



SWITCH

The Swiss Education & Research Network

Integrating Campus Identities with Grid Operations

Chad La Joie
Internet 2 Member Meeting
October 9th, 2007

SWITCHaai - Shibboleth-based AuthN/AuthS Infrastructure

- ~75% of Swiss higher education (160k) AAI-enabled
- 10% use accounts to access ~100 resources

National Grid Efforts

- Nascent SWISS National Grid (SWING)
- Grass roots, disciple, and aspect specific grids
 - Swiss BioGrid (www.swissbiogrid.org)
 - XtremWeb-CH (www.xtremwebch.net)



Enabling Grids for E-science (EGEE)

- International Grid: 240 institutions, 45 countries, 36k CPUs, 30k jobs
- Based on gLite software
- GSI, X.509-based security
- SWITCH joined EGEE in April '06

Short-lived Credential Service (SLCS)

- Service used to create short-lived grid credentials (X.509 certificate)
- Components:
 - CA with Shibboleth SP front-end
 - Client side library that replicates “browser” in Shib SSO profile
- Organization managers can enable/disable their users.
- Certificates become invisible to users
- SWITCH production deployment EUGridPMA accredited

VOMS Attributes from Shibboleth (VASH)

- Service used to make Shibboleth attributes available as VOMS attributes
- Component: Shibboleth protected GUI allows user to push some attributes into VOMS and requires other attributes to be added (e.g. name is required, user may opt to make email available).

Break connection between client-side security token and grid service required security token.

Security Token Service (STS)

- Base on OASIS WS-Trust Standard
- Converts one security token; initial focus:
 - Username/Pass -> SAML
 - SAML -> X.509
- Supports token request, renewal, validity check, destruction
- Capable of collecting attributes from disparate sources like VOMS
- Allows client to transform between tokens it has and tokens it needs for a particular grid service

Phase 1: Client changes SAML from IdP into x.509 cert

- Standards-based
- Hides complexity with cert creation (e.g. proprietary protocols, change of VO solution, collection of attributes from many sources)
- Capable of preserving some security aspects lost in IdP-Proxy model
- Provides a gateway for crossing security domains
- May be configured to maintain tokens on STS, instead of client-side, allowing for client mobility

Phase 2: Introduce SAML into a web/grid service

- Client can forgo transformation into x.509
- Service can use STS to get the cert needed for other services, if necessary

Phase 3: Rinse and Repeat

Progressive introduction of SAML (or other security tokens) where they make sense. Keeps options open.