Interoperability Shibboleth - gLite

Christoph Witzig, SWITCH
(P.Flury, T.Lenggenhager, V.Tschopp)

EGEE-06, Sep 27, 2006

www.eu-egee.org

Information Society and Media

EGEE and gLite are registered trademarks

Outline

- **Introduction:**
  - SWITCH
  - Shibboleth
- **SWITCHaai: The Swiss Shibboleth-based Federation**
- **Interoperability Shibboleth-gLite**
- **Current Status**

SWITCH

- SWITCH The Swiss Education & Research Network **is the Swiss NREN (new partner in EGEE-II)**
- **Four strategic areas:**
  - Network
  - Domain name registration
  - Netservices
  - Security
    - CERT
    - Middleware
      - *AAI (Shibboleth)*
      - *Mobile*
      - *PKI*
      - *Grid*

Shibboleth

- **AAI = Authentication and Authorization Infrastructure**
- **Developed by internet2**

- **Web-based single sign on (SSO)**
  - When user accesses a resource
    - Authentication takes place at an Identity Provider (independent of the resource)
    - Resource receives Attributes describing the user from the Identity Provider and uses them for the authorization decision
- **SAML: security assertion markup language**

How does it work?

SWITCHaai

- 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 (75%) members of the Swiss higher education sector have AAI-enabled accounts
  - Approx. 10% use SWITCHaai to access about 100 resources on a regular basis

Shibboleth and grids

- SWITCH was an early adopter of Shibboleth, but in the meantime Shibboleth federations are being deployed and operated in many countries
- US, Finland, UK, Australia, Belgium, France as well as others
- Interest to leverage these (national) campus infrastructures against grids
- SAML vs X.509 user certificates

Shibboleth and EGEE-II

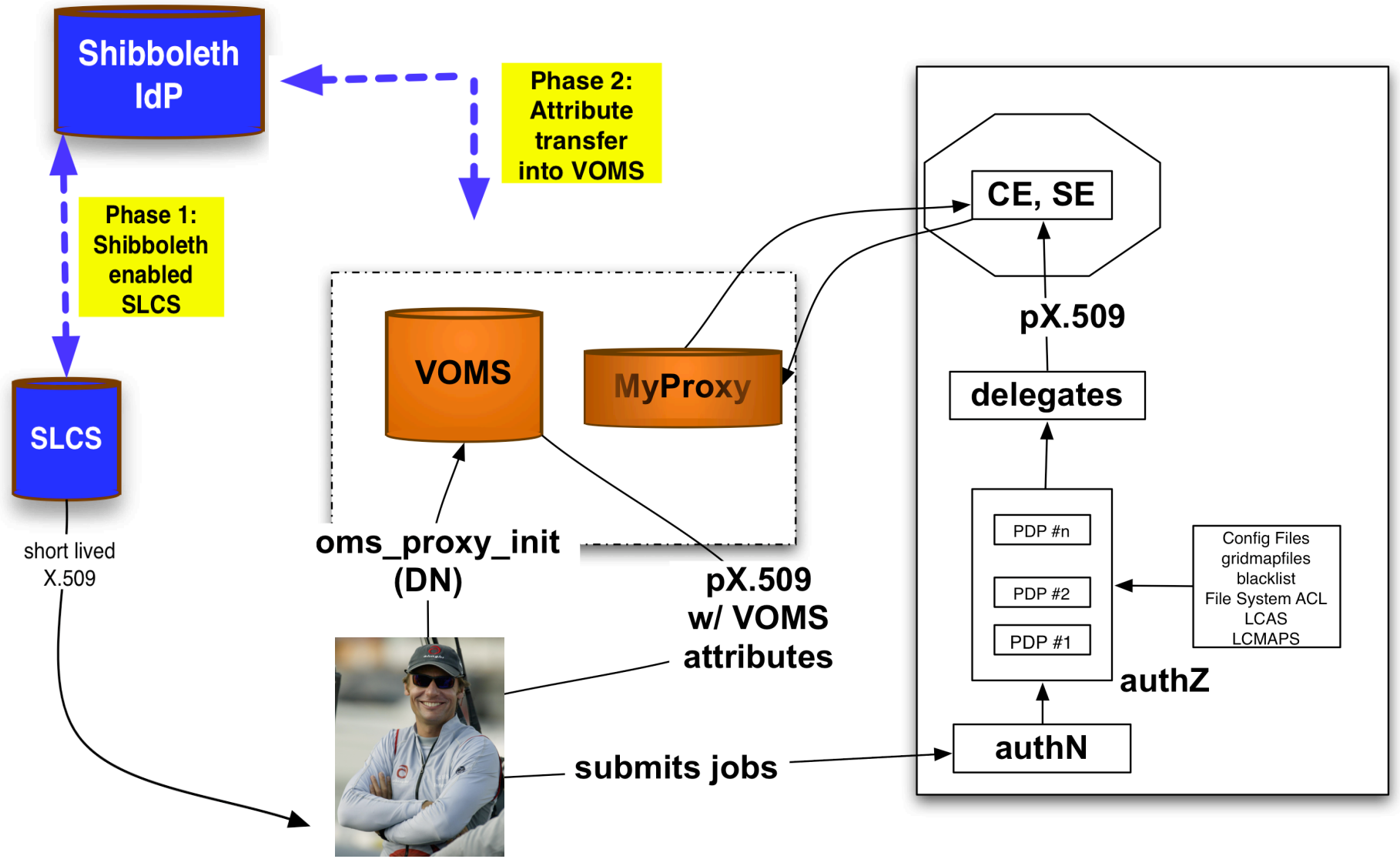
- Focus is on
  - Interoperability (NO replacement for X.509)
  - Specific for EGEE-2 infrastructure (VOMS etc)
  - Integrate, re-use, re-engineer existing code, write new code only as needed

