Abstract:
This document describes the motivation for and the software implementation of a service that enhances VOMS attribute certificates with attributes from a Shibboleth Identity Provider. This service has been implemented as the second phase of the work item “interoperability Shibboleth gLite” within the JRA1 activity.
Copyright notice:
Copyright © Members of the EGEE-II Collaboration, 2006.
See www.eu-egee.org for details on the copyright holders.

EGEE-II (“Enabling Grids for E-sciencE-II”) is a project co-funded by the European Commission as an Integrated Infrastructure Initiative within the 6th Framework Programme. EGEE-II began in April 2006 and will run for 2 years.

For more information on EGEE-II, its partners and contributors please see www.eu-egee.org

You are permitted to copy and distribute, for non-profit purposes, verbatim copies of this document containing this copyright notice. This includes the right to copy this document in whole or in part, but without modification, into other documents if you attach the following reference to the copied elements: “Copyright © Members of the EGEE-II Collaboration 2006. See www.eu-egee.org for details”.

Using this document in a way and/or for purposes not foreseen in the paragraph above, requires the prior written permission of the copyright holders.

The information contained in this document represents the views of the copyright holders as of the date such views are published.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE MEMBERS OF THE EGEE-II COLLABORATION, INCLUDING THE COPYRIGHT HOLDERS, OR THE EUROPEAN COMMISSION BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trademarks: EGEE and gLite are registered trademarks held by CERN on behalf of the EGEE collaboration. All rights reserved.

### Document Log

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Comment</th>
<th>Author/Partner</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>12/12/2006</td>
<td>TOC</td>
<td>P.Flury/SWITCH</td>
</tr>
<tr>
<td>0.9</td>
<td>21.12.2006</td>
<td>Integrated comments from SWITCH Middleware</td>
<td>P.Flury, V.Tschopp, T.Lenggenhager, C.Witzig</td>
</tr>
<tr>
<td>0.95</td>
<td>12.1.2007</td>
<td>Integrated comments by reviewer</td>
<td>P.Flury, C.Witzig</td>
</tr>
</tbody>
</table>

### Document Change Record

<table>
<thead>
<tr>
<th>Issue</th>
<th>Item</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1. INTRODUCTION .................................................................................................................. 4
  1.1. PURPOSE ............................................................................................................................. 4
  1.2. DOCUMENT ORGANISATION ............................................................................................ 4
  1.3. APPLICATION AREA .......................................................................................................... 4
  1.4. REFERENCES ...................................................................................................................... 4
  1.5. DOCUMENT AMENDMENT PROCEDURE ........................................................................... 5
  1.6. TERMINOLOGY .................................................................................................................. 5

2. MOTIVATION .......................................................................................................................... 7
  2.1. MOTIVATION FOR ATTRIBUTE BASED AUTHORIZATION IN GRID INFRASTRUCTURES .............................................................................................................................................. 7
  2.2. MOTIVATION FOR ENHANCING AUTHORIZATION WITH SHIBBOLETH ATTRIBUTES ....................................................................................................................... 7

3. DESIGN OPTIONS .................................................................................................................. 10
  3.1. OPTION 1: SHIBBOLETH ATTRIBUTES IN ATTRIBUTE CERTIFICATES .................................................................................................................................................... 11
  3.2. OPTION 2: SHIBBOLETH ATTRIBUTES IN X.509 USER CERTIFICATE ........................................................................................................................................................ 11
  3.3. OPTION 3: GRID RESOURCE REQUESTS SHIBBOLETH ATTRIBUTES ...................................................................................................................................................... 11
  3.4. OPTION 4: SHIBBOLETH ATTRIBUTES IN VOMS ................................................................ 12

4. THE DESIGN OF THE SERVICE ............................................................................................. 12
  4.1. DESIGN PRINCIPLES .......................................................................................................... 14

5. DESCRIPTION OF THE VASH SERVICE .............................................................................. 14
  5.1. USER’S VIEW OF THE VASH SERVICE ............................................................................. 14
  5.2. FUNCTIONAL DESCRIPTION .............................................................................................. 15
    5.2.1. Mapping between the Shibboleth User Identity and the VOMS DN/CA Identity .............................................................................................................. 16
    5.2.2. Attribute Management ............................................................................................... 17

6. SOFTWARE IMPLEMENTATION ............................................................................................. 20

7. OPERATION IN A TEST BED .................................................................................................. 21

8. SUMMARY AND OUTLOOK ................................................................................................... 22
  8.1. ACKNOWLEDGMENTS ...................................................................................................... 22
1. INTRODUCTION

1.1. PURPOSE
The purpose of this document is to describe the second phase of work aimed at providing interoperability between Shibboleth and gLite. This work has been done by SWITCH as part of the EGEE-II project. Whereas the first phase of this work concentrated on authentication, this second phase puts the emphasis on authorization by implementing a mechanism, which enables grid services to use Shibboleth attributes in authorization decisions.

