SLCS, VASH, and LCAS/LCMAPS Plugins

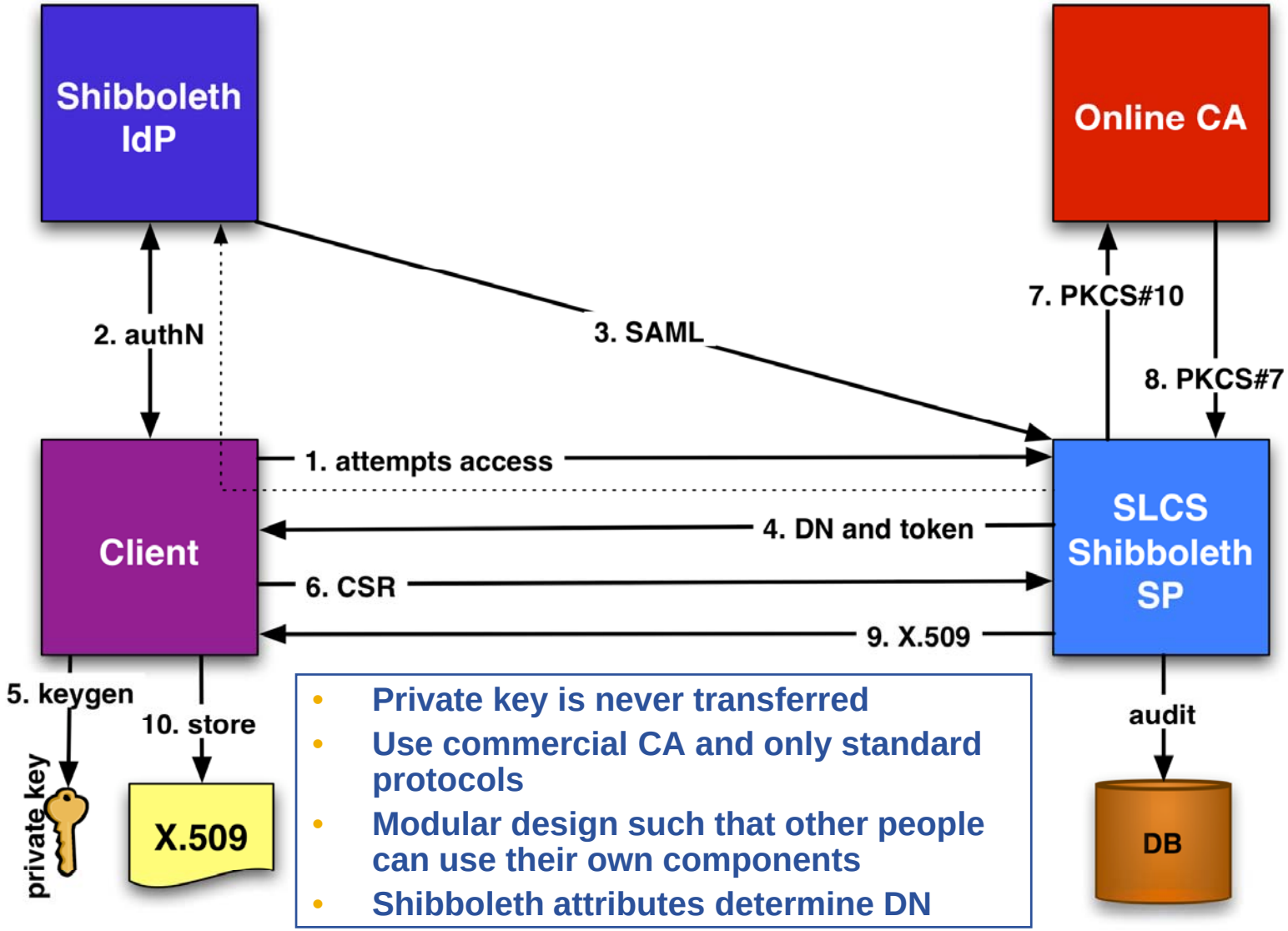
All-Hands Meeting Helsinki **Placi Flury, SWITCH**

