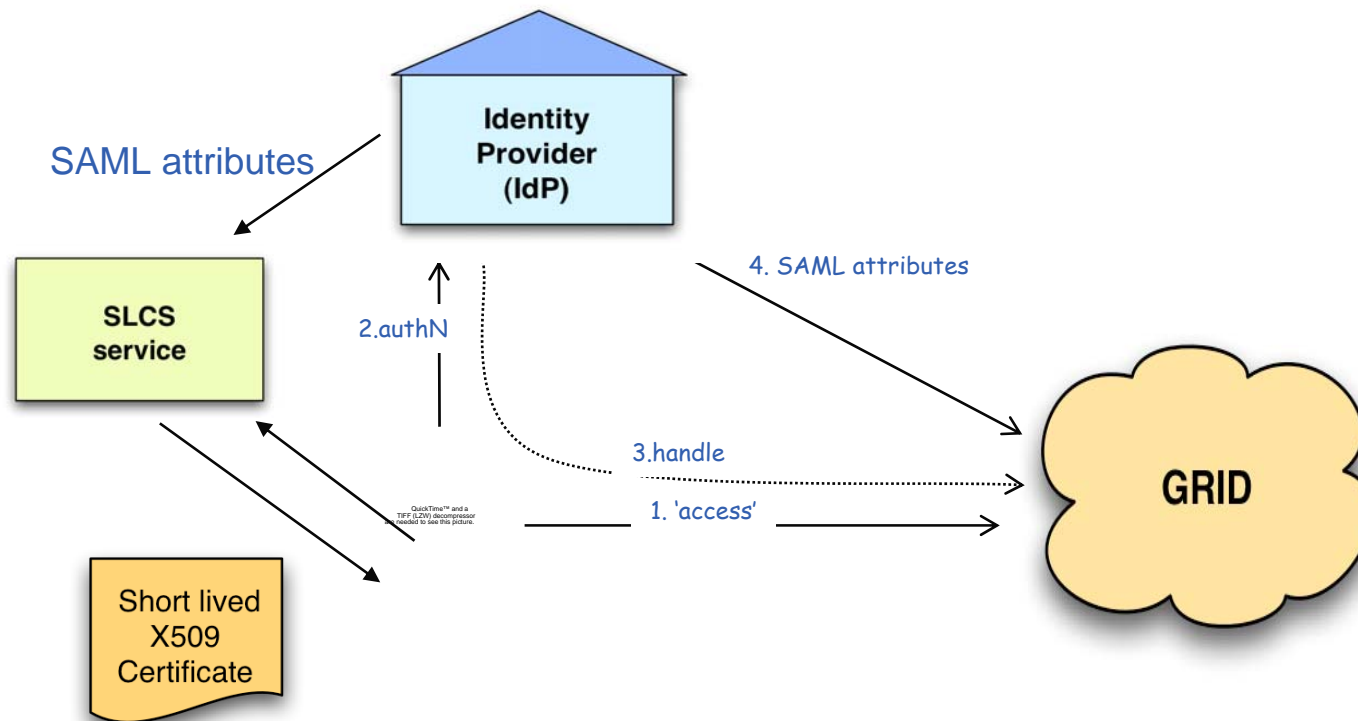


VOMS Attributes from Shibboleth (VASH)