The audience of this document are members of the EGEE-II JRA1 activity, Shibboleth and grid system administrators as well as interested grid users.

We assume that the reader is familiar with Shibboleth [R1], [R2], the SLCS service [R3] and VOMS [R4].

1.2. DOCUMENT ORGANISATION
In section 2 we explain the motivation for attribute-based authorization in grid infrastructures and the advantages of using Shibboleth attributes in authorization decisions. In section 3, we compare four design options for enabling authorization decisions using Shibboleth attributes. Section 4 describes the chosen solution and outlines the software design. In section 5 we present the user’s view of the service, followed by its functional description. In section 6 we give an overview of the software architecture. Section 7 handles the deployment issues and section 8 concludes with a summary and an outlook.

1.3. APPLICATION AREA
This document applies to the implementation of Shibboleth - gLite interoperability through the transfer of Shibboleth attributes to VOMS.

1.4. REFERENCES

<table>
<thead>
<tr>
<th>Table 1: Table of references</th>
</tr>
</thead>
<tbody>
<tr>
<td>R 1</td>
</tr>
<tr>
<td>R 2</td>
</tr>
<tr>
<td>R 3</td>
</tr>
<tr>
<td>R 4</td>
</tr>
<tr>
<td>R 5</td>
</tr>
<tr>
<td>R 6</td>
</tr>
</tbody>
</table>

---

1 In the first phase, a service called SLCS, was developed, which issues short-lived X.509 certificates to grid users. It is described in [R3].
R 7 | VOMS C API documentation [http://egee-jra1-wm.mi.infn.it/egee-jra1-wm/voms_guides.shtml](http://egee-jra1-wm.mi.infn.it/egee-jra1-wm/voms_guides.shtml)
---|---
R 8 | gLite CVS repository, module org.glite.security.voms. See [https://edms.cern.ch/document/468700/0.7](https://edms.cern.ch/document/468700/0.7) for information how to access the source code.

### 1.5. DOCUMENT AMENDMENT PROCEDURE


### 1.6. TERMINOLOGY

A complete project glossary is provided in the EGEE glossary [http://egee-jra2.web.cern.ch/EGEE-JRA2/Glossary/Glossary.html](http://egee-jra2.web.cern.ch/EGEE-JRA2/Glossary/Glossary.html).

#### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAI</td>
<td>Authentication and Authorization Infrastructure</td>
</tr>
<tr>
<td>AC</td>
<td>Attribute Certificate: Structure similar to a public key certificate with the main difference that it does not contain a public key. See <a href="http://www.ietf.org/rfc/rfc3281.txt">http://www.ietf.org/rfc/rfc3281.txt</a> for details. For the context surrounding AC and VOMS see <a href="http://grid-auth.infn.it/docs/AC-RFC.pdf">http://grid-auth.infn.it/docs/AC-RFC.pdf</a></td>
</tr>
<tr>
<td>Attribute</td>
<td>A property of an end entity. In the context of Shibboleth Identity Provider attributes are used to characterize a user.</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority: An internal entity or trusted third party that issues, signs, revokes and manages digital certificates.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Information issued by a trusted party. Used to identify an individual or system.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Evidence asserting the user’s right to access certain systems (e.g. username, password, etc)</td>
</tr>
<tr>
<td>DN</td>
<td>Distinguished Name: Subject of an X.509 certificate</td>
</tr>
<tr>
<td>EGEE</td>
<td>Enabling Grids for E-sciencE: EU funded grid project</td>
</tr>
<tr>
<td>End Entity</td>
<td>System (individual, host, service) that receives a certificate expressing its identity</td>
</tr>
<tr>
<td>Federation</td>
<td>Collection of organizations that agree to interoperate under a certain rule set.</td>
</tr>
<tr>
<td>Federated Identity</td>
<td>Management and use of identity information across security domains, e.g. between members of a federation. Federated identity inevitably deals with issues like liability, security, privacy and trust.</td>
</tr>
<tr>
<td>gLite</td>
<td>Middleware stack developed by the EGEE project</td>
</tr>
<tr>
<td>Identity Provider</td>
<td>Authority responsible for generating and asserting authentication, authorization and identity information about their users in a security domain</td>
</tr>
<tr>
<td>IGTF</td>
<td>International Grid Trust Federation: Body with the goal to harmonize and synchronize PMAs policies to establish and maintain global trust relationships in e-Science. See <a href="http://www.igtf.org">http://www.igtf.org</a> for details.</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union: International organization established to standardize and regulate international radio and telecommunication.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ITU-T</td>
<td>International Telecommunication Standardization Sector</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure: Processes and technologies used to issue and manage digital certificates, enabling third parties to authenticate individual users, services and hosts.</td>
</tr>
<tr>
<td>SAML</td>
<td>Security Assertion Markup Language: an XML framework for exchanging authentication and authorization information. SAML is a standard of OASIS and is the first standard for federated identity.</td>
</tr>
<tr>
<td>Service Provider</td>
<td>A collection of resources in the terminology of Shibboleth. Normally a Service Provider only contains one resource.</td>
</tr>
<tr>
<td>Shibboleth</td>
<td>Federated identity management solution from Internet2/MACE (Middleware Architecture Committee for Education). It is the name of the architecture as well as the name of the open source implementation.</td>
</tr>
<tr>
<td>Short-lived X.509 certificate</td>
<td>An X.509 certificate with a life time of less than 1 million seconds (approx. 11 days)</td>
</tr>
<tr>
<td>SLCS</td>
<td>Short-lived credential service: A service returning a short-lived X.509 certificate to a requester after successful authentication</td>
</tr>
<tr>
<td>SWITCHaai</td>
<td>Shibboleth Federation operated within the Swiss higher education and research sector. See <a href="http://www.switch.ch/aai">http://www.switch.ch/aai</a> for details.</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface: host from where the user interacts with the grid software in the gLite middleware environment.</td>
</tr>
<tr>
<td>VASH</td>
<td>Voms Attribute from Shibboleth: the name of the Shibboleth Service Provider described in this document. It transfers Shibboleth user attributes into VOMS.</td>
</tr>
<tr>
<td>VO</td>
<td>Virtual Organization: arbitrary grouping of people and resources with the goal of conducting a project.</td>
</tr>
<tr>
<td>VOMS</td>
<td>Virtual Organization Membership Service: A grid service, which describes and manages the members of a virtual organization.</td>
</tr>
<tr>
<td>X.509 certificate</td>
<td>Certificate compliant with the format as specified in the X.509 standard.</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Mark-up Language</td>
</tr>
</tbody>
</table>
2. MOTIVATION

