SWITCH

The Swiss Education & Research Network

X.509 user certificates in the Grid world: current state and future directions

SWITCHpki RAO Meeting
Mar 28, 2006

Christoph Witzig
SWITCH

Outline

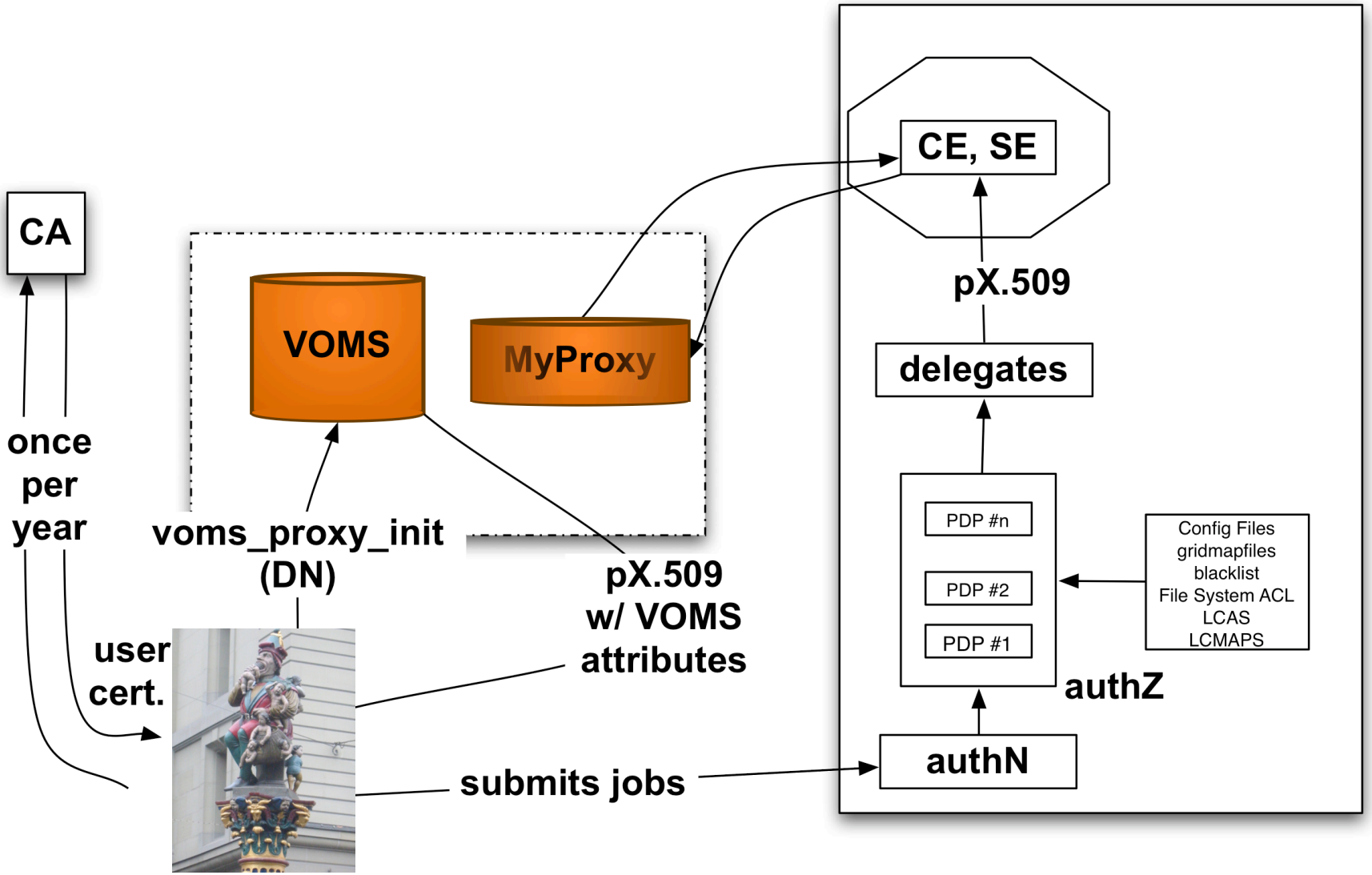
SWITCH
The Swiss Education & Research Network