JRA1 All-Hands meeting Catania 8 March 2007

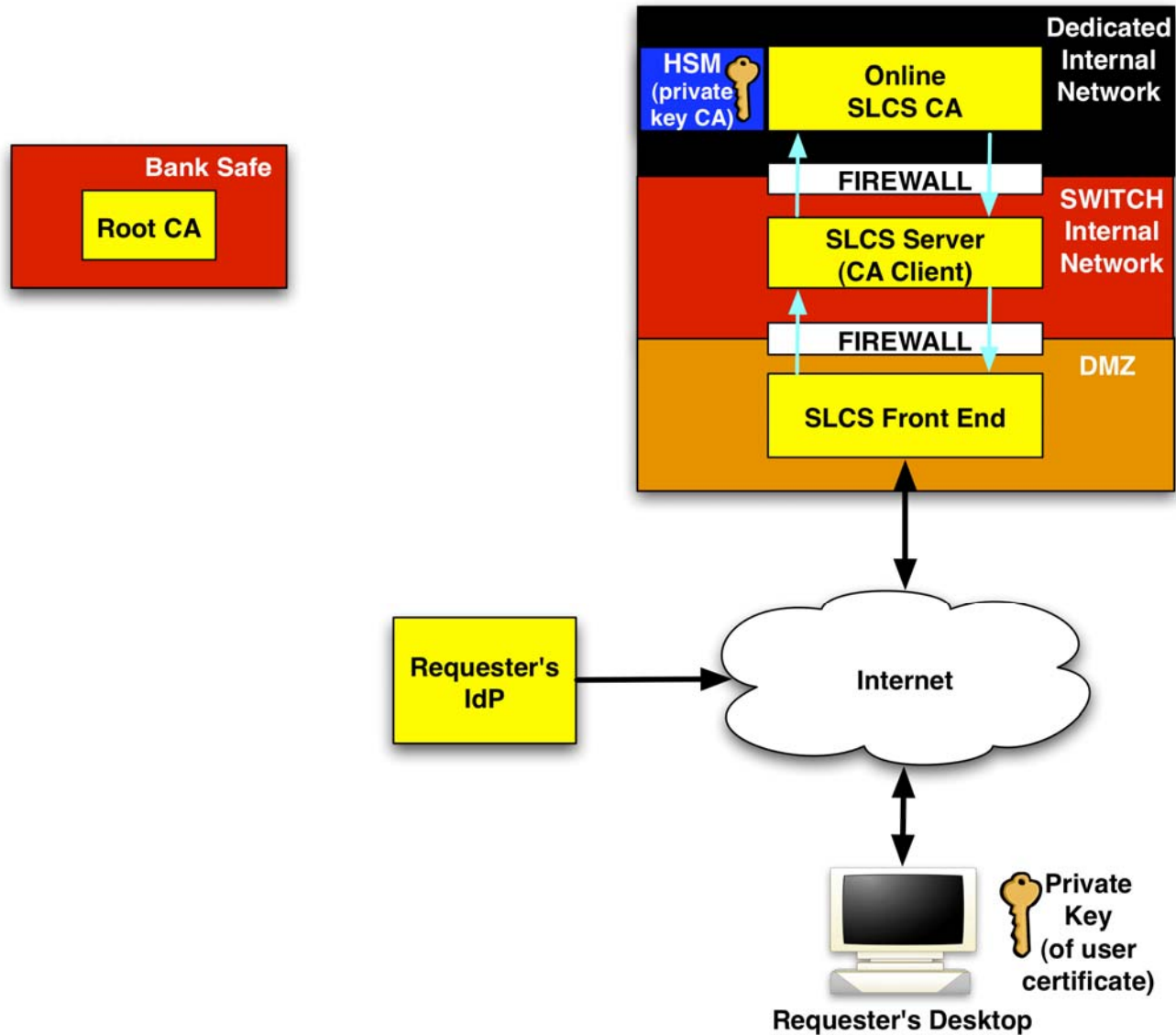
- **Shibboleth: Grid, yet another resource?**
 - highly attractive (typically for academia)
 - *but* ‘resource’ protected by different authN/authZ concepts and mechanisms
- **Grid: get/use authZ information from authoritative sources outside of the grid-universe**
 - permitting more granular authorization
 - decouple management & maintenance responsibilities
 - common understanding of semantics of authZ info (open issue)
- **Common to both: leverage of existing identity management and allow easy access to grid ‘resource’**

