
# AAI - Authentication and Authorization Infrastructure

# SWITCHaai Federation

## Document management

| | | |
|---|---|---|
| Version/status: | 0.5 / draft | |
| Date: | 10-NOV-03 | |
| Author(s): | Christoph Graf | SWITCH |
| | Daniela Isch | at rete ag |
| | Thomas Lenggenhager | SWITCH |
| | André Redard | at rete ag |
| File name: | AAI_Federation_v05.doc | |
| Replacing: | | |
| Approved by: | | |

## Table of Content

# 1. Introduction

The implementation of an Authentication and Authorization Infrastructure (AAI) is a solution to the problem of inter-organizational authentication and authorization. The core functionality of an AAI is to tightly couple together the three basic interactions between a user, his or her Home Organization and a Resource during the authentication and authorization process. These three basic interactions are user authentication, access request and delivery of authorization attributes from the Home Organization to the Resource.

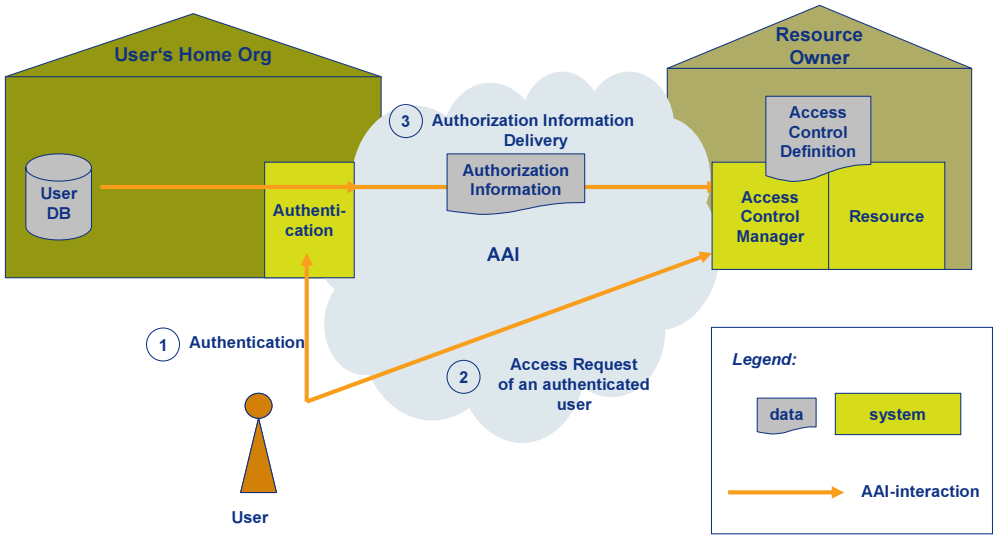


Figure 1: AAI-Model

Establishing an AAI to ease interactions between end users and information providers across organizations not only requires a legal framework which allows participants to exchange information, but also the mutual trust of organizations.

The purpose of this document is to give an overview of the organizational and legal framework of the AAI.

# 2. The SWITCHaai Federation

## 2.1 Definition

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 a Shibboleth based AAI infrastructure. They agree to abide by a common set of policies and practices, such as:

- business rules governing the registration of users and the exchange and use of user attributes,
- best practices on associated technical issues, typically involving security and attribute management, and
- a set of rules on how the Federation can evolve.

