AAI – Authentication and Authorization Infrastructure

VHO Service Description
&
VHO Registration Policy

Document management

Version/status:	1.0 / final	
Date:	25. January 2005	
Author(s):	Ueli Kienholz	SWITCH
	Thomas Lenggenhager	SWITCH
	André Redard	at rete ag
	Daniela Isch	at rete ag
File name:	VHO_Policy_v10.doc	
Replacing:		
Approved by:		

Table of Contents

1. Introduction

Typically, not all of the End Users of an AAI resource are registered at an existing AAI home organization. Examples of such End Users are

1. project partners at private companies
2. project partners at foreign universities
3. software developers at private companies (for development and ongoing support)
4. employees of project sponsors

There are two options of how a resource can support such End Users:

A. A resource might implement a separate login method for non-AAI users and manage user credentials locally at the resource.

B. Include those End Users into the Virtual Home Organization (VHO) operated by SWITCH, which turns them into AAI users for that resource.

This policy defines the rules for resource owners and SWITCH when choosing option B.

2. Definitions

AAI	means Authentication and Authorization Infrastructure
Attributes	End User data needed for access control decisions
Authentication	Process of proving the identity of a previously registered End User
Authorization	Process of granting or denying access rights for a resource to an authenticated End User
End User	means a registered member of a Home Organization or a Virtual Home Organization
Federation	means the AAI Federation
Federation Member	means the contracting party with SWITCH
Home Organization	means participating institutions such as universities or hospitals which accredit End Users
Resource Owner	means the Entity owning a resource and offering resource access to End Users
Resources	means material to which access is granted, e.g. applications, websites, databases, systems, etc.
VHO Service Subscriber	means the organization ordering SWITCH's VHO service
Virtual Home Organization (VHO)	means an institution which accredits End Users not belonging to a Home Organization
End User Administrator	a person appointed by the resource owner that is responsible for the user data maintenance for that resource

3. The VHO Service

3.1 Service Description

The VHO Service is provided by SWITCH and can be subscribed by Resource Owners or Home Organizations of SWITCHaai Federation Members[1].It enables the Resource Owner to create “AAI-enabled” accounts for users not belonging to a Home Organization. Such an account will only be valid for a single resource (or a limited set of resources) belonging to such a Resource Owner.

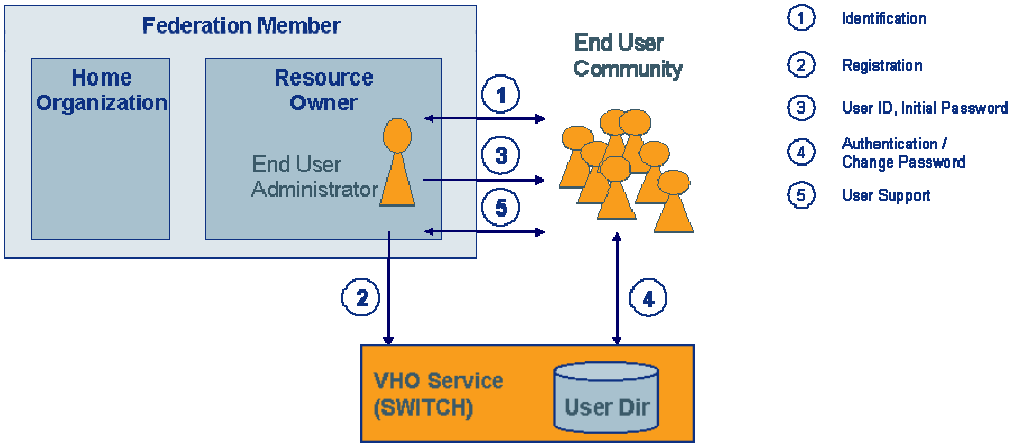

Figure 1 VHO Service Interactions

The VHO application consists of an End User Directory with web-based End User Administrator and End User interfaces.

The VHO Service Subscriber appoints at least one End User Administrator. He/she can

(1), (2) register new End Users, define user ID and initial password, and delete and modify existing End Users.

(3) set new passwords

The End User can

(4) accept Terms of Use and change his or her password

(5) get support from the End User Administrator

For the initial load of End User information, the End User Administrator can send a file with the minimal set of End User attributes (user ID[2], surname, given name; see [AAIAttr]) and the initial password to SWITCH. This file will be imported to the End User directory by SWITCH.

When an End User logs in for the first time, he/she has to accept the Terms of Use (ToU, see Appendix [B]).

