Interoperability
Shibboleth - gLite

Christoph Witzig, SWITCH
GGF 18, Washington, Sep 11, 2006
• SWITCH built up and operates now SWITCHaai - a national Shibboleth-based AAI

• AAI efforts started in 2002, since last summer in production mode

• Current Status:
  – Approx. 160’000 members of the Swiss higher education sector have AAI-enabled accounts
  – Approx. 12’000 use SWITCHaai on a regular basis

• Among other things SWITCH also operates SWITCHpki
• SWITCH work on interoperability of Shibboleth and gLite is part of EGEE-2 proposal (by SWITCH in EGEE NREN Federation)

• Focus is on
  – 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:
  – Home institution of the user should be the Identity Provider
  – Home institution provides some attributes
  – But VO is needed for (grid specific) attributes
Work plan

• Work started in April 2006 and lasts for 2 years

• Our plan consists of three phases
  – Two initial, shorter phases with the goal
    ▪ Start small and hook up Shibboleth AAI to a gLite grid with minimum amount of changes (in particular no change at the CE)
    ▪ Build up knowledge and expertise
    ▪ April 06 --> fall/winter
  – A longer third phase
    ▪ SAML support at the resource end
    ▪ Design during phase 1 and 2
    ▪ Implementation in 2007
Overview Phase 1 and 2

Enabling Grids for E-sciencE

Phase 1: Shibboleth enabled SLCS

Phase 2: Attribute transfer into VOMS

SLCS

short lived X.509

Shibboleth IdP

VOMS

MyProxy

pX.509

CE, SE

degrees

Config Files
gridmapfiles
blacklist
File System ACL
LCAS
LCMAPS

authZ

authN

submits jobs

pX.509 w/ VOMS attributes

oms_proxy_init (DN)

EGEE-II INFSO-RI-031688
gLiteShib: GGF 18, Sep 11, 2006
• SLCS = Short-lived Credential Service: IGTF profile

• Minimum requirements:

<table>
<thead>
<tr>
<th>SLCS</th>
<th>Traditional user certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automated generation based on user management system</td>
<td>“Traditional” RA (e.g. copy of passport)</td>
</tr>
<tr>
<td>Lifetime &lt; 1mio sec</td>
<td>Lifetime &lt; 1year + 1month</td>
</tr>
<tr>
<td>Revocation handling optional</td>
<td>Revocation handling mandatory</td>
</tr>
</tbody>
</table>
Phase 1: SLCS (2)

• Design goals:
  – Private key is never transferred
  – Use commercial CA and only standard protocols
  – Modular design such that other people can use components
Phase 1: SLCS (3)

Online SLCS CA

Private key >= 2048 bits
HSM optional
Validity < 20 years
No CRL

Online CA Client

SLCS Server
Tomcat

DB

Internal network

2. PKCS#10
3. PKCS#7

Protocol?

SLCS Front End
Apache + Shibboleth SP

DMZ

1. CSR
4. Certificate

1. CSR
Phase 2: Attribute Exchange with VOMS

- **Goal:** Put a subset of Shib attributes into VOMS, such that they automatically appear in the VOMS extension and can be evaluated at the CE.

- **VO specific Shibboleth SP,** where an authorized user can log on and approve the release of his attributes to VOMS.

- **Two modes can be envisaged:**
  - “automatic”: once enabled, the attributes are sync-ed in regular time intervals.
  - “on demand”: user only releases the attributes for a given amount of time and then they are removed from VOMS (unless renewed after email reminder).

- **Which attributes are being transferred?**
  - Configurable by SP administrator.
  - Expect small subset of rather general attributes: identity provider, study branch and level, affiliation -> 5 - 10 attributes.

- **Evaluation by plug-in in LCMaps**
Q & A
• Big bullet
  – Smaller Bullet
    ▪ Even smaller
      • Tiny weenie
        o Micro bullet
  – Another Smaller Bullet
• Big bullet with highlights (please use this dark yellow)
  – Smaller bullet with hyperlink or http://egee