SWITCH

The Swiss Education & Research Network

AAI – Authentication and Authorization Infrastructure

SWITCHaai Federation – Organization and Processes

Document management

Version/status:	1.0 / final	
Date:	15-JAN-04	
Author(s):	Christoph Graf	SWITCH
	Thomas Lenggenhager	SWITCH
	André Redard	at rete ag
	Daniela Isch	at rete ag
File name:	AAI_Org_Processes_v10.doc	
Replacing:	0.4 / 7-JAN-04	
Approved by:		

Table of Content

Figures

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, as shown in Figure 1:

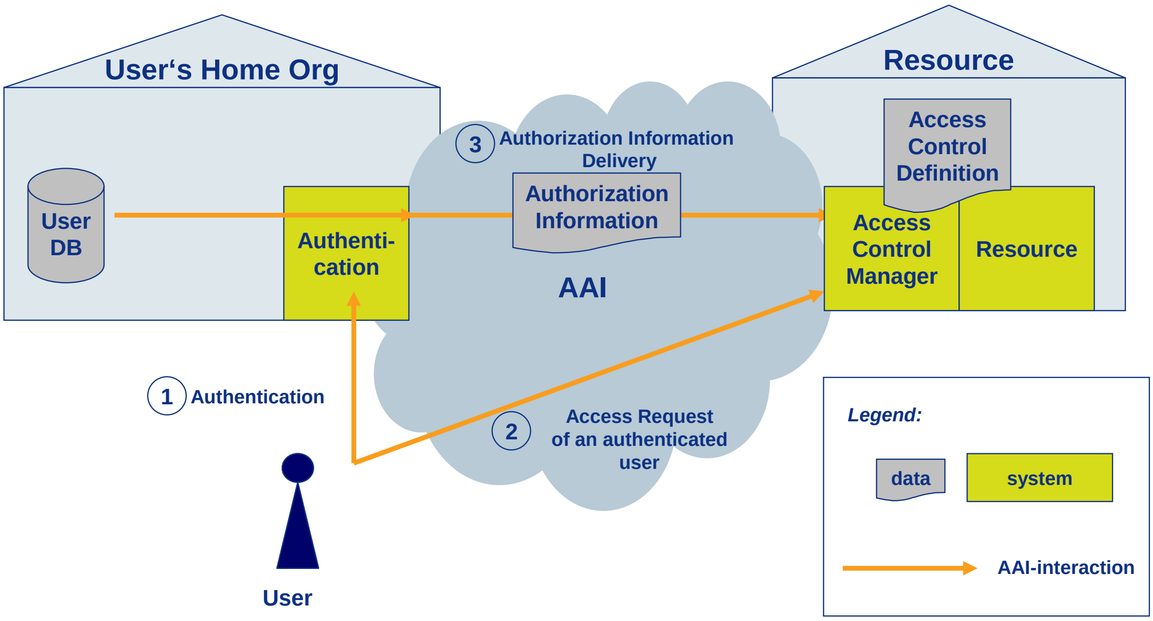


Figure 1: AAI model

The purpose of this document is to define the organizational structure and the processes necessary to operate the AAI. It includes step-by-step instructions (procedural, not technical) of how to integrate resources and Home Organizations within the AAI and practical hints at how to become compliant with the legal framework.

2. The SWITCHaai Federation

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 SWITCHaai Federation serves these purposes by setting up rules for the participants’ behavior by means of service agreements and a policy document.

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. The organizations 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

Figure 2 gives an overview of the participating parties:

