



Enabling Grids for E-science

SLCS and VASH Service

Interoperability of Shibboleth and gLite

Christoph Witzig, SWITCH
(*witzig@switch.ch*)

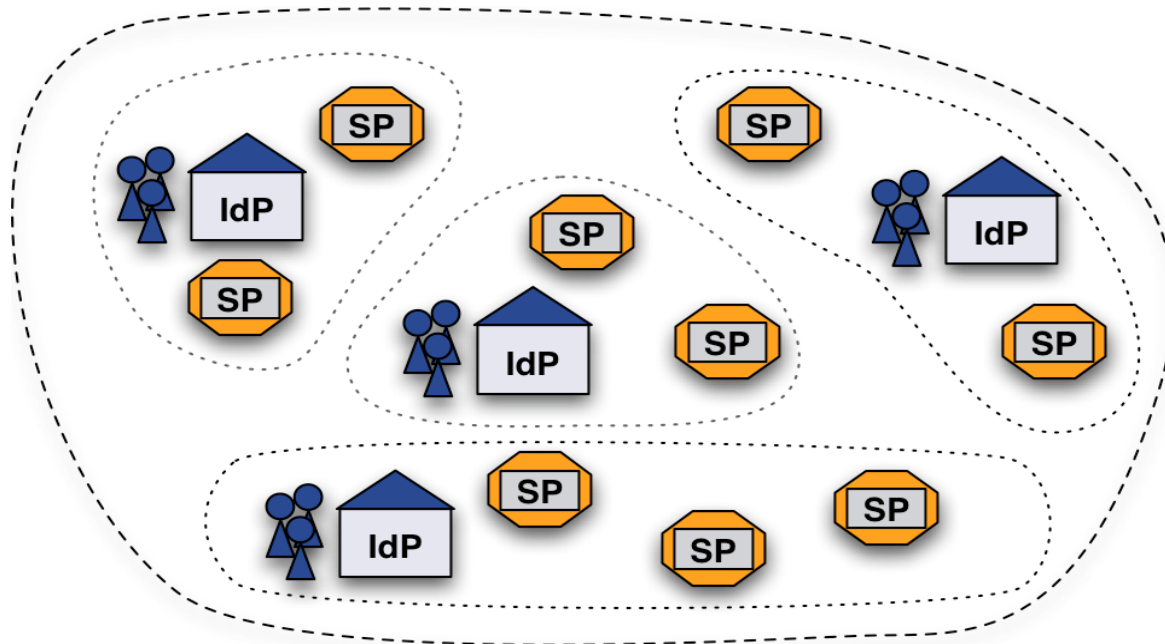
NREN Grid Workshop Nov 30th, 2007 - Malaga

