Interoperability Shibboleth - gLite

Christoph Witzig, SWITCH

MWSG Mar 1, 2007

www.eu-egee.org

Information Society and Media

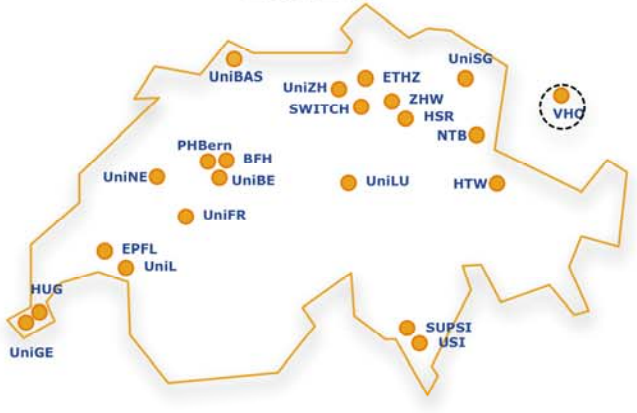
Outline

- **Introduction**
  - Background: SWITCHaai Federation
  - Work Plan
- **Phase 1: Short-lived credential service (SLCS)**
- **Phase 2: Attribute exchange to VOMS**
- **Outlook: Phase 3**
- **Summary**

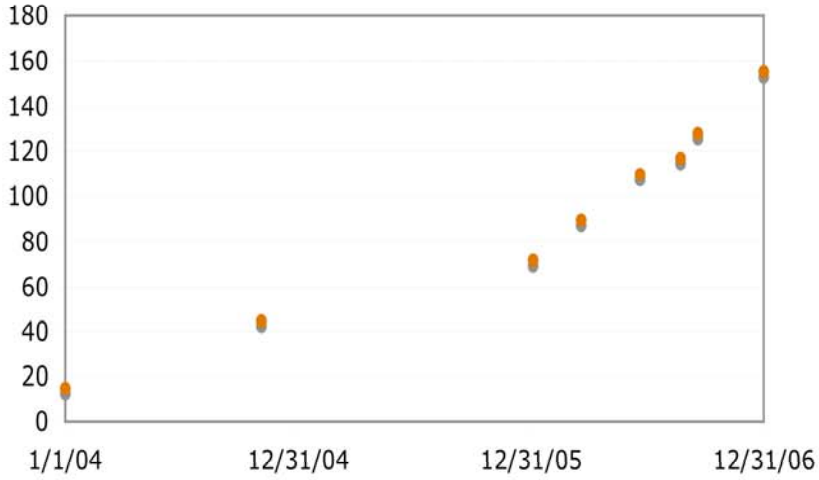
SWITCHaai Federation

Operative Home Organizations
Ende 2004

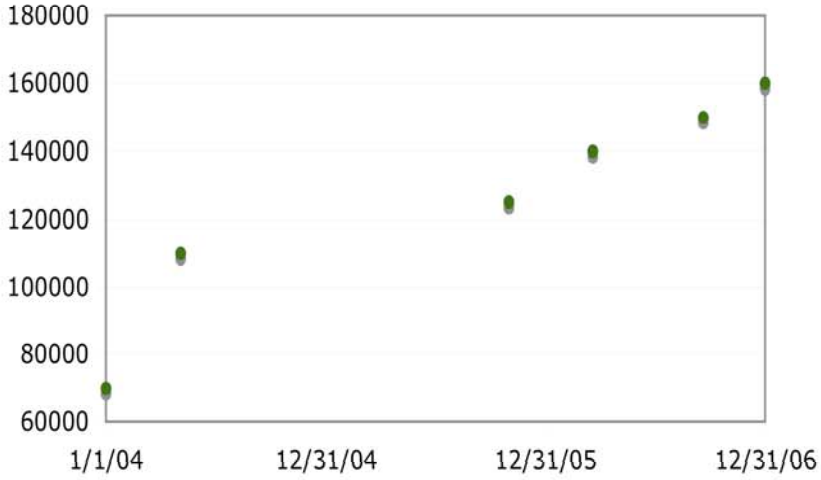
Operative Home Organizations
Ende 2006



Number of Resources
2004-2006



Number of Accounts
2004-2006



AAI and Grid in Switzerland

- **Current Status:**
  - **Approx. 160’000 (75%) members of the Swiss higher education sector have AAI-enabled accounts**
  - **Approx. 10% use SWITCHaai to access about 160 resources on a regular basis**
- **No “national” grid infrastructure**
  - **Various grid efforts (e.g. LCG Tier 2 center, Swiss Bio Grid, …)**
- **Effort underway to launch a national Grid initiative**
- **Motivation for enabling interoperability Shibboleth - Grid within EGEE-II**