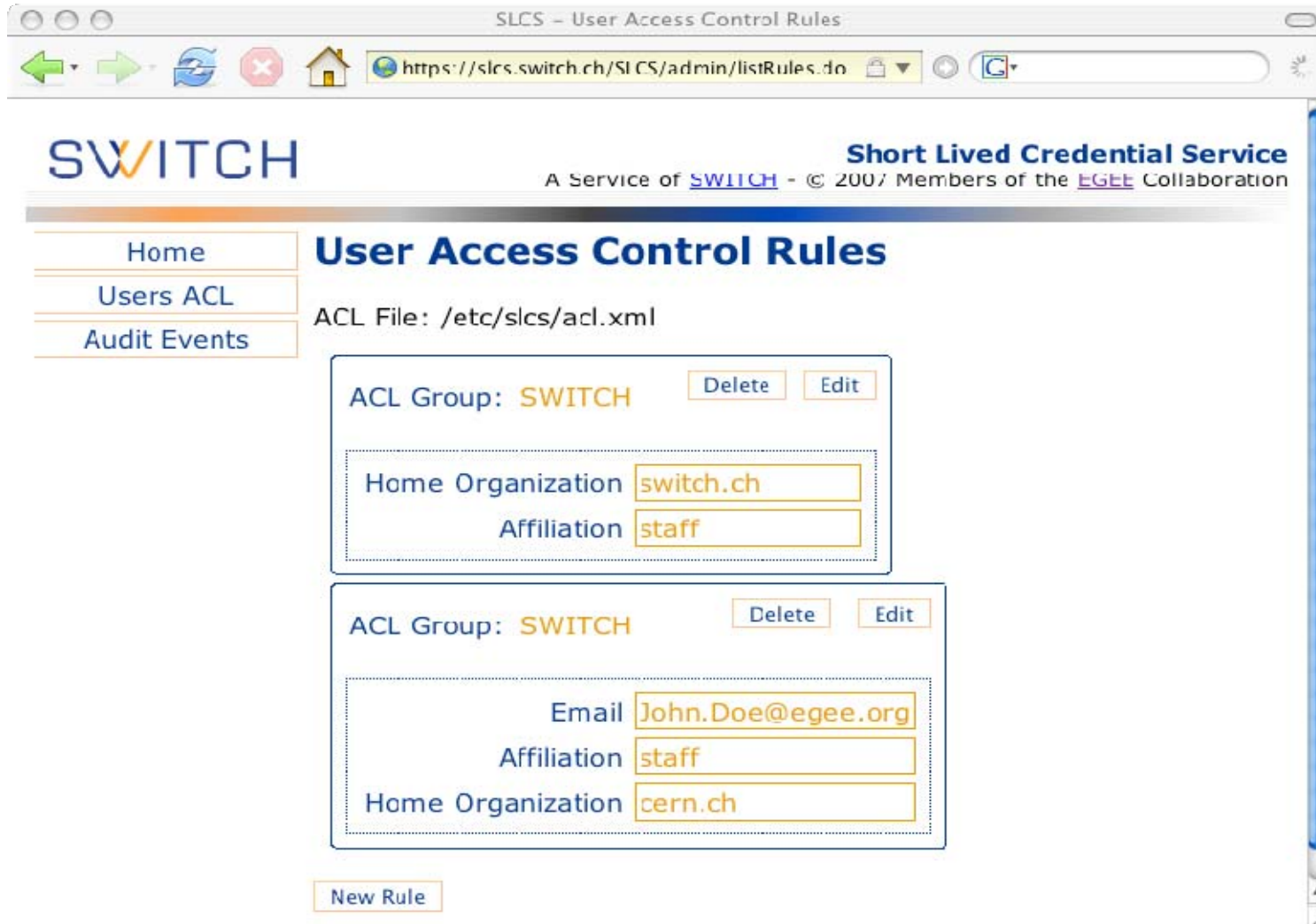
Phase 1: SLCS service



- **Presented in Abingdon**
- **CP/CPS accredited**
 - Accredited by EuGridPMA
 - <http://www.switch.ch/pki/grid>
- **Operation of SLCS TEST CA in test-bed since November**
 - <http://www.switch.ch/pki/grid/test>
- **Production infrastructure ready (Online CA, HSM)**
- **Admin interface finished**
 - User management (ACL based activation of users etc.)
- **MJRA1.4 document: <https://edms.cern.ch/document/770102/1>**
- **Todo's : finish documentation, ETICS integration**

CP/CPS: Certificate Policy and Certification Practice Statement





The screenshot shows a web browser window titled "SLCS - User Access Control Rules" with the URL <https://slcs.switch.ch/SLCS/admin/listRules.do>. The page header includes the SWITCH logo and the text "Short Lived Credential Service" and "A Service of SWITCH - © 2007 Members of the eGEE Collaboration".

On the left, there is a navigation menu with the following items:

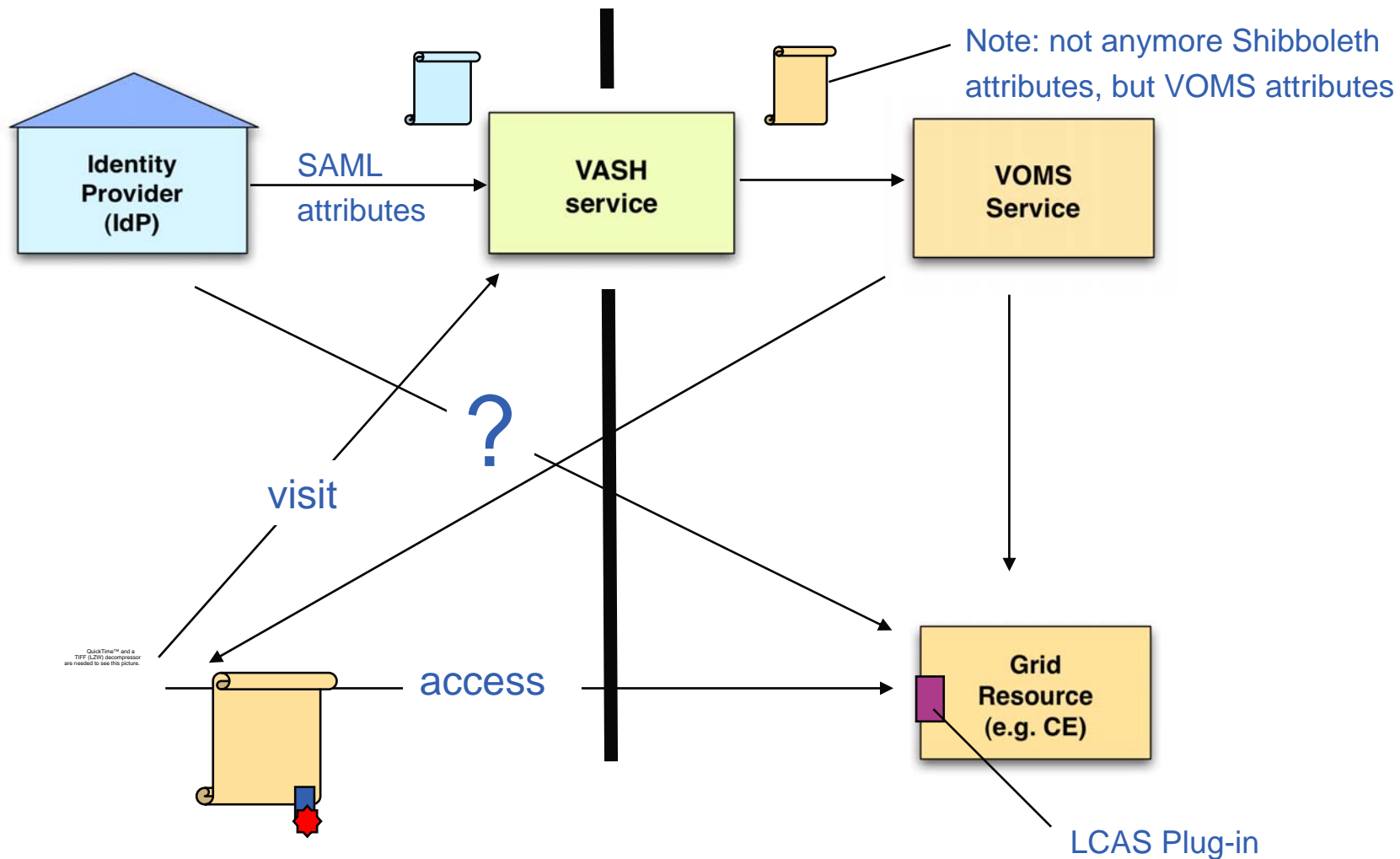
- Home
- Users ACL
- Audit Events

The main content area is titled "User Access Control Rules" and displays the ACL File: `/etc/slcs/acl.xml`. It lists two ACL rules, each with a "Delete" and "Edit" button:

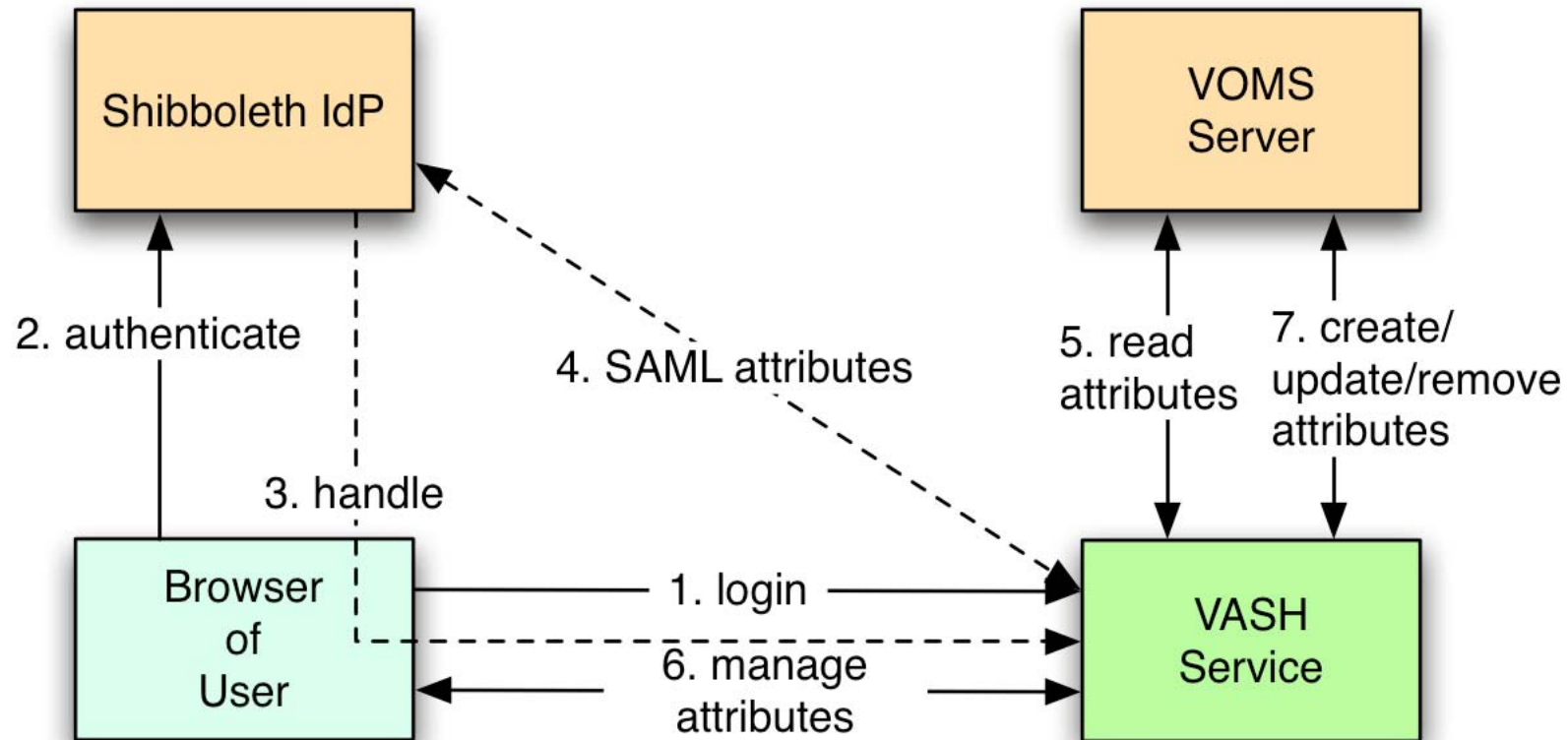
- ACL Group: SWITCH**
 - Home Organization:
 - Affiliation:
- ACL Group: SWITCH**
 - Email:
 - Affiliation:
 - Home Organization:

At the bottom of the page, there is a "New Rule" button.