2.1. MOTIVATION FOR ATTRIBUTE BASED AUTHORIZATION IN GRID INFRASTRUCTURES

Grid infrastructures currently use X.509 certificates for authenticating and authorizing grid users. Authentication is based on the fact that a trusted Certificate Authority (CA) issued the X.509 certificate.

Authorization on the other hand is achieved through:

- the examination of the Distinguished Name (DN) of the X.509 certificate, e.g. through the use of grid-mapfiles\(^2\); or
- the user’s membership of a Virtual Organization (VO), which are cross-institution groups of users, and are often used to identify the members of a project.

These authorization schemes, while very simple and powerful, only allow decisions, based on the identity of the user. However, there are cases, where fine-grained authorization decisions are desirable.

The Virtual Organization Membership Service (VOMS) is a grid service that describes the membership of users in VOs as well as the membership in groups within that VO. Users are identified through the combination of the DN and the issuing CA\(^3\) of their X.509 certificate. In addition to the membership information, there is an additional “role” parameter, which is used to specify valid roles that a grid user can assume and choose on a case-by-case basis.

Normally, the user presents a proxy certificate and not his X.509 certificate to grid services, which he obtains by executing the command `voms-proxy-init` on the command line of the User Interface (UI). This command also contacts the VOMS server and an attribute certificate (AC) is obtained and inserted into the proxy certificate. This AC, signed by the VOMS server, contains the information about the group memberships, role and capability of the user within the context of the VO.

VOMS is being currently expanded to support arbitrary attributes in the form of key value pairs, besides the already mentioned groups and roles. This feature, while not yet supported by many grid resources, will allow fine-grained authorization decisions in the future. However, these attributes have to be maintained in VOMS and are therefore typically specific to a given VO.

2.2. MOTIVATION FOR ENHANCING AUTHORIZATION WITH SHIBBOLETH ATTRIBUTES

In recent years Authentication and Authorization Infrastructures (AAI) were introduced in the academic and research sector. Often these AAIs were driven by national research and education networks (NREN) and are based on campus user databases. Examples of AAI-architectures are Shibboleth (developed within the Internet2 project [R1], [R2]), A-Select (initiated by SURFnet), and PAPI (developed by RedIRIS). Shibboleth itself has attracted significant interest and has found the widest following with national deployments in countries such as the USA, Switzerland, Finland, France, the UK and Australia. In addition, it is currently also under consideration in further European countries such as the Czech Republic, Denmark, Germany and Sweden.

---

\(^2\) grid-mapfiles are ASCII files which are installed on grid resources and contain a list of DNs, which are accepted by this resource, together with a mapping to a local user account.

\(^3\) Here we denote this unique combination of DN and the issuing CA of a user X.509 certificate as DN/CA.

\(^4\) There is also a “capability” parameter, which is not widely used.
There is a strong motivation for adding interoperability between these national AAIs and grid middleware. Within the gLite middleware, a first step in enabling interoperability has already been achieved. Grid users can obtain a short lived certificate based upon a successful authentication at a Shibboleth Identity Provider (IdP), hence authenticating himself against the campus user database as described in detail in [R3]. However, this first step does not take any information about the user as given by the Shibboleth attributes into account. This document describes a mechanism, which makes this information available for grid services and is therefore the natural next step beyond [R3].