Shibboleth Mechanism

Prerequisites

- **Our work is part of EGEE (gLite)**
- **Aim to be open for other grid middleware (if possible)**
- **Must take deployment into account**
  - existing infrastructure

Work Plan

- **EGEE-II:**
  - April 2006 - Mar 2008
  - Year 1: Phase 1 and 2
    - Add interoperability by starting “small” with minimal changes to gLite
    - Decides from the beginning against attribute “pull”
  - Year 2: Phase 3: Extend SAML to selected grid resources

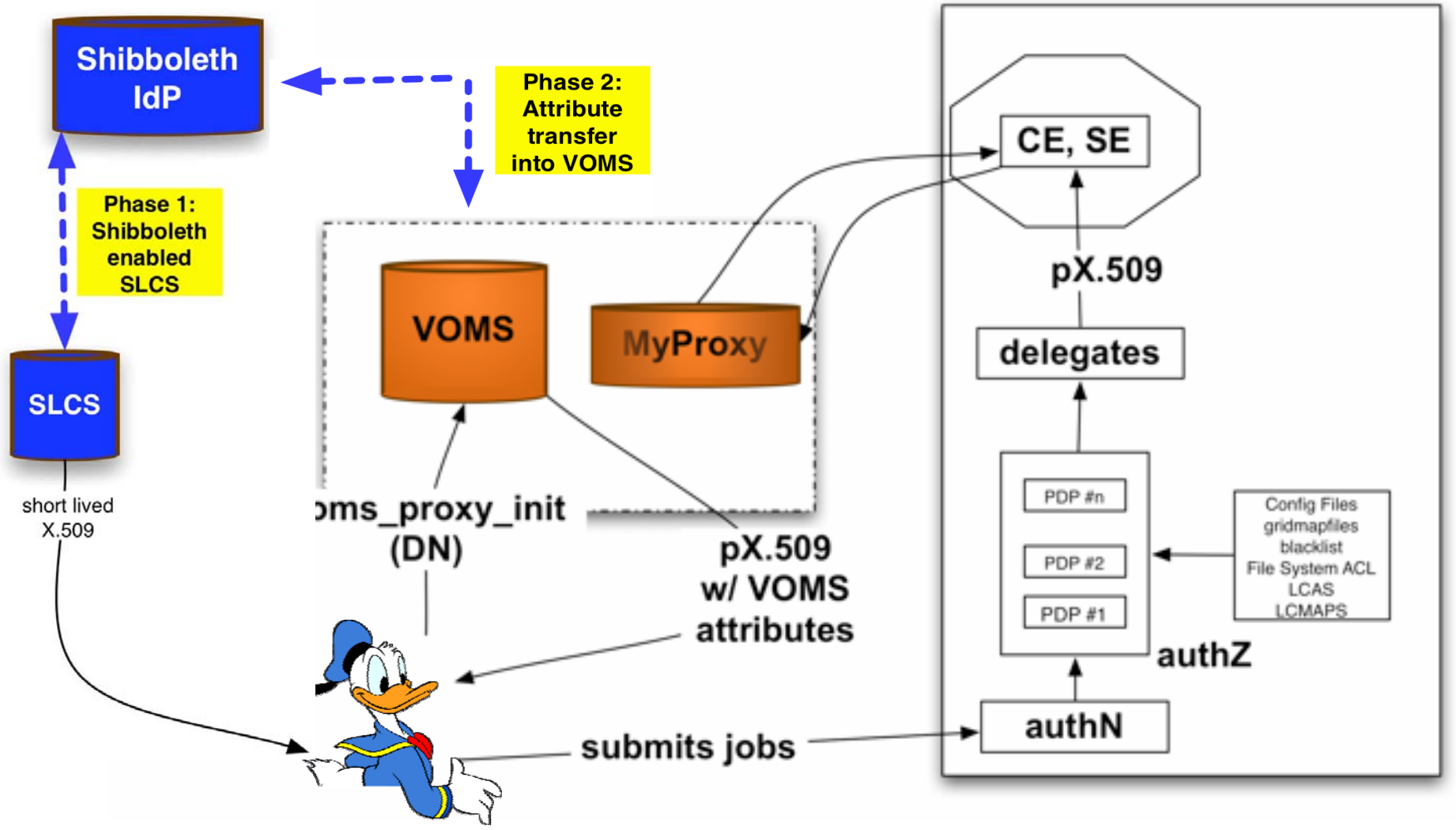
- **EGEE-III:**
  - Continuation in EGEE-III

