SWITCH

The Swiss Education & Research Network

# SWITCHslcs
## Access to the Grid with AAI Identities

**Christoph Witzig**

**witzig@switch.ch**

# SWITCHslcs

- Authentication and Authorization on the Grid
- SWITCHslcs
  translating AAI credentials to Grid credentials
- Status of SWITCHslcs

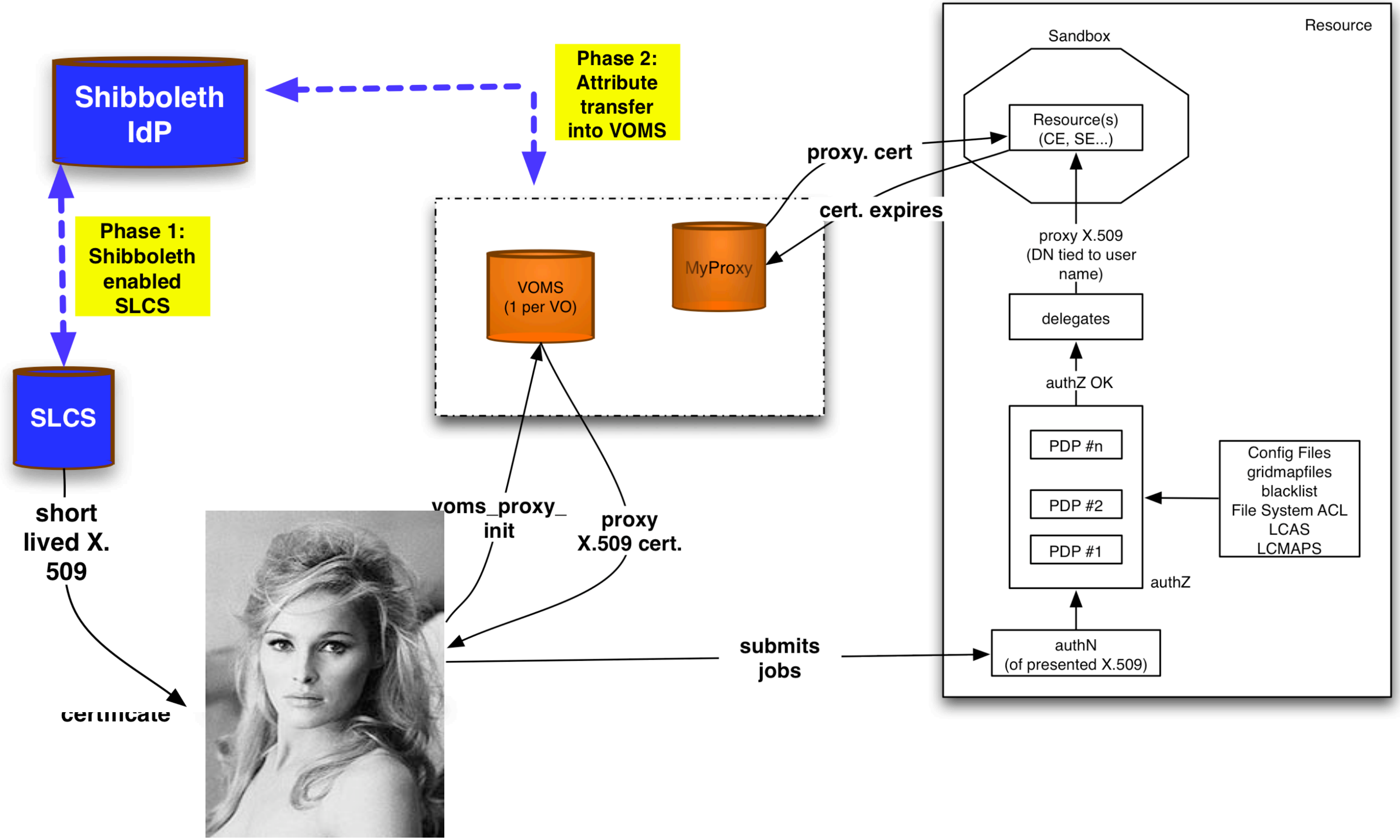
# SWITCH's work in EGEE-II

- EGEE-II: 2nd phase of Enabling Grid's for E-sciencE
  - April 2006 - April 2008
  - SWITCH responsible for "interoperability Shibboleth - gLite"

