Shibboleth for Grid Portals

Christoph Witzig, SWITCH

EGEE07 conference - 4.10.2007

www.eu-egee.org

Information Society and Media

Outline

- **Introduction to Shibboleth**
- **Shibboleth and gLite integration**
  - SLCS and VASH
- **Integration of Shibboleth in Grid Portals**
  - gLiteShib for Portal
- **Summary**

Shibboleth

- **Federated Identity**
- **Based on SAML**
  (Security Assertion Markup Language)

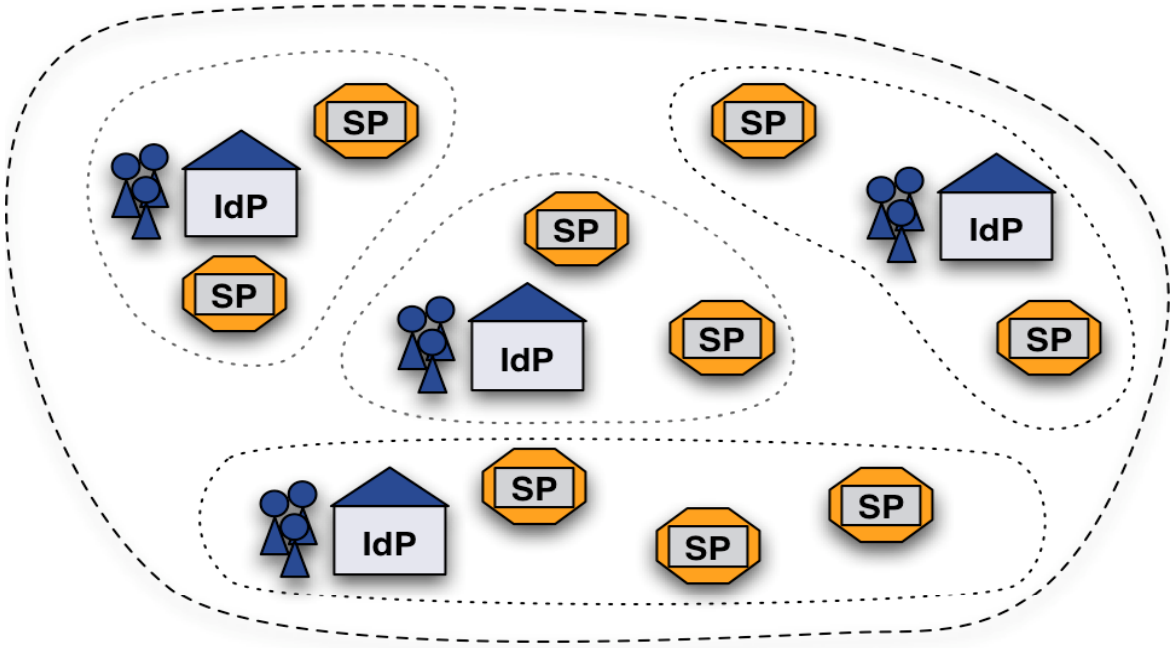
- **Web resources SSO (Single Sign-On)**
- **Open Source**
- **Developed by Internet2**