Key Concepts

- **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**

Overview Phase 1 and 2



Design Decisions

- **SLCS CA and "VOMS SP" should be independent of each other**
  - Separate Service Providers
  - Deployed independently
- **SLCS CA should be independent of the Grid middleware**
- **VOMS SP should only be dependent on VOMS**

Outline

- **Introduction**
  - Background: SWITCHaai Federation
  - Work Plan
- **Phase 1: Short-lived credential service (SLCS)**
- **Phase 2: Attribute exchange to VOMS**
- **Outlook: Phase 3**
- **Summary**

SLCS Profile

- SLCS = short lived credential service
- IGTF profile

- Minimum requirements:

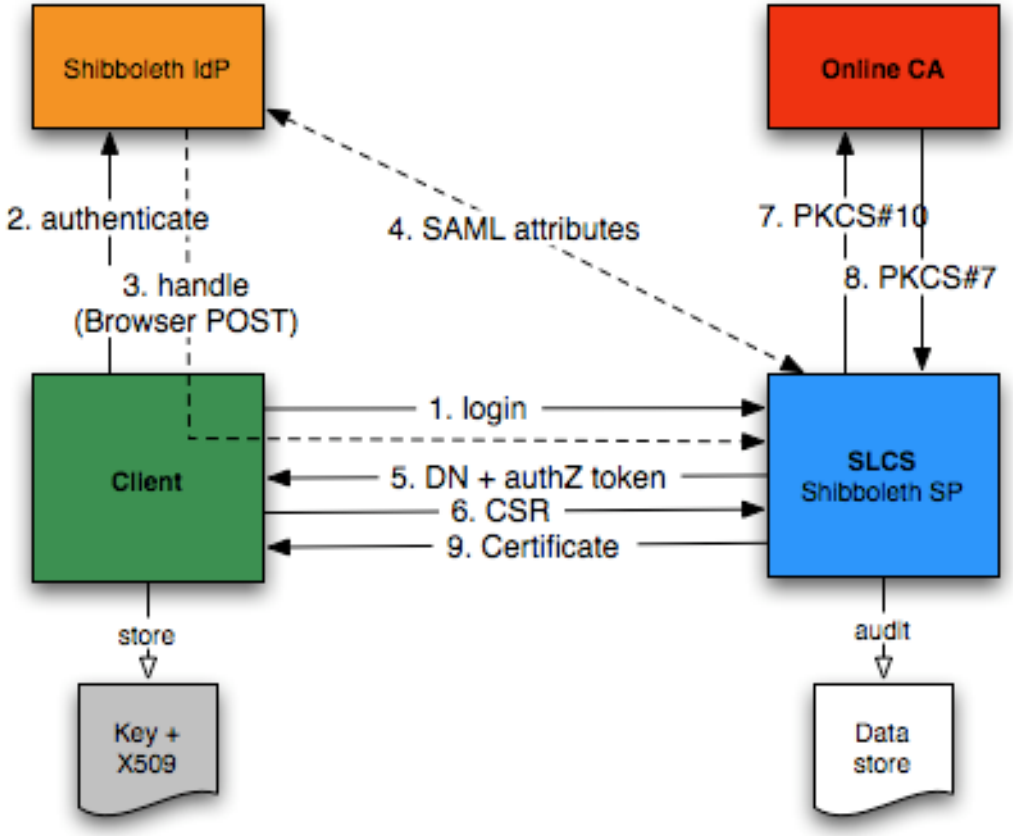
SLCS	X.509 Certificate
Certificate is generated based on Identity Management system	“traditional” Registration Authority (e.g. passport)
Lifetime < 1mio sec	Lifetime < 1 year + 1 month
Revocation handling optional	Revocation handling

