



# SWITCH

The Swiss Education & Research Network

## **SWITCHslcs & VASH**

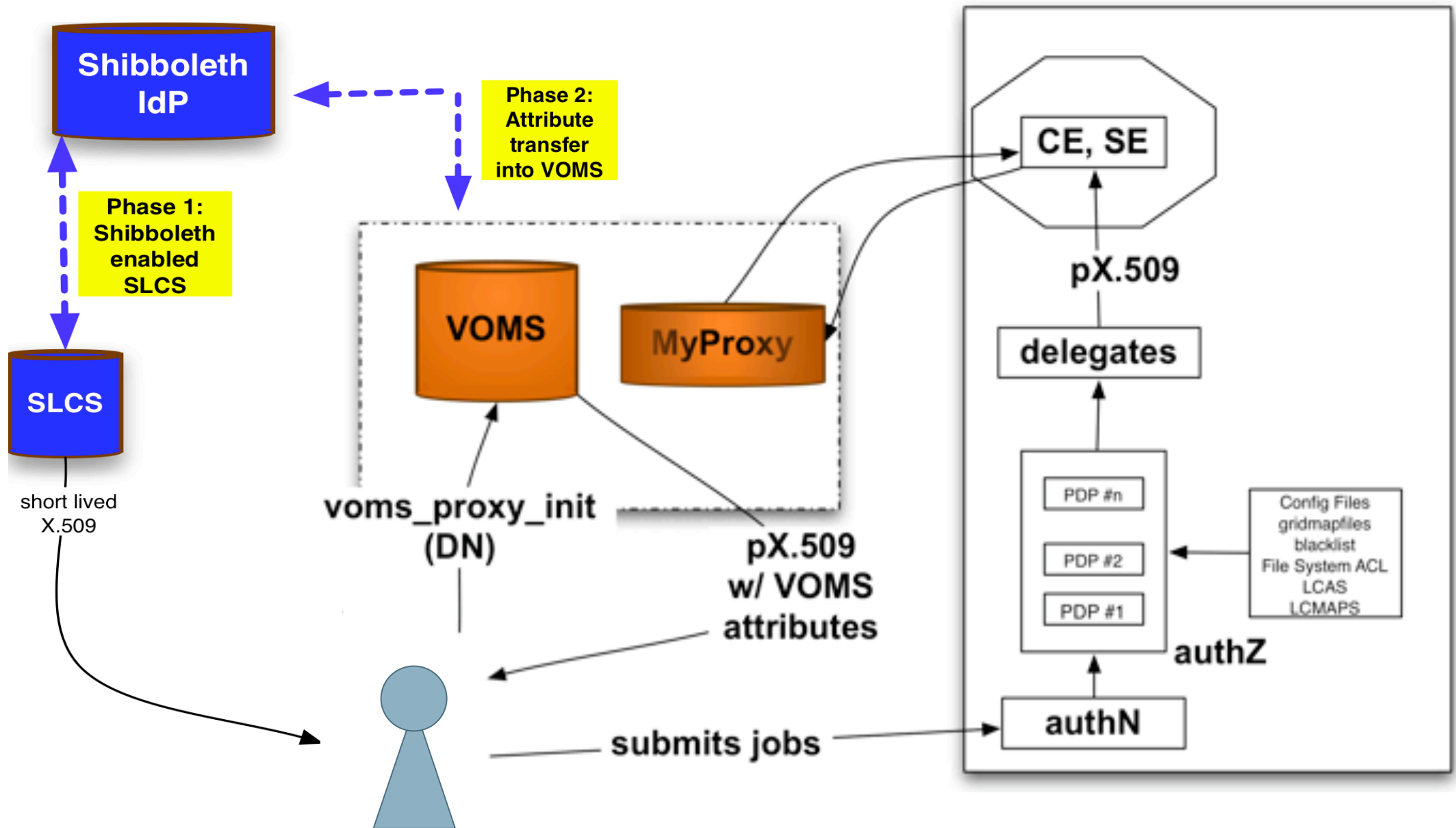
**Thomas Lenggenhager, SWITCH**  
presenting work done by SWITCHgrid team

## Bringing Shibboleth & gLite together work of SWITCHgrid team is part of EGEE-II

- **Phase 1**
  - **Short-lived credential service → SLCS**
  
- **Phase 2**
  - **VOMS Attributes from Shibboleth → VASH**

- **Focus**
  - 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**
  - Identity provider is the home institution of the user
  - Home institution provides some attributes
  - Grid-VO is needed for grid specific attributes