- **Grid: get/use authZ information from authoritative sources outside of the grid-universe**
 - permitting more granular authorization
 - decouple management & maintenance responsibilities
 - common understanding of semantics of authZ info (open issue)
- **Consolidate/integrate authZ information provided by different sources (IdPs)**
 - **transparent** integration of authZ info from ‘non-Grid’ authorization information providers
 - alternative; explicit **awareness** of grid resource for external authZ information.
 - feature since VOMS 1.7.10 permitting to define attributes besides user/role/group concept



Scenario. User already registered on VOMS



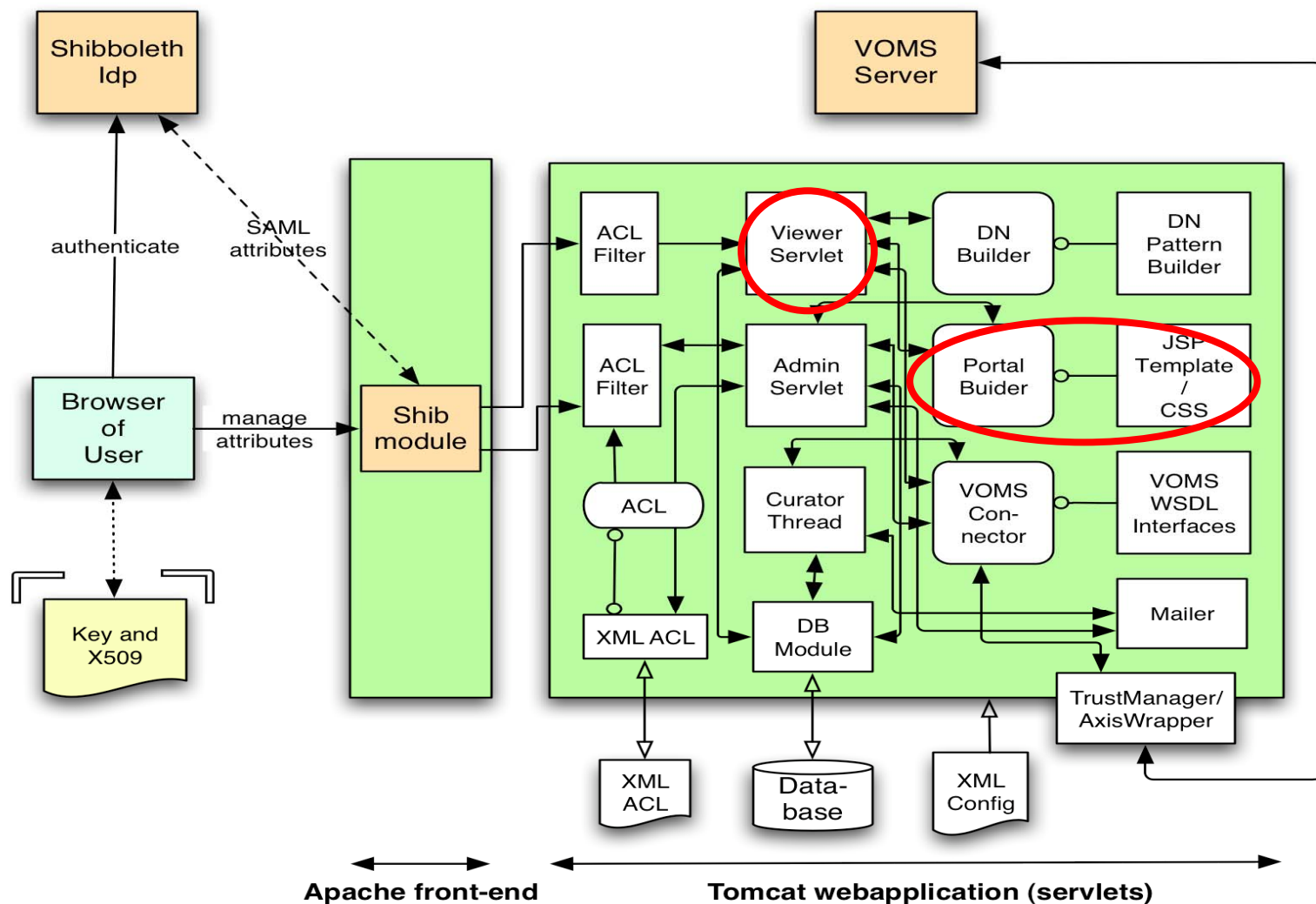
- **transparent** integration of Shibboleth attributes in Grid (as VOMS attributes)
- no changes on existing Grid code...just add plug-ins
- decoupled administrative domains
- from point of view of Shibboleth, VASH is just another service (web resource)
- identity mapping done by user (low admin. burden)
- no IGTF certificates on Shibboleth IdP
- no performance penalties