19 June 2007

Outline

- **Status**
  - Short-lived credential service (SLCS)
  - VOMS attributes from Shibboleth (VASH)
- **Access for Grid Users to Shib SP(Phase 1b)**
  - from Grid to Shib (and back)
- **AuthZ and AuthZ with Shibboleth Attributes**
  - use case (scenario)
  - a closer look on LCAS and LCMAPS plugins for generic attributes
  - xml-based mapping rules
- **Open Issues & Outlook**
- **Summary**

SLCS Status



- Private key is never transferred
- Use commercial CA and only standard protocols
- Modular design such that other people can use their own components
- Shibboleth attributes determine DN

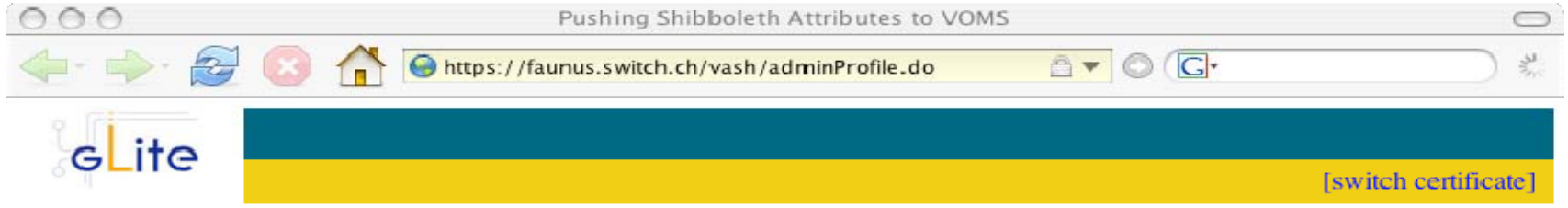
SLCS Status

- **CLI: Possibility to store key&certificate as pkcs12**
  - import in browsers
- **Administrator Interface (web-based)**
  - user management tool
  - ACL editor
  - audit viewer
- **Productive (for SWITCH Federation)**
  - http://www.switch.ch/grid/slcs/documents/webadmin
- **ToDos:**
  - Server documentation
  - ETICS server build
  - yaim, service configuration (?)

VASH Status

- **New feature: SLCS users pre-registration on VOMS**
  - Situation SLCS user not yet registered on VOMS
    1. VASH initiates pre-registration on VOMS
    2. User gets mail with cookie and user registration request number
    3. User visits VASH again to confirm pre-registration
    4. VOMS admin accepts/rejects registration request
- **GUI finished**
- **ToDos:**
  - replace mailing module (currently uses velocity)
  - ETICS build
  - documentation (admin, installation, and user manuals)
  - Shibboleth attribute enforcement

VASH Status



USER INTERFACE

- Welcome
- View Your Profiles
- Administer Your Profile
- Help
- Contact
- Administrator Interface

Copyright EGEE
Software Licence
Version: 0.9

Administer Your 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 most convenient to you.