Shibboleth®

http://shibboleth.internet2.edu

Federated Identity

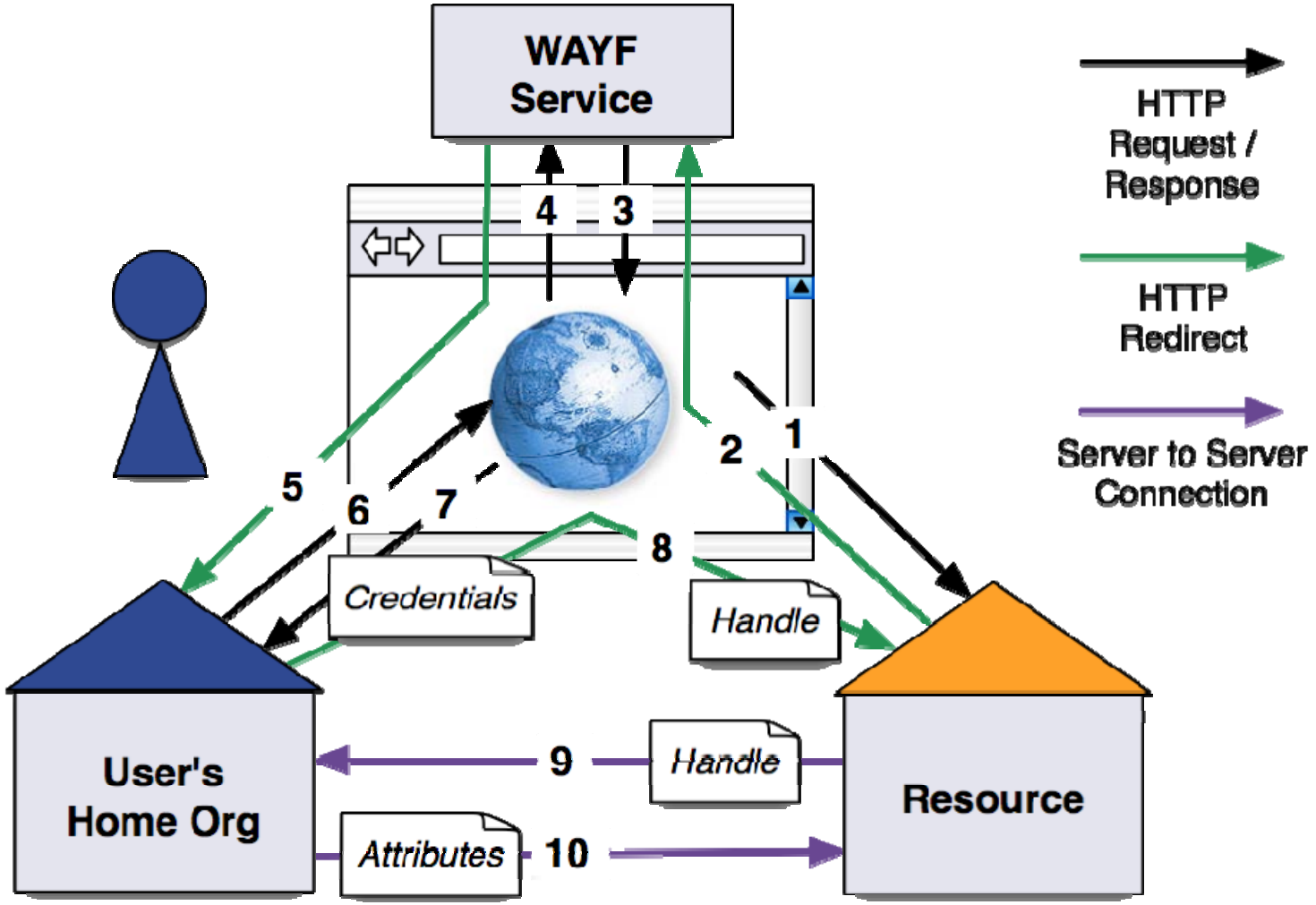
- Identity Providers (IdP) authenticate their users
- Service Providers (SP) trust the Identity Providers (IdP) and authorize the users
- Cross domain authentication and authorization based on trust relation



International Coverage

- **Growing coverage of Shibboleth based federations**
- **In production**
  - Finland - HAKA
  - France - CRU
  - Switzerland - SWITCHaai
  - UK - UK Access Management Federation
  - US - InCommon (and further federations on state level)
- **In pilot or preparation phase**
  - Australia - MAMS test bed
  - Belgium - Associatie K.U.Leuven
  - Czech Republic
  - Denmark - DK-AAI
  - Germany - DFN-AAI
  - Slovenia
  - Sweden - SWAMID