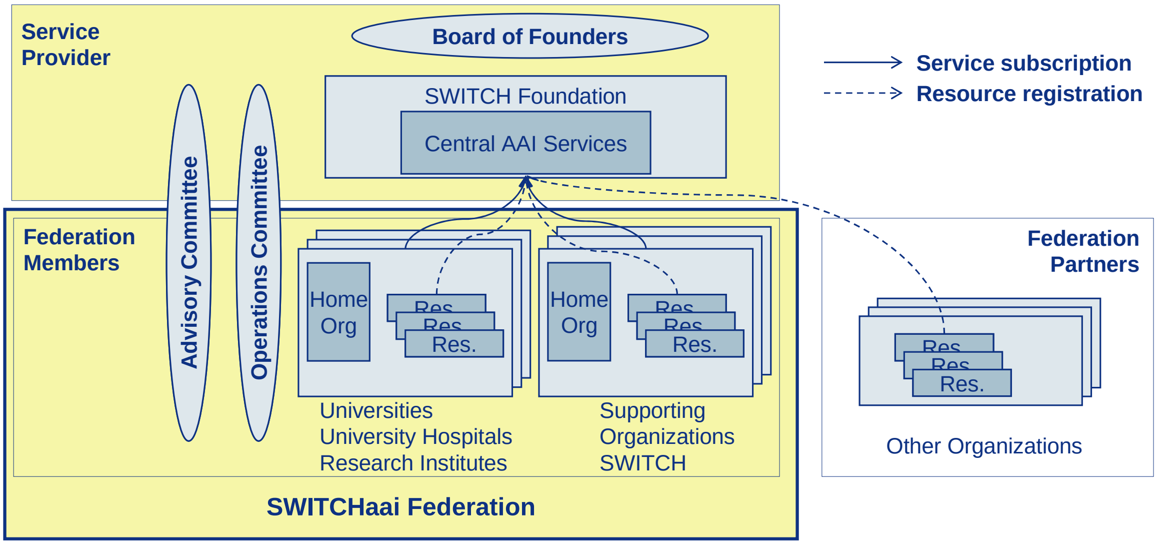


Figure 2: The SWITCHaai Federation and related organizations

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 in 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 sciences, 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 sciences, 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 [AAIServ].

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

2.2.3 Federation Partners

Federation Partners are organizations that offer AAI-enabled resources to Federation Members. However, Federation Partners cannot act as Home Organizations, i.e. they do not represent user communities.

In the future, they will be 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. To date, no AAI service agreement for Federation Partners has been worked out. It will be done as soon as there is a need to integrate such resources within the AAI. Thus, the processes described in this document are valid only for Federation Members. They will be enhanced as soon as needed.

2.3 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 SWITCH's Board of Founders, which includes representatives from the Swiss Confederation, the university cantons, the universities, the universities of applied sciences, and similar organizations, we propose to have two AAI-related committees: an Advisory Committee and an Operations Committee (cf. Figure 2). The roles of these committees are defined in Table 1; see [AAIPol] for a more detailed description.

Committee	Roles
Board of Founders	Strategic decisions about SWITCH's AAI Services (organizational, technical, financial aspects)
Advisory Committee	Committee representing the Federation members and SWITCH; acting in a purely advisory capacity as regards the management of inter-institutional AAI projects and the long-term AAI strategy
Operations Committee	Committee acting in a purely advisory capacity as regards short-term decisions and operational or technical issues

Table 1: Role of committees

3. Legal Framework

The Federation SWITCHaai and the AAI itself are legally based on

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

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

The SWITCHaai Federation is established implicitly; it comprises all organizations of category A or B that have signed the bilateral service agreement with SWITCH [AAIServAgr]. SWITCH itself can only be a Federation Member when acting as a Home Organization or Resource Owner, but not in its role as a Service Provider.

The Service Agreement regulates the rights and obligations between SWITCH as Service Provider and the signing organizations, while the AAI Policy [AAIPol] rules the relationship between the Federation Members. Besides, the AAI Policy is also necessary for establishing trust between all parties.