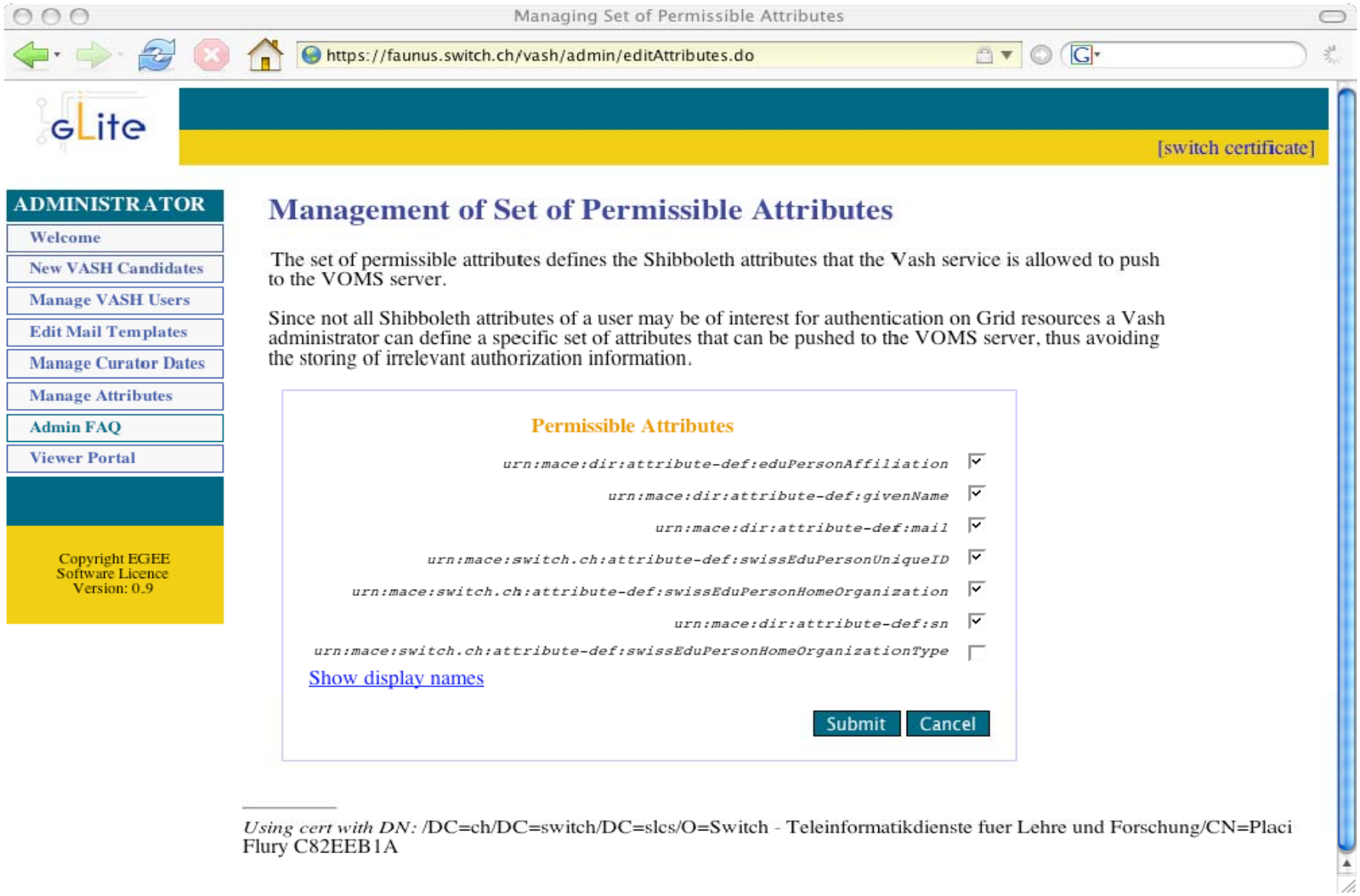
	Value on VOMS	Will Change to
Affiliation	----	staff
Firstname	Placi	Placi
Email	placi.flury@switch.ch	placi.flury@switch.ch
Unique ID	521780@switch.ch	521780@switch.ch
Home Organization	switch.ch	switch.ch
Lastname	Flury	Flury