Shibboleth Demo



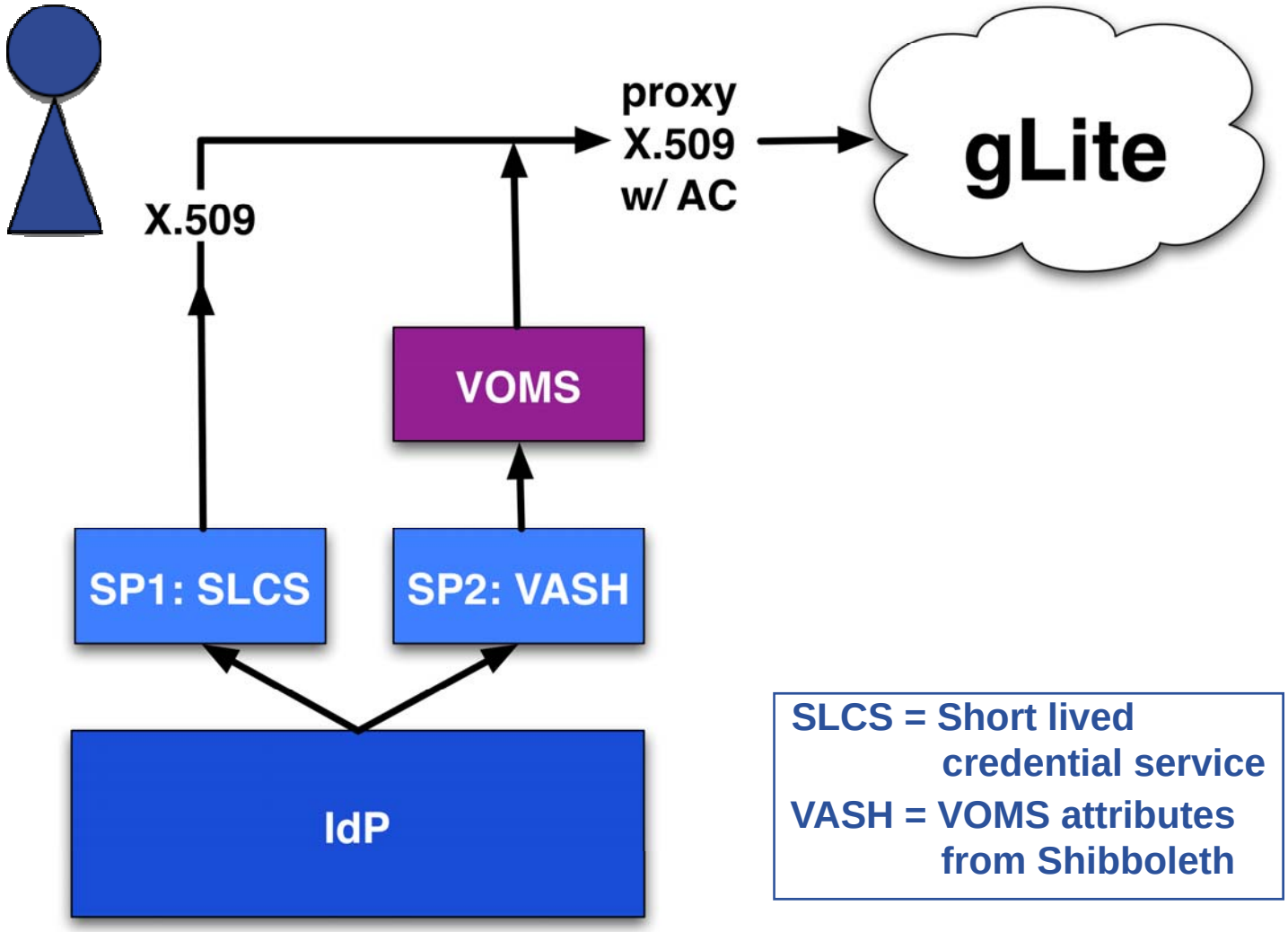
http://www.switch.ch/aai/demo

SLCS and VASH

- **SLCS (Short Lived Credential Service)**
  - Generate short-lived X.509 certificate based on Shibboleth user's attributes
  - EUGridPMA accredited
  - Already in production
- **VASH (VOMS Attributes from Shibboleth)**
  - Push Shibboleth user's attributes in VOMS
  - Proxy certificate contains the generic attributes
  - Plug-in for LCAS/LCMAPS for generic attributes available
  - Development finished