We now first review the information that campuses provide about users and possible use cases before describing the mechanism for making this information available to grid service. We take SWITCHaai [R5], the national AAI for the higher education and research sector in Switzerland, as an example. Other AAIs may have different information about their users, but there is similar information available.

In SWITCHaai every campus stores the attributes describing the user [R6] in databases, such as LDAP, various SQL databases, Active Directory etc. Within the federation there is a set of attributes that has to be defined and maintained for every user; other attributes are optional or recommended. Table 2 gives a complete listing of the currently used attributes. Individual institutions may, in addition, define further attributes that are specific only for intra-institutional or bilateral use and have no meaning at the federation level.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>LDAP Name</th>
<th>derived / adapted from</th>
<th>Implementation Status</th>
<th>Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>unique ID</td>
<td>swissEduPersonUniqueID</td>
<td></td>
<td>X X</td>
<td></td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td></td>
<td>X X</td>
<td></td>
</tr>
<tr>
<td>Given name</td>
<td>givenName</td>
<td></td>
<td>X X</td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td>swissEduPersonDateOfBirth</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td>swissEduPersonGender</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Preferred language</td>
<td>preferredLanguage</td>
<td></td>
<td>X X</td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>mail</td>
<td></td>
<td>X X</td>
<td></td>
</tr>
</tbody>
</table>

5 More precisely: A few Shibboleth attributes such as first name, last name and institution are used to construct the DN of the X.509 certificate, but these are just a small subset of the available Shibboleth attributes.
The attributes of the user can be divided into two groups:

- Information private to the user, such as his first name, last name, email address, preferred language, postal address, mobile telephone number, etc
- Information describing the activity and role of the user within the institution, such as his affiliation (student, staff, professor), study branch and level, staff category and entitlement.

We consider the second group of attributes as the ones, which will mostly be used in authorization decision. These are also attributes that tend not to change often, which is an important criterion for linking attribute values to authorization decisions.

Furthermore, given the content of these attributes, it is natural that data privacy laws have to be taken into account when this data is exposed to third parties.

Simple authorization and prioritization decisions uses can be envisaged based on the information in Table 2 such as

- Filtering on the type of organization the user belongs to (university, hospital, library, etc)
• Sending grid jobs to higher or lower priority queues in a computing element based on the affiliation of the user (student, staff, etc)
• Accepting or rejecting users of a given study level in a given study branch (e.g. all students in the computer science department which have completed the first two years of their studies)
• Enabling access based on entitlements (membership to a given group) or staff category (teachers, researchers, others).

Last but not least we would like to point out that these attributes could theoretically also be maintained at the level of the virtual organization. However, from a practical point of view, this should be avoided because it requires that VO administrators maintain attributes, which are specific to another domain (namely the institution where the user is employed). In the same way, a campus administrator should not maintain VO specific attributes, which have no meaning within the campus infrastructure. Hence the best solution accommodates two sources of attributes, one for the VO and one for the campus environment.

3. DESIGN OPTIONS

Our basic approach in designing a system to make Shibboleth attributes available for grid services authorization is to consolidate all the authorization data at one location (as opposed to consolidating the corresponding authorization mechanisms). More precisely, the user attributes from Shibboleth federations are merged at one location with the user’s credentials and their attributes from the grid infrastructure. These latter attributes are typically user specific VO data associated with the user’s certificate.

![Figure 1 Entities and their natural associations](image)

Figure 1 illustrates the main entities that are involved in the authorization process. A user wants to access a grid service. The credentials he owns are a X.509 certificate, an AC from VOMS and
Shibboleth attributes. We assume that the grid service requires information from all three sources for the authorization of the user.

We now describe four options how the information from VOMS and Shibboleth IdPs can be merged and explain, why the last of these options was chosen.

3.1. OPTION 1: SHIBBOLETH ATTRIBUTES IN ATTRIBUTE CERTIFICATES

Before accessing any grid resource the user requests his credentials consecutively from the VOMS server and from the Shibboleth Identity Provider (IdP). He then inserts them into a proxy certificate, which he presents to the grid resources. (This is the mechanism currently in use with VOMS ACs).

The advantage of this approach is that it handles attributes coming from two different sources (Shibboleth IdP and VOMS) in a transparent way. However, this option has also disadvantages. Shibboleth IdPs exchange user attributes as SAML assertions, but this approach requires attributes in ACs. Therefore, either the user must generate the AC from the SAML assertions or modifications made to the Shibboleth IdP such that it can also issue ACs.

AC creation by the user requires special mechanisms to provide integrity and authenticity, as the IdP is the attribute authority and not the user. The better alternative is to let the Shibboleth IdP issue ACs, which would require source code changes at the IdP.

The Shibboleth IdP would act like VOMS. Thus, it has to be trusted by all grid entities using Shibboleth authorization information. This implies that all Shibboleth IdPs use EUGridPMA certificates and all grid resources would require to maintain a list of trusted Shibboleth IdPs (as is done currently with VOMS).