SWITCHslcs: Operation

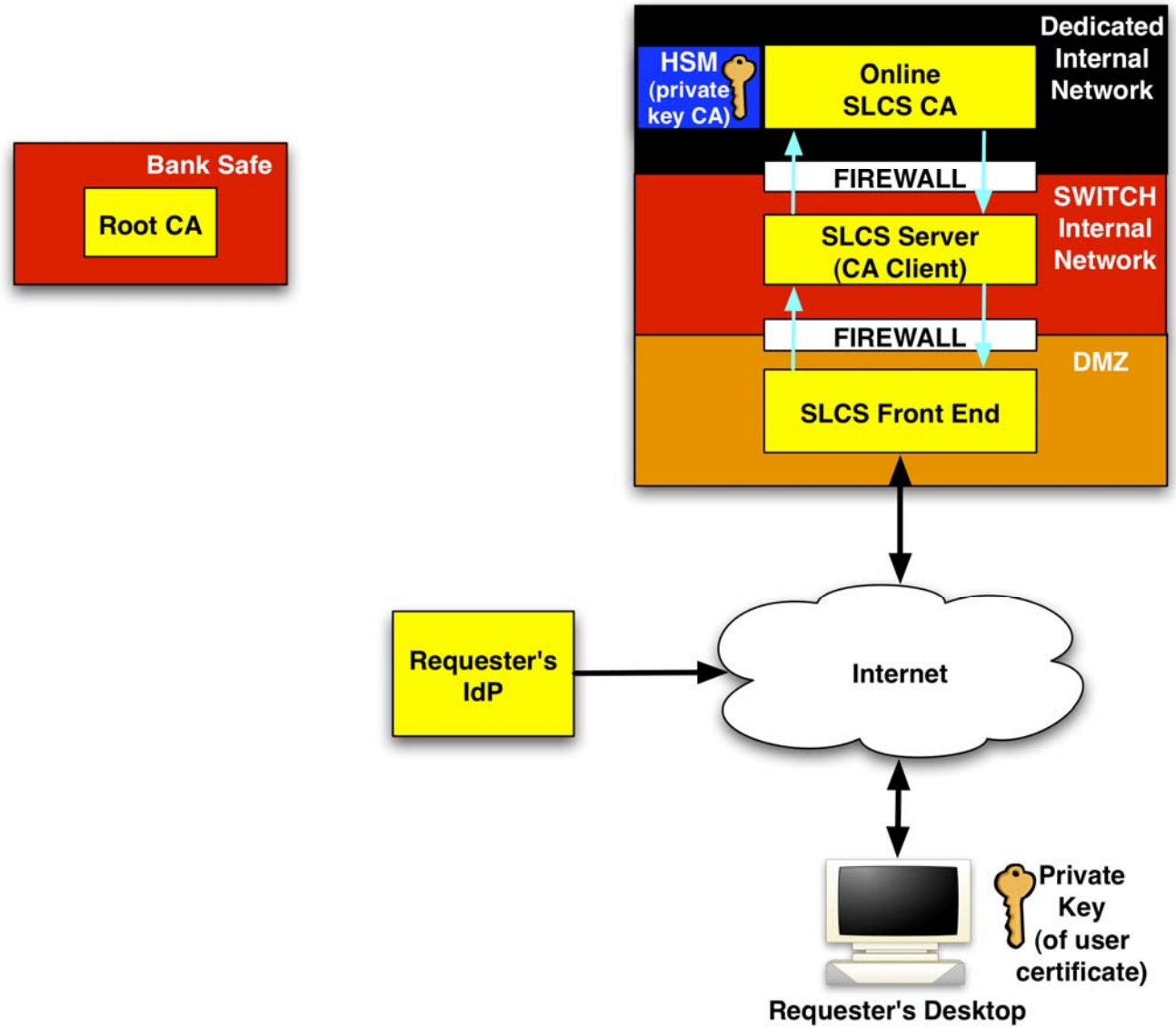
- **For the user:**
  - **from the command line: invisible**
  - **part of gLite UI (3.1) (can be installed independently)**
- **For the RA from web-based admin tool:**
  - **Can enable or disable individual users (only for his institution)**
  - **Requirements formulated in CP/CPS**
  - **Can obtain log information**
- **SWITCH:**
  - **Operates the service**
  - **Strict access control**
  - **Operate also a second test CA (everything being installed on the MSCS CA will be tested there *first*)**