www.eu-egee.org

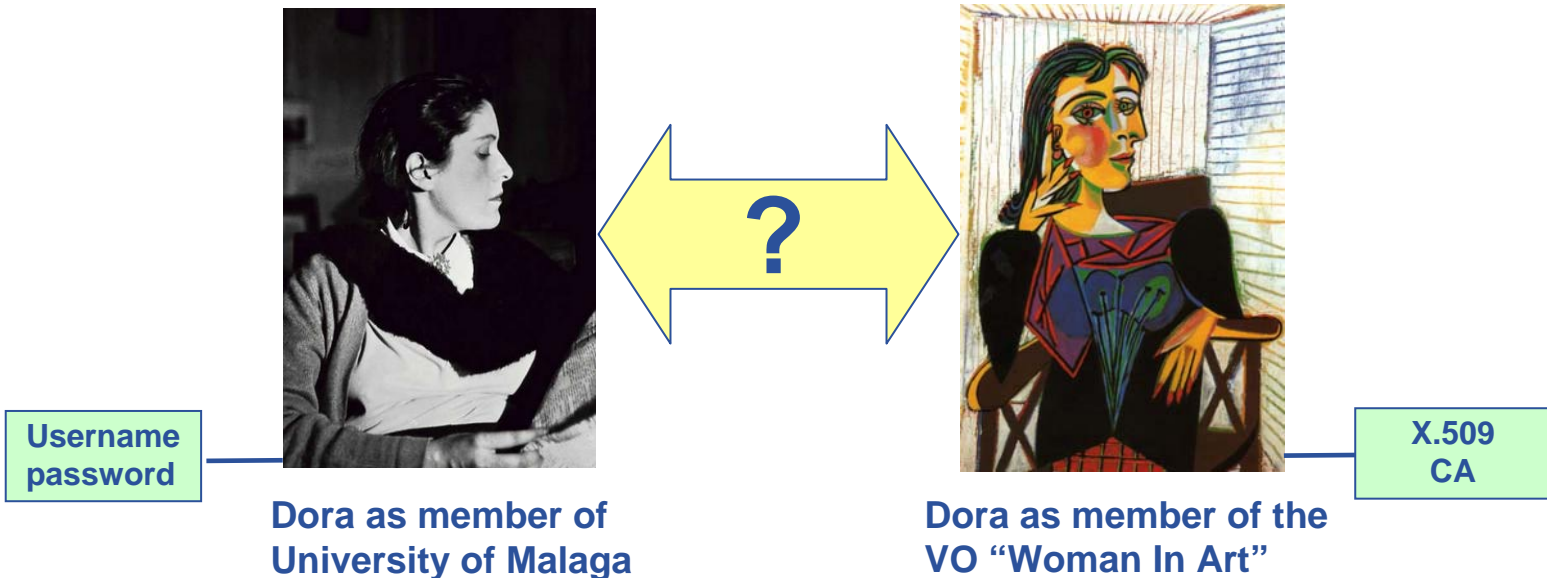


- **Introduction**
 - Interoperability Shibboleth - gLite
- **Short-Lived Credential Service (SLCS) (Phase 1)**
- **VOMS Attributes for SHibboleth (VASH) (Phase 2)**
- **Outlook: SAML Support in Grids (Phase 3)**
- **Summary**

- Identity Providers (IdP) **authenticate** their users
- Service Providers (SP) **trust** the Identity Providers (IdP) and **authorize** the users
- Cross domain authentication and authorization based on trust relation



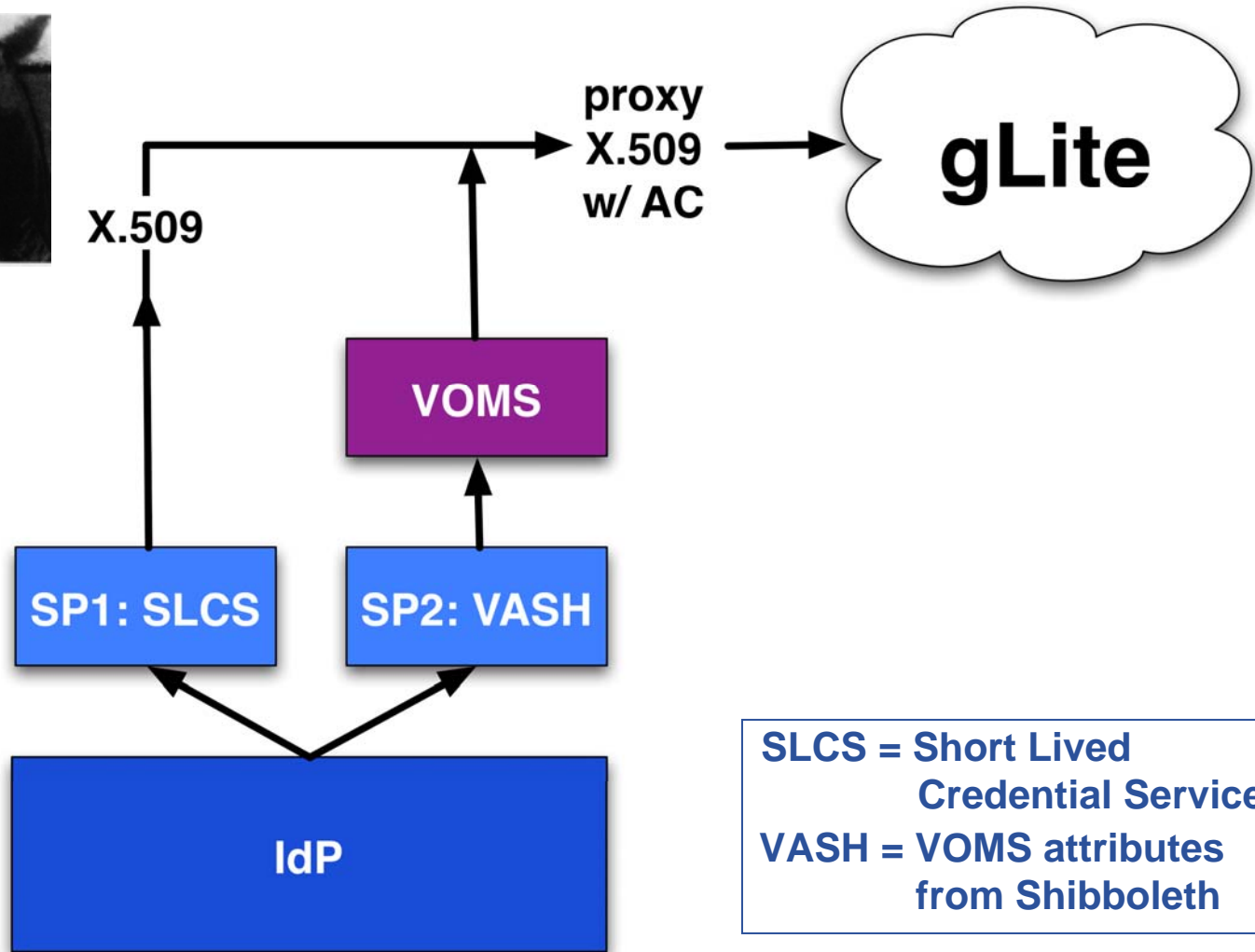
- Real organizations have built AAls
- Grids are being built around Virtual Organizations (VO)
- How do you relate the member of the “real” organization to the member of the organization?



