Interoperability Shibboleth - gLite Phase 3

Christoph Witzig, SWITCH

JRA1 Mar 8, 2007

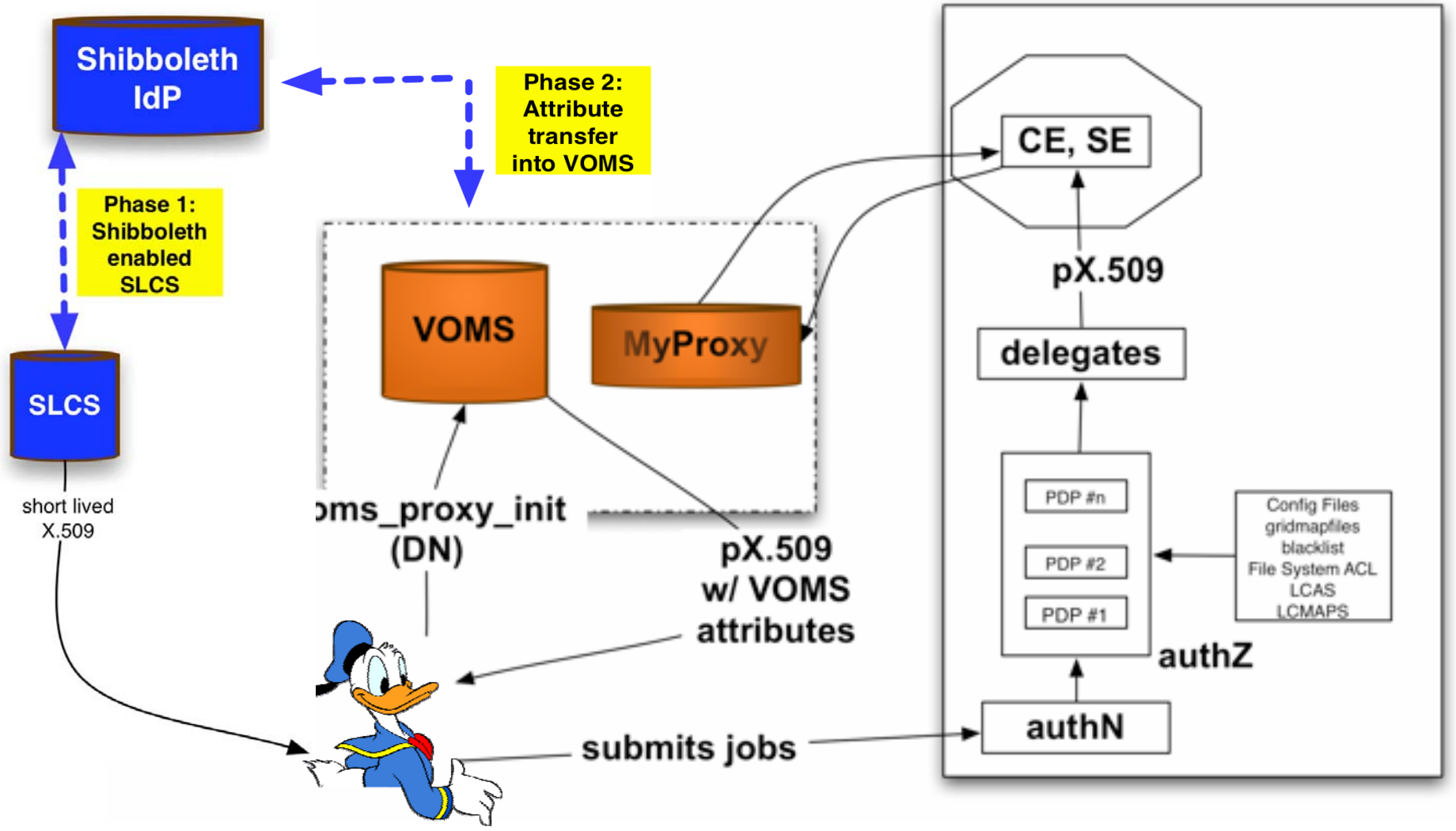
Outline

- **Outlook: Phase 3**

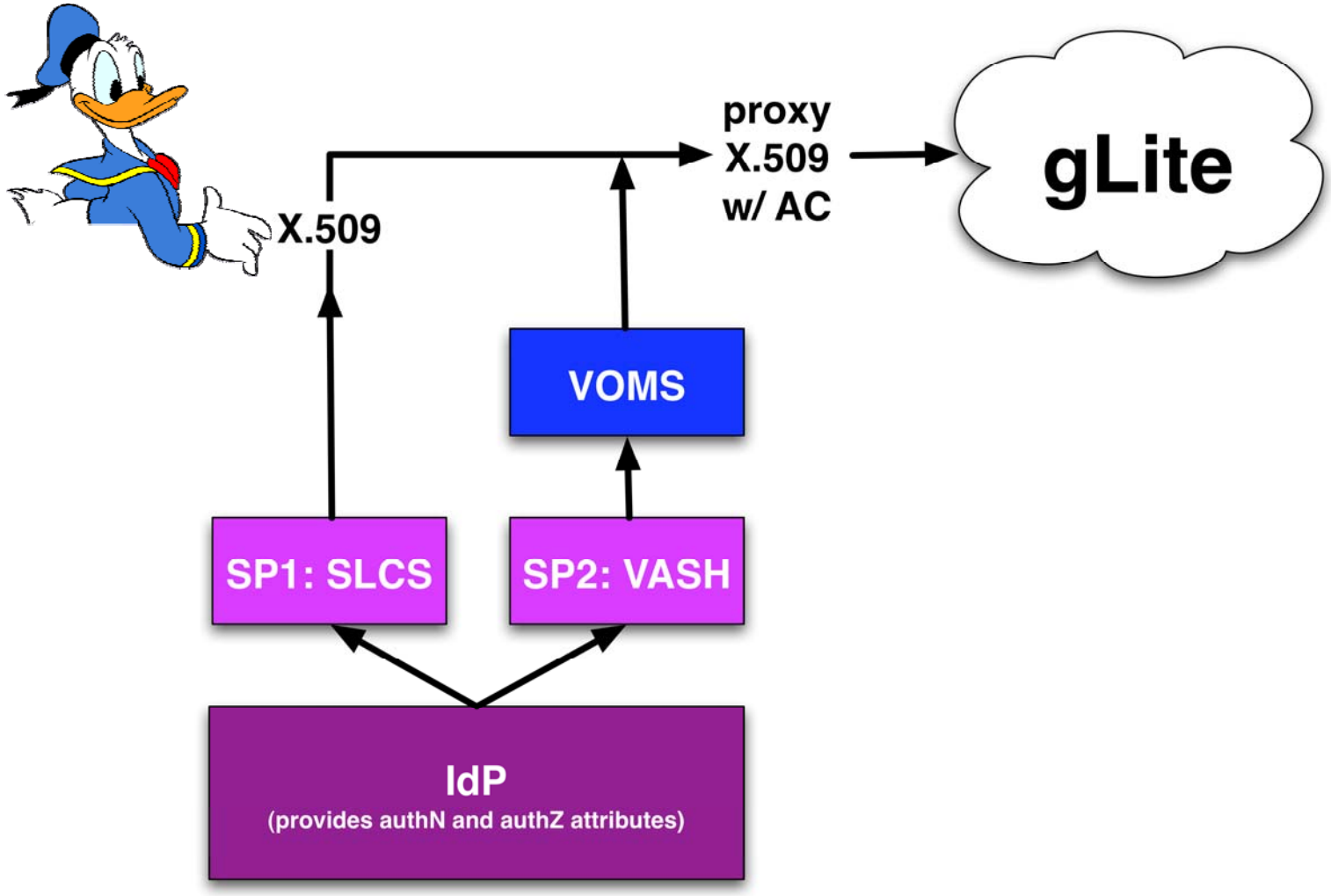
Note:

