VOMS Attributes from Shibboleth (VASH)

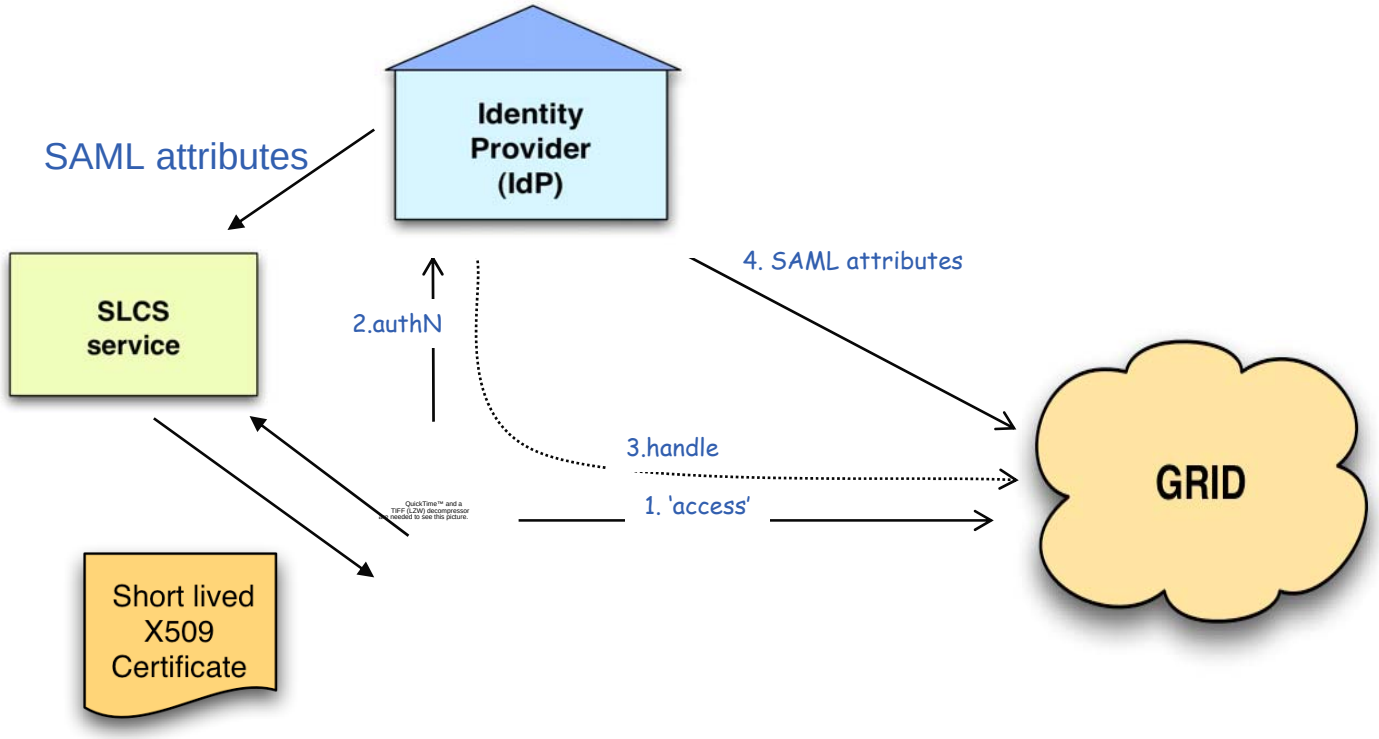
JRA1 All-Hands meeting Catania 8 March 2007

Motivation

- **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’**

Grid, yet another Shib resource?

Phase 1: SLCS service



SLCS Service (Status)