SWITCHslcs

- Private key is never transferred
- Use commercial CA and only standard protocols
- Modular design such that other people can use components
- Shibboleth attributes determine DN



SWITCHslcs: CA Setup



Status SLCS

- **Software development is finished**
- **MJRA1.4 document: https://edms.cern.ch/document/770102/1**
- **Operation of SLCS TEST CA in test-bed since November**
  - http://www.switch.ch/pki/grid/test
- **CP/CPS:**
  - **Accredited by EuGridPMA**
  - http://www.switch.ch/pki/grid
- **Production CA setup: in progress (RSN)**

Outline

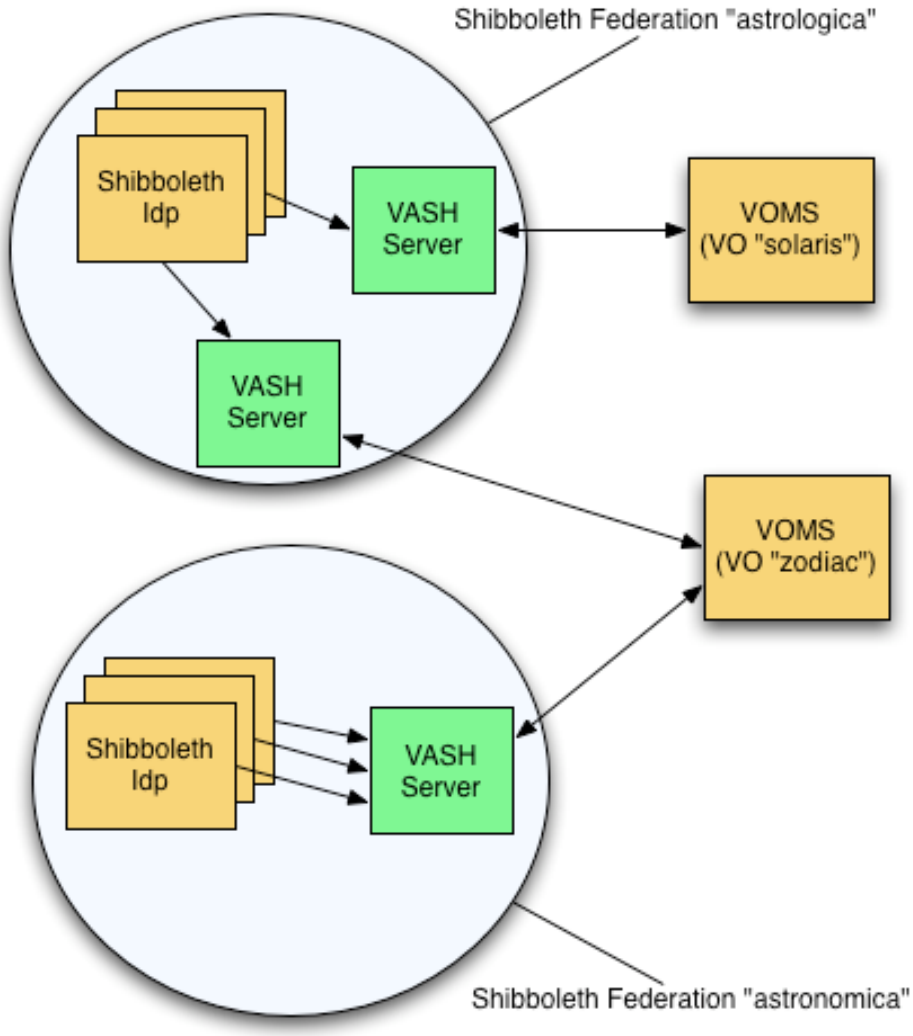
- **Introduction**
  - Background: SWITCHaai Federation
  - Work Plan
- **Phase 1: Short-lived credential service (SLCS)**
- **Phase 2: Attribute exchange to VOMS**
- **Outlook: Phase 3**
- **Summary**