Submit Cancel

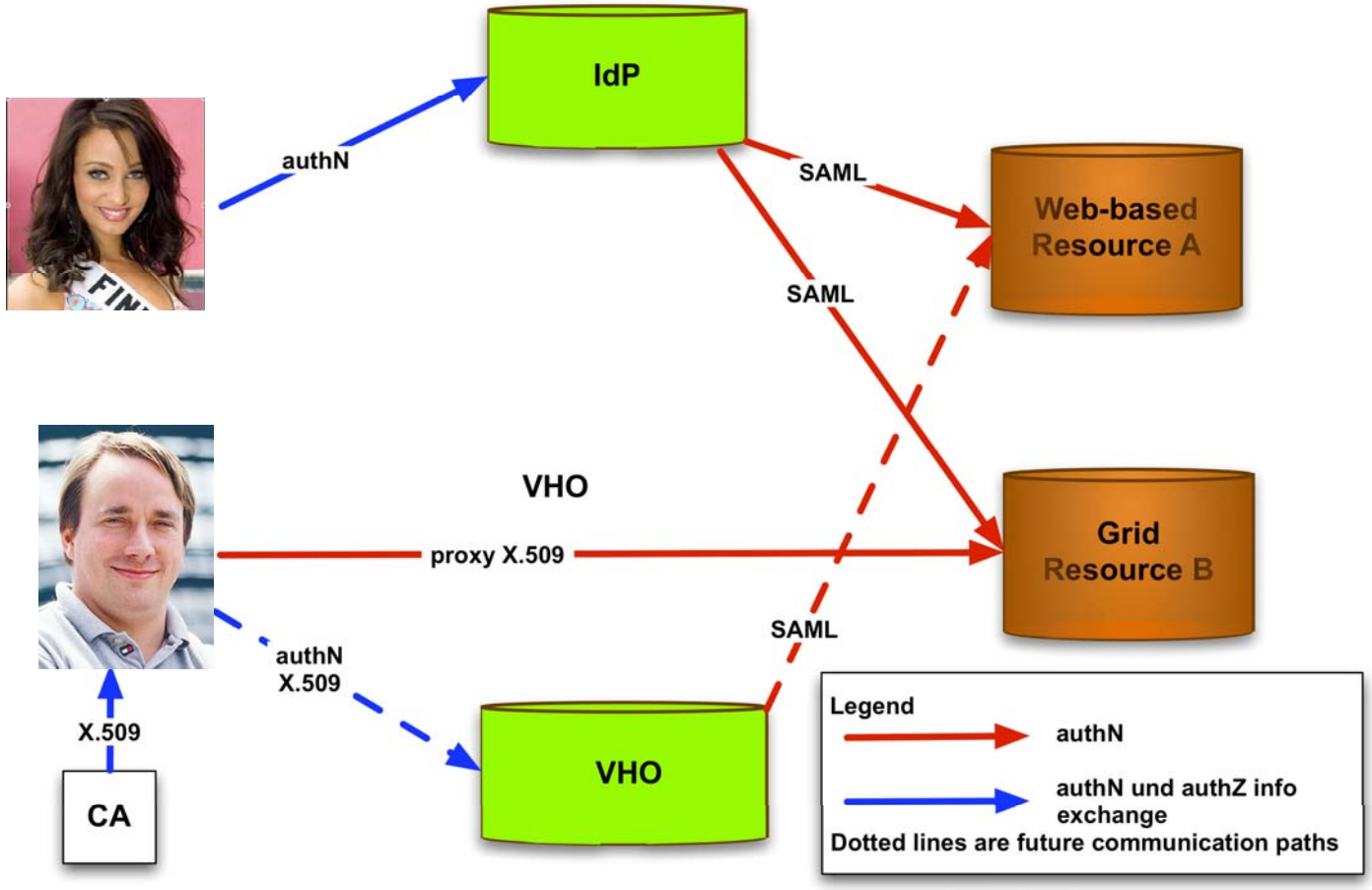
Your home organization attributes as currently set on the VOMS server are valid until *2008/3/15 23:30*. You will be notified to refresh them (by visiting this site) by *2008/1/5 12:30* under following e-mail address *placi.flury@switch.ch*.