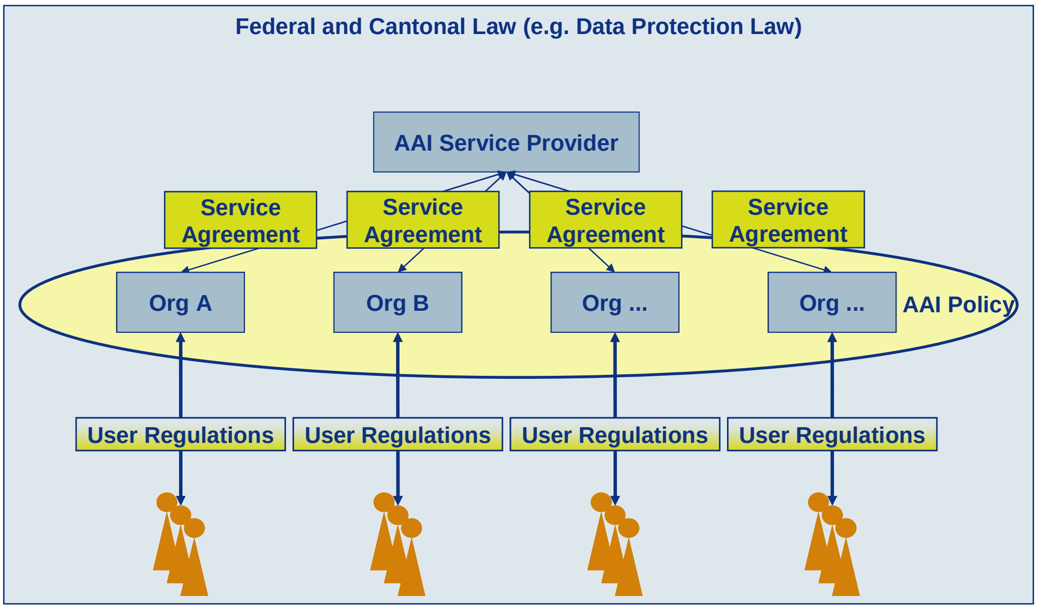


Figure 3: Legal framework

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 Exhibit 5 [AAIAUP] of the AAI Service Agreement.

[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
- Cantonal university laws comprising the legal basis for the handling of personal data
- Cantonal laws governing the liability in case of abuse of the AAI

4. Service Delivery and Support Processes

The processes to deliver and support the AAI-related services described in this document are based on the service process model and the best practices defined by ITIL[3] (IT infrastructure library). These generic processes may be a good starting point also for Resource Owners or Home Organizations to design their specific processes and to act as a "common language" among organizations.

The following chapters describe the core processes of the AAI:

- How to AAI-enable Home Organization
- How to AAI-enable Resources
- Incident and problem management
- Change management
- Release management

4.1 How to AAI-enable Home Organizations

4.1.1 Preconditions

The following preconditions have to be fulfilled before a Home Organization can be integrated within the AAI:

- it is able to register its users and operates an Authentication System for them;
- it operates a User Directory which contains at least the mandatory authorization attributes as defined in [AAIAttr]; and
- it fulfills the requirements to become a holder of a server certificate issued by a Certificate Authority accredited by SWITCH; at least the SWITCH CA will be such an accredited CA.

Technical requirements for the Authentication System and User Directory are described in [AAISpec].

If a Home Organization is not ready to provide an Authentication System and/or User Directory, SWITCH offers temporary or permanent AAI outsourcing services as described in [AAIServ].

4.1.2 Home Organization Integration Process

Figure 4 illustrates the necessary steps to AAI-enable a Home Organization. A legend of the used symbols is shown in Appendix B.

1. The Home Organization signs the AAI Service Agreement for the AAI Service Base Package [AAI-ServAgr].

2. The Home Organization implements the AAI components and integrates them with its Authentication System and User Directory (cf. [AAISpec]). Deployment guides and the necessary software are available at http://www.switch.ch/aai. SWITCH also provides technical support, an AAI test environment and test server certificates.

3. Before the AAI-enabled Authentication System and User Directory can be deployed within the production environment, server certificates from a Certificate Authority accredited by SWITCH have to be ordered and installed. Further details about the sub-process "Create Server Certificate" can be found in the documentation of either the SWITCH CA service or in the documentation of another accredited CA service.

4. The Home Organization registers its AAI components with SWITCH and provides the necessary administrative information (e.g. contact names) and security information (e.g. public keys). SWITCH lists the Home Organization on the "Where are you from" server (WAYF).

[3] see also http://www.itil.co.uk

5. Periodically, the Home Organizations checks whether there are new Resources available. If its users are allowed to access these resources, the Home Organization adjusts its Attribute Release Policy (ARP) according to the needs of the resources, i.e. releases the necessary attributes (see chap. 4.2.2 and Figure 6 for a detailed description of the sub-process “Resource Registration”).

