AAI - Authentication and Authorization Infrastructure

Exhibit 3
AAI Policy

Document management

Version/status:	0.91/draft		1.12
Date:	3. 2. 2004		7 July 2004
Author(s):	Nicole Beranek Zanon	SWITCH	Hans Rudolf Trüeb
	Christoph Graf	SWITCH	
	Daniela Isch	at rete ag	
	André Redard	at rete ag	
File name:	040603_Anhang_3.doc		X1055939-3.doc
Replacing:	AAI Policy 1.0 / 6-FEB-03		V. 0.91
	SWITCHaai Federation 0.5 / 10-NOV-03		
Approved by:			

Table of Content

1. Introduction

Establishing an AAI to ease interactions between End Users and Resources 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. The standing orders of the SUK of February 22, 2001 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.

The policy is an integral part of the AAI Service Agreement between SWITCH and the signing Organization and rules the relationship between the AAI Participants.

2. The SWITCHaai Federation

2.1 Definition

The SWITCHaai Federation is a group of organizations which cooperate in the area of inter-organizational authentication and authorization and, for this purpose, operate a common infrastructure.

2.2 Participants

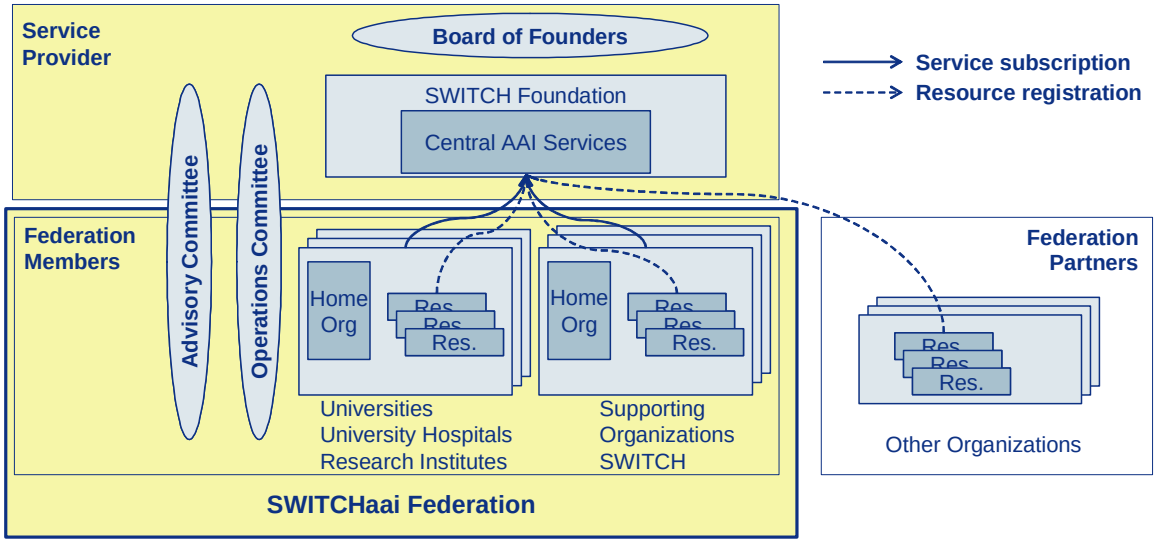

Figure 1: The SWITCHaai Federation and related organizations

[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
- Cantonal university laws comprising the legal basis for the handling of personal data
- Cantonal acts of public responsibility governing the abuse of the AAI

2.2.1 Federation Members

All entities and organizations meeting the *Membership Requirements* as posted on the dedicated SWITCH AAI website and amended from time to time, may become Federation Members. Any revision of these *Membership Requirements* will become effective and will be deemed accepted 30 days from posting on the SWITCH AAI website. Then current Federation Members will receive an electronic message indicating such revision.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 Services according to Exhibit 2.

2.2.3 Advisory Committee

The Advisory Committee, representing the Federation members and SWITCH, acts in a purely advisory capacity as regards the management of inter-institutional AAI projects and the long-term AAI strategy.

2.2.4 Operations Committee

The Operations Committee, representing the Federation members and SWITCH, acts in a purely advisory capacity as regards short-term decisions and operational or technical issues.

2.2.5 Federation Partners

Federation Partners are organizations that offer AAI-enabled Resources to Federation members. They are allowed to integrate their Resources within the AAI and to use a minimal set of central AAI services necessary for a smooth operation of the AAI.

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

Service subscriptions of Federation Partners are subject to separate agreements with SWITCH.

3. Policy

3.1 Advisory Committee

3.1.1 SWITCH decides on the membership composition of the Advisory Committee. Ideally, the Committee is composed as follows:

(a) one representative of the universities
(b) one representative of the universities of applied sciences
(c) one representative of SWITCH
(d) one representative of CRUS
(e) one to three representatives of important Resource Owners (e.g. Library Consortium, SVC)
(f) one representative of the provider of subsidies
(g) one jurist familiar with AAI-related legal issues

3.1.2 The Advisory Committee acts in a purely advisory capacity as regards the management of inter-institutional AAI projects and the long-term AAI strategy including but not limited to the following issues:

(a) initiation and controlling of inter-institutional AAI projects;
(b) financing of AAI projects and operations;
(c) Federation strategy (membership, relation to other federations, etc.);
(d) AAI strategy (architecture, functionality);
(e) policies and business rules;
(f) accreditation of CAs (Certificate Authorities);
(g) risk assessments and service continuity management; and
(h) further development of SWITCH's AAI Services.

3.1.3 SWITCH is responsible for the preparation of meetings and for all administrative concerns.

3.2 Operations Committee

3.2.1 SWITCH decides on the membership composition of the Operations Committee. Ideally, the Committee is composed as follows:

(a) one representative per Federation Member
(b) if needed, experts with specific skills

3.2.2 The Operations Committee acts in a purely advisory capacity as regards short-term decisions and operational or technical issues including but not limited to:

(a) best practices on AAI-related technical, operational and security issues;
(b) attribute specification, common entitlements; and
(c) release planning.

.

3.3 Home Organizations

3.3.1 Home Organizations have the obligation to disclose their registration and authentication process on request of an AAI Participant.

3.3.2 Home Organizations operate a help desk for their End Users which attends to AAI-related issues.

3.3.3 Home Organizations keep their Attribute Release Policy up to date for all Resources that the Home Organizations' user communities are entitled to access.

3.3.4 Home Organizations will use for all their AAI elements server certificates provided by an accredited CA.

3.3.5 Home Organizations keep authentication information according to the legal provisions for at least 6 months at the moment.

3.4 Resource Owners

3.4.1 Resource Owners indicate which attributes they need for authorization; these indications are entered into the Resource Registry.

3.4.2 Resource Owners ensure that the meta-data they use is always up to date by using the automatic updating service provided by Shibboleth.

3.4.3 Resource Owners keep login information and log files according to the legal provisions for at least 6 months at the moment.

3.4.4 Resource Owners will use for all their AAI elements server certificates provided by an accredited CA.

3.4.5 In case of End User abuse, the abused party gets hold of the abuser. Resource Owners provide log information to the Home Organization on request.