SLCS and VASH for gLite

gLite UI



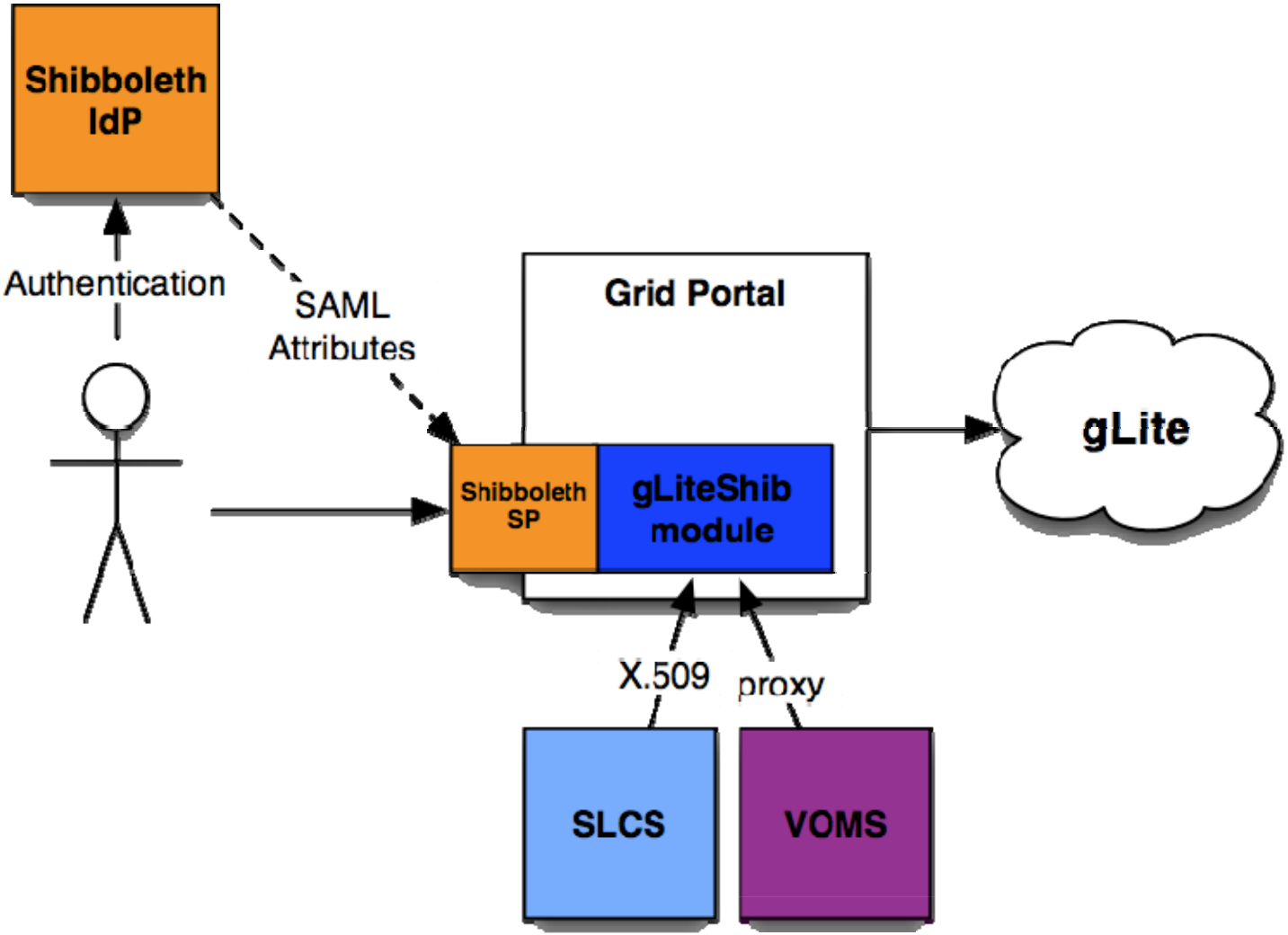
SLCS = Short lived credential service

VASH = VOMS attributes from Shibboleth

gLiteShib for Portal

- **Idea: Portal becomes Shibboleth SP**
  - Integrate Shibboleth in Portal
  - Use SLCS to generate short-lived X.509 certificate
  - Use VOMS to get proxy certificate w/AC

gLiteShib for Portal



Virtual Home Organisation

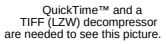
- **Problem:**
  - How to jump start the use of Shibboleth IdP's?
  - Setting up IdP's and federation building takes a lot of time
- **Virtual Home Organization (VHO)**
  - "home for the homeless" (GN2 term)
  - Operate an IdP (within or outside a federation) that provides a Shibboleth IdP account to users
    - Assurance level of this IdP must be decided (with consequences for the quality of the account)
- **VHOs can serve two purposes:**
  - Jump start a Shibboleth user community / federation
  - Provide access to certain SP for the "homeless"

VHO Implementations

- **SWITCHaai VHO**
  - Written and maintained by SWITCH, open source
  - V2 now being deployed
  - Used to provide access to certain SP for non-SWITCHaai users
  - User accounts are maintained by SP administrator

- **GN2 JRA5 VHO (edugain)**
  - Written from scratch based on SWITCH VHO v1
    - In close collaboration with SWITCH

SWITCHaai VHO Screenshots



SWITCHaai VHO Screenshots (2)