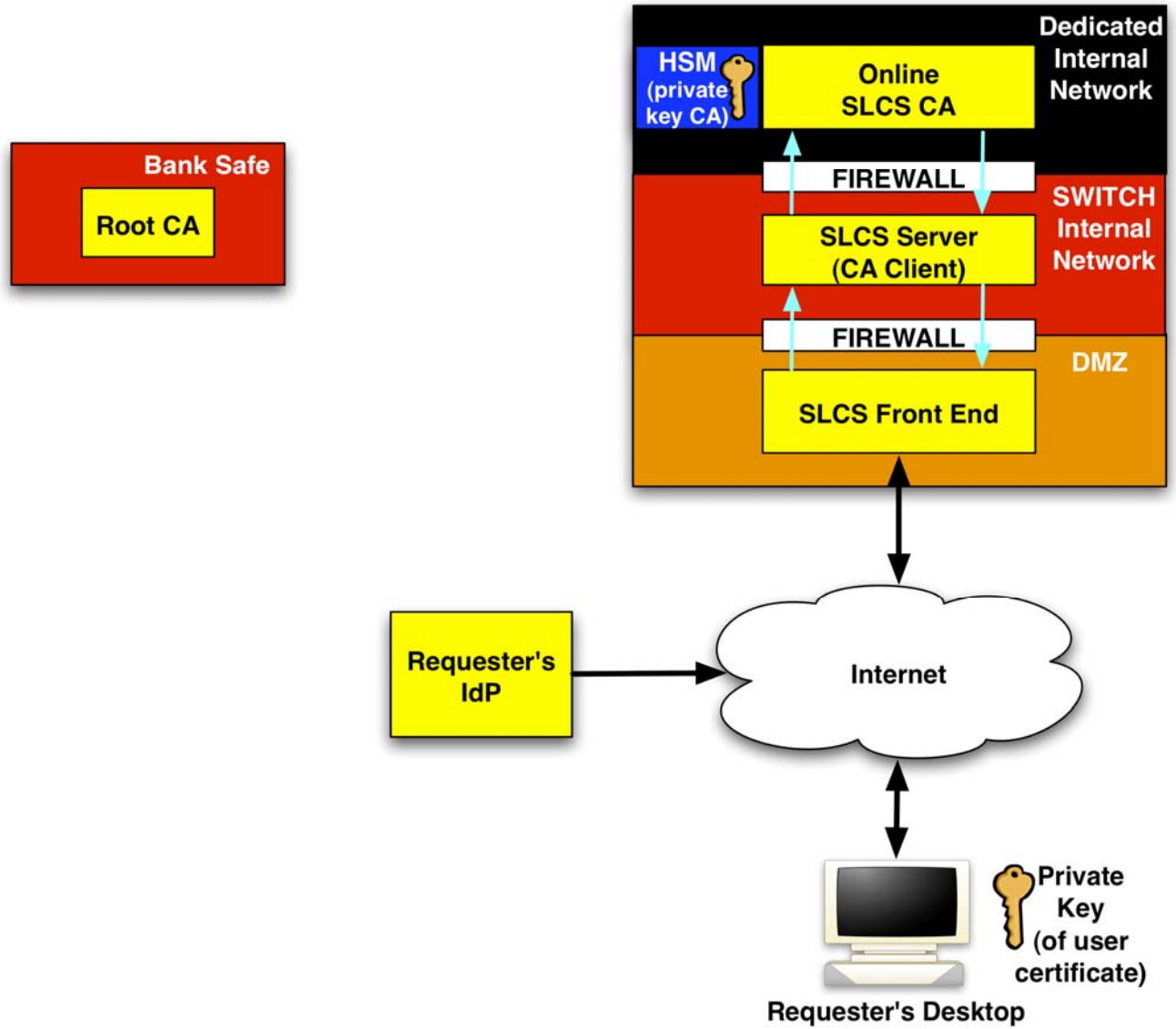
- **Presented in Abingdon**
- **CP/CPS accredited**
  - Accredited by EuGridPMA
  - http://www.switch.ch/pki/grid
- **Operation of SLCS TEST CA in test-bed since November**
  - http://www.switch.ch/pki/grid/test
- **Production infrastructure ready (Online CA, HSM)**
- **Admin interface finished**
  - User management (ACL based activation of users etc.)

- **MJRA1.4 document: https://edms.cern.ch/document/770102/1**

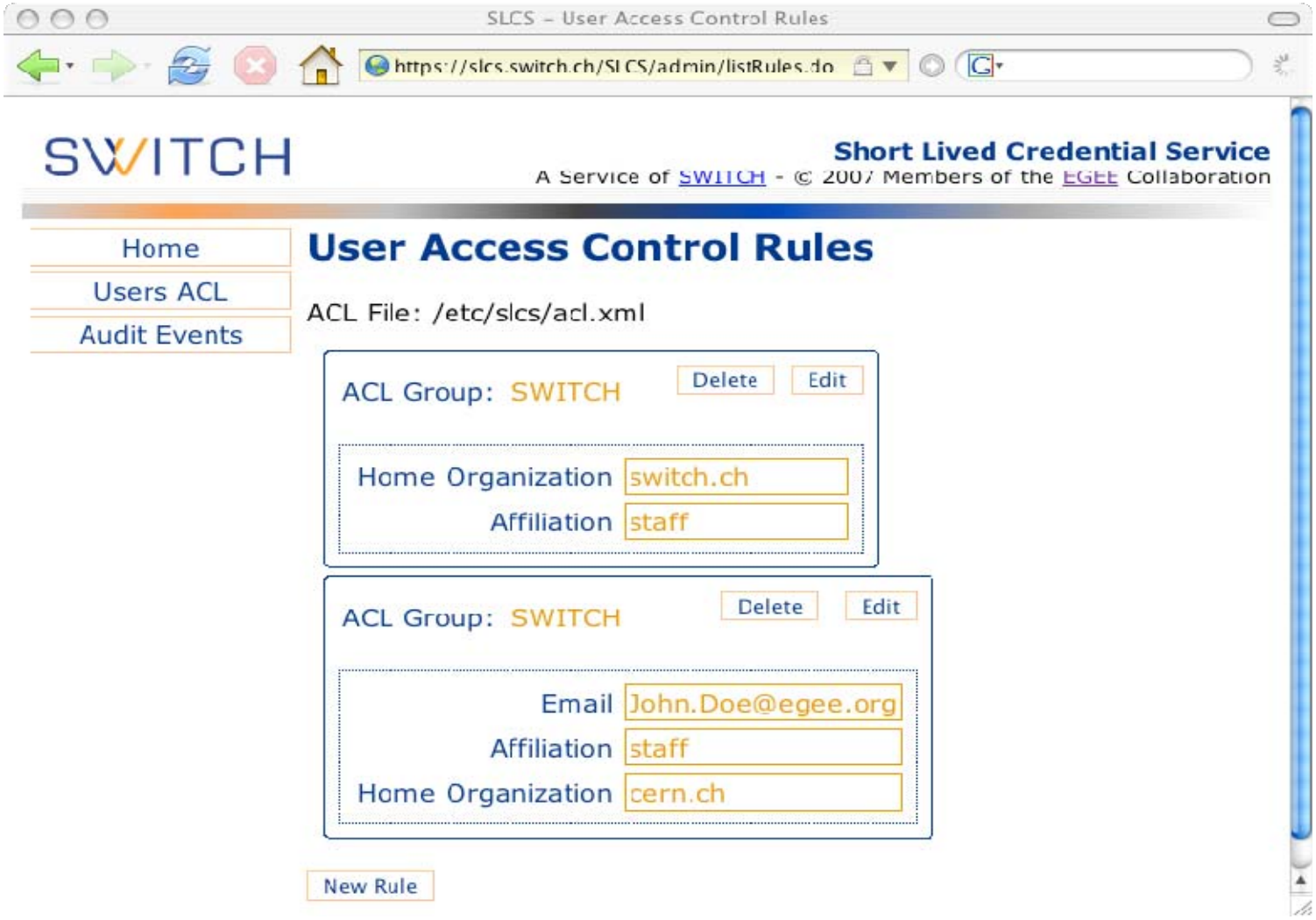
- **Todo's : finish documentation, ETICS integration**