- X.509 Certificates in the Grid World ?
- SLCS - a slick solution for a slick problem ?
- Policy issues
- Future Steps
- Discussion

„slick“ = geschickt, glatt, glitschig

X.509 in the Grid World

SWITCH
The Swiss Education & Research Network



SLCS - a slick solution for a slick problem?

SWITCH
The Swiss Education & Research Network

- SLCS = short lived credential service

- Idea: map local credentials to a X.509 certificate
  - but only for a short time
  - just to access the grid

- But …
  - Use weaker form of authN to obtain stronger form of authN?
  - How do they relate to long lived X.509?
  - Who should issue SLCS - every institution - how about trust?

Minimum requirements

SWITCH
The Swiss Education & Research Network

Minimum requirements for SLCS and traditional user certificates

SLCS	Traditional user certificates
Several SLCS	One CA per country
Automated generation based on user management system	“Traditional” RA (e.g. copy of passport)
Lifetime < 1mio sec	Lifetime < 1year + 1month
Revocation handling optional	Revocation handling mandatory

Profiles of EUGRIDPMA and TAGPMA

Policy Issues

SWITCH
The Swiss Education & Research Network

- **Question 1: why two minimum requirements documents?**
  - **Wouldn't it be easier to have one document and simply state the differences where appropriate?**

- **Question 2: Why distinguish between SLCS and "traditional" certificates?**
  - **If you really trust your identity management systems, why not generate the traditional certificates?**

Interoperability SWITCHaai - gLite

SWITCH
The Swiss Education & Research Network

- SWITCH joined the grid project “Enabling Grids for E-sciencE” EGEE-II
- 2-year project, co-financed by the EU (FP6)
- Work item “interoperability Shibboleth - gLite”
- authN, authZ on the grid based on SWITCHaai
- Work in three phases
  - Phase 1 consists of a “shibbolized credential service”