---

1 To become a Federation Member, organizations have first to sign the SWITCH AAI Service Agreement [AAIServAgr].

2 The user ID has the form <prefix>-<individual part>, e.g. “resourceA-12345”. SWITCH defines the user ID – prefix for each.VHO.

3.2 Obligations of SWITCH

For the proper functioning of the VHO Service, SWITCH, as provider of the VHO Service, must meet the following requirements:

1. SWITCH adheres to the policy for Home Organizations defined as part of the AAI Policy [AAIPol].
2. SWITCH maintains the Attribute Release Policy of the VHO in accordance with the needs of the VHO Service Subscriber.
3. In order to clearly distinguish VHO-users from 'regular' users, SWITCH has to guarantee that some attributes are set as defined below:

   ```
   swissEduPersonHomeOrganization     = vho-switchaai.ch
   swissEduPersonHomeOrganizationType = vho
   eduPersonAffiliation               = affiliate
   ```

   These attributes always have to be part of the set of released attributes.
4. SWITCH indicates technical and administrative contact information to the VHO Service Subscribers.
5. SWITCH takes the necessary steps to ensure seamless operation of the service, monitors service availability and supports End User Administrators. Outages due to planned maintenance operations are announced in advance.

3.3 Obligations of the VHO Service Subscriber

1. The VHO Service Subscriber registers End Users as defined by the rules in the VHO Registration Policy (see chapter 4).
2. The VHO Service Subscriber provides 1st Level support for its registered End Users.
3. The VHO Service Subscriber indicates technical and administrative contact information to SWITCH.
4. On request, the End User Administrator informs SWITCH of the number of users administered at that time and of how many of them are associated with which organization.

3.4 Cost of the VHO Service

Presently, the VHO Service is free of charge. SWITCH reserves the right to introduce charges (upon 6 months' notice).

3.5 Service modifications

With advance notice of 3 month, SWITCH reserves the right to introduce changes, if need be, to functionality, requirements, processes, attributes etc. of the VHO or its users at the beginning of a semester (i.e. 1st of March and 1st of September).

4. VHO End User Registration Policy

While the VHO Service (hard- and software) is operated by SWITCH, the registration of the End Users and the maintenance of End User data is under the responsibility of the VHO Service Subscriber. They have to adhere to the data protection clauses defined in the AAI Service Agreement [AAIServAgr].

Data registration is carried out by the End User Administrator. He/she or a trusted third party (e.g. a representative of the foreign partner university) has to identify new users based on official documents (e.g. passport, matriculation document, student card)[3] and has to be able to link the user ID of a registered End User to a real person anytime (except for demo and guest accounts, see below).

The End User Administrator is responsible in particular

- that End User data is correct and well maintained (e.g. deleted when an End User is not authorized to use the resource any longer)
- for generating a username and initial password and transmitting these credentials to the End User

Demo and guest accounts constitute a special case. They should only be opened in case no personal account is feasible. Guest accounts are primarily intent for participants in a course. Passwords of guest accounts have to be changed after the termination of the course. Its not allowed to publish passwords of guest or demo accounts on public information sources (e.g. web sites, e-mail archives, journals …).

The surname and entitlement attribute of demo and guest accounts have to follow these rules:

	surname starts with	entitlement ends with
demo account	demo-	#demo
guest account	guest-	#guest

For each demo and guest account, the User Administrator must be advised of a responsible contact person (possibly in an external organization) who is able to identify the actual user, if necessary.

[3] Alternatively, the trusted third party may provide a list of formerly registered users (e.g. staff or students) if the former registration process is as accurate as the registration process for VHO users (e.g. based on official documents).

5. References

[AAIAttr]	AAI Authorization Attributes, Version 1.1, 15-JAN-2004 http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf
[AAIAUP]	SWITCH – AAI Service Agreement, Exhibit 5: Sample Clause http://www.switch.ch/aai/docs/AAI_Sample_Clause.pdf
[AAIPol]	SWITCH – AAI Service Agreement, Exhibit 3: AAI Policy http://www.switch.ch/aai/docs/AAI_Policy.pdf
[AAIServAgr]	SWITCH – AAI Service Agreement http://www.switch.ch/aai/docs/AAI_Service_Agreement.pdf