# Overview Phase 1 and 2



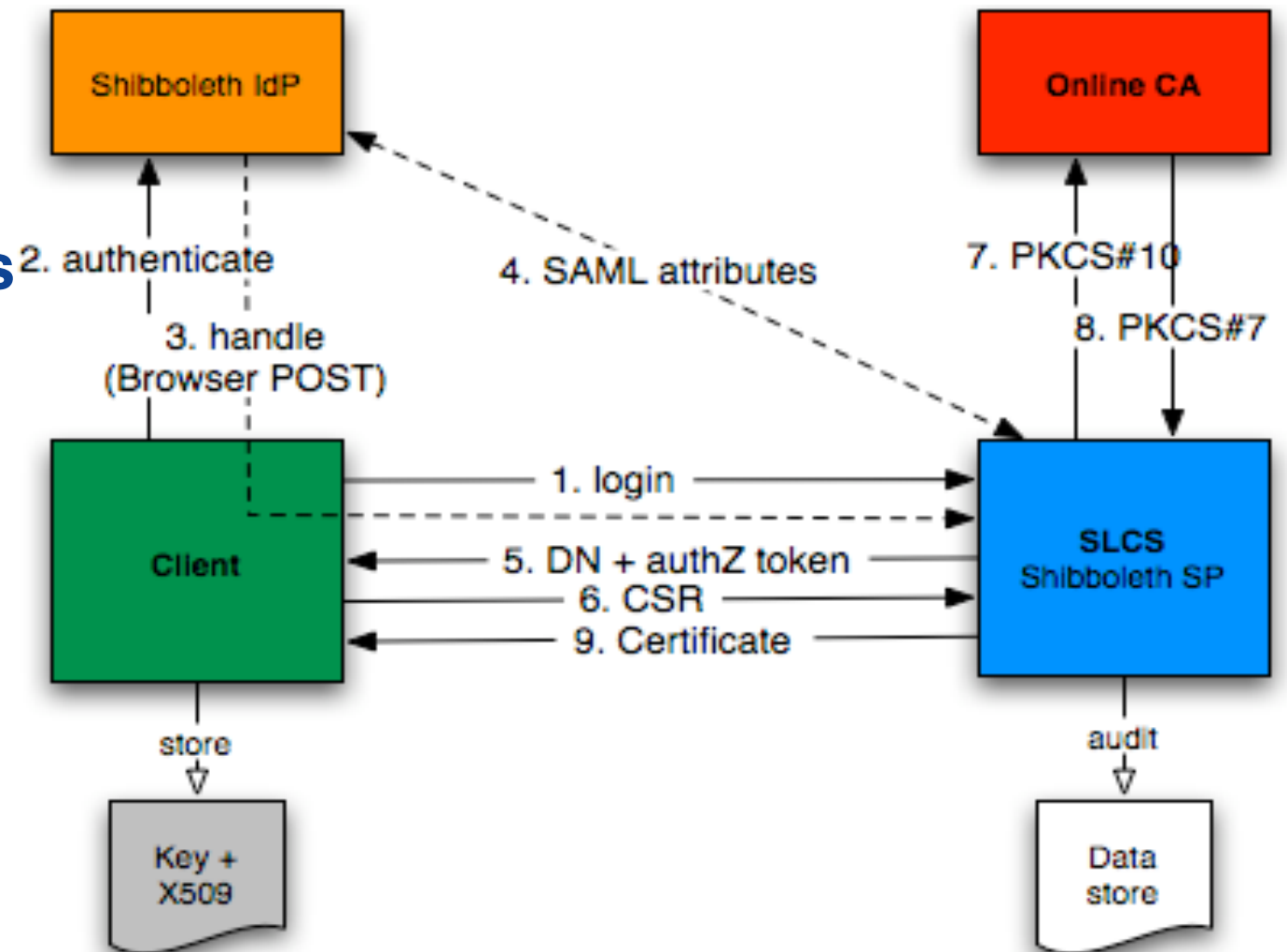
- **SLCS CA and “VOMS SP” should be independent of each other**
  - **Separate Service Providers**
  - **Deployed independently**
- **SLCS CA should be independent of the Grid middleware**
- **VOMS SP should only be dependent on VOMS**