The Problem

- **Phase 1 ties**
  - AAI authentication to issuance of X.509 certificate\
  - AAI attributes are used to construct the DN
- **Phase 2 intends to make AAI attributes available to grid resources for authorization decisions**
  - Which AAI attributes are of interest to grid resource?
  - How does resource obtain attributes? (pull vs push)
  - Relation to VO attributes
  - Deployment issues

Design

- **VASH:**
  - VOMS Attributes from Shibboleth
- **Shibboleth SP**
  - Browser-based
  - Specific for
    - Federation
    - VO
- **“lightweight” SP**
  - No administrator duties
  - No management of attributes
  - Simply transfers attributes upon user request



Design (2)

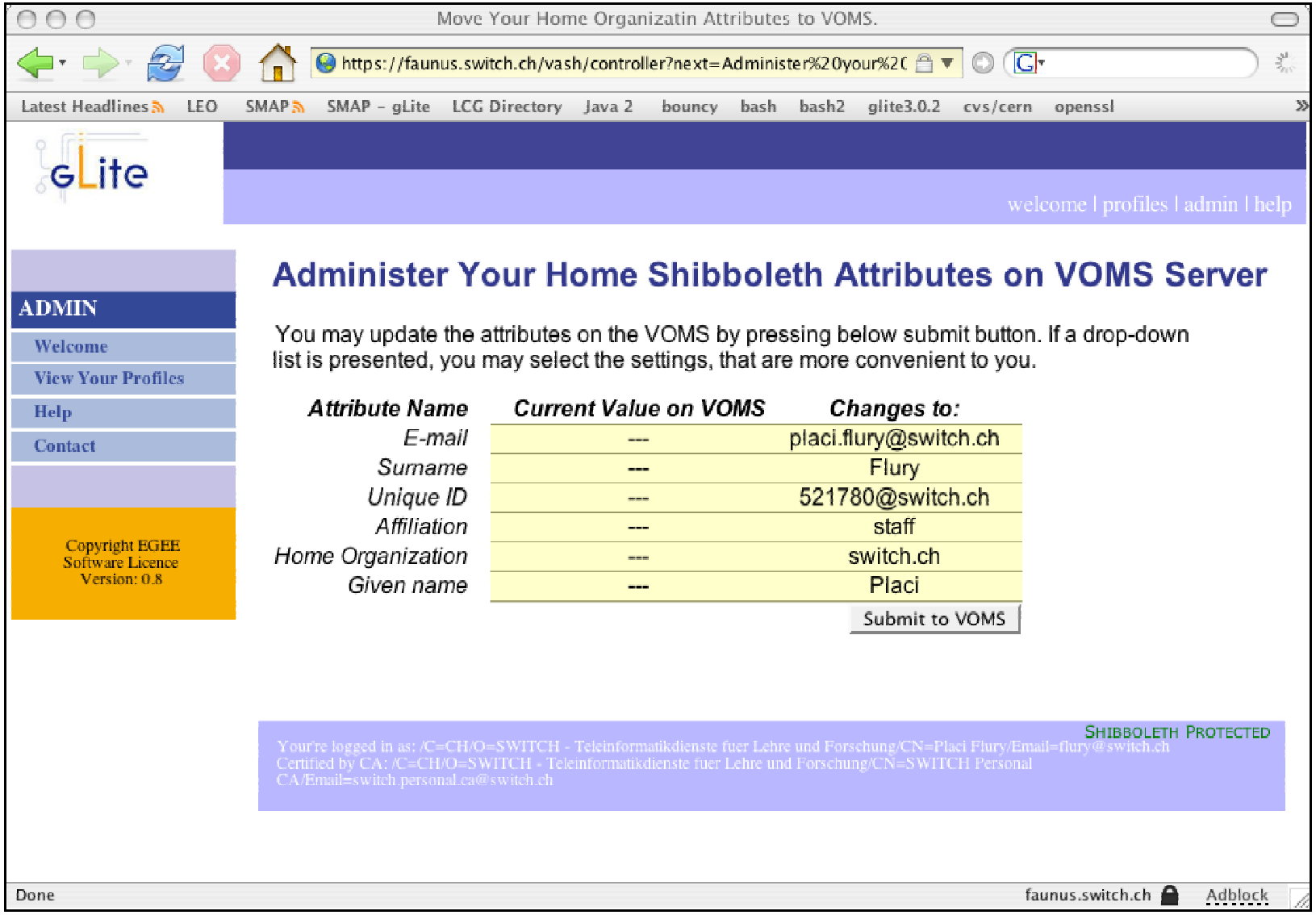
- **X.509 and proxy X.509 with VOMS AC unchanged**
- **No change in VOMS**
  - Needs version 1.7.10 or higher
- **VO registration not changed**
- **Administrative domain between Shibboleth federation and VOMS fully decoupled**
- **User manages mapping between DN in VOMS and Shibboleth user id (for classic X.509 and SLCS X.509)**
- **Becomes a service which knows the mapping Shibboleth userid - DN**
- **Has to respect data privacy laws**