X.509 and SWITCHaai

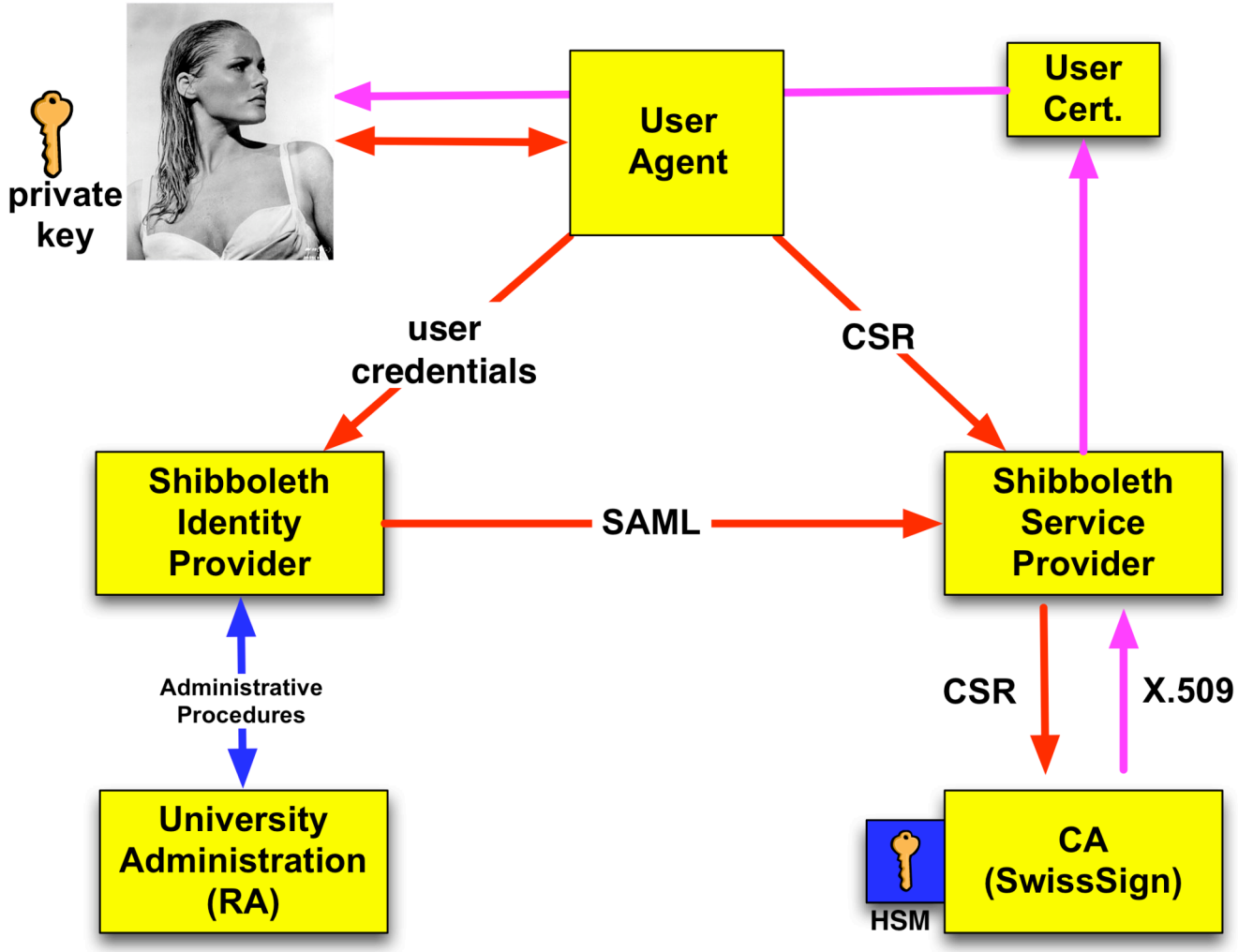
SWITCH
The Swiss Education & Research Network

Generation of X.509 by Shib Service Provider based on AuthN at IdP

User generates key pair and submits certificate signing request

Admin. Procedures are key for quality of user management System (EUGRIDPMA compliant)

Different kinds of assurance levels



Issue of certificates by SWITCHpki

SWITCH
The Swiss Education & Research Network

- **Generation of long lived X.509 based on SWITCHaai is not desirable at this point**
  - **No assurance levels in SWITCHaai**
  - **Shouldn't generate strong form of authN based on a weak form of authN (username/password)**

- **Envisaged workplan:**
  - **Use SWITCHaai for generating short lived certificates (for use by the grid community)**
    - **Summer/fall 2006**
  - **Introduce assurance levels and strong authN in SWITCHaai**
    - **2006 / 2007**
  - **Use SWITCHaai for distributing long lived certificates**

Advantages

SWITCH
The Swiss Education & Research Network

- One set of requirements for all certificates
  - simplicity of policy
- One infrastructure to handle all certificate requests
- Only valid or revoked certificates at all times
- Capitalize on the high standards of the user management system of SWITCHaai
  - for those institutions who follow the more stringent requirements

Summary

SWITCH
The Swiss Education & Research Network

- **Long term goal of using SWITCHaai authN for issuing X.509 certificates**
- **Medium term goal: short lived credential service**
- **Many technical "details" need to be solved soon, among them**
  - **X.509 DN = function(SWITCHaai attributes)**
  - **Policy (EUGRIDPMA accredited)**
  - **SwissSign**
  - **Archiving / auditing**

Discussion

SWITCH
The Swiss Education & Research Network

Q & A

???