- Focus is on
  - Interoperability (NO replacement for X.509)
  - Specific for EGEE-2 infrastructure (VOMS etc) but general enough such that it can be extended to other grids

- 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

# AA on the Grid



# SWITCHslcs

- SLCS = short lived credential service
- A Shibboleth SP
  - One per federation
  - Operated by SWITCH
- Issues a X.509 credential to a user upon successful authentication at the IdP
- Short-lived credentials are specifically targeted for use in the grid environment

# SLCS Profile

- SLCS = Short-lived Credential Service: IGTF profile

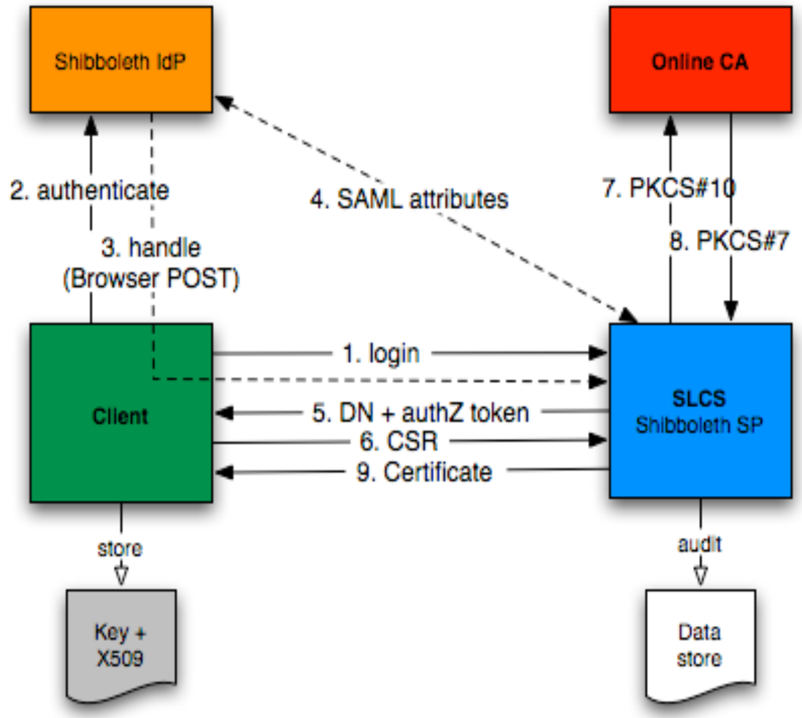
- Minimum requirements:

| SLCS | Traditional user certificates |
|---|---|
| Automated generation based on user management system | “Traditional” RA (e.g. copy of passport) |
| Lifetime < 1mio sec | Lifetime < 1year + 1month |
| Revocation handling optional | Revocation handling mandatory |

# How the SLCS works…

SWITCH
The Swiss Education & Research Network

- **Design goals:**
  - **Private key is never transferred**
  - **Use commercial CA and only standard protocols**
  - **Modular design such that other people can use components**



# SLCS: User’s View

- From the user’s perspective:
  - obtains a short-lived certificates (<11 days) upon execution of a shell command
  - no need to worry about the private key
  - no need to copy private key and certificate to every host he/she uses
  - no need to re-new certificate once it is about to expire
  - free of charge
  - independent of grid middleware

- Prerequisites:
  - User has to have an SWITCHaai account
  - Registration step at his home organization
    - Home org admin enables access through a web interface

- Schedule:
  - Operates in test mode now
  - Home Org administrators and RA operators are being contacted in December/January
  - EUGRIDPMA accreditation in early 2007

# Summary

- SWITCH developed as part of EGEE-II a short lived credential service (SWITCHslcs), which allows SWITCHaai users access to Grid infrastructures

- Service currently operates in a test mode, until it is accredited by the EUGRIDPMA (IGTF)

- Authorization based on SWITCHaai attributes will be added in Q1 2007 by transferring SWICHaai attributes into Grid proxy X.509 certificates through VOMS