CP/CPS: Certificate Policy and Certification Practice Statement

SWITCHslcs: CA Setup



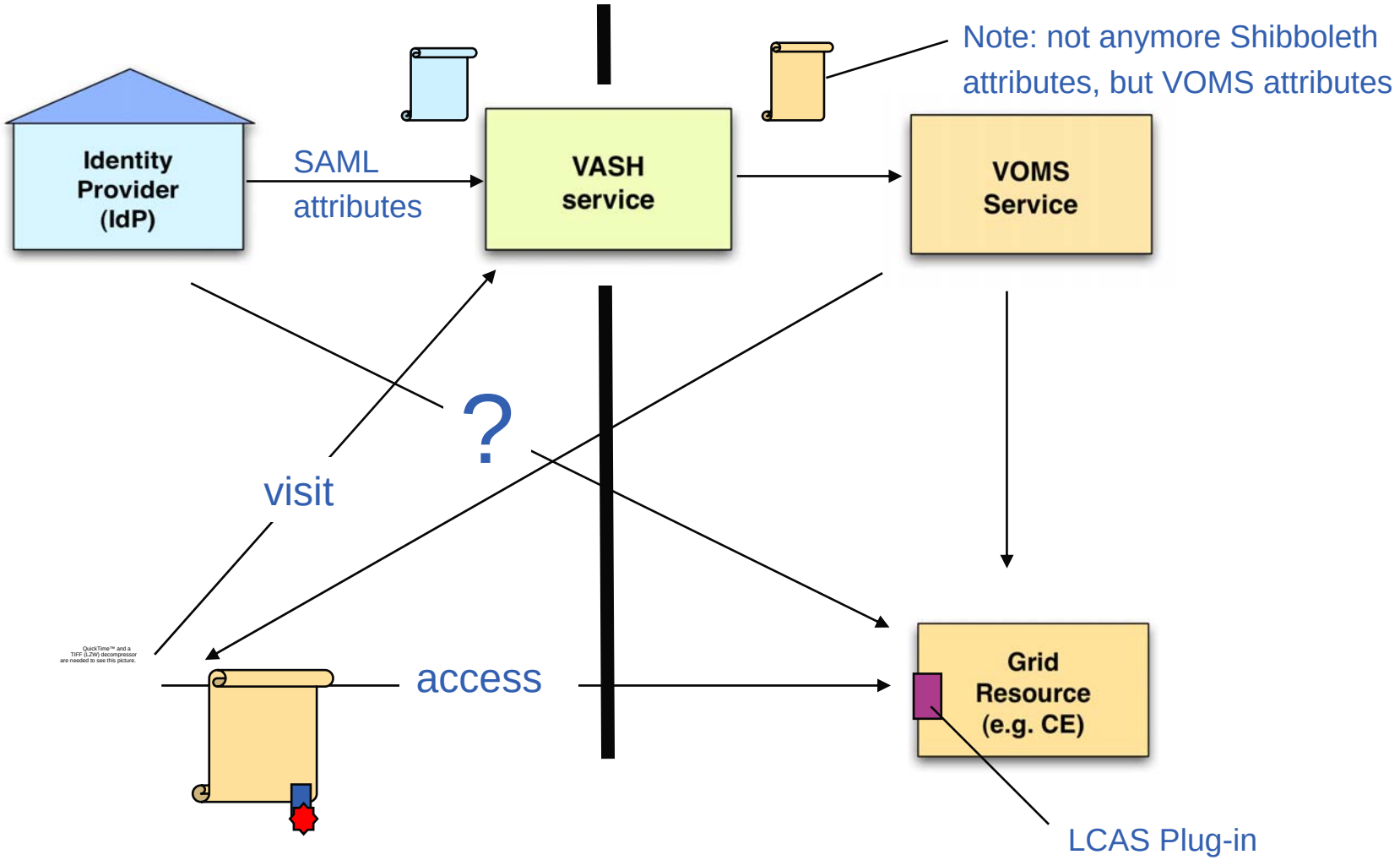
SLCS Admin


SLCS – User Access Control Rules
https://slcs.switch.ch/SLCS/admin/listRules.do
SWITCH
Short Lived Credential Service
A Service of SWITCH - © 2007 Members of the EGEE Collaboration
Home
Users ACL
Audit Events
User Access Control Rules
ACL File: /etc/slcs/acl.xml
ACL Group: SWITCH
Delete
Edit
Home Organization switch.ch
Affiliation staff
ACL Group: SWITCH
Delete