Using cert with DN: /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A

VASH Status

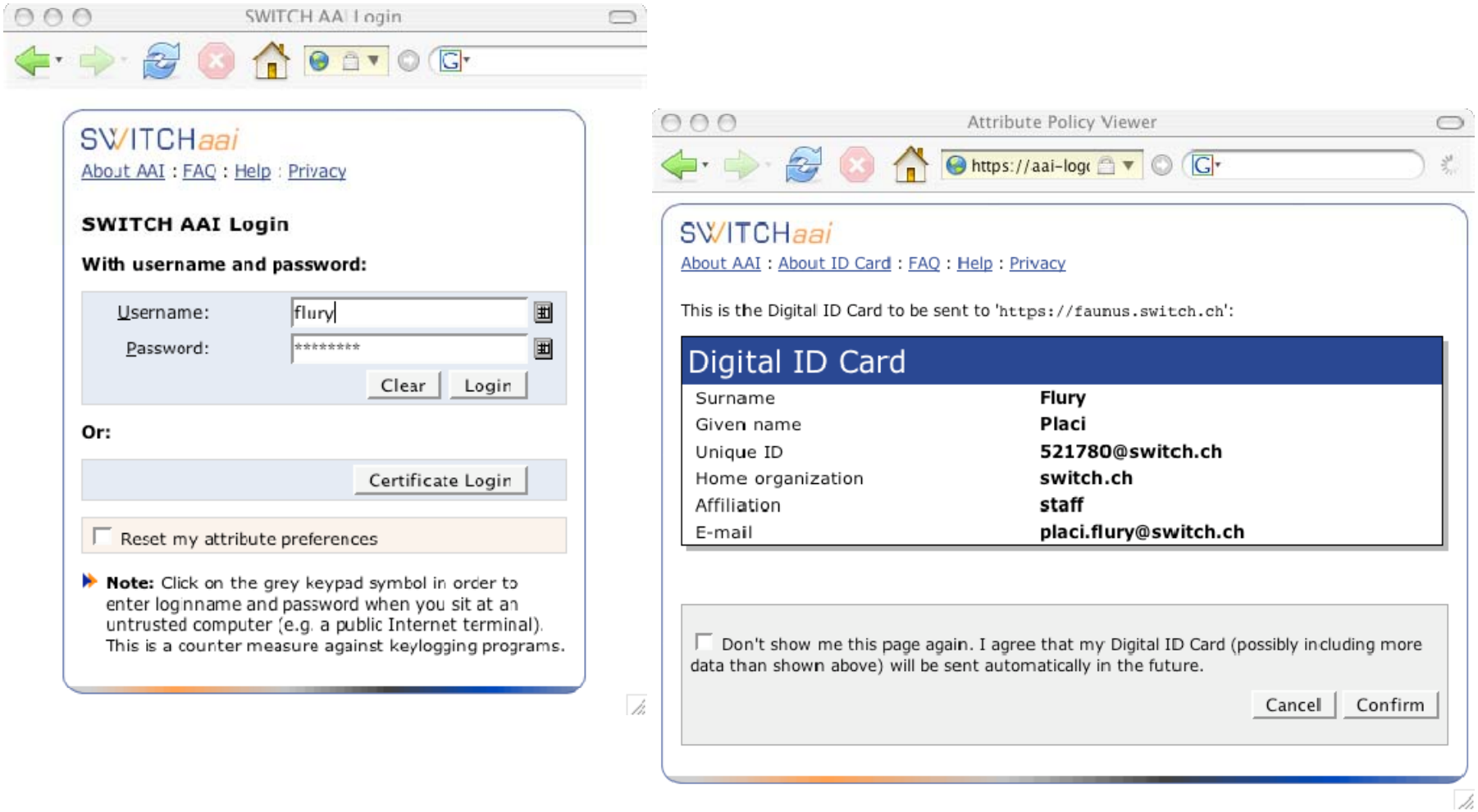

Managing Set of Permissible Attributes
https://faunus.switch.ch/vash/admin/editAttributes.do
gLite
[switch certificate]
ADMINISTRATOR
Welcome
New VASH Candidates
Manage VASH Users
Edit Mail Templates
Manage Curator Dates
Manage Attributes
Admin FAQ
Viewer Portal
Copyright EGEE
Software Licence
Version: 0.9
Management of Set of Permissible Attributes
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 Attributes
urn:mace:dir:attribute-def:eduPersonAffiliation
urn:mace:dir:attribute-def:givenName
urn:mace:dir:attribute-def:mail
urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID
urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization
urn:mace:dir:attribute-def:sn
urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganizationType
Show display names
Submit
Cancel
Using cert with DN: /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A