Shibboleth Attributes

- Need common understanding of attributes
  - given within a federation
  - but inter-federation access (?)
- Attributes are based on eduPerson
- Only a subset of attributes are really interesting for grid resources

Attribute	Derived / Adapted from				Status			Grid
unique ID				X	X			
Surname	X				X			
Given name			X		X			
Date of birth							X	
E-mail			X			X		
Home Organization					X			X
Home Organization Type					X			X
Affiliation				X	X			X
Study branch 1							X	X
Study branch 2							X	X
Study branch 3						X		X
Study level						X		X
Staff category				X		X		X
Member of				X			X	X

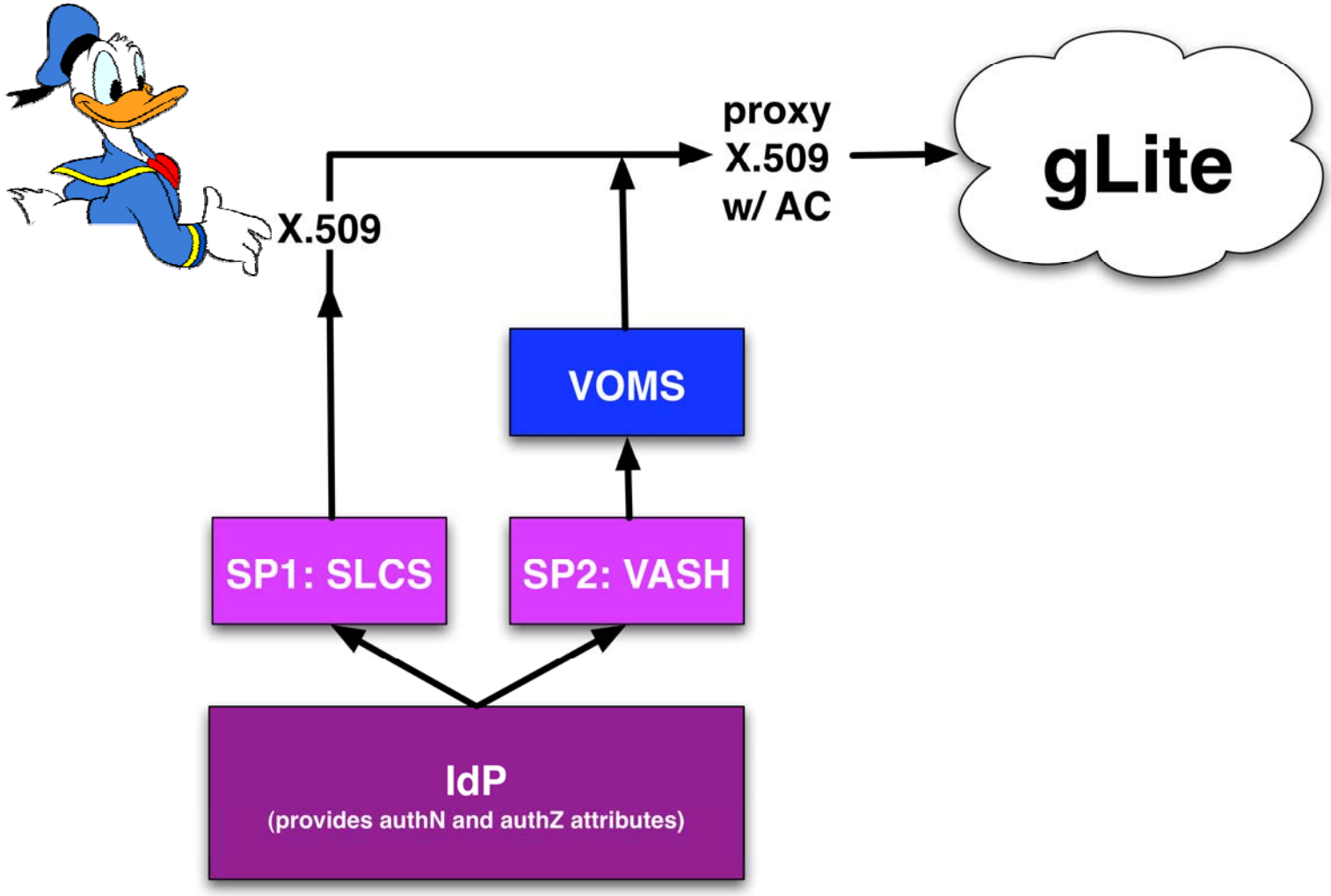
Web Interface VASH Service



Status

- **Software implementation done**
- **MJRA1.5 document: https://edms.cern.ch/document/807849/1**
- **Need to develop plug-ins and mechanisms to evaluate the Shibboleth attributes at the grid resource**
  - Access to VOMS AC

Review Phase 1 and 2



Alternative Scenarios (1)

- **Instead of SP1 issuing a short-lived X.509 certificate**
  - Keep using X.509 certificate from a (“classical”) CA
    - IdP not used for authN
    - May make sense if one wants to use only IdP attributes
  - Generate proxy X.509 if authN at IdP successful
    - authN from CA and IdP
  - Issue (long-lived) X.509 credential based on auth at IdP
    - TAGPMA MICS profile
    - User has to maintain long-lived certificate
  - Use a “low quality” CA (i.e. not accredited)
    - Much less work