- **Interoperability Shibboleth - gLite by SWITCH**
 - **Part of EGEE-II**
- **Focus is on**
 - **Interoperability (NO replacement for X.509)**
 - **Specific for EGEE II 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**



gLite UI



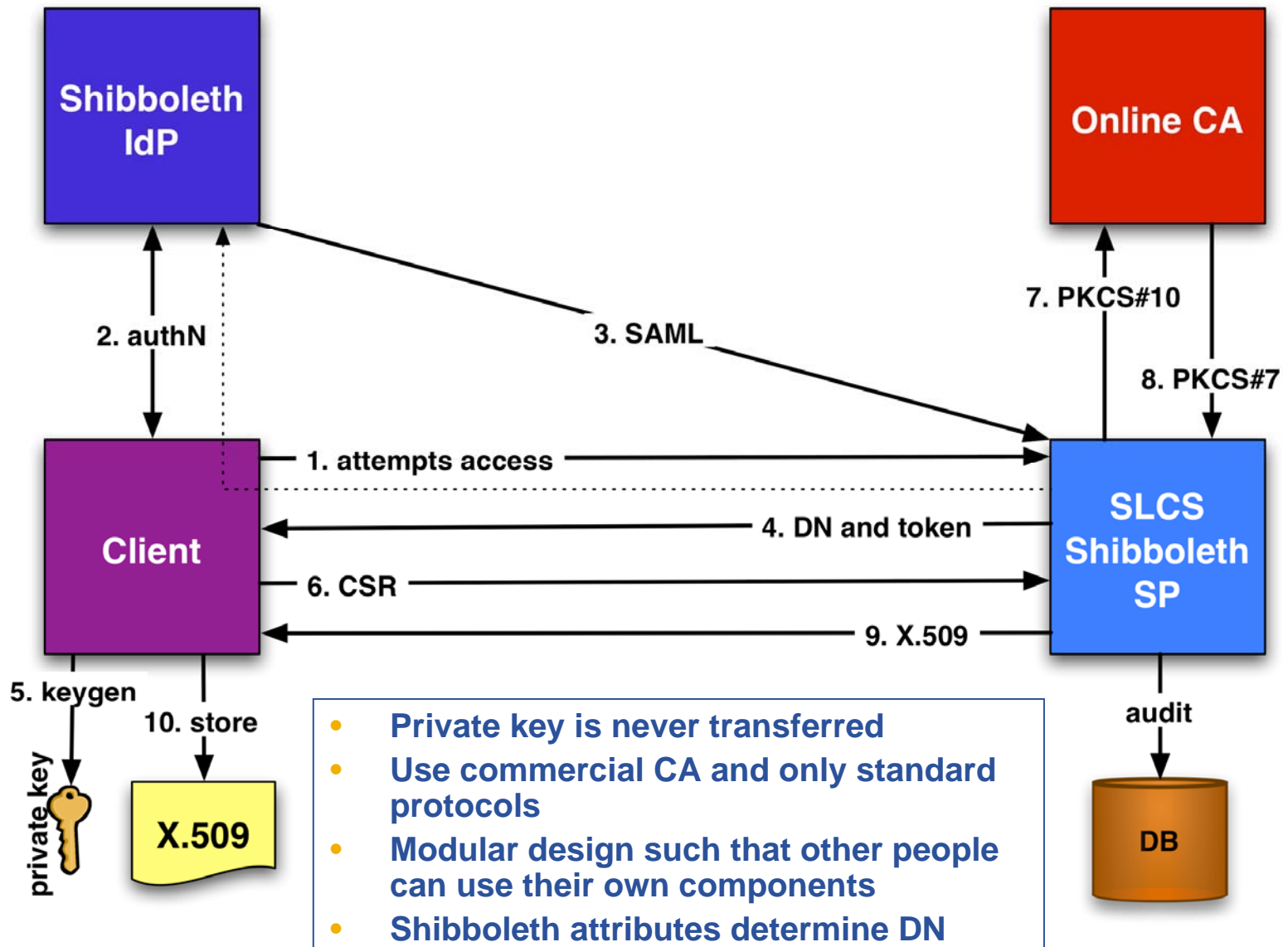
SLCS = Short Lived
Credential Service
VASH = VOMS attributes
from Shibboleth