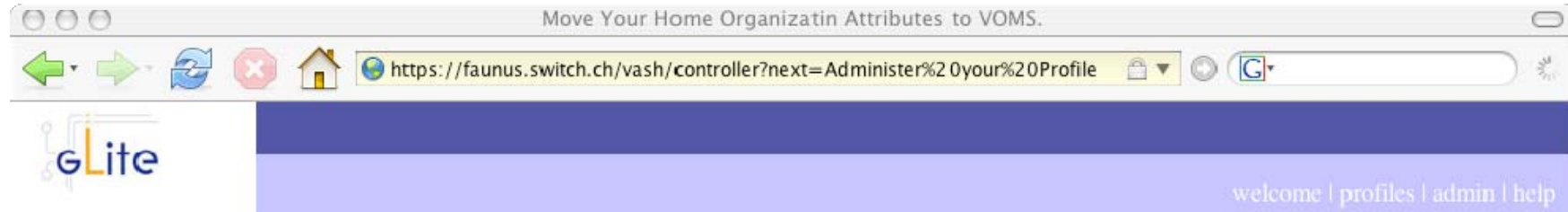
Notice: everything VASH puts on VOMS, VASH does also maintain

- **push Shibboleth attributes to VOMS**
- **enforce Shibboleth and VOMS conform security standards.**
- **enforce up-to-date attributes on VOMS (expiration of records)**
- **inform users**
- **auditing (to a certain degree)**
- **defines set of Shibboleth attributes that can be pushed**
- **provide administration facilities**
- **ease usage of SLCS certificates (not a task but a goody)**

Open:

- **SLCS pre-registration feature (work in progress)**
- **conversion of attribute names (for common understanding)**





ADMIN

- Welcome
- View Your Profiles
- Help
- Contact

Copyright EGEE
Software Licence
Version: 0.8

Administer Your Home Shibboleth Attributes on VOMS Server

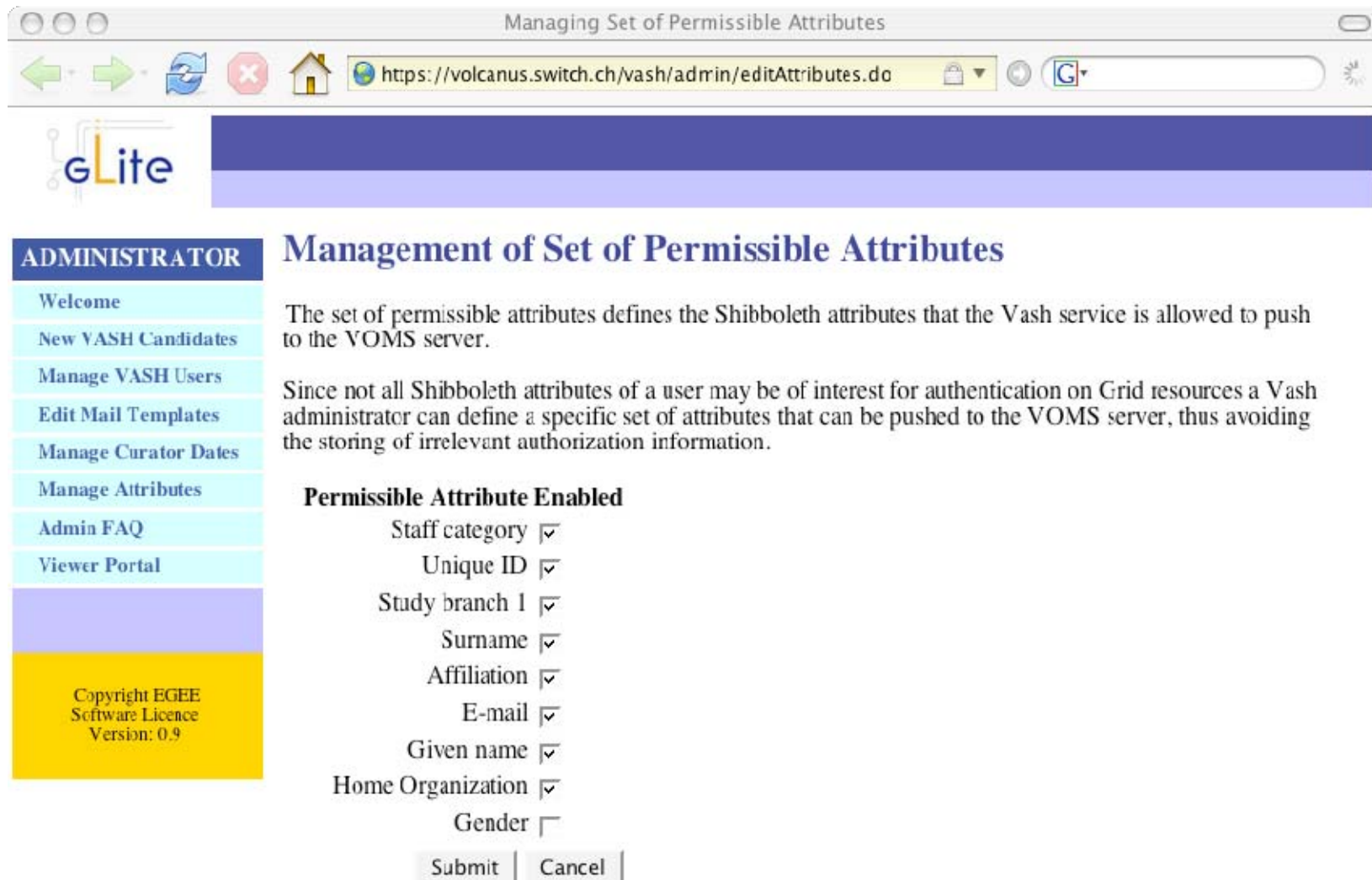
You may update the attributes on the VOMS by pressing below submit button. If a drop-down list is presented, you may select the settings, that are more convenient to you.