- **SLCS: short-lived credential service**
- **IGTF profile**
  
- **Minimum requirements**

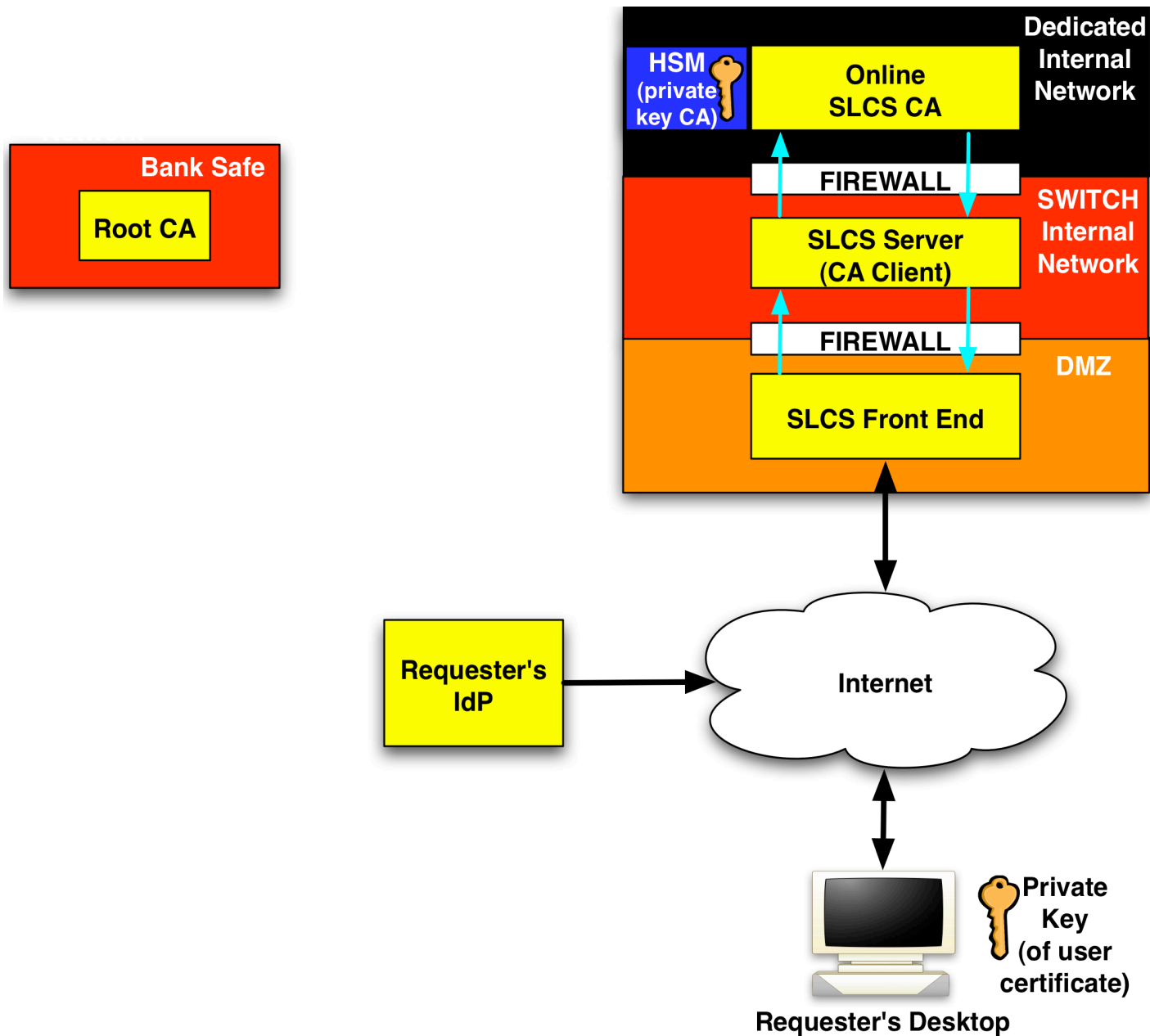
	<b>SLCS</b>	<b>X.509 Certificate</b>
<b>Identity Checking</b>	<b>Certificate generated based on Identity Management system</b>	<b>«traditional» RA (e.g. passport)</b>
<b>Lifetime</b>	<b>&lt; 1mio sec (ca. 11 days)</b>	<b>&lt; 1 year + 1 month</b>
<b>Revocation Handling</b>	<b>optional</b>	<b>mandatory</b>

- **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

- Private key is never transferred
- Use commercial CA and only standard protocols
- Modular design that others can reuse components
- Shibboleth attributes determine DN