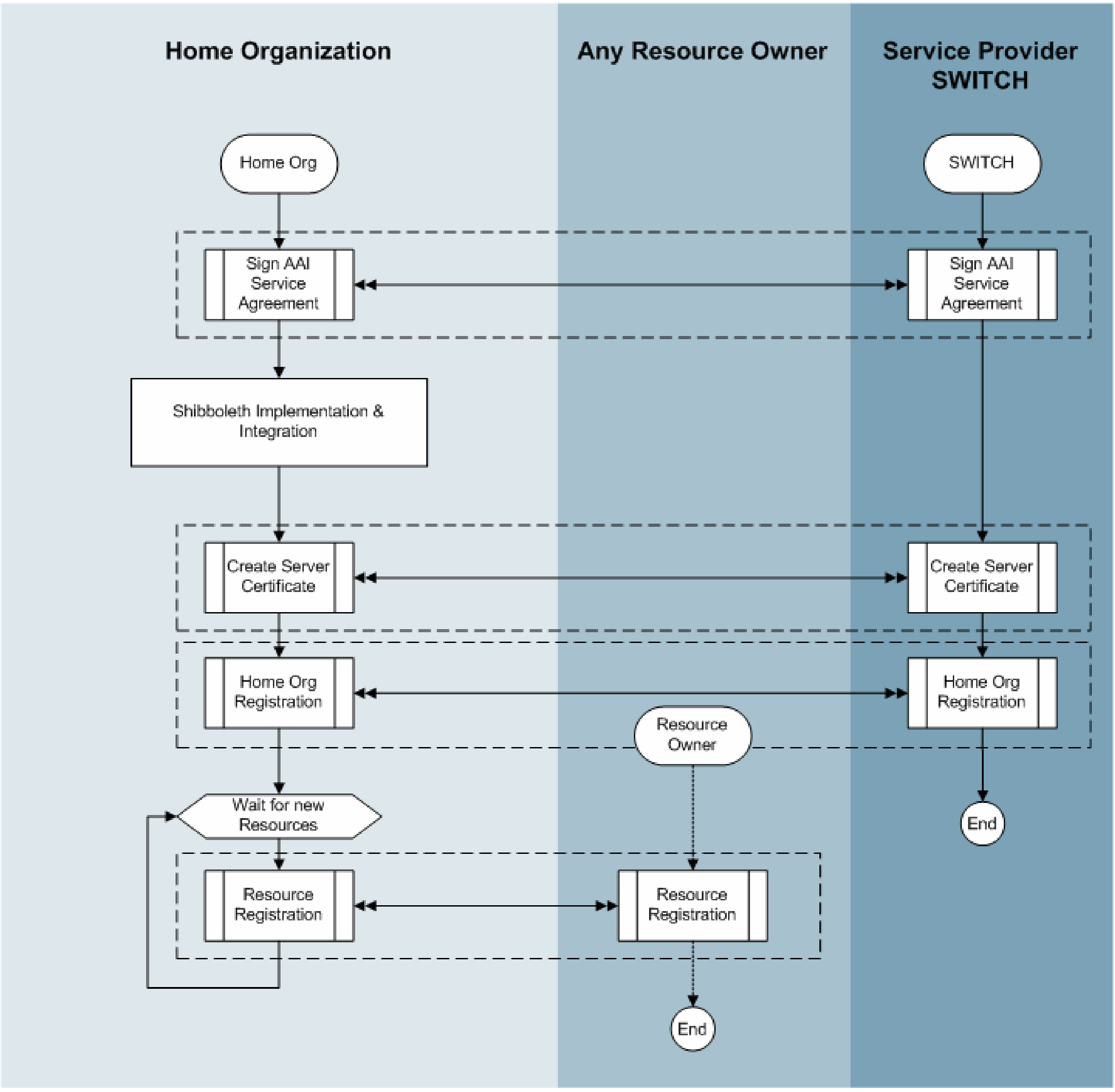


Figure 4: Home Organization integration process

4.2 How to AAI-enable Resources

This chapter describes the necessary steps to AAI-enable a resource of a SWITCHaai Federation Member.[4]

4.2.1 Preconditions

It is assumed that Resource Owners have established the following service delivery processes, irrespective of whether a resource is AAI-enabled or not:

- account management,
- service planning, and
- service development.

Where appropriate, service level agreements between the Resource Owner and its clients (i.e. organizations or individual users of Home Organizations) have to be defined and may contain the following aspects:

- target audience
- service deliverables
- service quality
- service tariff
- security aspects
- service support processes (e.g. incident, problem and change management for non-AAI related issues)

The following preconditions have to be fulfilled before a resource can be integrated within the AAI:

- the Resource Owner belongs to an organization which is a SWITCHaai Federation member; and
- the Resource Owner fulfills the requirements to become a holder of a server certificate issued by a Certificate Authority accredited by SWITCH. At least the SWITCH CA will be such an accredited CA.