3.2. OPTION 2: SHIBBOLETH ATTRIBUTES IN X.509 USER CERTIFICATE

One of the problems with the previously presented option is scalability, as it requires that every Shibboleth IdP becomes a grid entity (and there are far more Shibboleth IdPs than VOMS servers).

A remedy would be to integrate the Shibboleth credentials directly into the X.509 user certificate (as an extension), when the CA issues the certificate. This may be feasible, since Shibboleth attributes generally do not change frequently.

The advantage of this approach is that there is no change in the Shibboleth infrastructure. In addition, the Shibboleth IdP does not need to be known by the grid services.

The drawback of this approach is that the X.509 user certificate now contains additional information and is no longer a standard X.509 certificate. The user cannot decide whether to expose this information or not, which raises data privacy issues. This is particularly unattractive if the certificate is also used for purposes outside the grid context. In addition, the certificate needs to be revoked whenever the Shibboleth attributes change.

From the point of view of the CA the new X.509 extension would have to be registered (request for an OID) and software to extract the authorization information for grid entities would have to be implemented. This requires the implementation of functionality that is parallel to the VOMS functionality, but at the level of the X.509 user certificate (and not the proxy certificate).

3.3. OPTION 3: GRID RESOURCE REQUESTS SHIBBOLETH ATTRIBUTES

In this approach the grid service directly requests the Shibboleth user attributes from the Shibboleth IdP every time a user accesses the resource. The approach requires the addition of SAML functionality
at every grid service. The main intention of this second phase of the interoperability work is to make Shibboleth attributes available with minimal changes in the existing grid middleware. Therefore, it was decided to tackle this approach and its problems at a later stage of our work (MJRA1.7 Shibboleth interoperability with SAML support).

3.4. OPTION 4: SHIBBOLETH ATTRIBUTES IN VOMS

This approach targets at keeping all grid relevant authorization information about a user in a single place, with VOMS as the obvious candidate. The main advantage is that the authorization mechanism used by the grid services need not to be changed\(^6\); this eliminates many of the drawbacks of the other options. There are two possible models for transferring the attributes: the push and the pull model.

- In the pull model the VOMS server retrieves the Shibboleth attributes directly from the Shibboleth IdP provider. To do so, the VOMS server needs to know to which Shibboleth IdP a user belongs and what his identity in the IdP is. In addition, the Shibboleth protocol would require modifications to permit such a delegated access. Therefore we do not consider the approach at this point.

- The push model suggests that the Shibboleth attributes are pushed by some means to the VOMS server. We propose to use an intermediate entity for this purpose and that the push procedure is triggered by the user. We call this intermediate entity VOMS Attributes from Shibboleth (VASH) service.

4. THE DESIGN OF THE SERVICE

Our design consists of implementing a service, which transfers a user’s Shibboleth, attributes to VOMS upon request of the user. There is one instance of this service for every Shibboleth federation and every VO (see Figure 2). The main advantages of this design are:

- The X509 user certificate remains unchanged (no attributes in the X.509 extensions).
- The Shibboleth credentials are transparently integrated into VOMS ACs. Using the credentials for authorization in grid requires minimal changes at the grid service itself. In particular, no Shibboleth specific code has to be added to the grid service and no changes are needed at the Shibboleth IdP.
- VOMS servers do not have to be changed and do not need to become Shibboleth Service Providers (in contrast to the pull model as mentioned in option 4 above).
- The VO user registration does not have to be changed. This is important, as some VOs have implemented their own registration software and procedures (e.g. VOMRS).
- The administrative domains of VOMS and Shibboleth are fully decoupled, i.e. the VOMS administrator manages only VO specific information and the Shibboleth IdP administrator manages only campus relevant information.
- For the Shibboleth IdPs this service is just another Shibboleth Service Provider (web resource).

\(^6\) Some work is required as a plug-in to the existing authorization module LCMAPS has to be implemented.
• The user itself as registered in the VOMS server manages the mapping of the user identity between the Shibboleth IdP and the DN of the user’s X.509 certificate. Therefore, the administrative burden for the VASH administrator is kept to a minimum. In addition, the new service becomes a repository where the mapping of the Shibboleth IdP and the DN is stored and made available to other (properly authorized) services.

• No IGTF certificates have to be installed on the Shibboleth IdP.

• This approach does not have any performance penalties.

![Diagram of Shibboleth Federation, VOMS, and VASH relationships]

**Figure 2 Relationships between Shibboleth IdP's, VOMS and VASH**

There are three different views of the VASH service:

• For the grid user: It is a Shibboleth Service Provider, which he accesses through his web browser to push a subset of his Shibboleth attributes into VOMS.

• For the Shibboleth administrator: The VASH service looks like any other Shibboleth Service Provider.