6. Appendix A: Sample Attribute file

Attribute	LDAP Name	Example	Demo Account
Unique ID	*swissEduPersonUniqueID*	*<code>@vho-switchaai.ch* *<code> is automatically generated by VHO Software encoding the user ID*	
Surname	*surname*	*Muster*	*demo-1*
Given name	*givenName*	*Peter*	*n.a.*
Date of birth	*swissEduPersonDateOfBirth*	*n.a.*	*n.a.*
Gender	*swissEduPersonGender*	*n.a.*	*n.a.*
Preferred language	*preferredLanguage*	*n.a.*	*n.a.*
E-mail	*mail*	*peter.muster@uniXy.ch*	*n.a.*
Home postal address	*homePostalAddress*	*n.a.*	*n.a.*
Business postal address	*postalAddress*	*n.a.*	*n.a.*
Private phone number	*homePhone*	*n.a.*	*n.a.*
Business phone number	*telephoneNumber*	*n.a.*	*n.a.*
Mobile phone number	*mobile*	*n.a.*	*n.a.*
Home Organization	*swissEduPersonHomeOrganization*	*vho-switchaai.ch*	*vho-switchaai.ch*
Home Organization type	*swissEduPersonHomeOrganizationType*	*vho*	*vho*
Affiliation	*eduPersonAffiliation*	*affiliate*	*affiliate*
Study branch 1	*swissEduPersonStudyBranch1*	*n.a.*	*n.a.*
Study branch 2	*swissEduPersonStudyBranch2*	*n.a.*	*n.a.*
Study branch 3	*swissEduPersonStudyBranch3*	*n.a.*	*n.a.*
Study level	*swissEduPersonStudyLevel*	*n.a.*	*n.a.*
Staff category	*swissEduPersonStaffCategory*	*n.a.*	*n.a.*
Organization path	*eduPersonOrgDN*	*n.a.*	*n.a.*
Organizational unit path	*eduPersonOrgUnitDN*	*n.a.*	*n.a.*
Member of	*eduPersonEntitlement*	*http://resource.unixy.ch/xyz*	*http://resource.unixy.ch/xyz#demo*

7. Appendix B: Terms of Use

SWITCH AAI Services
Terms of Use
(*ToU*)

Version 1.00 of 13 October 2004

1. By clicking on the "AGREE" button below, you consent to be bound by these ToU. Read these terms carefully prior to registering and using the inter-organizational authentication and authorization services (hereinafter: the *Services*) provided by SWITCH. SWITCH reserves the right to alter and amend the ToU without prior notice. Accordingly, you should visit the following link periodically to stay abreast of the latest changes: http://www.switch.ch/AAI/[•].html.
2. In order to benefit from the Services, you need a User ID (*UID*) and a Personal Identification Code (*PIC*). UID and PIC are for your sole use and may not be assigned or transferred. Protect you UID and PIC with adequate care. You are personally responsible for any abuse of your UID and PIC. Any such abuse or any other breach of the ToU will entail a suspension or cancellation of your account.
3. You may not access or use of the Services for other purposes than defined herein. You commit to access and use the Services in good faith only and in accordance with these ToU and all applicable laws and regulations.
4. You hereby acknowledge that personal data about you is compiled from generally available sources and from communications received from you, educational organizations and off-site sources. Such data will be used, inter alia, to authenticate and authorize the access to and use of various resources (hereinafter: the *Approved Uses*) which are offered by members and partners of the Swiss AAI Federation (see http://www.switch.ch/aai/ for details). You hereby consent 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 organizations and content providers, inter alia by employing cookies and electronically exchanging, caching and storing personal authorization attributes.
5. SWITCH does not make any representation or give any warranty as to the Services or their use. To the extent permitted by the applicable law, you hereby waive all and any claims for cost and damages, whether direct or indirect, incidental, or consequential (including, inter alia, loss of use and lost profits), both in contract and in tort, arising from the use or in any way related to the Services. This waiver of claims shall be valid and effective in relation to all participants and partners of the Swiss AAI Federation including SWITCH and its affiliates, officers, employees and agents.
6. You hereby commit to adhere to the SWITCH Acceptable Use Policy (hereinafter: AUP), i.e. the General Rules of Use for SWITCH Services and the General Service Conditions, as posted at http://www.switch.ch/network/aup.html#GRU. As these ToU, the AUP are subject to changes without prior notice. We strongly recommend that you visit the above link periodically to stay abreast of such changes. In case of discrepancies between the AUP and these ToU, the latter shall prevail.
7. These ToU and your use of the Services shall be governed by Swiss law, and you submit to the exclusive jurisdiction of the courts of 8001 Zurich.