Design currently in progress - open for all kind of feedback

Overview Phase 1 and 2



Review Phase 1 and 2



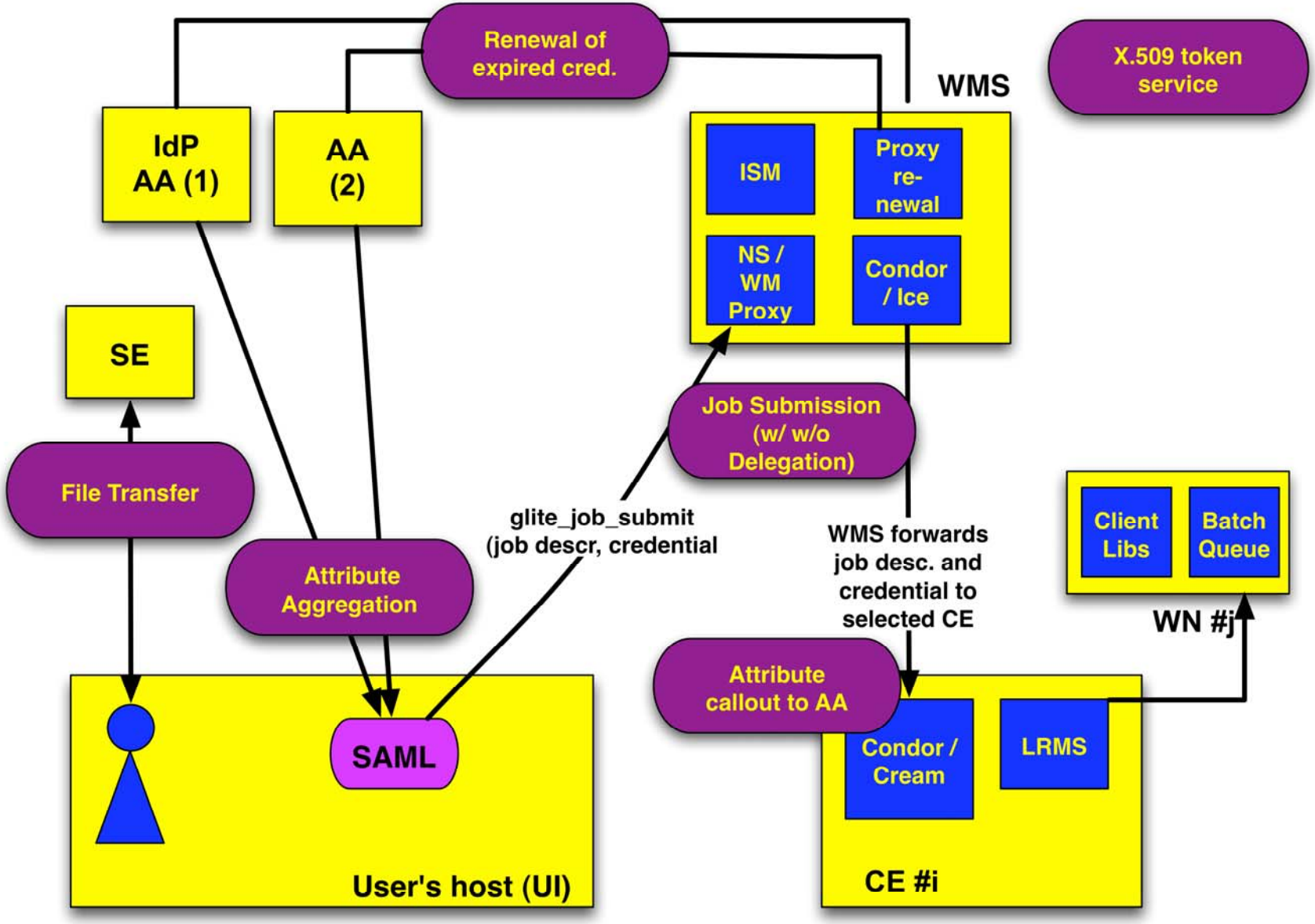
Phase 3 (1)

- **Work program for EGEE-II year 2 and beyond:**
  - Operational use of phase 1 and 2 within Switzerland
  - Inter-federation access with other partners (EGEE-III) ?
  - Phase 3
- **Goal of phase 3: Extend use of SAML in grids beyond what is already provided by phase 1 and 2**
- **3 options:**
  - Option 1: Embed SAML assertions in certificates and let them evaluate by grid resources
  - Option 2: SAML-enable selected grid resources
  - Option 3: extend certificate-based security infrastructure with SAML
- **Option 2 preferred**
  - Option 1: what is additional value beyond phase 1 and 2 ?
  - Option 3: means to modify every grid service - neither desired nor realistic

Phase 3 (2)

- **Phase 3 is currently being designed**
- **Started with general use case of gLite job submission mechanism and broke down into different steps**
- **See document “Grid Use-Cases for Shibboleth” https://edms.cern.ch/document/826978/1**

Job Submission Use-Case



Idea Phase 3

- **SAML-enable those service, with which the user interacts directly**
  - WMS
  - File access

- **Benefits:**
  - (Average) User has no certificates any more
  - Introduce SAML gently beyond phase 1 and 2, gain experience
  - No modifications on most grid software (--> deployment)
  - Compatible with Shibboleth roadmap (2.0, 2.1) and ID-WSF implementation
  - All options open for future

Interoperability SAML - X.509

- **Part of Grid infrastructure is SAML-capable, part is pure X.509 - how to interconnect them?**

- **XTS (X.509 translation/token service)**
  - Aka STS
  - Translates a SAML assertion into a X.509 certificate
  - Webservice
  - Is being contacted by grid service if it receives a SAML assertion, but it only understands X.509
  - One coupling element between the SAML world and the X.509 world
    - Avoid coupling every grid resource with every Shibboleth IdP

Summary

- **Interoperability gLite - Shibboleth:**
  - Phase 1: SLCS service (short lived credential service)
    - Online CA issuing X.509 certificates based upon authN at Shibboleth IdP
    - SWITCHslcs CA EuGridPMA accredited
  - Phase 2: VASH (VOMS Attributes from Shibboleth)
    - Transfers Shibboleth attributes into VOMS
    - (Shib) attributes are available to grid resources as part of VOMS AC
    - Software development finished
  - Phase 3:
    - Currently being designed
    - Idea to SAML-enable a selected (small) number of grid resources (those close to the user)

Q & A