SWITCHslcs & VASH

Thomas Lenggenhager, SWITCH
presenting work done by SWITCHgrid team
Outline

Bringing Shibboleth & gLite together
work of SWITCHgrid team is part of EGEE-II

• Phase 1
  • Short-lived credential service ➔ SLCS

• Phase 2
  • VOMS Attributes from Shibboleth ➔ VASH
Key Concepts

• Focus
  • Interoperability, **NO** replacement for X.509
  • Specific for EGEE-2 infrastructure (VOMS etc)
  • Integrate, re-use, re-engineer existing code
    write new code only as needed

• Key Concepts
  • Identity provider is the home institution of the user
  • Home institution provides some attributes
  • Grid-VO is needed for grid specific attributes
Overview Phase 1 and 2

Shibboleth IdP

Phase 1: Shibboleth enabled SLCS

Phase 2: Attribute transfer into VOMS

SLCS

short lived
X.509

voms_proxy_init (DN)

pX.509
w/ VOMS attributes

pX.509
delegates

CE, SE

authZ

authN

submits jobs

MyProxy

VOMS

Config Files
gridmapfiles
blacklist
File System ACL
LCAS
LCMAPS
Design Decisions

- SLCS CA and “VOMS SP” should be independent of each other
  - Separate Service Providers
  - Deployed independently

- SLCS CA should be independent of the Grid middleware

- VOMS SP should only be dependent on VOMS
### SLCS Profile

- **SLCS**: short-lived credential service  
- **IGTF** profile

### Minimum requirements

<table>
<thead>
<tr>
<th>Identity Checking</th>
<th>SLCS</th>
<th>X.509 Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate generated based on Identity Management system</td>
<td>«traditional» RA (e.g. passport)</td>
<td></td>
</tr>
<tr>
<td>Lifetime</td>
<td>&lt; 1 mio sec (ca. 11 days)</td>
<td>&lt; 1 year + 1 month</td>
</tr>
<tr>
<td>Revocation Handling</td>
<td>optional</td>
<td>mandatory</td>
</tr>
</tbody>
</table>
SWITCHsIcs: Operation

- For the user
  - from the command line: invisible
  - part of gLite UI (3.1) (can be installed independently)

- For the RA from web-based admin tool
  - Can enable or disable individual users (only for his institution)
  - Requirements formulated in CP/CPS
  - Can obtain log information

- SWITCH
  - Operates the service
  - Strict access control
  - Operate also a second test CA
SWITCHslcs

- Private key is never transferred
- Use commercial CA and only standard protocols
- Modular design that others can reuse components
- Shibboleth attributes determine DN
SWITCHslcs: CA Setup

Bank Safe

Root CA

Online SLCS CA

Dedicated Internal Network

HSM (private key CA)

FIREWALL

SLCS Server (CA Client)

FIREWALL

SLCS Front End

DMZ

Requester's IdP

Internet

Private Key (of user certificate)

Requester's Desktop
VASH: The Idea

• Phase 1 ties
  • AAI authentication to issue an X.509 certificate
  • AAI attributes are used to construct the DN

• Phase 2 intends to make AAI attributes available to grid resources for authorization decisions
  • Which AAI attributes are of interest to grid resource?
  • How does resource obtain attributes? (pull vs push)
  • Relation to VO attributes
  • Deployment issues
VASH Design

VASH

• VOMS Attributes from Shibboleth

• VASH Server
  • Browser-based Shibboleth SP
  • One per Federation and per VO

• «lightweight» SP
  • No administrator duties
  • No management of attributes
  • Simply transfers attributes to VOMS upon user request
VASH Design (2)

• VOMS Attribute Certificates unchanged

• No change in VOMS
  • Needs version 1.7.10 or newer

• VO registration unchanged

• Administrative domains decoupled Shibboleth federation and VOMS

• User links DN in VOMS with a Shibboleth unique identifier
Summary Phase 1 & 2

- **gLite**
- **proxy X.509 w/ AC**
- **X.509**
- **VOMS**
- **SP1: SLCS**
- **SP2: VASH**
- **IdP**
  (provides authN and authZ attributes)
References

• SLCS
  • EGEE MJRA1.4 document
    • https://edms.cern.ch/document/770102/1
  • CP/CPS
    • Accredited by EuGridPMA
      • http://www.switch.ch/pki/grid

• VASH
  • EGEE MJRA1.5 document
    • https://edms.cern.ch/document/807849/1

• Further Information
  • http://www.switch.ch/grid