Short Lived Credential Service (SLCS)



- **SLCS = Short Lived Credential Service**
- **International Grid Trust Federation (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 mandatory



- **For the user:**
 - **Command line: `slcs-init --idp <providerId>`**
 - **Part of gLite User Interface (gLite-UI 3.1)**
(can also 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 (audit)**

- **SWITCH:**
 - **Operates the service for the SWITCHai federation**

- 3 separate servers in increasingly secure environment (network and physical access)

- **Front End**

- Shibboleth SP

- **SLCS Server**

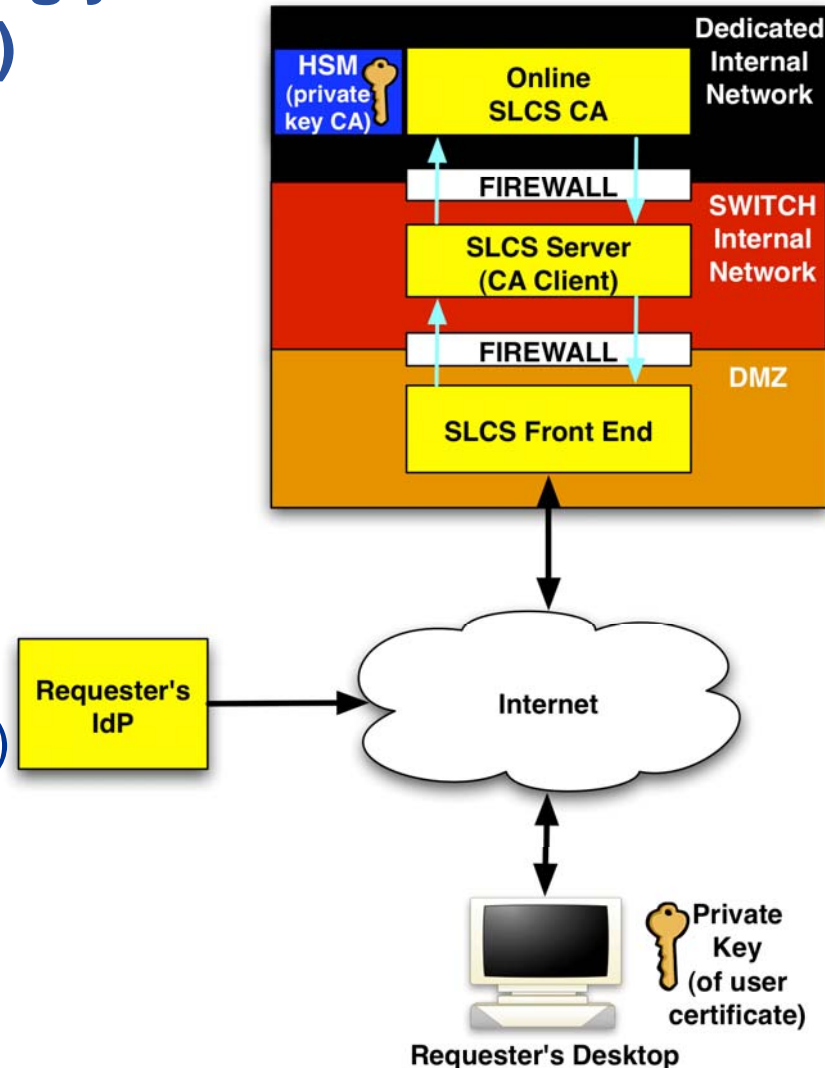
- Tomcat web app

- **Online CA**

- Microsoft Certificate Server
- Hardware Security Module (HSM)