    - Compatibility with existing infrastructure (EGEE, LCG)

Alternative Scenarios (2)

- **Instead of SP2 being independent of SP1**
  - Merge them into one utility, which
    - Issues a X.509 certificate containing the IdP attributes as an extension
      - *X.509 certificate is no longer a "bare" X.509*
      - *User cannot choose to not expose his/her attributes*
      - *Code must handle attributes from two sources: IdP attributes and the VOMS VO attributes*
      - *Revocation whenever attribute changes*
    - IdP issues an AC to be inserted into proxy X.509 (just like VOMS)
      - *IdP must be known to every grid resource*
      - *Requires code change at the IdP*
  - Attribute aggregation in SAML: Longer term project (dependencies on Shib 2 and future VOMS work)
  - Question: should data privacy be observed when releasing IdP attributes?

Outline

- **Introduction**
  - Background: SWITCHaai Federation
  - Work Plan
- **Phase 1: Short-lived credential service (SLCS)**
- **Phase 2: Attribute exchange to VOMS**
- **Outlook: Phase 3**
- **Summary**

Phase 3 (1)

- **Work program for EGEE-II year 2 and beyond:**
  - Deployment 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

Phase 3 (2)

- **Phase 3 is currently being designed**
- **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
    - Online CA issuing X.509 certificates based upon authN at Shibboleth IdP
    - currently being deployed
  - Phase 2: VASH
    - 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