## 2.2 Participants

The following figure gives an overview of the participating parties:

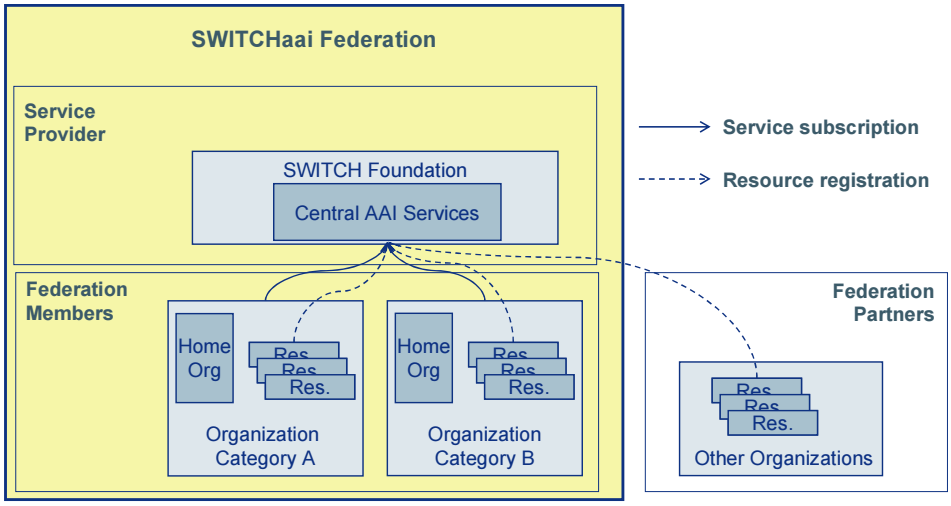


Figure 2: The SWITCHaai Federation and related organizations

### 2.2.1 Federation Members

In line with the *General Rules of Use for SWITCH Services*[1], there are two categories of organizations, which can participate within the Federation:

- Category A, "**Education and Research**", relates to all cantonal universities, Swiss Federal Institutes of Technology, research institutes in the FIT sector, universities of applied science, public research institutes and teaching hospitals. It comprises all organizations which, pursuant to the Law on Promotion of Higher Education, the Law on Research, and the Federal Law on universities of applied science, are supported by public subsidies. It also includes organizations engaging predominantly in primary and pre-competition research.
- Category B, "**Supporting Organizations**", comprises public institutions with which the organizations in category A collaborate by way of practice and support of their activities in education and research (e.g. libraries, Swiss National Science Foundation, Swiss University Conference, SWITCH).

Members can have different roles: they can act as representatives of user communities (Home Organizations), offer a variety of resources to the Federation (Resource Owners) and operate AAI components.

### 2.2.2 Service Provider SWITCH

SWITCH provides the central AAI Services and operates a resource registry. For further details see [AAIServD].

### 2.2.3 Federation Partners

Federation Partners are organizations that offer AAI-enabled resources to Federation members. They are allowed to integrate their resources within AAI and to use a minimal set of central AAI services necessary for a smooth operation of the AAI. It is up to a Home Organization whether to transfer attributes to such a Federation Partner or not.

Federation partners cannot act as a Home Organization, i.e. they do not represent user communities.

[1] http://www.switch.ch/network/aup.html#GRU

## 2.3 Legal Framework

The Federation SWITCHaai and the AAI itself are legally based on

- legal regulations already in force[2]
- the standing orders of the SUK of February 22, 2001

In the preparatory study phase (see [AAIStudy]), it was assumed that SUK could make a decision which regulates data protection and liability issues among participating organizations. However, since the AAI is an infrastructure project, SUK is not in the position to make such a decision. Therefore, a new legal framework has to be defined. During the AAI pilot phase, two different models were considered:

A. The Federation as a synonym for the group of subscribers of SWITCH's AAI service:
   The SWITCHaai Federation is established implicitly; it comprises SWITCH and all organizations of category A or B that have subscribed the central AAI Service provided by SWITCH.

B. The Federation as a legal Entity:
   Organizations of category A and B interested in AAI found the Federation as a new legal entity (e.g. like the Library Consortium).

