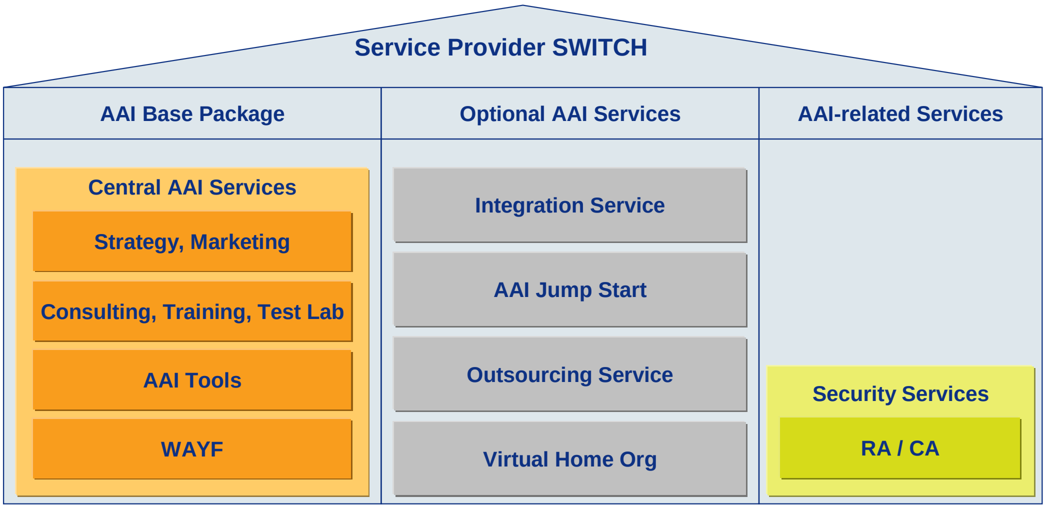

Figure 1: Service overview

In short, the individual services are characterized as follows:

Central AAI Services:

- Development and operation of central AAI systems
- Center of competence (test lab, training and consulting)
- Development of generic add-ons to Shibboleth
- Strategy and marketing

Integration Service

- Integration of Resources or Home Organization systems

AAI Jump Start Service:

- Temporary service for a limited number of resources and users
- Facilitates a Home Organization's joining the AAI Federation

Outsourcing Service:

- Permanent outsourcing service for Home Organizations

Virtual Home Organization Service:

- Operation of a virtual home organization, mainly for people with a legal right to access AAI-protected resources but without formal relationship to a “real” Home Organization

Security Services:

- Issuance of server certificates

For a better understanding of the optional AAI services, Figure 2 shows their mapping to the generic processes “Implementation/Integration” and “Operation”.

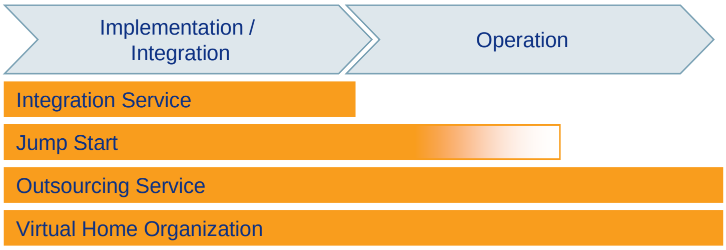

Figure 2: Characterization of the optional AAI services

2.1 Central AAI Services

In order to participate in the AAI, Home Organizations have to subscribe to the AAI Base Package, which covers central services necessary for running an AAI. The subscription includes the participation of all Resources belonging to a Home Organization.

General services rendered to more or less all participants equally such as information events, deployment guides, low-key consulting and training, test infrastructure etc. are included, while special services for individual organizations are charged separately. The AAI Base Package comprises the following services:

1. Center of Competence: Consulting, Training, Test Infrastructure

   SWITCH operates a test infrastructure not only to check new components and build up know-how it can share with other organizations, but also to provide a test Home Organization, Resource and WAYF-server which organizations can use as a counterpart for testing their own installations.