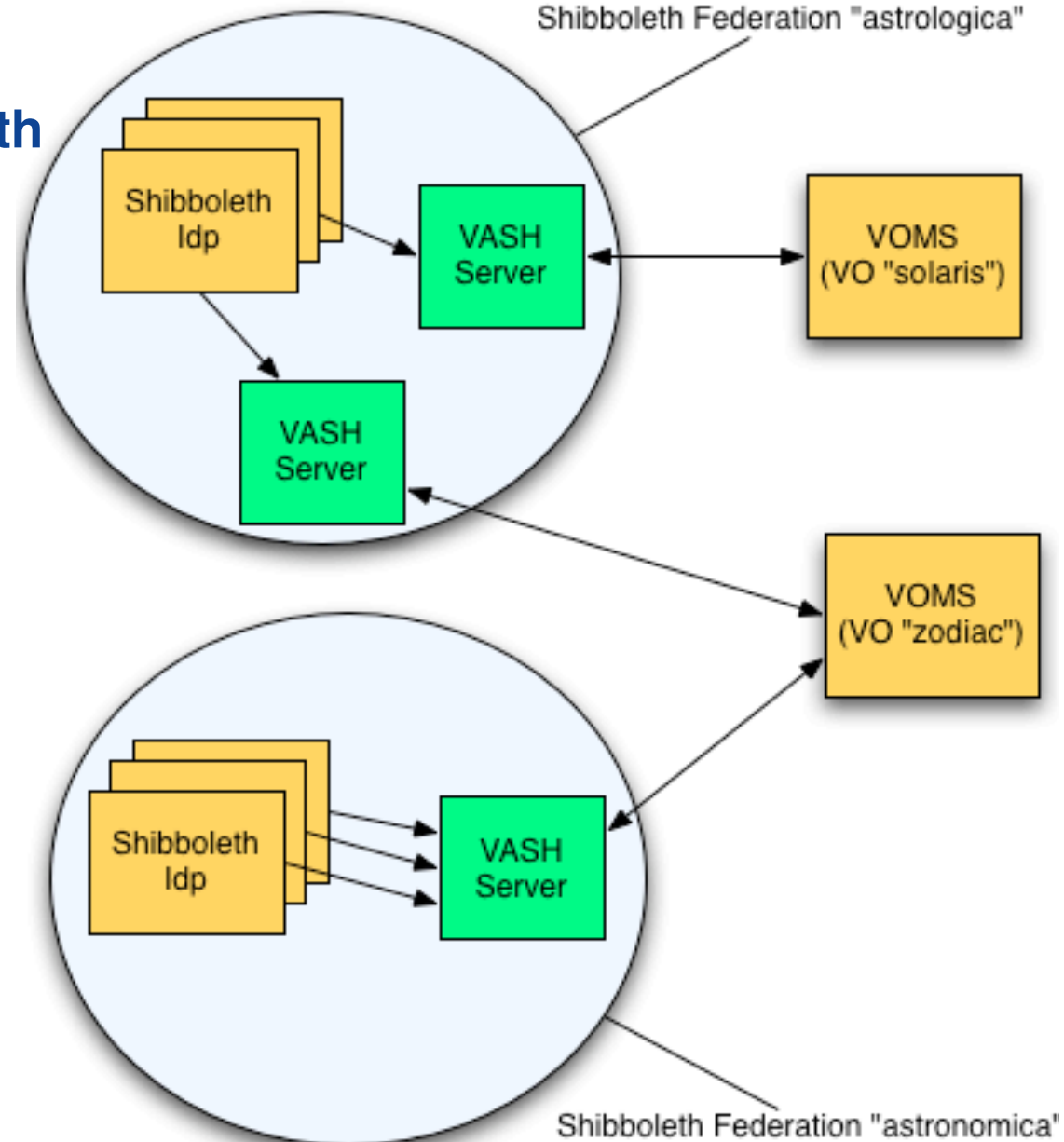
# SWITCHslcs: CA Setup



- **Phase 1 ties**
  - **AAI authentication to issue an 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**