The AAI steering committee decided to implement the Federation based on model A because of the following arguments:

- Today, there are no known legal or organizational requirements which enforce the foundation of a legal entity.
- The foundation of a new legal entity takes some time and, even more important, the engagement of organizations preferring such a model. Today, there are no such organizations. Since the federation should be operational in the 1st Quarter of 2004, the foundation of a new legal entity is not a feasible short-term solution. Nevertheless, it might be a well-suited legal model in the long run.
- SWITCH, as the established provider of network and network-related services for the participants of the AAI, is well positioned to act as an enabler of the Federation and to provide the necessary central AAI services. Since most of the potential members of the federation have a direct representation in the foundation board of SWITCH, they can influence and decide on the further direction of the AAI services and the form of the federation.

[2] - Federal and the different cantonal data protection laws
- Bundesgesetz über die Förderung der Universitäten und über die Zusammenarbeit im Hochschulbereich vom 8. Oktober 1999 (UFG)
- Verordnung zum Universitätsförderungsgesetz vom 13. März 2000 (UFV)
- Interkantonales Konkordat über die universitäre Koordination vom 9. Dezember 1999
- Vereinbarung zwischen dem Bund und den Universitätskantonen über die Zusammenarbeit im universitären Hochschulbereich vom 14. Dezember 2000

Within the selected model A, the data protection and liability issues have to be covered in the bilateral service contract with SWITCH and the binding AAI policy:

- Service contract with SWITCH for the central AAI services [AAI-SC]
- AAI Policy [AAIPol], which is an integral component of the service contract with SWITCH; it contains
  - Federation policy (membership, organization, decision rules, etc.)
  - rights and obligations of Federation members, e.g. attribute usage, liability, etc.
    - between members
    - between a member and partners
  - Resource Registration Policy

In addition, some of the organizations may have to adapt their "Acceptable Use Policy (AUP)". A sample clause that may be included can be found in Appendix B.

### 2.4 Organizational Framework

Since we expect about twenty members and dozens of resources, it is important to have an organizational structure that allows making decisions on an appropriate management level and within an appropriate time frame. In addition to the Foundation Board of SWITCH, which includes representatives from the Swiss Confederation, the university cantons, the universities, the universities of applied science, and similar organizations, we propose to have two AAI related committees:

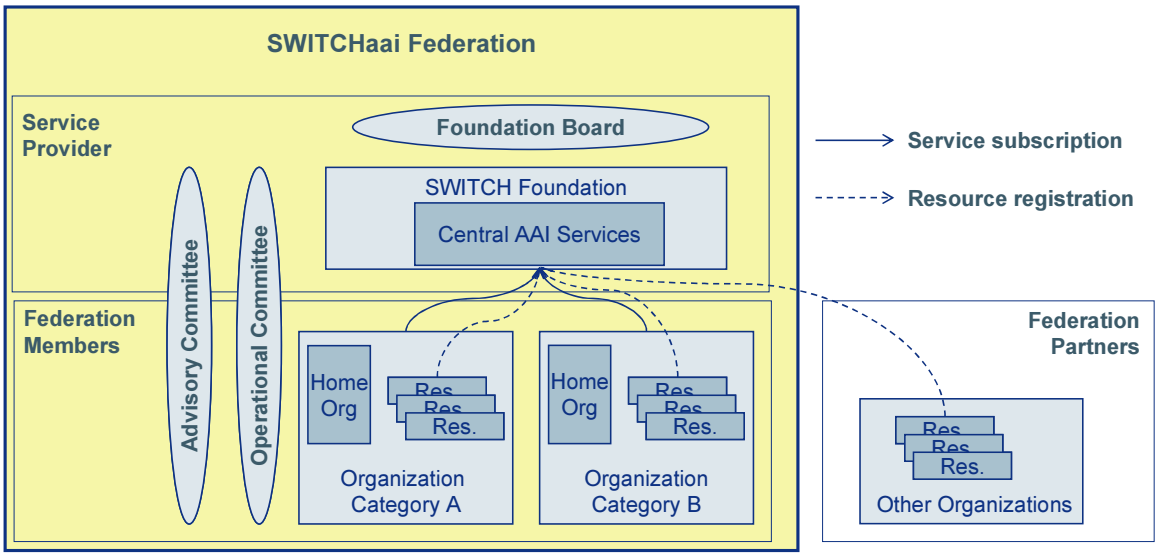


Figure 3: Steering Committees

| Committee | Responsibilities, Role |
|---|---|
| *Foundation Board* | Strategic decisions about SWITCH's AAI Services (organizational, technical, financial aspects). |
| *Advisory Committee* | Committee representing the Federation members and SWITCH; acting in an advisory capacity as regards the management of inter-institutional AAI projects and the long-term AAI strategy, e.g.:<br>• Initiation and controlling of inter-institutional AAI projects<br>• Financing of AAI projects and operations<br>• Federation strategy (membership, relation to other federations, etc.)<br>• AAI strategy (architecture, functionality)<br>• Policies and business rules<br>• Risk assessments and service continuity management<br>• Further development of SWITCH's AAI Services |
| *Operational Committee* | Committee representing the Federation members and SWITCH, responsible for short-term decisions and operational or technical issues, e.g:<br>• best practices on AAI related technical and operational issues<br>• Attribute specification, common entitlements<br>• Release planning<br>• Security audits<br>• Emergency shutdown<br><br>All its decisions have to respect the policies and long-term strategy. |

We recommend constituting the committees as follows

| | |
|---|---|
| *Advisory Committee* | • one representative of the universities<br>• one representative of the universities of applied science<br>• one representative of SWITCH<br>• one representative of CRUS<br>• one to three representatives of important Resource Owners (e.g. Library Consortium, SVC)<br>• one representative of the provider of subsidies<br>• one jurist familiar with AAI-related legal issues |
| *Operational Committee* | • one representative per federation member<br>• if needed, experts with specific skills not available from the federation members |

## 3. References


[AAIStudy] AAI Preparatory Study, Version 1.0, 15-JUL-2002

[AAIPol] AAI Policy, Version 2.0, dd-mmm-2003

[AAI-SC] SWITCH – AAI Service Contract, Version 1.0, dd-mmm-2003

[AAIServD] AAI Service Description, Version 0.5/draft, 28-OCT-2003


Unless otherwise indicated, the referenced documents are available on http://www.switch.ch/aai

## Appendix A Terms and Abbreviations

| | |
|---|---|
| *SWITCHaai Federation* | Group of Swiss Academic Organizations cooperating within the area of inter-institutional authentication and authorization (see chap. 2.1) |
| *Federation Member* | Member of the SWITCHaai Federation (see chap. 2.2.1) |
| *Federation Partner* | Non-member organization providing Resource(s) to Federation Members (see chap. 2.2.3) |
| *(User's) Home Organization* | Organization representing a user community:<br>• registers its users and stores information about them<br>• is able to authenticate its users |
| *Resource Owner* | Entity owning a resource and offering resource access to users. |
| *Resource* | Application, web site |
| *Service Provider SWITCH* | Organization providing the services offered by the Federation (see chap.2.2.2) |
| *Operational Committee* | Committee representing the Federation members and SWITCH, responsible for short-term decisions and operational or technical issues |
| *Advisory Committee* | Committee representing the Federation members and SWITCH; advises on the long-term AAI strategy |

## Appendix B Acceptable Use Policy (AUP)

The relationship between User and Home Organization has to be set up in the AUP, in particular for data protection reasons. The following clause has to be inserted in the Home Organization's use regulation and should be signed by the user:

*"The user notes that personal data about the user is compiled from generally available sources and from communications received from the user and other universities as well as from off-site sources. The policy relating to the use and procession of such data is posted on the University website at XXX. Such data will be used inter alia to authenticate and authorize the access to and use of various resources within the University and on other sites (Approved Uses). The user hereby consents to the collection, processing, use and release of such data to the extent reasonably necessary for the Approved Uses. Such consent includes (but is not limited to) the release of personal data to other institutions by employing cookies and electronically exchanging, caching and storing personal authorization attributes."*