Access for Grid Users to Shib SP(Phase 1b)



- **Grid users access Shibboleth protected resources**
  - Symmetric access, Applications not affected

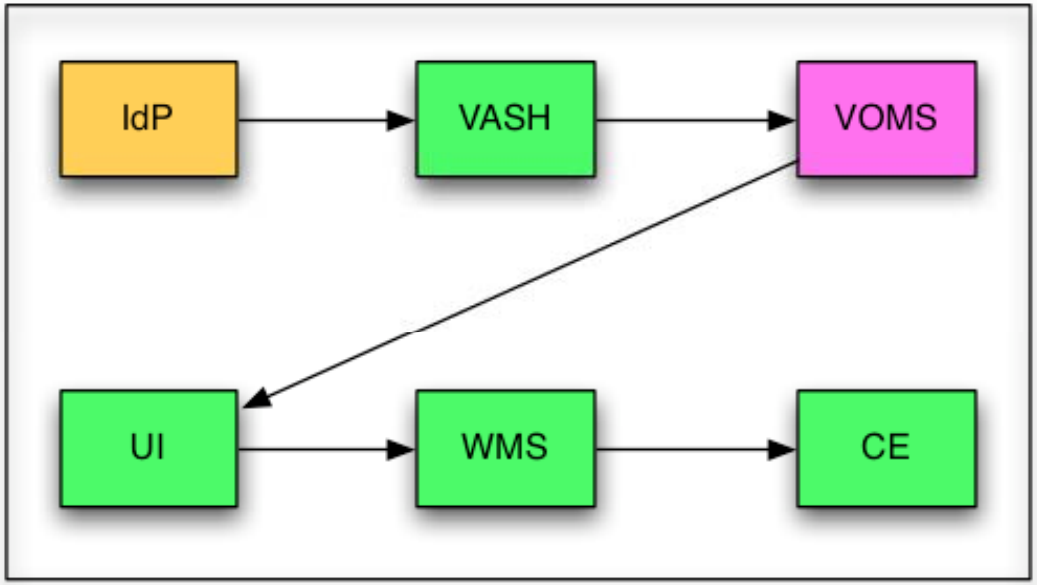
Access for Grid Users to Shib SP(Phase 1b)



Test-bed SWITCH INFN in summer 2007

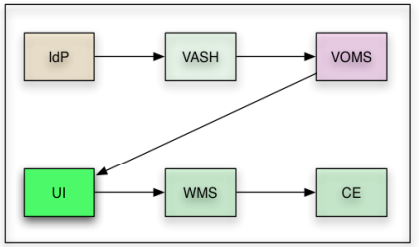
AuthZ and Mapping with Shibboleth Attributes

Scenario: ***A user of VO switch wants to submits a job to the grid. Admission to the CE requires him to be member of the switch.ch home organization. The job shall get assigned to a higher priority queue if the user is a staff member.***



AuthZ and Mapping with Shibboleth Attributes

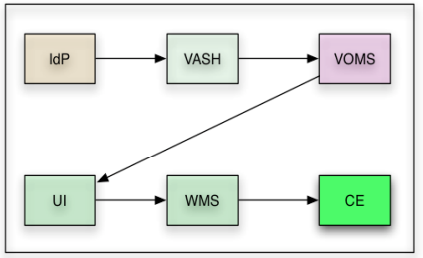
A user of VO switch wants to submits a job to the grid



