
Authentication and Authorization Infrastructure (AAI)
Pilot Phase

# Policy

6-Feb-03

## Document management

| | | |
|---|---|---|
| Version/status: | 1.0 | |
| Date: | 06-Feb-03 | |
| Author(s): | Christoph Graf | SWITCH |
| | Daniela Isch | at rete ag |
| | Wolfgang Lierz | ETH Library Zurich |
| | Pascal Py | University of Zurich |
| | Marc-Alain Steinemann | University of Berne |
| | Martin Strässler | at rete ag |
| | Alex Sutter | University of Berne |
| | Bruno Vuillemin | University of Fribourg |
| File name: | AAI_Policy_v10.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.

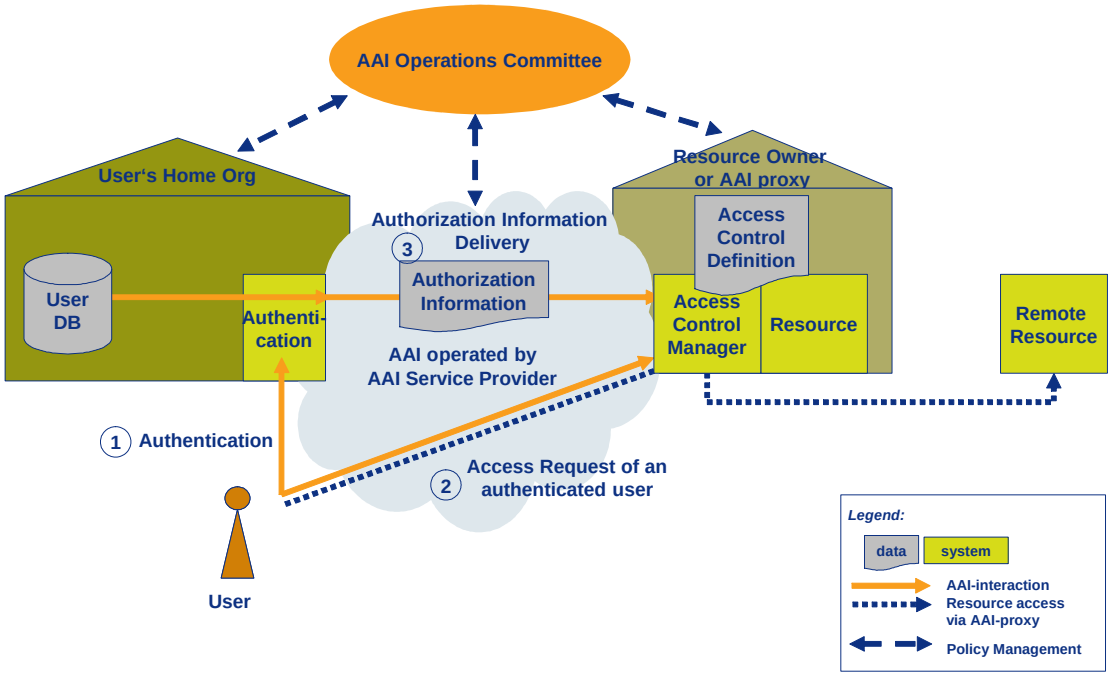


Figure 1: AAI-Model

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 AAI bases on legal regulations already in force[1] and participants in the AAI can only act within these boundaries. In addition, the standing orders of the SUK from February 22, 2001 and a further decision of this board, expected in April 2003, will ease additional cooperation. However, it is also necessary that AAI Service Provider, Home Organizations and Resource Owners agree to a common set of guidelines – the AAI policy – which describes the rules of good conduct.

[1] - 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

This document is meant as a preliminary outline of the AAI policy. A more detailed version will be written when the system architecture has been selected and insights from the pilot projects can be integrated. The policy is expected to be integral component of a legal contract that each organization has to sign in order to become an AAI participant.

## 2. Policy

Relevant for the AAI are all interactions between the Service Provider, Home Organizations and Resource Owners (including Remote Resources) concerning authentication and authorization. Regulations concerning the use of the contents of a resource (e.g. accounting or billing) are not within the scope of the AAI and have to be dealt with on a bi- or multilateral basis.

### 2.1 Policies for All AAI Participants

2.1.1 The AAI participants are obliged to install as well as to update new AAI software releases according to the agreed schedule maintained by the Operations Committee.

2.1.2 Sensitive personal data is handled in compliance with the applicable data protection law regime, both Federal and Cantonal. This concerns specifically collecting, transferring, storing, and caching data. In particular, AAI participants are responsible for the correctness and relevance of the data they store or transfer, as well as for protecting it from unauthorized access and/or use. Holders of databases are obliged to disclose, update and correct the contents of the database if requested by the owner of the data. Organizations may be made liable for any misuse resulting from violations of e.g. criminal law or data protection law.[2]

2.1.3 As little data transfer as necessary and as much data security/correctness as possible should occur. (according to DP)

2.1.4 Information policy towards people concerned should be as clear and preventive as possible. Each person concerned by a data collection has the right to get informed about his or her personal data.