- **Offline CA**

- Sign the Online CA
- Stored in a bank safe



- **Software development finished in 2006**
- **SWITCH SLCS Root CA accredited by EuGridPMA in February 2007**
- **SWITCH SLCS in production since April 2007**
- **<http://www.switch.ch/grid/slcs>**

VOMS attributes from Shibboleth (VASH)

- **SLCS ties**
 - AAI authentication to issuance of X.509 certificate
 - AAI attributes are used to construct the DN

- **SLCS 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

VASH:

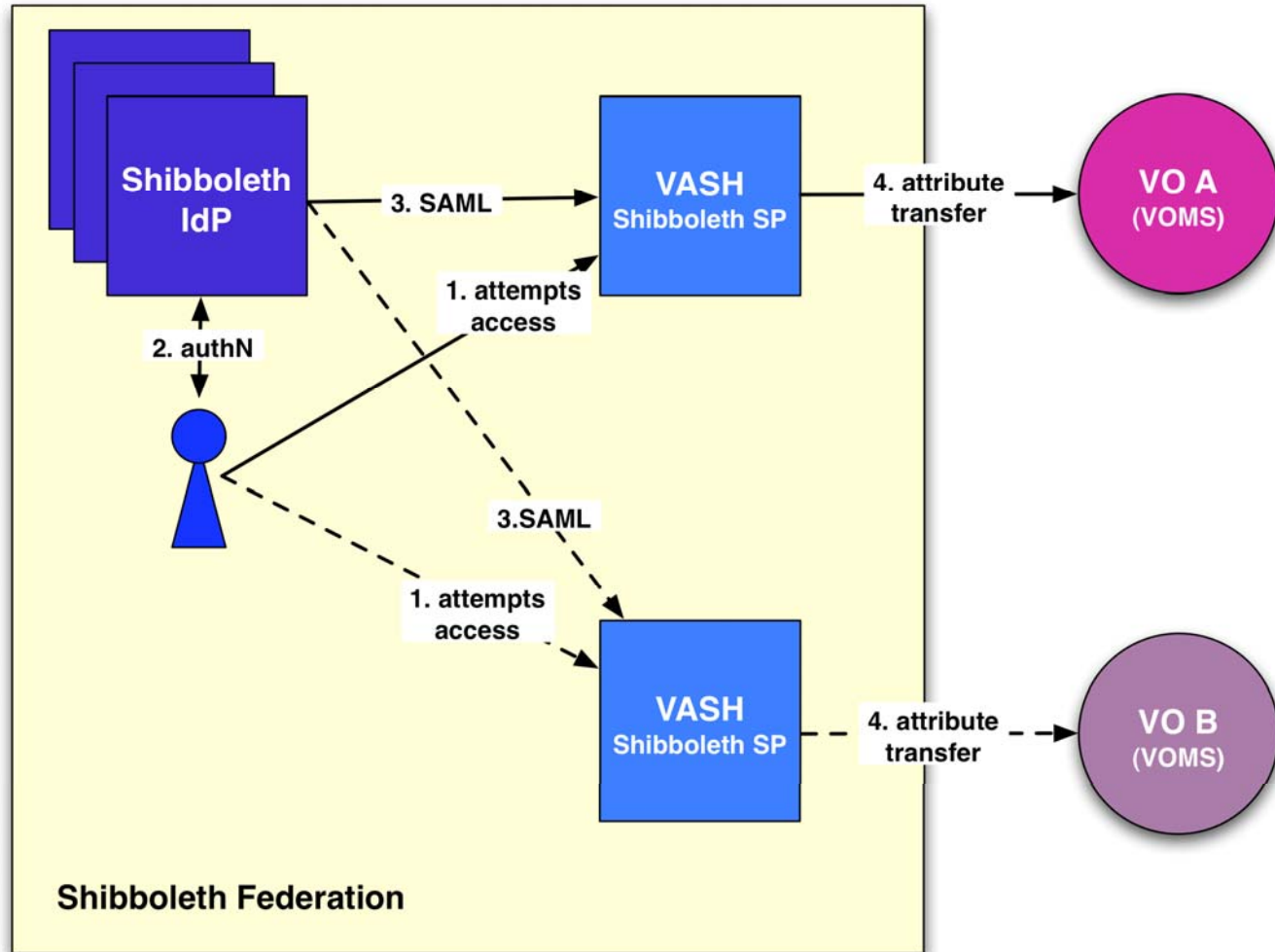
- VOMS Attributes from Shibboleth

Shibboleth SP

- Browser-based
- Specific for
 - Federation
 - VO

“lightweight” SP

- No administrator duties
- No management of attributes
- Simply transfers attributes upon user request



- **X.509 and proxy X.509 with VOMS AC unchanged**
- **No change in VOMS**
 - Requires VOMS 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)

Move Your Home Organization Attributes to VOMS.

https://faunus.switch.ch/vash/controller?next=Administer%20your%20...
 Latest Headlines LEO SMAP SMAP - gLite LCG Directory Java 2 bouncy bash bash2 glite3.0.2 cvs/cern openssl

gLite welcome | profiles | admin | help

Administer Your Home Shibboleth Attributes on VOMS Server

You may update the attributes on the VOMS by pressing below submit button. If a drop-down list is presented, you may select the settings, that are more convenient to you.

Attribute Name	Current Value on VOMS	Changes to:
E-mail	---	placi.flury@switch.ch
Surname	---	Flury
Unique ID	---	521780@switch.ch
Affiliation	---	staff
Home Organization	---	switch.ch
Given name	---	Placi

Copyright EGEE
Software Licence
Version: 0.8

SHIBBOLETH PROTECTED
 You're logged in as: /C=CH/O=SWITCH - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury/Email=flury@switch.ch
 Certified by CA: /C=CH/O=SWITCH - Teleinformatikdienste fuer Lehre und Forschung/CN=SWITCH Personal
 CA/Email=switch.personal.ca@switch.ch

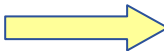
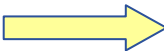
Done faunus.switch.ch Adblock

- **Option 1:**
 - As an add-on to an existing VOMS-based VO
- **Option 2:**