[4] The steps to integrate a resource of a SWITCHaai Federation Partner will be described in a later release of this document as soon as the legal conditions to become Federation Partner are defined.

4.2.2 Resource Integration Process

Figure 5 illustrates the necessary steps to AAI-enable a resource:

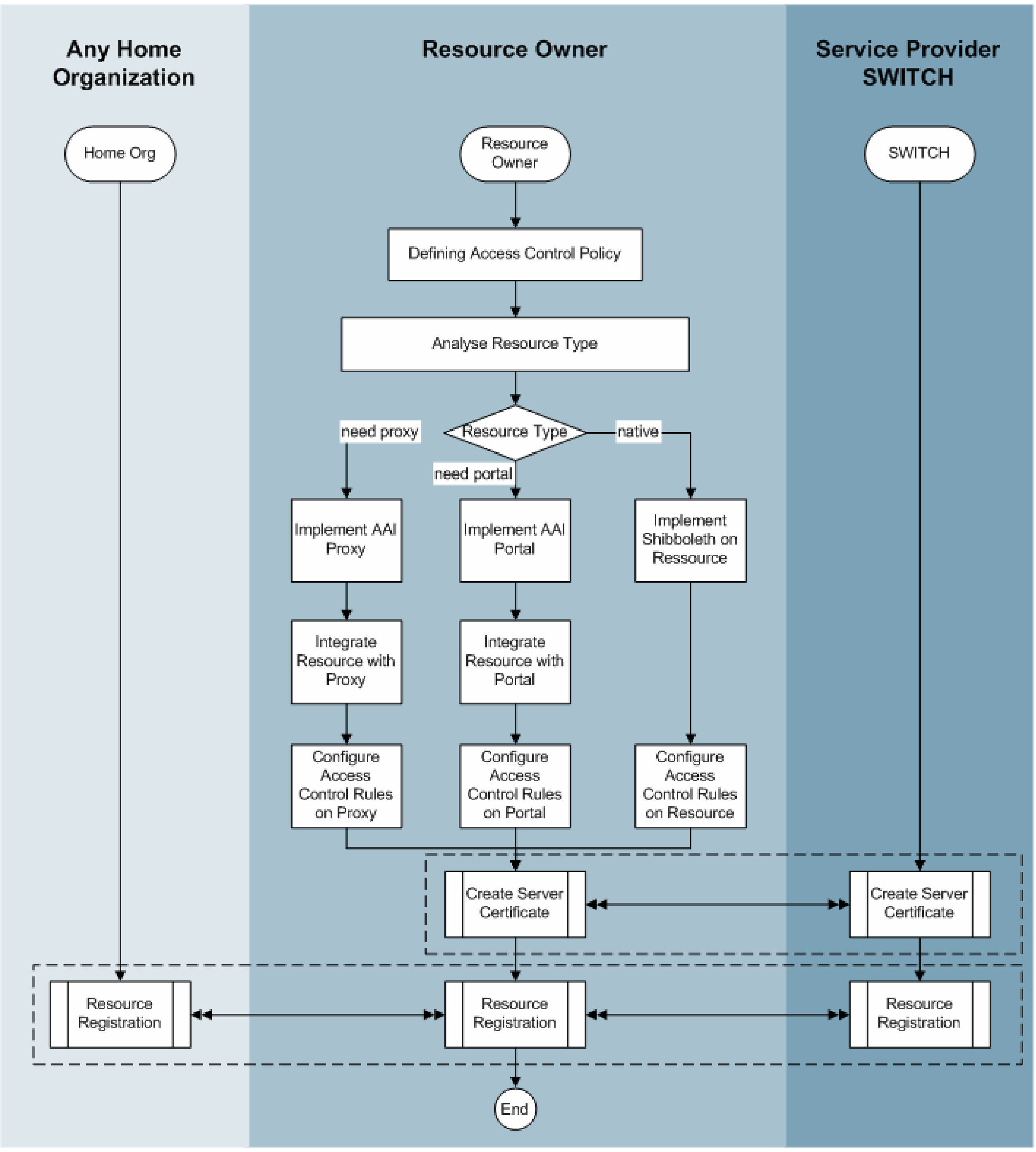

Any Home Organization
Resource Owner
Service Provider SWITCH
Home Org
Resource Owner
SWITCH
Defining Access Control Policy
Analyse Resource Type
need proxy
Resource Type
native
need portal
Implement AAI Proxy
Implement AAI Portal
Implement Shibboleth on Ressource
Integrate Resource with Proxy
Integrate Resource with Portal
Configure Access Control Rules on Proxy
Configure Access Control Rules on Portal
Configure Access Control Rules on Resource
Create Server Certificate
Create Server Certificate
Resource Registration
Resource Registration
Resource Registration
End

Figure 5: Resource integration process

6. The Resource Owner has to define its Access Control Policy based on the available authorization attributes from Home Organizations (see [AAIAttr]. At this stage, existing Service Level Agreements with clients of the resource should be reviewed and changed where necessary (i.e. to allow authentication and authorization via AAI).

7. Depending on the type and architecture of the resource, the Resource Owner decides whether the resource can be integrated directly with Shibboleth or whether an intermediary solution like the AAI Proxy or AAI Portal is necessary (see [AAISpec] for technical details about these options). The Ac-

cess Control Policy has to be configured on the appropriate system; e.g. within the Attribute Acceptance Policy file (AAP).
The integrated resource can be tested within the AAI test environment provided by SWITCH. Test server certificates are available from SWITCH.

8. Before the AAI-enabled resource can be deployed within the production environment, a server certificate from a Certificate Authority accredited by SWITCH has to be ordered and installed. Further details about the sub-process “Create Server Certificate” can be found in the documentation of either the SWITCH CA service or in the documentation of another accredited CA service.

9. The sub-process “Resource Registration” is described in Figure 6:

   (a) Resource Owners register their resource within the Resource Registry provided by SWITCH;
   (b) authorized staff of the Federation member the resource belongs to confirms
       - that the resource belongs to the Federation member, and
       - that it is operated under the conditions of the AAI service contract between the Federation member and SWITCH;
   (c) Home Organizations of users who are allowed to access the resource adjust their Attribute Release Policy (ARP) according to the needs of the resource, i.e. they release the necessary attributes; and
   (d) all participants make sure that the stored information is kept accurate.