<i>Attribute Name</i>	<i>Current Value on VOMS</i>	<i>Changes to:</i>
<i>E-mail</i>	---	placi.flury@switch.ch
<i>Surname</i>	Flury	Flury
<i>Unique ID</i>	521780@switch.ch	521780@switch.ch
<i>Affiliation</i>	staff	staff
<i>Home Organization</i>	switch.ch	switch.ch
<i>Given name</i>	Placi	Placi

Your home organization attributes as currently set on the VOMS server are valid until null. You will be notified to refresh them (by visiting this site) two weeks before expiration time under following e-mail address: flury@switch.ch.

SHIBBOLETH PROTECTED

You're logged in as: /C=CH/O=SWITCH - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury/Email=flury@switch.ch
 Certified by CA: /C=CH/O=SWITCH - Teleinformatikdienste fuer Lehre und Forschung/CN=SWITCH Personal CA/Email=switch.personal.ca@switch.ch



The screenshot shows a web browser window titled "Managing Set of Permissible Attributes" with the URL <https://volcanus.switch.ch/vash/admin/editAttributes.do>. The interface includes a "gLite" logo and a navigation menu on the left with the following items: ADMINISTRATOR, Welcome, New VASH Candidates, Manage VASH Users, Edit Mail Templates, Manage Curator Dates, Manage Attributes, Admin FAQ, and Viewer Portal. The main content area is titled "Management of Set of Permissible Attributes" and contains the following text:

The set of permissible attributes defines the Shibboleth attributes that the Vash service is allowed to push to the VOMS server.

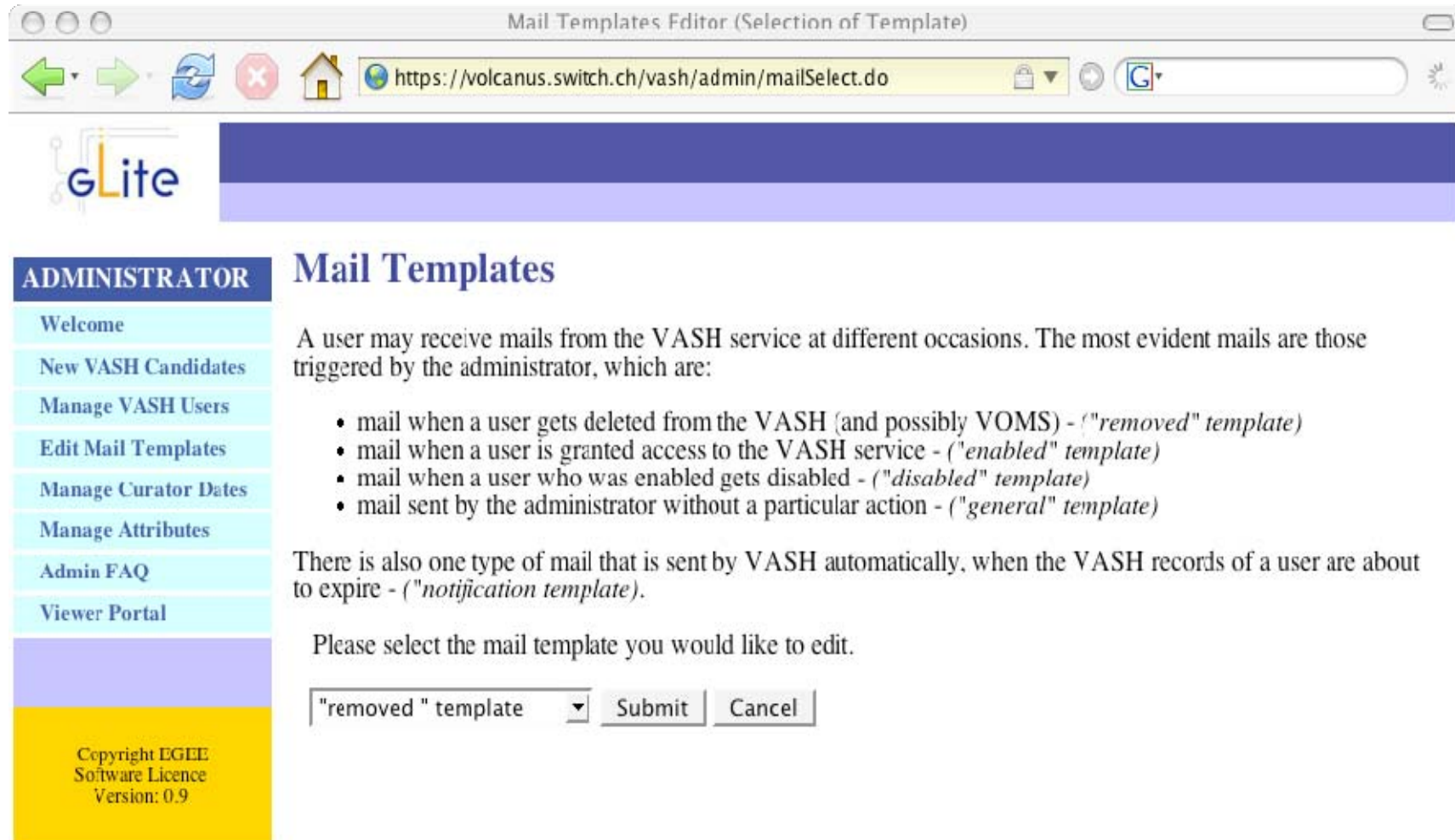
Since not all Shibboleth attributes of a user may be of interest for authentication on Grid resources a Vash administrator can define a specific set of attributes that can be pushed to the VOMS server, thus avoiding the storing of irrelevant authorization information.