Edit
Email John.Doe@egee.org
Affiliation staff
Home Organization cern.ch
New Rule

Consolidation of authZ info

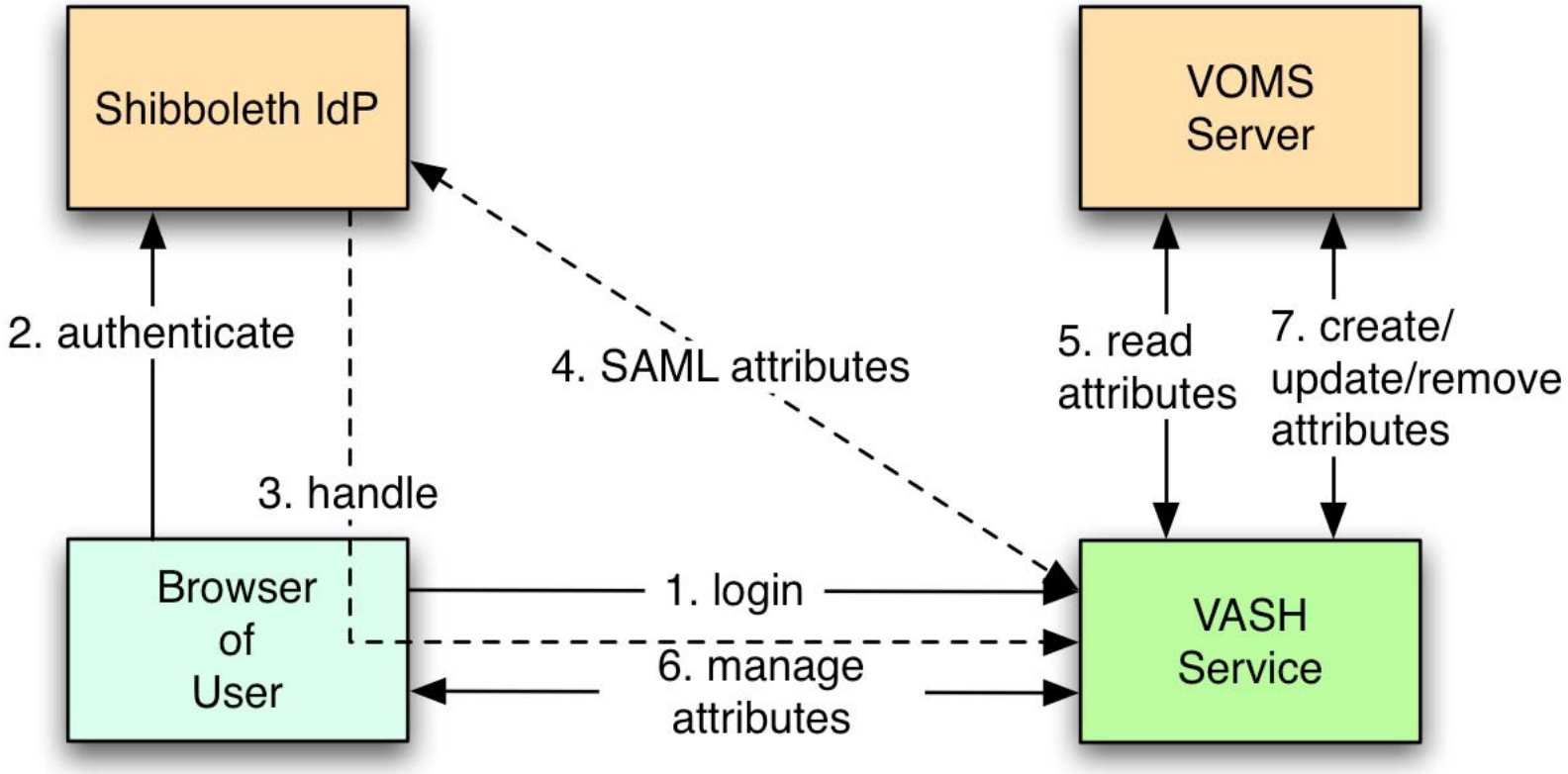
- **Grid: get/use authZ information from authoritative sources outside of the grid-universe**
  - permitting more granular authorization
  - decouple management & maintenance responsibilities
  - common understanding of semantics of authZ info (open issue)
- **Consolidate/integrate authZ information 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