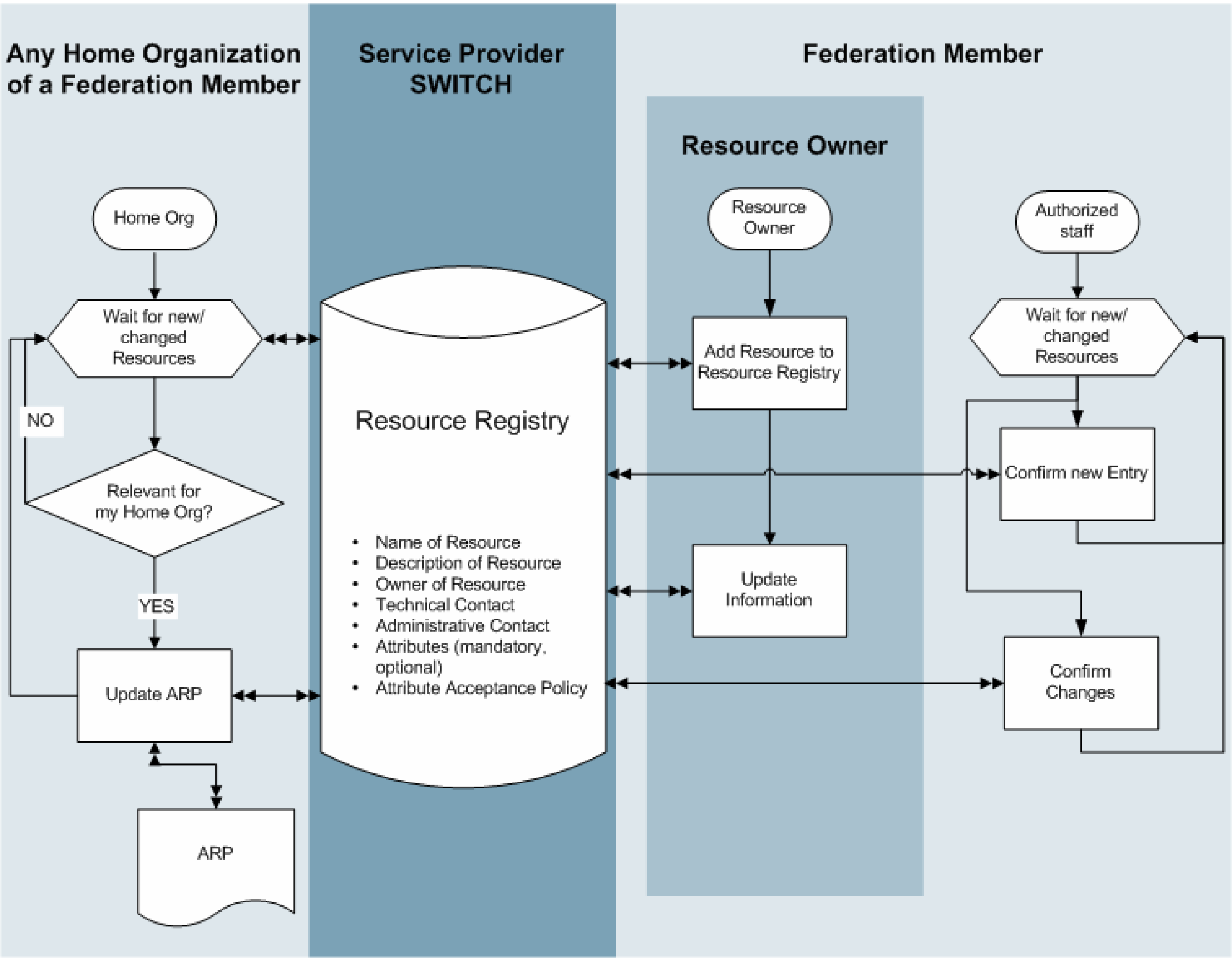


Figure 6: Resource registration process

4.3 Incident and Problem Management

The goal of the incident management is to reestablish a service after a failure. The problem management consists of the systematic identification, analysis, localization and correction of problems; not only reactive, but also proactive.

4.3.1 Assumptions

We assume that each Home Organization offers a service desk (Single Point of Contact, helpdesk) to its users and that SWITCH (as Service Provider), Resource Owners and administrators of Home Organization systems (Authentication System and User Directory) provide second/third level support for their systems.

4.3.2 Incident and Problem Handling Rules

For the handling of AAI-related incidents, we postulate the following rules:

- for users, the single point of contact for AAI-related issues is always the service desk of their Home Organization;
- the Service Provider SWITCH does not have to provide end user support, but second level support to AAI administrators of Home Organizations and Resource Owners; and
- for non AAI-related incidents occurring when a user accesses a Resource (e.g. problems with the provided functionality or content), its up to the Resource Owner to define the incident and problem management processes, e.g. as part of its SLA (not covered in this document).

Figure 7 illustrates the interactions between a user, the service desk of his/her Home Organization (1st level support) and the administrators of the systems involved.