Permissible Attribute Enabled

- Staff category
- Unique ID
- Study branch 1
- Surname
- Affiliation
- E-mail
- Given name
- Home Organization
- Gender

At the bottom of the list are two buttons: "Submit" and "Cancel".





Mail Templates Editor (Selection of Template)

https://volcanus.switch.ch/vash/admin/mailSelect.do

gLite

ADMINISTRATOR

- Welcome
- New VASH Candidates
- Manage VASH Users
- Edit Mail Templates
- Manage Curator Dates
- Manage Attributes
- Admin FAQ
- Viewer Portal

Copyright EGEE
Software Licence
Version: 0.9

Mail Templates

A user may receive mails from the VASH service at different occasions. The most evident mails are those triggered by the administrator, which are:

- mail when a user gets deleted from the VASH (and possibly VOMS) - ("*removed*" template)
- mail when a user is granted access to the VASH service - ("*enabled*" template)
- mail when a user who was enabled gets disabled - ("*disabled*" template)
- mail sent by the administrator without a particular action - ("*general*" template)

There is also one type of mail that is sent by VASH automatically, when the VASH records of a user are about to expire - ("*notification*" template).

Please select the mail template you would like to edit.

"removed" template

Granting Access to new VASH Users

<https://volcanus.switch.ch/vash/admin/candidates.do>

Granting Access to new VASH Users

The table below lists the users that accessed the VASH service but are not (yet) permitted to push their Shibboleth attributes to VOMS.

The administrator is supposed to verify whether the user identity (e.g. Given Name) and the certificate the user used to access VASH are a plausible match. If so he may grant the user full access. If they do not match, the administrator ought to delete the entry.

The notification of a user is always put in the context of the action the administrator is applying on the particular user. That is, a user that gets "enabled" will be notified by an email telling the user got enabled, and a user that got deleted will get notified by an email telling that access got denied.

The mails that are sent to the user can be customized under [Edit Mail Templates](#) menu.

Given Name	Surname	Shibboleth Id	DN	CA	Email	Last modified	Enabled	Notify	Delete
Demouser	SWITCHHaai	773443@aaitest.switch.ch	/O=GRID-FR/C=CH/O=SWITCH/OU=MIDDLEWARE/CN=Placi Flury	/C=FR/O=CNRS/CN=GRID-FR	flury@switch.ch	2007-01-04 10:44:05.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Demouser	SWITCHHaai	773443@aaitest.switch.ch	/CN=Placi Flury/C=CH/O=Switch/Email=flury@switch.ch	/CN=Ubizen OnlineGuardian Customer CA/C=BE/O=Ubizen nv/OU=Ubizen OnlineGuardian	flury@switch.ch	2007-03-06 15:54:46.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Submit Cancel

- LCAS plug-in written; currently testing it
- ACL xml file
- todo: documentation

Example:

```

<AccessControlList>
  <AccessControlRule>
    <Attribute name="eduPersonAffiliation">bigBoss</Attribute>
  </AccessControlRule>
  <AccessControlRule>
    <Attribute name="swissEduPersonStudyLevel"> master studies</Attribute>
  </AccessControlRule>
  <AccessControlRule>
    <Attribute name="swissEduPersonHomeOrganization">unizh.ch</Attribute>
    <Attribute name="eduPersonAffiliation">staff</Attribute>
  </AccessControlRule>
</AccessControlList>
  
```

- **Software implementation done,**
 - integration of 'existing' SLCS admin features to be done
 - improve look'n'feel (strutifying viewer servlet)
- **finish testing**
- **finish documentation**
- **ETICS**
- **MJRA1.5 document:**
<https://edms.cern.ch/document/807849/1>

Questions?

swissEduPersonUniqueID: 12343@flury.switch.ch

Surname: Flury

givenName: Placi

E-mail: flury@switch.ch

swissEduPersonGender: male

swissEduPersonHomeOrganization: ethz.ch

telephoneNumber: 012 345 67 89

swissEduPersonStudyBranch1: electrical
engineering

eduPersonAffiliation: student

swissEduPersonStudyLevel: master studies

- **Need common understanding of attributes**
 - given within a federation
 - but inter-federation access (?)
- In Grid, interpretation of attribute meaning still open issue. Experience in Shibboleth may promote a consens.

swissEduPersonHomeOrganization: ethz.ch

swissEduPersonStudyBranch1: electrical engineering

eduPersonAffiliation: student

swissEduPersonStudyLevel: master studies