VOMS Attributes from Shibboleth



Scenario. User already registered on VOMS

VASH Service



VASH Key Features

- **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

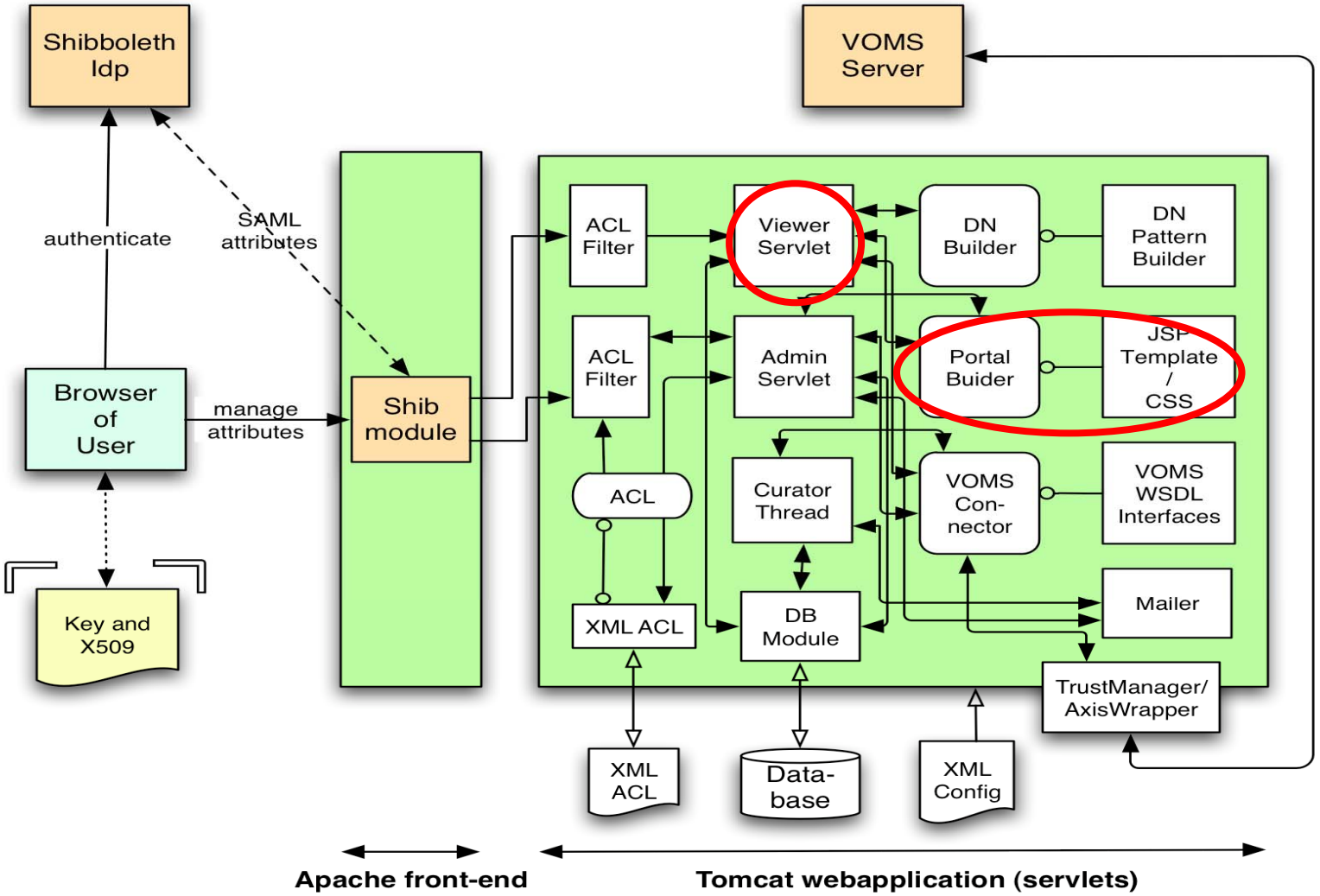
VASH Tasks

- 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)