   Furthermore, SWITCH establishes regular contacts with the developers of Shibboleth in order to coordinate AAI issues and to introduce AAI-specific requirements.

2. WAYF-Server

   SWITCH operates the central WAYF-server, a register of the AAI federation’s authentication services used by Resources. In addition, SWITCH is responsible for the coordination of all the WAYF-servers in the Federation operated by individual organizations.

3. AAI Tools

   SWITCH develops and implements special AAI tools that facilitate the integration of resources, like AAI Proxy or AAI Portal, or enable an efficient operation of the AAI components, such as a resource registry.

4. Strategy and Marketing

   As the success of the AAI depends on the participation of as many organizations as possible, it is important to ensure that the organizations' changing requirements are met as much as possible and that organizations learn about the possibilities and advantages the AAI offers. Adequate marketing initiatives are therefore necessary as well as a strategic, well-coordinated further development of the AAI, both nationally and internationally. SWITCH has proven to be in an ideal position for these tasks so far and will therefore keep the responsibility for them.

Customers	• Home Organizations
Description	• Base Package: mandatory for all AAI participants • Center of competence • low-key consulting and training • test infrastructure (Home Org, Resource, WAYF-server) • Operation of central WAYF-server and coordination of individual WAYF-servers • Development of AAI tools • Strategy and marketing activities
Customer's responsibility	• Complying with AAI Policy
SWITCH's responsibility	• Complying with AAI Policy

2.2 Integration Service

Depending of the complexity of the Resources or Home Organization systems, their integration within AAI may require in-depth knowledge of Shibboleth and web technologies.

Therefore, SWITCH supports Home Organizations and Resource Owners in their integration projects. For the integration of complex Resources, SWITCH can provide a set of AAI tools as an intermediary between Shibboleth and the Resource, like e.g. the AAI Proxy and AAI Portal.

Customers	Home Organizations and Resource Owners
Description	• Professional Service in order to integrate Resources and Home Organizations systems within AAI • Implementation of AAI tools (e.g. AAI Proxy and AAI Portal) • Exact scope of the service to be defined depending on the specific project
Customer's responsibility	tasks according to the agreed project plan
SWITCH's responsibility	tasks according to the agreed project plan

2.3 AAI Jump Start

The AAI Jump Start service is aimed at Home Organizations that would like to participate in the AAI at short notice with as little effort as possible. The service is designed as a temporary service only and is meant to bridge the time gap until Home Organizations have the know-how and/or capacity to perform the tasks themselves. As a temporary service, it is only meant for a limited number of Resources and users.

SWITCH undertakes the task of operating a basic authentication system and AAI attribute directory, a web-based user interface for password administration by the end user as well as a simple Attribute Release Policy (ARP). As for the latter, the Home Organization defines the content of the ARP, while SWITCH is responsible for formal aspects and its correct implementation. SWITCH also carries out file-based bulk imports of user data provided by a Home Organization and, optionally, converts the data into AAI format.

Figure 3 shows in detail the interactions between SWITCH and the Home Organization that occur in the AAI Jump Start service:

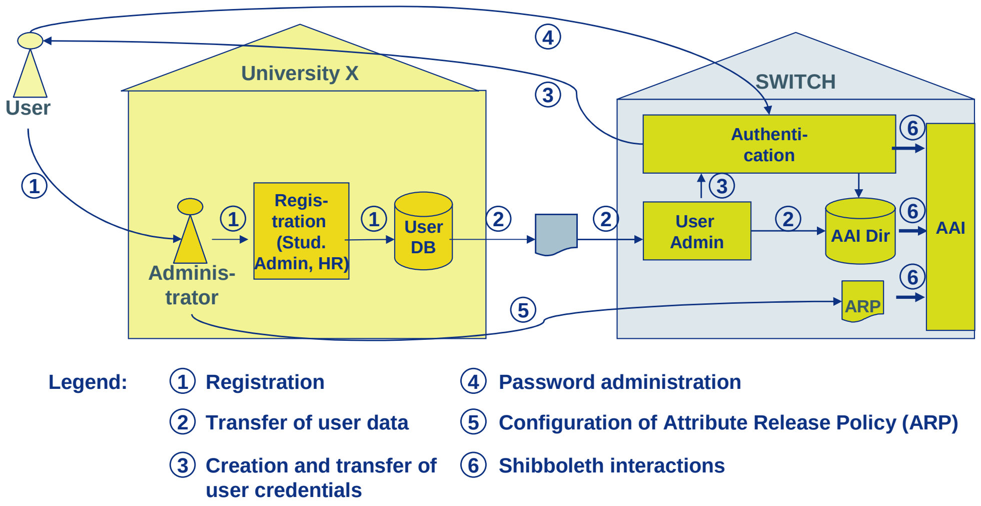
User
University X
SWITCH
4
3
1
Adminis-trator
1
Regis-tration (Stud. Admin, HR)
1
User DB
2
2
Authenti-cation
3
User Admin
2
AAI Dir
ARP
6
6
6
AAI
5
Legend:
1 Registration
2 Transfer of user data
3 Creation and transfer of user credentials
4 Password administration
5 Configuration of Attribute Release Policy (ARP)
6 Shibboleth interactions

Figure 3: AAI Jump Start service interactions

Notice that SWITCH acts on behalf of the Home Organizations, which means that the authorization attribute “Name of Home Organization” of the university X will be “X.ch”.

Customers	Home Organizations
Description	• Temporary service only • For a limited number of Resources and users • Basic authentication system and AAI attribute directory operated by SWITCH • Web-based user interface for password administration by end user • File-based bulk import of user data provided by Home Organization; data conversion into AAI format (optional) • Simple Attribute Release Policy (ARP)
Customer’s responsibility	User registration, correctness of delivered user data
SWITCH’s responsibility	Operation of authentication system, AAI directory, and Shibboleth on behalf of a Home Organization, based on SLA

2.4 Outsourcing Service

In contrast to the AAI Jump Start Service, the Outsourcing Service is meant for Home Organizations that want to outsource authentication permanently. The service is enhanced insofar as it offers on the one hand a web-based user interface for Attribute Release Policy configuration by both Home Organization and end user, and on the other hand real-time coupling between the

AAI directory and a Home Organization's user database as well as automatic data conversion into AAI format. Same as with the AAI Jump Start Service, the authorization attribute "Name of Home Organization" of the university X will be "X.ch".

Organizations have maximum flexibility as to the degree of outsourcing: user directory, authentication and/or installation and maintenance of Shibboleth can be outsourced individually.

Certificate, SmartCard or SecureID solutions can be provided on request.

Customers	Home Organizations
Description	• Authentication system and AAI attribute directory operated by SWITCH • Web-based user interface for Attribute Release Policy configuration by Home Organization / by end user • Web-based user interface to password administration by end users • Real-time coupling between AAI directory and the Home Organization's user databases, automatic data conversion into AAI format • Upon request: Certificate, SmartCard and/or SecureID solutions
Customer's responsibility	User registration, correctness of user data
SWITCH's responsibility	Operation of authentication system, AAI directory and/or Shibboleth on behalf of a Home Organization, based on SLA

2.5 Virtual Home Organization

The Virtual Home Organization Service (VHO) is aimed at individuals that are not registered with a Home Organization (i.e. neither student nor staff), or members of organizations that do not belong to the AAI federation. These may be organizations temporarily or permanently working together with a Resource Owner of the federation, e.g. In order to facilitate such cross-organizational work, SWITCH acts as a Virtual Home Organization in that it undertakes the complete set of tasks of a "real" Home Organization.