[flury@aurora flury]$ **slcs-init -i switch.ch**
Shibboleth Password:
New Key Password:
Key password is empty, using Shibboleth password.
[flury@aurora flury]$ **voms-proxy-init -voms switch**
Enter GRID pass phrase:
Your identity: /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
Creating temporary proxy ..... Done
Contacting egeria.switch.ch:15015 [/O=GRID-FR/C=CH/O=SWITCH/OU=MIDDLEWARE/CN=egeria.switch.ch] "switch" Done
Creating proxy ..... Done
Your proxy is valid until Fri Jun 15 05:17:32 2007
[flury@aurora flury]$ **voms-proxy-info -all**
subject : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A/CN=proxy
issuer : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
identity : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
type : proxy
strength : 512 bits
path : /tmp/x509up_u965
timeleft : 11:59:46
=== VO switch extension information ===
VO : switch
subject : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
issuer : /O=GRID-FR/C=CH/O=SWITCH/OU=MIDDLEWARE/CN=egeria.switch.ch
attribute : /switch/Role=NULL/Capability=NULL
attribute : urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID = 521780@switch.ch (switch)
attribute : urn:mace:dir:attribute-def:sn = Flury (switch)
attribute : urn:mace:dir:attribute-def:givenName = Placi (switch)
attribute : urn:mace:dir:attribute-def:mail = placi.flury@switch.ch (switch)
attribute : urn:mace:dir:attribute-def:eduPersonAffiliation = staff (switch)
attribute : urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization = switch.ch (switch)
timeleft : 11:59:46

AuthZ and Mapping with Shibboleth Attributes

Admission to the CE requires him to be member of the switch.ch home organization



- **Authorization**
  - LCAS plugin
  - *org.glite.security.lcas-plugins-voms-attr*
  - *transparent handling of VOMS' generic attributes*
  - *authorization by ACL (xml-file)*
    - *parser for rules: org.glite.security.acl-parser*

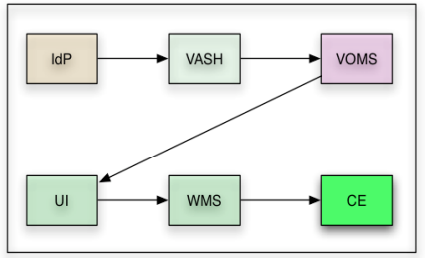
- ACL file:

```
<AccessControlList>
    <AccessControlRule>
        <Attribute name= "urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization"> switch.ch
        </Attribute>
    </AccessControlRule>
</AccessControlList>
```

- Plugin log:

```
LCAS   0: lcas.mod-lcas_run_va(): authorization granted by plugin /opt/glite/lib/modules/lcas_userban.mod
LCAS   0: lcas_voms_attr - is_rule_match(): ACL rule(1) matched
LCAS   0: lcas.mod-lcas_run_va(): authorization granted by plugin /opt/glite/lib/modules/lcas_voms_attr.mod
```

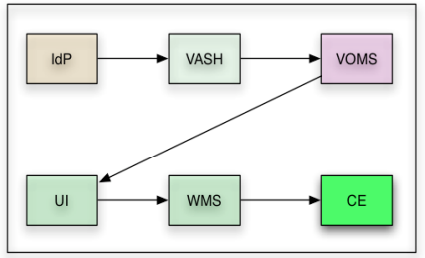
AuthZ and Mapping with Shibboleth Attributes



The job shall get assigned to a higher priority queue if the user is a staff member.

- **Mapping:**
  - LCMAPS plugin
  - *org.glite.security.lcmaps-plugins-voms-attr*
  - *transparent handling of VOMS' generic attributes*
  - *Mapping rules defined in xml-file*
    - *parser for rules: org.glite.security.lcmaps-rules-parser*

AuthZ and Mapping with Shibboleth Attributes

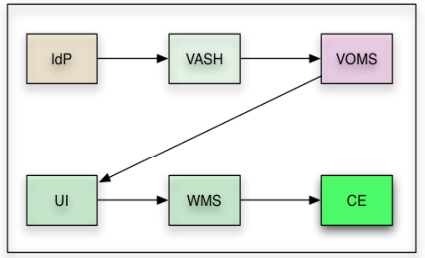


- ***Why XML based mapping rules?***
  - *'limitations' of conventional grid-mapfile:*
    - *Management of grid-mapfile*
    - *FQAN + 2 generic attributes example*

/switch/Role=production/Capability=NULL/urn:mace:dir:attriutedef:eduPersonAffiliation=staff/
urn:mace:switch.ch:attributedef:swissEduPersonHomeOrganization=switch.ch
.switchsgm