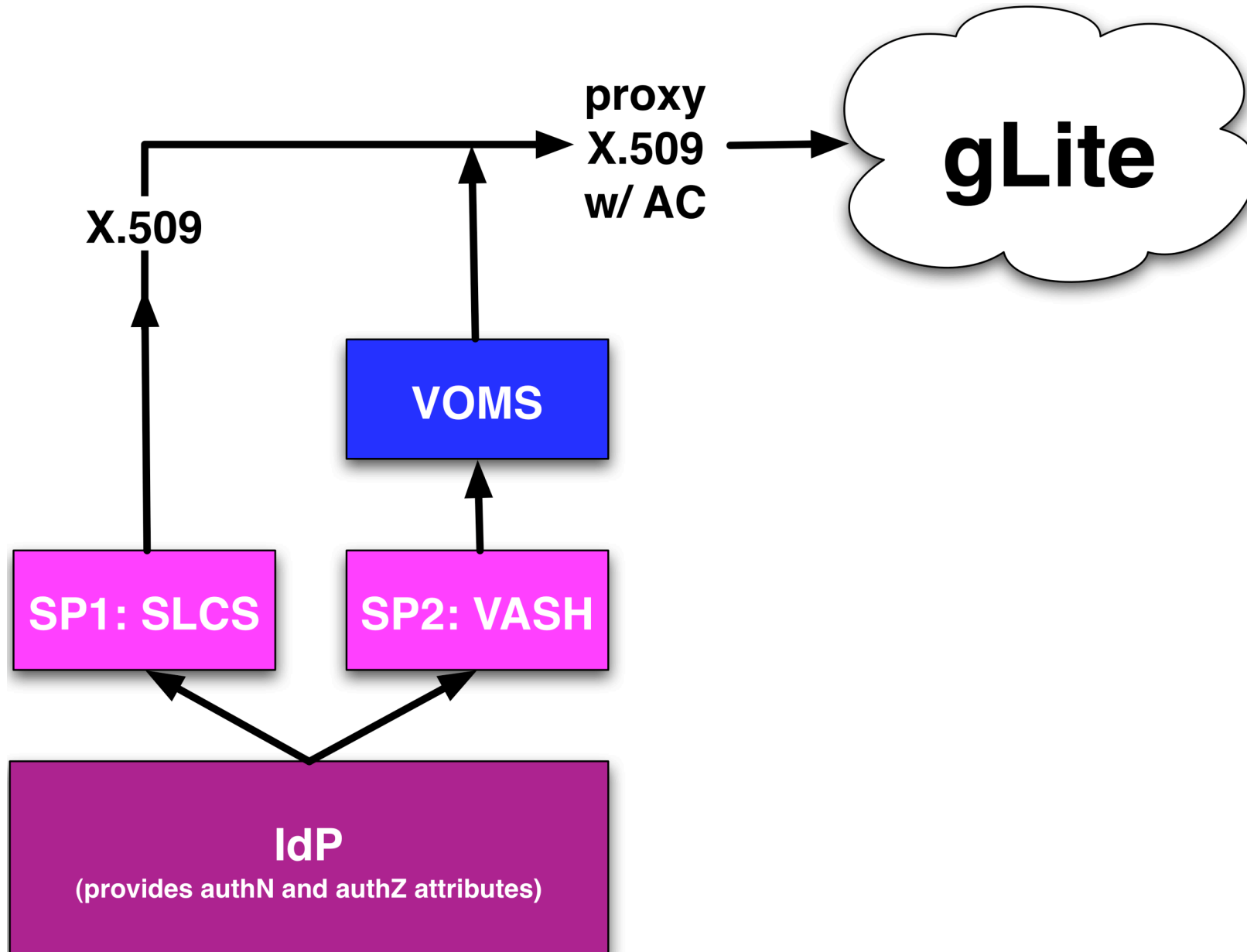
## VASH

- VOMS Attributes from Shibboleth
- VASH Server
  - Browser-based Shibboleth SP
  - One per Federation and per VO
- «lightweight» SP
  - No administrator duties
  - No management of attributes
  - Simply transfers attributes to VOMS upon user request



- **VOMS Attribute Certificates unchanged**
- **No change in VOMS**
  - Needs version 1.7.10 or newer
- **VO registration unchanged**
- **Administrative domains decoupled  
Shibboleth federation and VOMS**
- **User links DN in VOMS with a Shibboleth unique identifier**

# Summary Phase 1 & 2



- **SLCS**
  - **EGEE MJRA1.4 document**
  - <https://edms.cern.ch/document/770102/1>
  - **CP/CPS**
    - **Accredited by EuGridPMA**
    - <http://www.switch.ch/pki/grid>
- **VASH**
  - **EGEE MJRA1.5 document**
  - <https://edms.cern.ch/document/807849/1>
- **Further Information**
  - <http://www.switch.ch/grid>