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Next Steps

- Portal work currently not in the default workplan for EGEE-2 or EGEE-3
- Depending on recommendation of Portal WG and/or clear need from user community we would add this to our workplan
- Deliverable: framework with which portal builders can easily create Shibboleth-enabled portals

Summary

- **Integrate existing components in Portal**
  - Reuse Shibboleth, SLCS and VOMS
- **Leverage existing Identity Management Systems**
  - Semi-automated users management in Portal
- **User friendly**
  - Same credential as usual
  - No certificate problem anymore

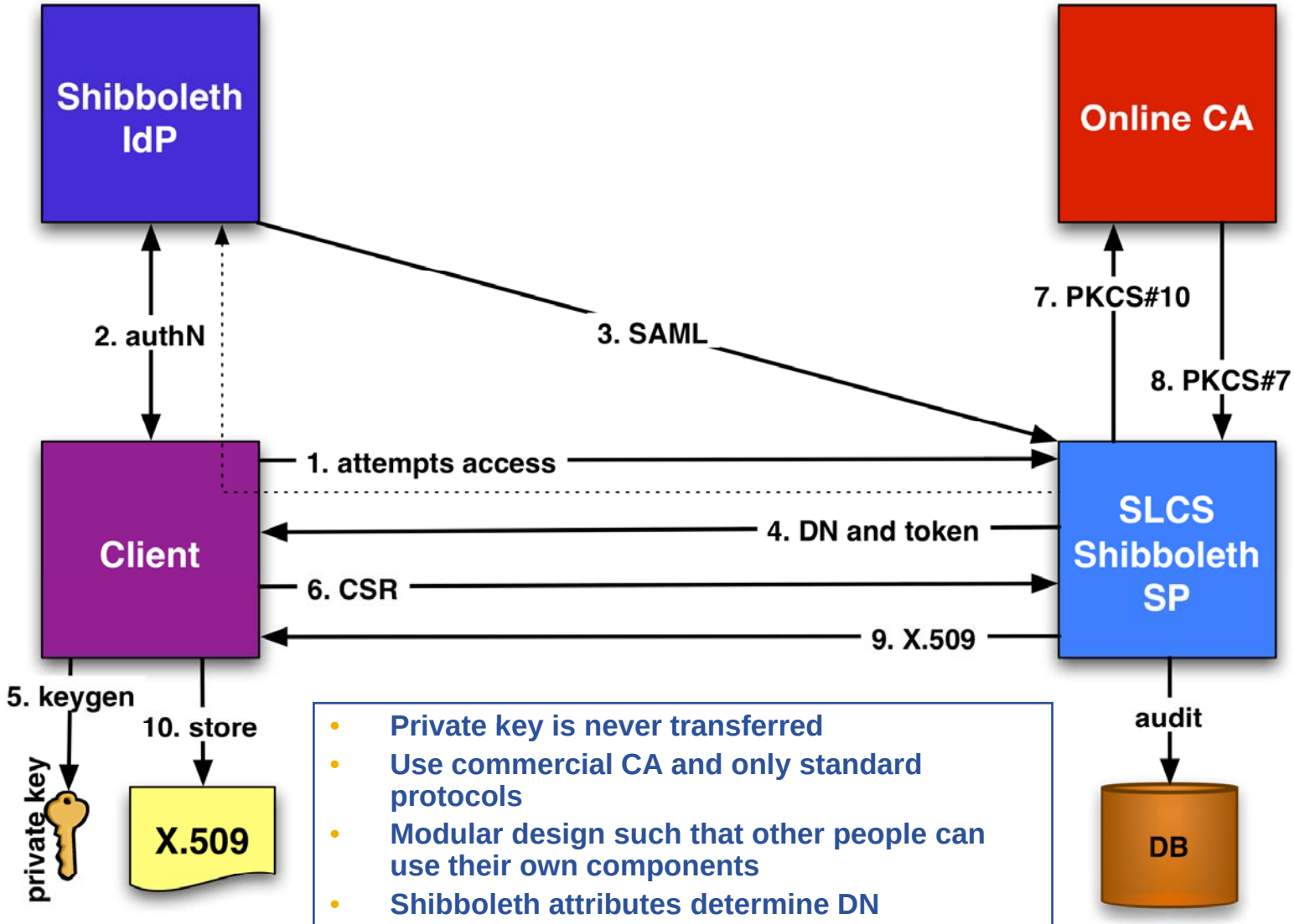
Q & A

SLCS Profile

- 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

SLCS



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