European Union
European Regional Development Fund
digitalgreece
Everything is possible
Operational Programme
"Digital Convergence"
NSRF 2007-2013
programme for development
Quality of life for everyone
The project is co-financed by Greece and the European Union

Hellenic Academic Libraries Link
HEAL LINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Authentication and Authorization Infrastructure
AAI

Shibboleth.

HEAL-Link Federation

Higher Education & Research

Exhibit – 4

VHO

Service Description and Registration Policy

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 HEAL-Link, which turns them into AAI users for that resource.

This policy defines the rules for resource owners and HEAL-Link when choosing option B.

2 DEFINITIONS

AAI	Authentication and Authorization Infrastructure.
Affiliate	As to a person or entity, another person or entity which exercises control over such person or entity, or is under Control by it, or is under common Control by the same person or entity (HEAL-Link is a non profit organization and does not have any issues of shared capital with any organization.
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.
Federation Member	Defined in the AAI Policy Document.
Home Organization	Participating institutions (other than Federation Partners) such as universities or hospitals which register Authorized Users, it being understood that the Members may have several Home Organizations.
Resource owner	The Organization that provides the resources to the Consortium's members.
Resources	Material to which access is granted, e.g. applications, websites, databases, systems, etc on the basis of the SD -agreement with Elsevier dating 23 November 2004.
VHO Service Subscriber	means the organization ordering HEAL-Link's VHO service.
Virtual Home Organization or VHO	A user directory that allows Resource owner to register Authorized Users that are not otherwise registered with a Home Organization, allowing these Authorized Users to access certain Resources.
End User Administrator	A person appointed by the resource owner or HEAL-Link Federation, that is responsible for the user data maintenance for the specified resource or for the specified HEAL-Link member accordingly.

3 THE VHO SERVICE

3.1 Service Description

The VHO Service is provided by HEAL-Link and can be subscribed by Resource Owners or Home Organi- zations of HEAL-Link Federation Members[1]. It enables the Resource Owner to create "AAI-enabled" ac- counts for users not belonging to a Home Organization. Such an account will only be valid for all set of resources belonging to such a Resource Owner.

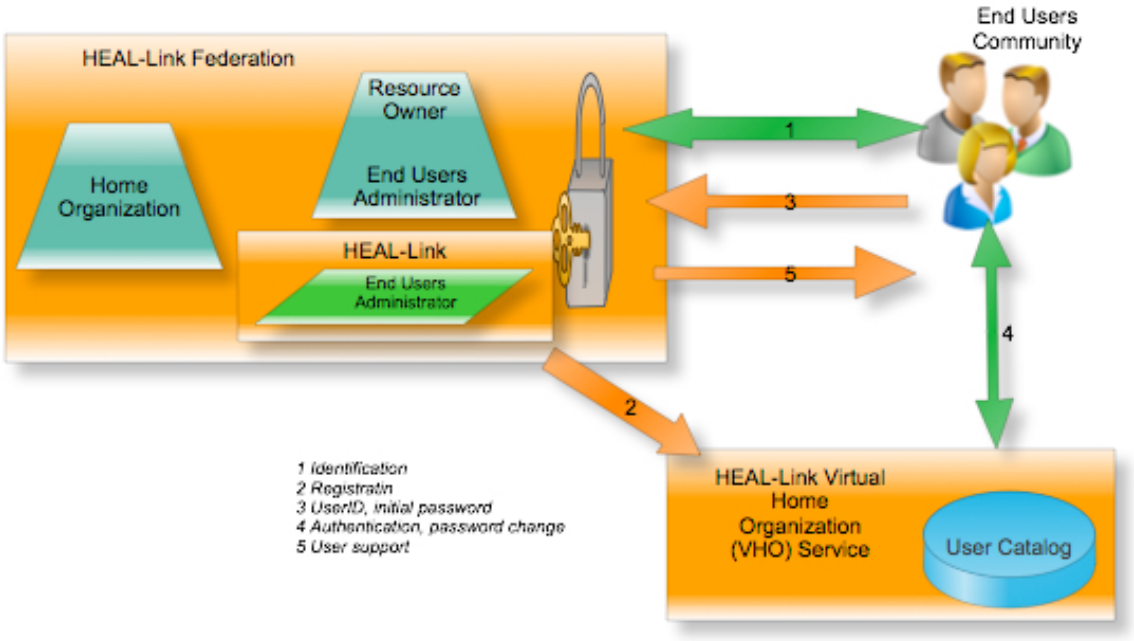

Figure 1 VHO Service Interactions

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. which can:

- register new End Users.
- define user ID[2] and initial password.
- delete and modify existing End Users.
- set new passwords

---

[1] All Federation Members must have already signed the HEAL-Link AAI Service Agreement.

[2] The user ID has the form <prefix>-<individual part>, e.g. “VirtOrg1-uid123”. HEAL-Link defines the user ID – prefix for each VHO.

The End User can:

- accept Terms of Use and change his or her password.
- get support from the End User Administrator.

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

3.2 Obligations of HEAL-Link Federation

For the proper functioning of the VHO Service, HEAL-Link Federation, as provider of the VHO Service, must meet the following requirements:

1. HEAL-Link Federation adheres to the policy for Home Organizations defined as part of the HEAL-Link AAI Policy.
2. HEAL-Link Federation 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, HEAL-Link Federation has to guarantee that some at- tributes are set as defined below:

   eduPersonScopedAffiliation = *affiliate@vho-heal-link.gr*

   eduPersonAffiliation = *affiliate*

   eduPersonOrgDN = *dc=vho-heal-link,dc=gr*
4. HEAL-Link Federation indicates technical and administrative contact information to the VHO Service Subscribers.
5. HEAL-Link Federation 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 HEAL-Link.
4. On request, the End User Administrator informs HEAL-Link of the number of users administered at that time and of how many of them are associated with which organization and the exact type of the association.

3.4 Service modifications

With advance notice of 3 months, HEAL-Link reserves the right to introduce changes, if need be, to functionality, requirements, processes, attributes etc. of the VHO or its users.

4 VHO END USER REGISTRATION POLICY

While the VHO Service is operated by HEAL-Link, 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.

The End User Administrator carries out data registration. He/she or a trusted third party (e.g. a representative of the foreign partner) 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 etc).

The surname of demo and guest accounts has to follow these rules:

demo account:	surname starts with demo-
guest account:	surname starts with 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).

This Document is based on the corresponding document: **SWITCHaai (AAI – Authentication and Authorization Infrastructure VHO Service Description & VHO Registration Policy, Switzerland).**