- 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

- **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 third phase**
    - SAML support at the resource end
    - Design during phase 1 and 2
    - Implementation in 2007

Overview Phase 1 and 2



SLCS (1)

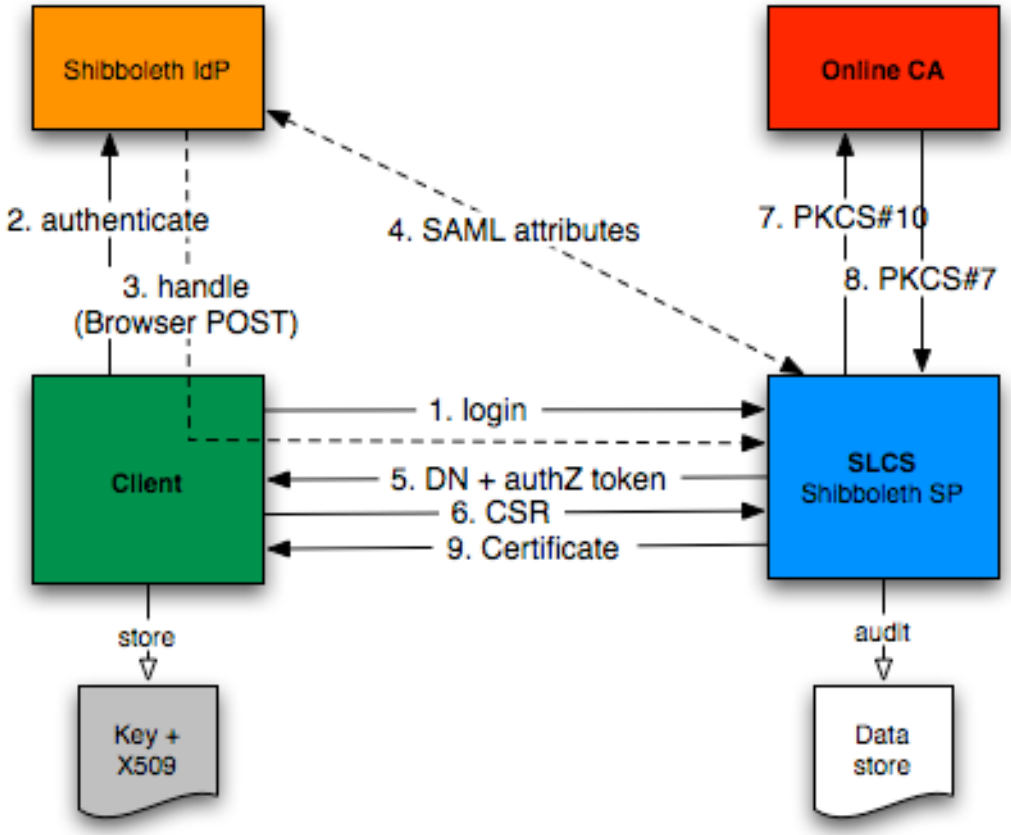
- SLCS = short lived credential service

- Minimum requirements:

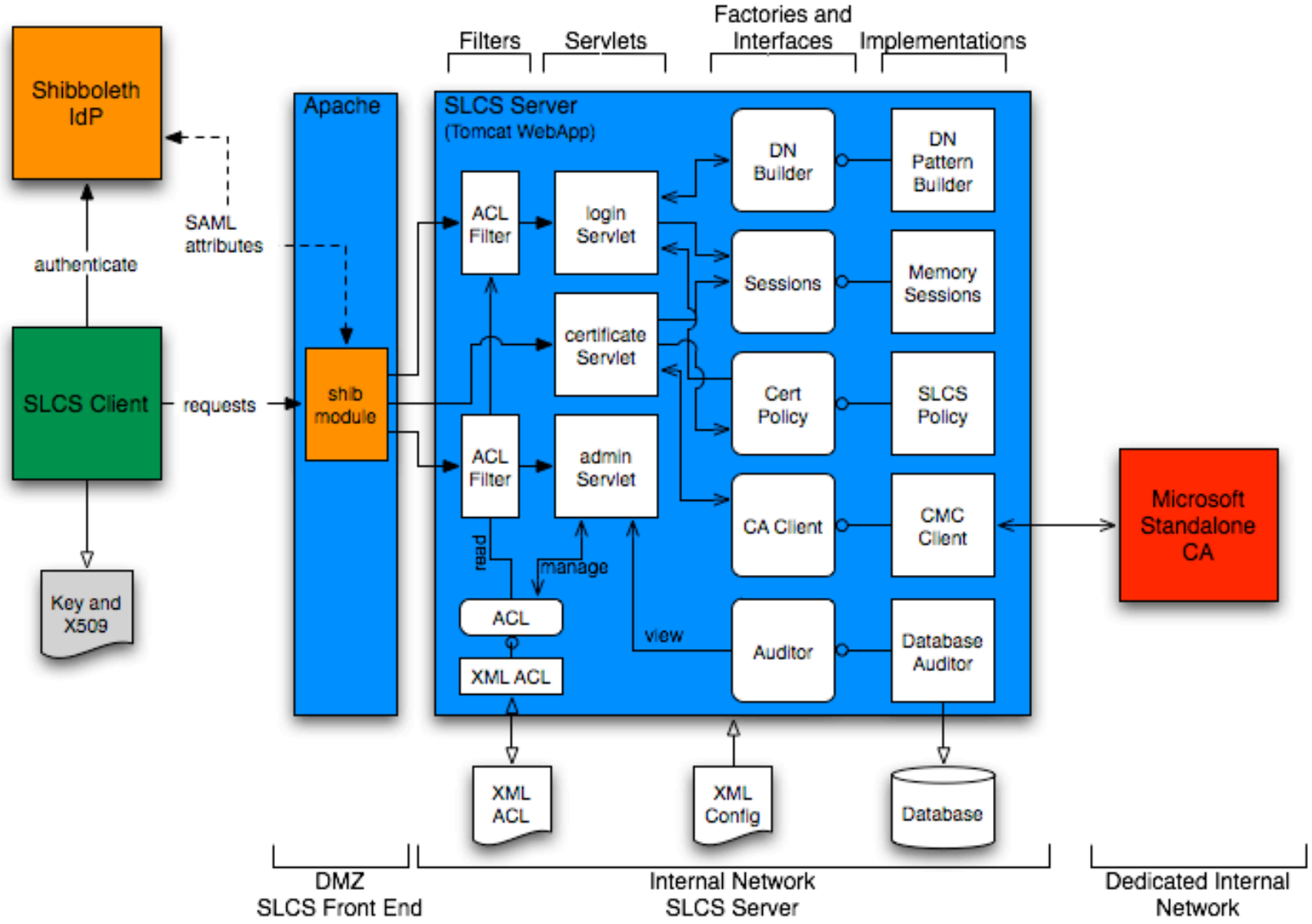
SLCS	X.509 Certificate
Certificate is generated based on Identity Management system	“traditional” Registration Authority (e.g. passport)
Lifetime < 1mio sec	Lifetime < 1 year + 1 month
Revocation handling optional	Revocation handling

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)



Status

- **Software development is finished, now in testing**
- **Nov/Dec: operation in test-bed**
- **CP/CPS:**
  - Internal Draft
  - Will be discussed at next EUGRIDPMA (October)
  - Accreditation early 2007

Phase 2: Attribute Exchange with VOMS

- Goal: Put a subset of Shib attributes into VOMS, such that they automatically appear in the VOMS attribute certificate 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