• For the VOMS administrator: The VASH service is a grid resource that invokes the VOMS web services interface. The VOMS administrator has to enable the access for the VASH service. The functionality provided by the VASH service is transparent to VOMS.
4.1. DESIGN PRINCIPLES

The software design of the VASH service is based on the following principles:

1. The user can only access the VASH service through a browser. There is no command line interface nor will VASH expose a web services interface.
2. It is programmed in Java.
3. The code should be very modular such that subcomponents can easily be exchanged.
4. Existing gLite libraries should be used where ever possible, in particular the security framework.
5. Synergies between the SLCS service [R3] implementation (design and code) should be exploited. For example such a synergy may permit a user to access the VASH service without a certificate in his browser (see 5.2.1 for details).
6. The error reporting should permit a user to understand the cause of an error or access denial. For example, VASH should be able to tell a user that the VOMS server cannot be reached.

5. DESCRIPTION OF THE VASH SERVICE

We start by describing the user’s view of the web interface of the VASH service. Then we proceed to discuss the functional description, where explain in detail how the Shibboleth user identity is mapped to the VOMS user identity. At the end we outline the attribute update mechanism between Shibboleth and VOMS.

5.1. USER’S VIEW OF THE VASH SERVICE

The prerequisites to access the VASH service are:

1. The user must have an account at a Shibboleth IdP
2. The user must be a member of a VO that is managed by VOMS
3. The user must have been given access to the VASH service by its administrator

The user accesses the VASH service with a web browser. Upon first access a mapping is established between the Shibboleth and the VOMS user identity. This may be done automatically or involve the confirmation of the mapping by the VASH administrator (see 5.2.1 for details). Once this mapping has been successfully established, the user gains access to a webpage (see Figure 3), where he can inspect his Shibboleth attributes and submit them to VOMS.

Once the Shibboleth attributes have been transferred into VOMS, they will be automatically present in the VOMS AC of the user’s next proxy certificate. For more details how attributes are stored and retrieved from the certificate we refer to the VOMS documentation [R7].
5.2. FUNCTIONAL DESCRIPTION

Figure 4 illustrates the sequence of actions if a user creates or updates his Shibboleth attributes in the VOMS server. Steps one through four are the standard Shibboleth browser profile.

1. The user accesses the Shibboleth protected VASH service with a browser that contains the certificate, with which he is registered in VOMS. (If SLCS certificates are used, they don’t have to be imported in the browser).
2. The VASH service redirects the user to the Shibboleth IdP, where the user authenticates himself with his credentials (e.g. username and password).

3. The Shibboleth IdP issues a handle to the VASH service through a browser POST.

4. The VASH service receives the attributes of the user from the IdP. These attributes are used to authorize the user (ACL based authorization).

5. The VASH service checks whether a user with the correct combination of DN/CA is registered in VOMS and whether the mapping of the DN/CA to the Shibboleth identity of a user is valid (see section 5.2.1 for details).

6. The VASH service presents the set attributes to the user, which it will write into VOMS upon user consent (see Figure 3). These attributes are called “permissible attributes” and are selected by the administrator of the service. If an attribute has several values\(^7\), then the user must decide, which one shall be transferred to VOMS.

7. VASH writes the permissible attribute set into VOMS once the user has pressed the “submit” button on the web interface. If the attributes do not exist in VOMS, they will be created. If their values have changed, they will be updated.

The user will get only access to the contact information and FAQ web page of the VASH service if the authorization fails. This kind of access is called restricted access.

5.2.1. Mapping between the Shibboleth User Identity and the VOMS DN/CA Identity

The user identity in Shibboleth has to be related to the user identity in VOMS in order to assign the Shibboleth attributes to the correct user in VOMS. In Shibboleth users are identified through their login name. In VOMS users are uniquely identified through the combination of the DN and issuing CA of the X.509 certificate, with which they have been registered in VOMS. In the following we name this combination DN/CA.

Figure 5 shows the mapping mechanism between the two identities that takes place in VASH (step 5 above):

1. The user accesses the service through a browser. The authentication at the Shibboleth IdP has been successful and the SAML attributes are available to the VASH service.

2. The access to the VASH service is checked based on the Shibboleth attributes of the user. If the access is granted, continue with step 3, if not the access to VASH is denied

3. Next it is checked whether a certificate is present in the browser. If this is the case continue with step 4, otherwise continue with step 6.

4. The DN/CA and the Shibboleth user identity are compared with the values in the local database. This step is needed to prevent (accidental) impersonation.\(^8\)

5. If the attempted mapping fails (because there is no mapping or the mapping does not match), then the request for access is put on hold until the VASH administrator either accepts or

---

7 Shibboleth attributes may have several values, and all values are transfers from the IdP to the SP.

8 For example Elvis may quickly use Igor’s computer and account to access a Shibboleth protected resource and does not close the browser to kill the session cookies. Two hours later Igor remembers to update his Shibboleth credentials in VOMS. He forgets Shibboleth’s single sign on capability and uses accidentally Elvis’ identity to create/update his(?) Shibboleth attributes on VOMS.) Access is granted to the user if the mapping test between the Shibboleth identity and the DN/CA is successful. If this mapping test is successful, then the user gets access.
rejects the access for this combination of DN/CA and Shibboleth user identity. On a positive decision, the user will have to re-visit the VASH service to push his Shibboleth credentials onto the VOMS server.