- **Discussions with**
  - LCMAPS developers (Oscar, NIKHEF), and site administrators (Maarten, local site admins)

AuthZ and Mapping with Shibboleth Attributes



XML Mapping Rules

- **Syntax and structure defined:**

  rule::= {attribute} [dns] [fqans] map
  attribute ::= attribute_name, attribute_value
  map ::= account, group |
  account | group
  dns ::= {dn}
  fqans ::= {fqan}

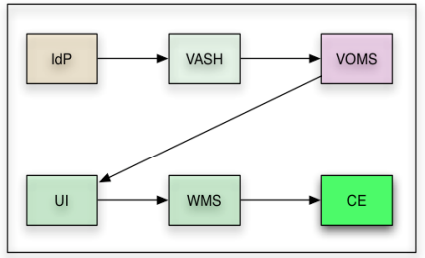
- **Semantic defined by plugin**
  - lcmaps-plugins-voms-attr interprets rule as follows:

    Rule matches if following conditions are met:
    1. All specified attributes must be present in the AC (name and value must match)
    2. If any DNs are specified, the DN in proxy cert must match one of these
    3. If any FQANs are specified, FQAN in proxy cert must match one of these

    (note if no DNs are specified any will match, the same for FQANs)

- **ToDos:**
  - VO info in rule -> attribute::= attribute_name, attribute_value, vo ?
  - wildcard support
  - Longest match first -> sort before doing the match?
  - Deny ‘flag’? (c.f Oscar’s talk)

AuthZ and Mapping with Shibboleth Attributes



Back to the example:
(XML Mapping Rules file)

```
<MappingRules>
      [cut]
      <MappingRule>
           <Attribute name="urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization"
              displayName="home organization">switch.ch</Attribute>
           <Attribute name= "urn:mace:dir:attribute-def:eduPersonAffiliation"
              displayName="Affiliation"> staff </Attribute>
          <FQAN>/switch/Role=NULL/Capability=NULL </FQAN>
           <Map account=".switch" group="switchprio"/>
       </MappingRule>
</MappingRules>
```

Plugin log :

```
LCMAPS 0: lcmaps.mod-runPlugin(): running plugin /opt/glite/lib/modules/lcmaps_voms_attr.mod
LCMAPS 0: lcmaps_voms_attr - get_mapping(): mapping  rule(2) matched
            [cut]
LCMAPS 0: lcmaps_voms_attr - plugin_run: lcmaps_voms_attr plugin succeeded
LCMAPS 0: lcmaps.mod-runPlugin(): found plugin /opt/glite/lib/modules/lcmaps_posix_enf.mod
LCMAPS 0: lcmaps.mod-runPlugin(): running plugin /opt/glite/lib/modules/lcmaps_posix_enf.mod
LCMAPS 6: lcmaps_plugin_posix_enf-log_cred():  uid=18911(switch001):pgid=45005(switchprio):sgid=2689(switch)
LCMAPS 0:   lcmaps_plugin_posix_enf-plugin_run(): posix_enf plugin succeeded
```

Open Issues & Outlook

- **SLCS/VASH**
  - etics build
  - docu, better enforcement of validity of generic attributes from Shibs on VOMS (moment global expiration time).
- **LCAS/LCMAPS plugins:**
  - extend LCMAPS framework
  - VO support in rules, etc.
  - input/comments on xml-format for ACL and XML mapping rules?
- **Phase 3 (enable SAML support for selected Grid resources)**
  - Still in design phase

Summary

- **Summary:**
  - **Development of SLCS and VASH completed. SLCS already productive. Documentation pending.**
  - **Phase 1.b, Symmetric access from Shibboleth resources by grid users needs to be implemented (SWITCH - INFN)**
  - **The LCAS/LCMAPS plugins for the generic VOMS attributes filled the missing gap to use Shibboleth for authZ and mapping of grid jobs.**

This is the end…

Thank’s a lot for your attention. Q?