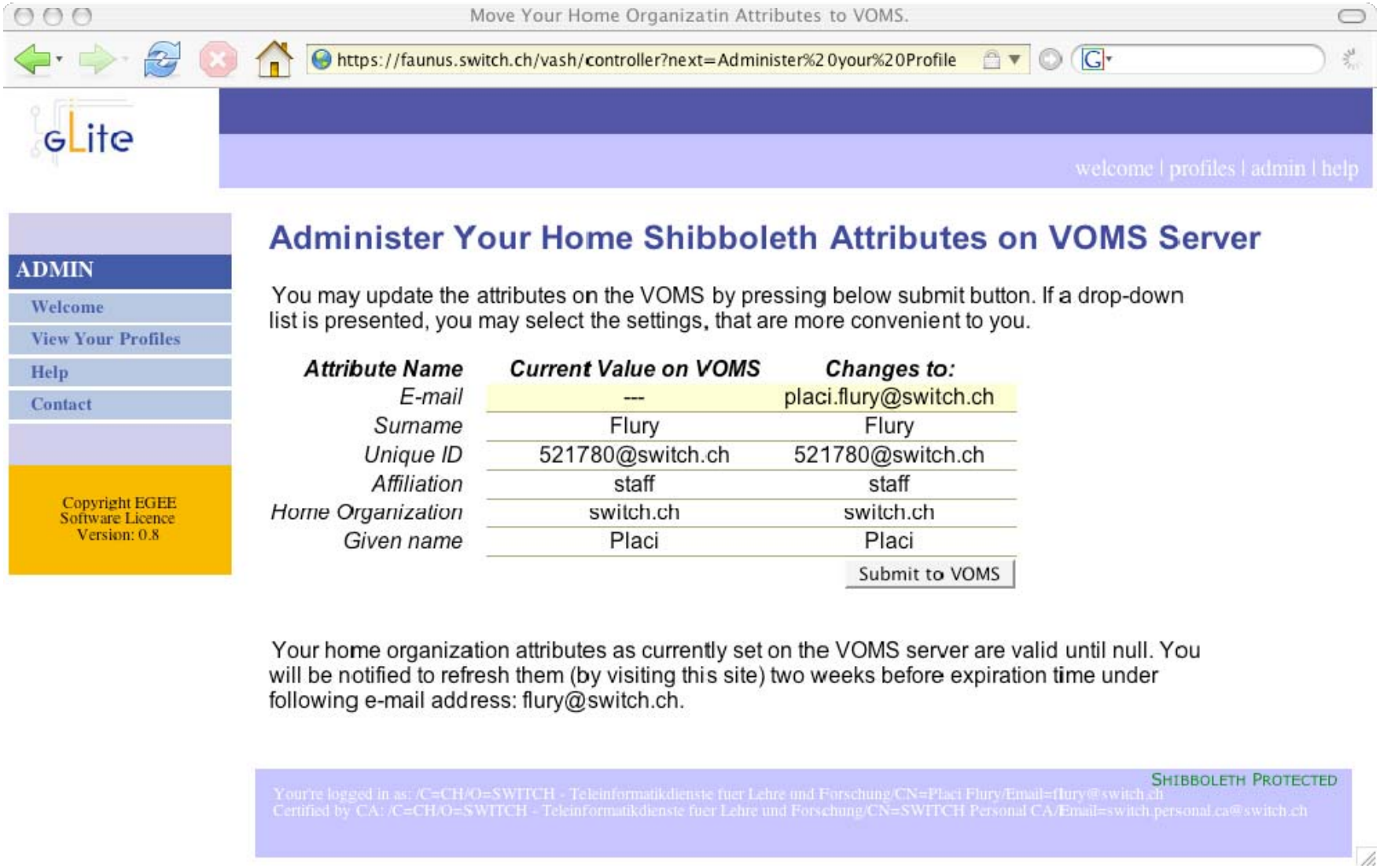
Open:

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

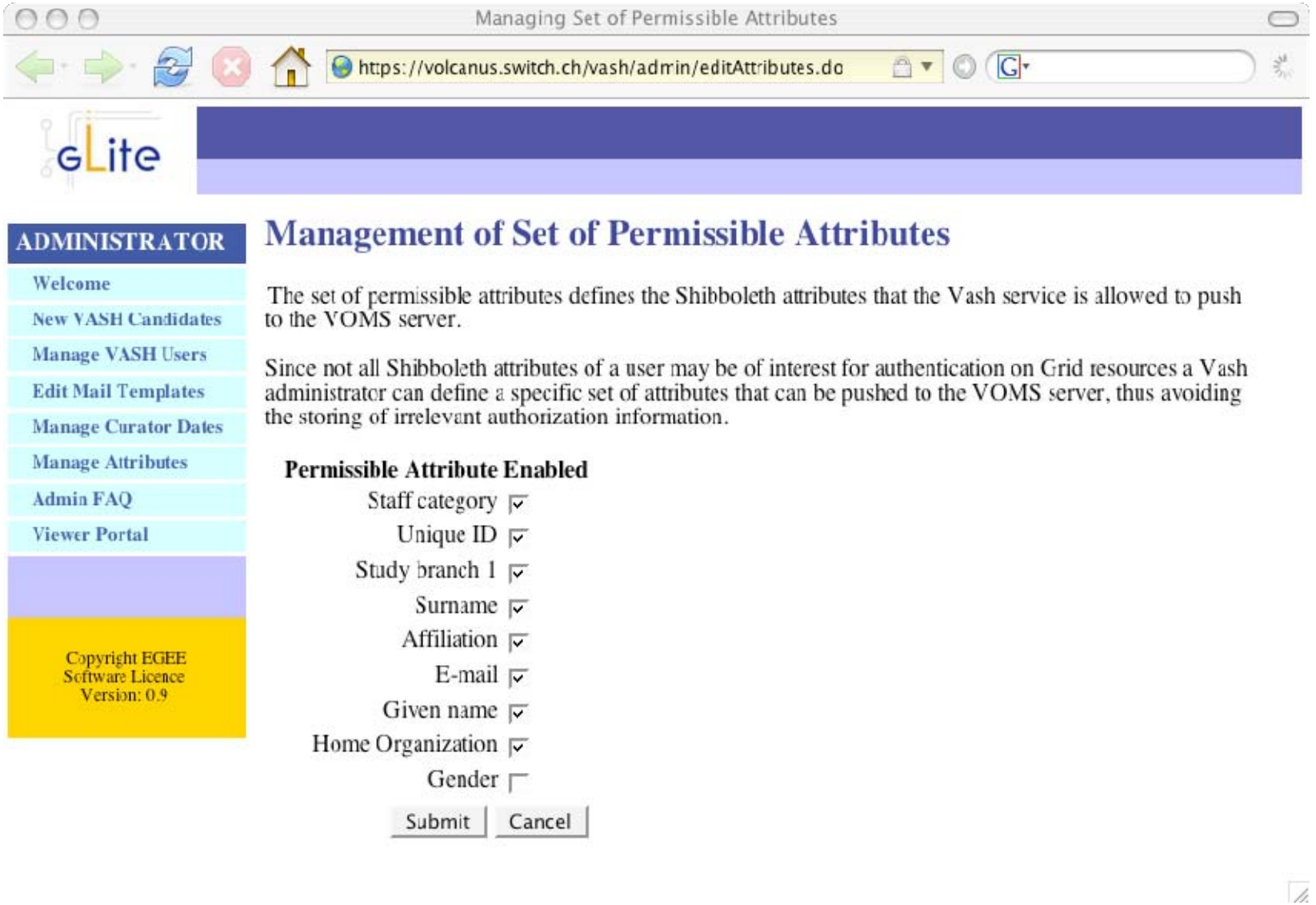
VASH Service Detailed



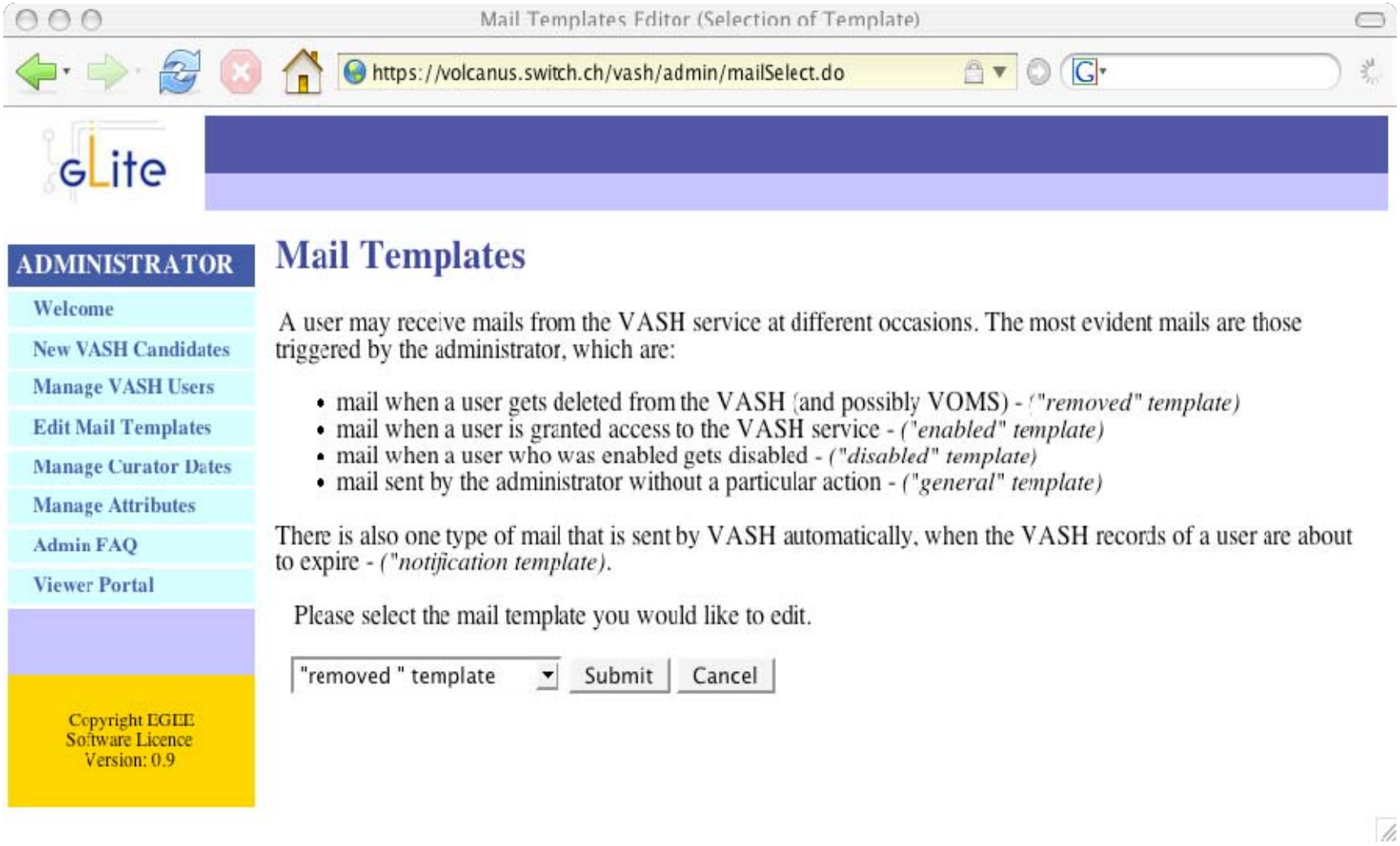
VASH Viewer Servlet



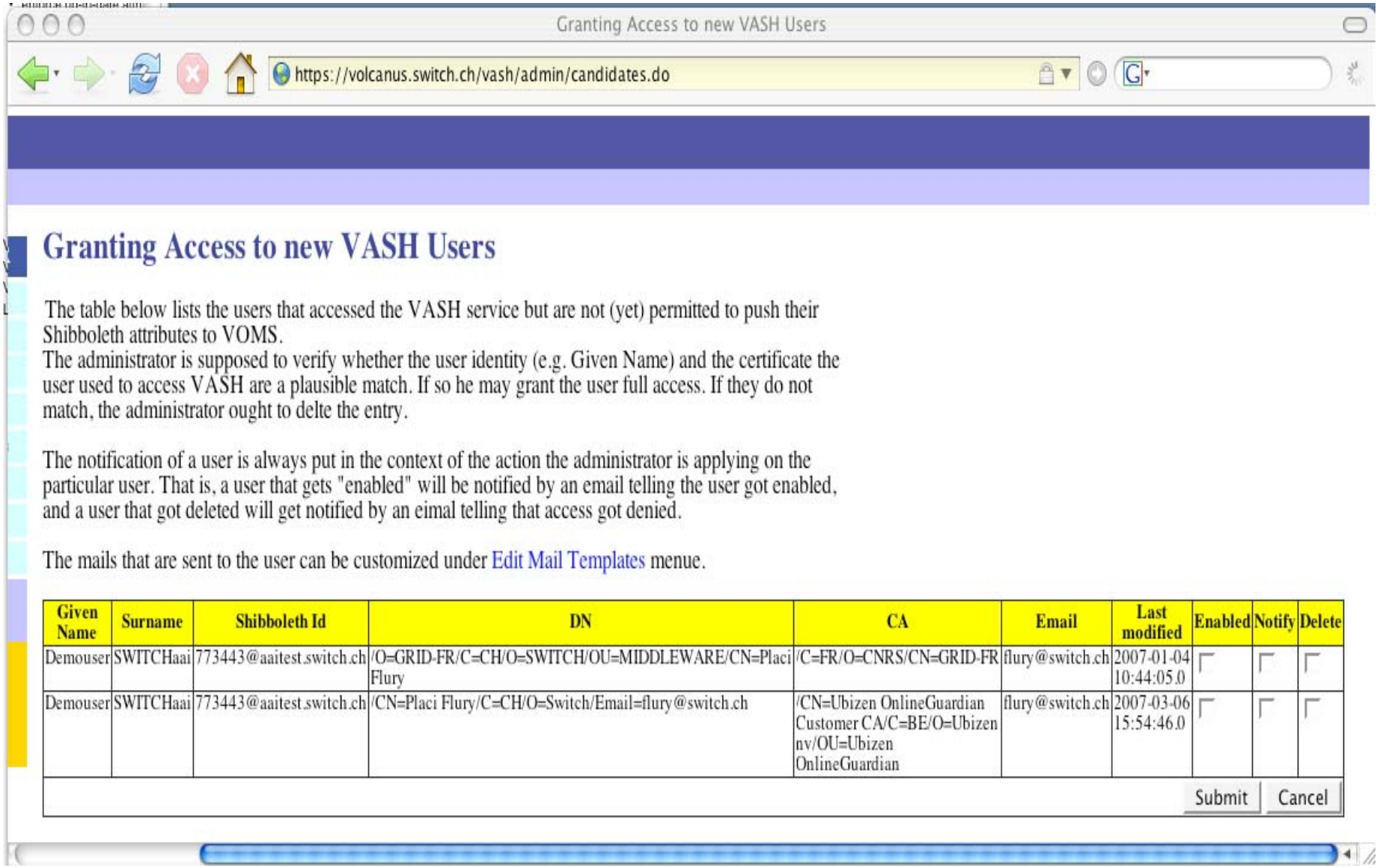
VASH Admin interface(1)



VASH Admin interface(2)



VASH Admin interface(3)



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 delte 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 eimal telling that access got denied.

The mails that are sent to the user can be customized under Edit Mail Templates menue.

Given Name	Surname	Shibboleth Id	DN	CA	Email	Last modified	Enabled	Notify	Delete
Demouser	SWITCHaai	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	☐	☐	☐
Demouser	SWITCHaai	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	☐	☐	☐

Submit Cancel

LCAS Plug-in

- 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>
```

Status

- **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?

Attributes sent to VASH

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

Attributes pushed to VOMS

- **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