6. If the user has a SLCS certificate, then the certificate does not have to be in the browser. In this case the VASH service executes the same algorithm as the SLCS service to relate the DN/CA with the Shibboleth user identity. Access is granted if a user with this (freshly computed) DN/CA exists on the VOMS server, otherwise it is denied.

![Diagram](image)

**Figure 5 Mapping between Shibboleth user identity and VOMS DN/CA identity**

### 5.2.2. Attribute Management

We mentioned the design objective to consolidate the information describing the user as available in the Shibboleth IdP and in VOMS. This is achieved by storing all attributes in VOMS with the VASH service acting as a mediator. Thus, the VASH service cleanly decouples the administrative domains of Shibboleth and VOMS, but at the same moment takes over responsibilities. These are:

- Validate the mapping of the Shibboleth user identity with the identity in VOMS. Note that VASH does not create the mapping, but only validates it. If automatic validation is not possible, then the VASH administrator has to confirm it.
- Maintain a set of permissible Shibboleth attributes that can be pushed into VOMS. Note that not all SAML attributes may be suitable authorization attributes in the grid context (see e.g. Table 2).
- Upon a change in the set of permissible Shibboleth attributes: remove obsolete attributes on VOMS for all users that had them pushed into VOMS

---

9 This of course requires that the SLCS and the VASH service belong to the same Shibboleth federation and use the same algorithm to construct the DN from the Shibboleth attributes.
• Define appropriate default values for the expiration times of the attributes in VOMS
• Notify users if their credentials are about to expire
• Remove expired attributes from VOMS (see below for details)
• Provide the means for a user to view the attributes before they are being pushed into VOMS. The user can choose the attribute value to be transferred to VOMS if the Shibboleth attribute has multiple values.

A central element of the VASH service is its database, which is used to comply with the above requirements. Figure 6 shows the two tables that describe the mapping between Shibboleth user and DN/CA. The tables are normalized. Primary keys are marked with an asterix (*).

The entries in the User table are filled with values received by Shibboleth. The DN and CA entries in the VomsUser table are taken from the certificate of the user. The email entry is taken from the corresponding Shibboleth attribute. The lastModified entry is a timestamp, tracking the last change in VOMS. The enabled entry states whether the mapping between userId and DN and CA is valid or has been approved by the VASH administrator (see 5.2.1 for details).

![Database tables describing the mapping between Shibboleth userid and VOMS user](image)

The tables in Figure 6 are used not only to describe the mapping between Shibboleth and VOMS but also to notify the user when their Shibboleth attributes in VOMS are about to expire.

Figure 7 illustrates the expiration mechanism with an example. On the time axis are three dates, which are the early bird time, the notification time and the expiration time. These times are global in the sense that they are the same for all users. The expiration time is the time when the Shibboleth attributes in VOMS are deleted. The notification time is the time when users get notified that their attributes are about to expire, and the early bird time is a demarcation line, which delineates expiring credentials from up-to-date credentials.

---

10 Shibboleth attributes can have multiple values. By taking the email address from the Shibboleth email attribute and associating it with the VomsUser database table, we give the user the choice of selecting different email addresses for different VO’s.
In order to illustrate this mechanism we consider the following example: Assume the current time is \( t = t_1 \). The database holds the records of users A (Ra), B (Rb), E (Re), and C (Rc). The timestamps in the records specify the time when the user attributes have been modified (refreshed) on the VOMS server. The attributes of user A, B and E are about to expire. User C, however, refreshed his VOMS credentials after the demarcation time. His credentials are considered up-to-date.

At time \( t = t_2 \) user A, B and E get notified that their credentials are about to expire. Note user D (Rd) is a new user and his credentials are up-to-date.

At time \( t = t_3 \), User B and E updated their credentials on VOMS before the expiration time. User A did not and his Shibboleth attributes in VOMS are removed by VASH, but all other information about the user in VOMS is untouched, of course.

Finally we would like to comment on the global nature of the expiration time. One could also envisage a solution, in which the expiration times of the attributes are managed on an individual basis. However, it was chosen not to adopt this solution for the following reasons:

1. The administrative duties of the VASH service should be kept to a minimum, as the main Identity Management systems are the Shibboleth IdP (for the user’s home organization) and VOMS (for the VO). In our view the administrative tasks of every intermediate service should be kept to a minimum. If a person leaves or joins the institution or the VO, then this change should be done within the Shibboleth IdP or VOMS and the VASH service should be unaffected.

2. As the Shibboleth attributes change rather rarely over the course of the year, it was deemed sufficient to guarantee periodic updates (e.g. every n months or so).

3. If a user’s attributes change and he needs the new value immediately to access grid resources, then he simply refreshes the attributes by visiting the VASH service web interface.