### 2.2 Policies for the Operations Committee

2.2.1 The Operations Committee finally decides on the admittance of new AAI participants and keeps a list of them up-to-date.

2.2.2 The Operations Committee collects all incidents of user abuse according to an agreed procedure. It coordinates and standardizes the measures for preventing or eradicating abuse across all AAI partners.

### 2.3 Policies for Home Organizations

General:

2.3.1 Each Home Organization has the obligation to disclose the registration and authentication process on request of a AAI partner (increasing trust).

[2] In the following, all regulations which are deducted from federal data protection law are marked as (DP§).

Registration/Administration:

2.3.2 Home Organizations collect a specified minimum set of attributes at the registration of users (see “Authorization Attribute Specification”, version 1.0, December 11, 2002).

Attribute transfer:

2.3.3 Users must be able to control the release of attributes to resources controlled by the AAI. (according to DP art.8)

2.3.4 Transfer of attributes is restricted to those attributes that are relevant for the use of a particular resource. (according to DP art. 4)

### 2.4 Policies for Resource Owners

Attribute transfer:

2.4.1 Resource Owners may only request attributes that are relevant to the application. (according to DP art. 4 al.3)

Storage of user information:

2.4.2 Resource Owners shall keep login information for at least 6 months.

2.4.3 Locally cached user information must not be stored longer than 12 months after the last successful login. This measure is meant to decrease the danger of storing outdated data. (according to DP art. 7)

User abuse:

2.4.4 The abused party gets hold of the abuser. Resource Owners provide log information to the Home Organization on request.

Remote Resources:

2.4.5 The rules for resources accessible through the AAI are valid regardless of the resource being accessed in a direct way or by means of an AAI proxy. Operators of AAI proxies are liable for proper usage of the user attributes they receive from the AAI. (according to DP 4, 7)

Not within the scope of the AAI:

2.4.6 Resource Owners needing additional attributes which have not been collected by a Home Organization contact the user directly.

2.4.7 Resource Owners wishing to charge for the use of their resource specify the terms in bilateral agreements with the Home Organizations or user.

### 2.5 Service Provider

Transport of Data, Integrity, Confidentiality:

2.5.1 The Service Provider accepts AAI messages only from AAI partners and ensures that messages are forwarded only to the AAI partners involved and without any unduly modifications. (according to DP art. 12 ff.)

Availability, Reliability:

2.5.2 The Service Provider takes the necessary steps to ensure seamless operation of the services under its control, monitors service availability and operates a helpdesk for AAI partners to report operational problems. Outages due to planned maintenance operations need to be announced in advance and should be restricted to pre-agreed maintenance windows.

2.5.3 The Service Provider maintains a software repository available to all AAI partners covering all available AAI components. The service provider makes AAI partners aware of bug fixes, security updates and upgrades of AAI components and coordinates efforts to keep the AAI operational and secure. The modalities of this service are covered by SLAs in the contract between the Service Provider and the AAI partners.

## 3. Glossary

| Term | Definition |
|---|---|
| *(Authorization) Attributes* | User data needed for access control decisions |
| *AAI* | Authentication and Authorization Infrastructure |
| *AAI message* | Information exchanged between Resource Owner, AAI Service Provider, and Home Organization related to the same basic AAI task (e.g. attribute request, attribute transfer) |
| *AAI partner / participant* | Home Organization, Resource Owner or Service Provider |
| *AAI proxy* | Proxy-Resource Owner that provides AA functionality on behalf of other Resources that cannot be AAI-enabled (technically) |
| *AAI Service Provider* | Organization providing central AAI services to Resource Owners and Home Organizations |
| *Authentication* | Process of proving the identity of a previously registered user |
| *Authorization* | Process of granting or denying access rights for a resource to an authenticated user |
| *DP* | Swiss federal protection law: used as a guideline for legal comprehension |
| *Home Organization* | Representative of a user community, e.g. universities, libraries, university hospitals etc.<br>• registers their users and stores information about them<br>• is able to authenticate their users |
| *Operations Committee* | Representatives of the AAI partners that coordinated and share information to ensue a smooth and stable operation of the AAI |
| *Registration* | Process of becoming an official member of a user community. During the registration, a person has to prove his/her identity |
| *Remote Resource* | Resource that has not installed AAI software for access control but relies on an AAI proxy for this purpose. |
| *Resource* | Application, web site |
| *Resource Owner* | Entity owning a resource and offering resource access to users |
| *SLA* | Service Level Agreement |
| *SUK* | Schweizerische Universitätskonferenz |
| *User* | Registered member of a Home Organization |

## 4. Further Information

http://www.switch.ch/aai

http://www.admin.ch/ch/d/sr/235_1/