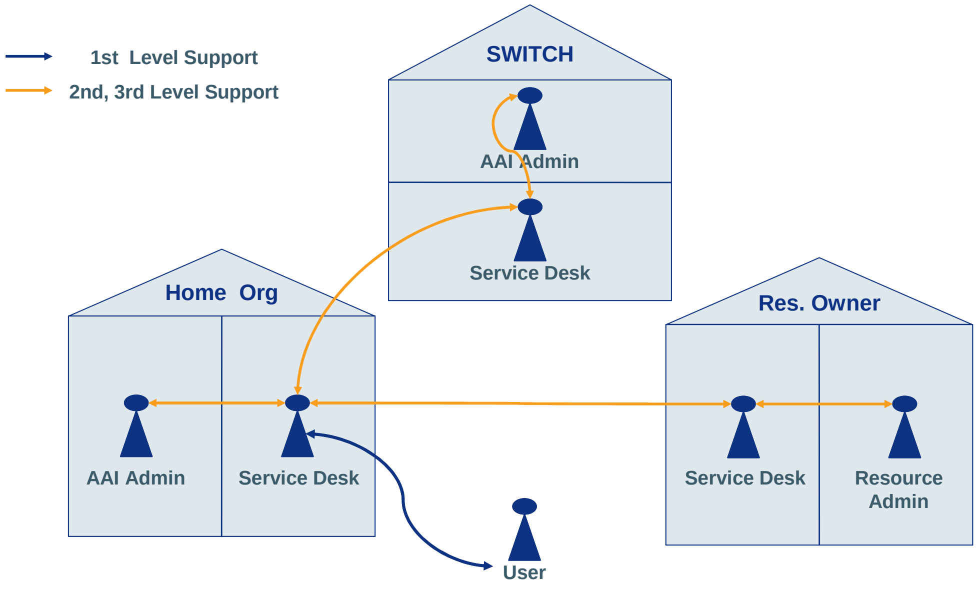


Figure 7: Incident management in resolving AAI related issues

Each organization may use its own trouble ticket system to track the incident and problem solving.

Recurring problems affecting more than one organization can be reported to SWITCH. SWITCH, together with the Operational Committee and/or the parties involved, will analyze the problem and initiate appropriate countermeasures.

4.4 Change Management

The goal of a well-defined change management process is to minimize the risks inherent to any changes and to implement authorized changes efficiently.

Any changes of the AAI system affecting more than one organization have to be well planned, tested and coordinated. For changes which are not backward compatible, SWITCH will consult the Operational Committee before implementing the change.

4.5 Release Management

The purpose of the release management is to create and provide tested software packages, including deployment guides and roll-out planning.

Each provider of AAI related software (e.g. AAI Portal, AAI Proxy) is asked to define a clear release policy and to provide only tested software packages together with accurate deployment guides to AAI participants.

For Shibboleth, SWITCH will test new releases, enhance the deployment guides provided by Internet2 where necessary and provide sample configuration files.

Software providers and Federation Members are encouraged to use the test environment provided by SWITCH.

5. References

[AAIStudy]	AAI Preparatory Study, Version 1.0, 15-JUL-2002
[AAIServAgr]	SWITCH – AAI Service Agreement
[AAIPol]	SWITCH – AAI Service Agreement, Exhibit 3: AAI Policy
[AAIAUP]	SWITCH – AAI Service Agreement, Exhibit 5: Sample Clause
[AAIServ]	AAI Service Description, Version 1.0, 15-JAN-2004
[AAIAttr]	AAI Authorization Attributes, Version 1.1, 15-JAN-2004
[AAISpec]	AAI System and Interface Specification, 1.0, 15-JAN-2004

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

Appendix A Terms and Abbreviations

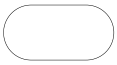
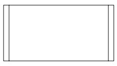
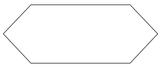
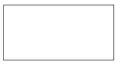
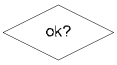
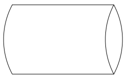
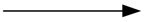
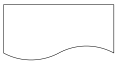
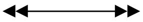
Access control definition[5]	Configuration parameters used by the access control manager implementing the access control policy
Access control manager[5]	Gatekeeper functionality of the resource which grants or denies access to the resource based on the access control definition and the authorization attributes retrieved
Advisory Committee	Committee representing the Federation members and SWITCH; advises on the long-term AAI strategy
Authentication system[5]	System which can authenticate a previously registered user
Authorization attributes[6]	User data needed for access control decisions
Federation	cf. SWITCHaai Federation
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)
Home Organization[5]	Organization representing a user community: • registers its users and stores information about them • is able to authenticate its users
Operational Committee	Committee representing the Federation members and SWITCH, responsible for short-term decisions and operational or technical issues
Resource[5]	Application, web site
Resource Owner[5]	Entity owning a resource and offering resource access to users.
Service Provider SWITCH	Organization providing the services offered by the Federation (see chap.2.2.2)
SWITCHaai Federation	Group of Swiss Academic Organizations cooperating within the area of inter-institutional authentication and authorization (see chap. 2.1)
User[5]	Registered member of a Home Organization
User Directory[5]	Directory or database storing information about a registered user, maintained by the Home Organization

[5] cf. [AAISpec]

[6] cf. [AAIAttr]

Appendix B Legend of symbols

The following symbols are used to describe the processes defined within this document:

	Initiator of a process		
	Process		Waiting for an event
	Task		Decision
	Database		Process flow
	File, Document		Data Flow