4. If the user’s attributes change and the VO wants to enforce an update, then the VO administrator simply removes the attributes from VOMS.
6. SOFTWARE IMPLEMENTATION

The software architecture is structured into two functional blocks (see Figure 8):

1. The front-end consisting of an Apache server configured as a Shibboleth Service provider.
2. The VASH server, which is a Java servlet running within the Tomcat servlet engine. The front-end connects to the VASH server by a standard interface for communication (mod_jk).

Figure 8 is a close-up of Figure 4 illustrating the functional components of the VASH server and their interactions. There are several common elements between the VASH and the SLCS service (see [R3] for details). The key features are:

• The access to the VASH server is controlled by Java filters (labelled ACL filters in Figure 8).
• There are two servlets in the VASH server: the Viewer servlet and the Admin servlet.
• The Viewer servlet handles the user commands. It provides a web page on which the user can review all his information in VOMS, the attributes as received from the Shibboleth IdP as well as the certificate information as obtained from the browser. (A screenshot of this webpage is shown in Figure 3). It provides a webpage, where the user can push his permissible Shibboleth attributes into VOMS, and some Web pages with contact information and a FAQ. The servlet is customizable and can be extended with additional Web pages.

The administrator manages the VASH server through the Admin servlet. It allows the administrator to edit the ACL filters, define the set of permissible attributes and confirm or reject a requested mapping between a Shibboleth identity and a DN/CA (see 5.2.1). The administrator can also set expiration, validity and early bird times. The servlet supports additional user management features, such as removing a user.

Many of the management tasks are handled by configurations, which are again read by threads such as the Curator Thread. This thread runs in the background and checks the expiration of attributes. It notifies users by email, and if a user’s attributes expired, it contacts the VOMS server to remove the attributes from VOMS.

The communication with the VOMS server is handled by the VOMS connector, which is a stub generated from the web services definition language (WSDL) interface of the VOMS admin service. It implements a reduced set of the operations of the VOMS web services interface. The VOMS connector attaches to the TrustManager/AxisWrapper, a module enforcing the gLite security framework for the authenticated and secure communication between the VASH and the VOMS server.

Two other important components are the DNbuilder and the DbModule. The DNbuilder returns the DN of a short-lived certificate based on the Shibboleth attributes. It is used to check the DN of users that use the short-lived certificate service (see 5.2.1 for details). The DbModule handles the interactions with the database. Currently only the MySQL database is supported.

---

11 As described in 5.2.2 only a subset of Shibboleth attributes can be transferred into VOMS. This set is called “permissible attributes”.
12 The Admin servlet will be released with the next version of the VASH service.
13 org.glite.security.utils
7. OPERATION IN A TEST BED

The VASH service has been tested in a SWITCH internal test-bed consisting of:

- A Shibboleth IdP participating in the SWITCH test federation
- A host running the VASH service under debian with the MySQL database on the same host
- A VOMS server running version 1.7.10
- A browser based client
- Use of the proxy certificate with the Shibboleth attributes in the SWITCH gLite test-bed (without evaluating the Shibboleth attributes by grid resources, such as the CE).

Future activities will include the development of plug-ins (e.g. for LCAS/LCMAPS or gJAF), which take authorization decisions based on the Shibboleth attributes as present in the proxy certificate. These plug-ins and various authorization scenarios can then be tested in the SWITCH internal gLite test-bed, which consists of a gLite UI, WMS, CE, WNs, LFC and SE.

Tests in a production environment depend on the deployment of the version of VOMS supporting key-value pair attributes (version 1.7.10 or higher).
8. SUMMARY AND OUTLOOK

In this document we described the motivation for and the software implementation of a service for making Shibboleth user attributes available to grid services for authorization decisions. This is achieved by transferring the Shibboleth attributes into the Virtual Membership Organization Service VOMS, from where they will be automatically written to the proxy certificates, which the user presents to grid services. Due to data privacy reasons it was decided to transfer the Shibboleth attributes to VOMS only at the user’s request. Therefore a service called VASH was described which acts as mediator between Shibboleth and VOMS.

The next release of the VASH service will add the following functionalities:

- Web-based administration of the VASH service (currently the administration is done by editing XML files).
- Development of a LCAS/LCMAPS and gJAF plug-in to allow authorization decisions at a gLite CE
- Automatic generation of a VOMS user registration request for users with a SLCS certificate.

In the longer-term, one can also envisage the automatic update of Shibboleth attributes in VOMS once the user has given to VASH his consent for the attribute transfer. However, this will require modifications at the Shibboleth Identity Provider.

SWITCH developed the code for this service as part of the EGEE-II project. The source code has been added to the gLite CVS repository as the module org.glite.security.vash [R8]

8.1. ACKNOWLEDGMENTS

We would like to thank Vincenzo Ciaschini, Andrea Ceccanti and Valerio Venturi from INFN-CNAF. Bologna, Italy, for their help and collaboration in accomplishing this work.