 - As a registration tool which allows the member of a Shibboleth IdP become a member of a VOMS-based VO
 - Suitable for production VOs as well as temporary VOs (e.g. summer schools, grid classes)

- **Software implementation done**
- **MJRA1.5 document:**
<https://edms.cern.ch/document/807849/1>
- **Plug-ins and mechanisms to evaluate the Shibboleth attributes at the grid resource available**
 - Access to VOMS AC
 - LCAS/LCMAPS plugin

Outlook: SAML Support in Grids

- **Goal of phase 3: Extend use of SAML in grids beyond what is already provided by phase 1 and 2**
- **SAML-enable those services, with which the user interacts directly**
 - WMS
 - File access
- **Benefits:**
 - (Average) User has no certificates anymore
 - Introduce SAML gently beyond phase 1 and 2, gain experience
 - Compatible with Shibboleth roadmap (2.0, 2.1) and WS-Trust STS implementation
 - Options open for future
- **Requires: A mean for service to transform a security tokens it has into a security token it needs**

- **Based on OASIS WS-Trust Standard**
- **Converts one security token into another**
 - Initial focus on
 - username/password  SAML
 - SAML  X.509
- **Supports token request, renewal, validity check, destruction**
- **Capable of obtaining attributes from different sources (e.g. Shibboleth IdP, VOMS)**

- **Grid:**
 - A central Grid resource (e.g. resource broker) obtains a user job with a SAML assertion as credential
 - Conversion into a security token that the other Grid services understand (X.509)

- **Non-browser based Shibboleth applications:**
 - User agent contacts Shibboleth IdP with credential (e.g. username, password)
 - User agent receives SAML assertion to be sent to a Shibboleth SP

- **Interoperability Shibboleth - gLite**
 - Phase 1: SLCS
 - Online CA issuing short-lived X.509 certificates based upon authentication at Shibboleth IdP
 - Operative and in production
 - 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: SAML
 - Actual phase: design of a WS-Trust STS for SAML and proxy X.509
 - Idea to SAML-enable a selected (small) number of grid services (those close to the user: WMS, ...)

- **Leverage the existing SWITCHai Shibboleth federation**

Q & A