Figure 4 shows the interactions between user and Virtual Home Organization:

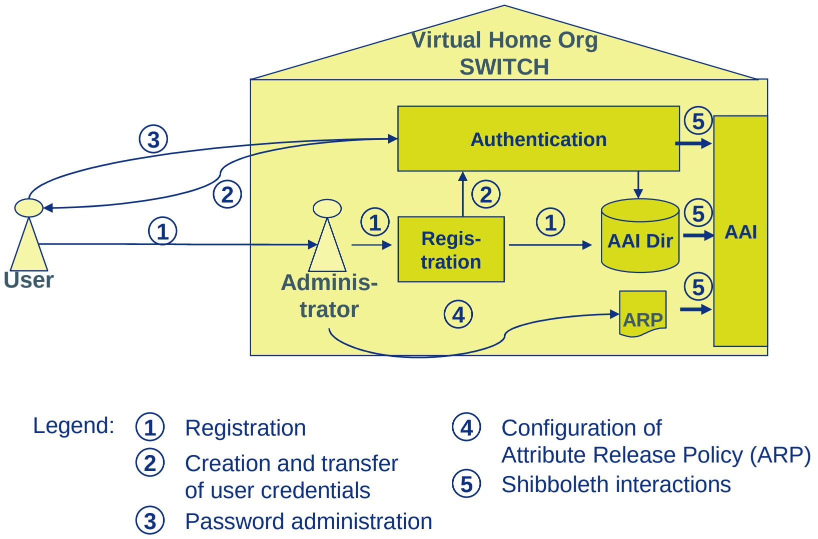
Virtual Home Org
SWITCH
Authentication
Regis-tration
AAI Dir
ARP
AAI
User
Adminis-trator
1
2
3
4
5
Legend:
① Registration
② Creation and transfer of user credentials
③ Password administration
④ Configuration of Attribute Release Policy (ARP)
⑤ Shibboleth interactions

Figure 4: VHO interactions

While the responsibilities of the individuals using this service will have to be defined in end user regulations, SWITCH guarantees for complying with the AAI Policy in all its actions. In particular, SWITCH commits to disclosing its registration policy for reasons of transparency.

Customers	• Individuals not registered with a Home Organization (i.e. no student, no staff) • Members of organizations that do not belong to the federation
Description	• Complete Home Organization service provided by SWITCH • user registration • user authentication • user attribute delivery
Customer's responsibility	tbd (end user regulation)
SWITCH's responsibility	• Complying with AAI Policy (Home Organization part) • Disclosure of registration policy

2.6 Service Comparison

As for the differences between the services, Table 1 shows which tasks are assigned to which organization:

Tasks	Outsourcing Service	Virtual Home Organization	AAI Jump Start
Registration	University	SWITCH	University
User directory	SWITCH or University	SWITCH	SWITCH or University
Authentication	SWITCH or University	SWITCH	SWITCH or University
Shibboleth	SWITCH	SWITCH	SWITCH
Registration policy	University	SWITCH	University
Correctness of user attributes	University	SWITCH	University
Attribute release policy	University	SWITCH	University
“Name of Home Org” attribute	e.g. UniXY.ch	e.g. switch-vho.ch	e.g. UniXY.ch
“Home Organization Type” attribute	university, uas, hospital, library, others	vho	university, uas, hospital, library, others

Table 1: Outsourcing services vs. virtual home organization

The main difference between them is that acting as a Virtual Home Organization SWITCH performs all the tasks and also appears as Home Organization in the attributes, whereas with AAI Jump Start and the Outsourcing Service only user directory, authentication and/or installation and maintenance of Shibboleth are performed by SWITCH.

3. RA/CA

Server certificates are needed for the encryption of data transfer between AAI components and for the verification of their identities. As such, they are mandatory for the participation in the AAI.

Starting 2004, SWITCH will operate a Root Certificate Authority (CA) as well as a subordinate CA. They will issue server certificates and sign them, or merely sign server certificates issued by organizations themselves. Furthermore, SWITCH will provide the possibility for Home Organizations to act as Registration Authorities (RA).

In the first phase of AAI, only server certificates signed by the SWITCH Root CA will be accepted.

As an AAI-related service, the issuance of server certificates is charged separately according to the tariff list of the SWITCH Root CA Service.