SWITCH

The Swiss Education & Research Network

SWITCHslcs

the new AAI-based short-lived credential service for Grid users

C.Witzig (witzig@switch.ch)

2nd SWITCHpki RAO Meeting, Berne, April 18, 2007

Outline

SWITCH
The Swiss Education & Research Network

Introduction

- SLCS
- SWITCH work in EGEE-II: Interoperability Shibboleth - gLite

SWITCHslcs Software Design

SWITCHslcs Hardware Layout

Registration Procedures and IdP Account Provisioning in SWITCHaai

CP/CPS Highlights

Current Status - Next Steps

What is it?

SWITCH
The Swiss Education & Research Network

SLCS Profile

SWITCH
The Swiss Education & Research Network

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

Outline

SWITCH
The Swiss Education & Research Network

Introduction

- **Shibboleth**
- **SWITCH work in EGEE-II: Interoperability Shibboleth - gLite**

SWITCHslcs Software Design

SWITCHslcs Hardware Layout

Registration Procedures and IdP Account Provisioning in SWITCHaai

CP/CPS Highlights

Current Status - Next Steps

Shibboleth and grids

SWITCH
The Swiss Education & Research Network

SWITCH was an early adopter of Shibboleth, but in the meantime Shibboleth federations are being deployed and operated in many countries

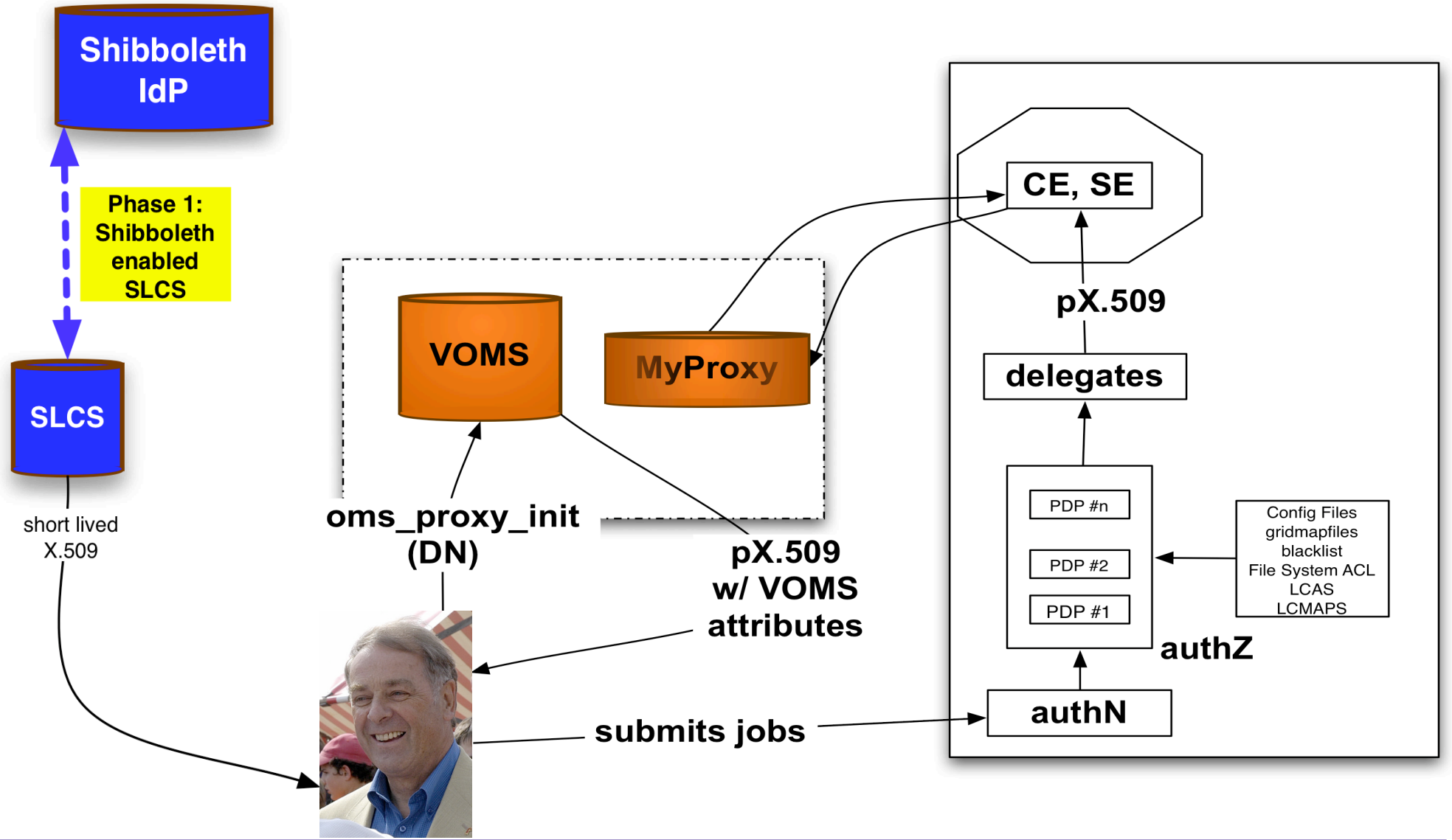
US, Finland, UK, Australia, Belgium, France as well as others

Interest to leverage these (national) campus infrastructures against grids

SAML vs X.509 user certificates

Grid Security Model and SLCS

SWITCH
The Swiss Education & Research Network



Outline

SWITCH
The Swiss Education & Research Network

Introduction

SWITCHslcs Software Design

SWITCHslcs Hardware Layout

Registration Procedures and IdP Account Provisioning in SWITCHaai

CP/CPS Highlights

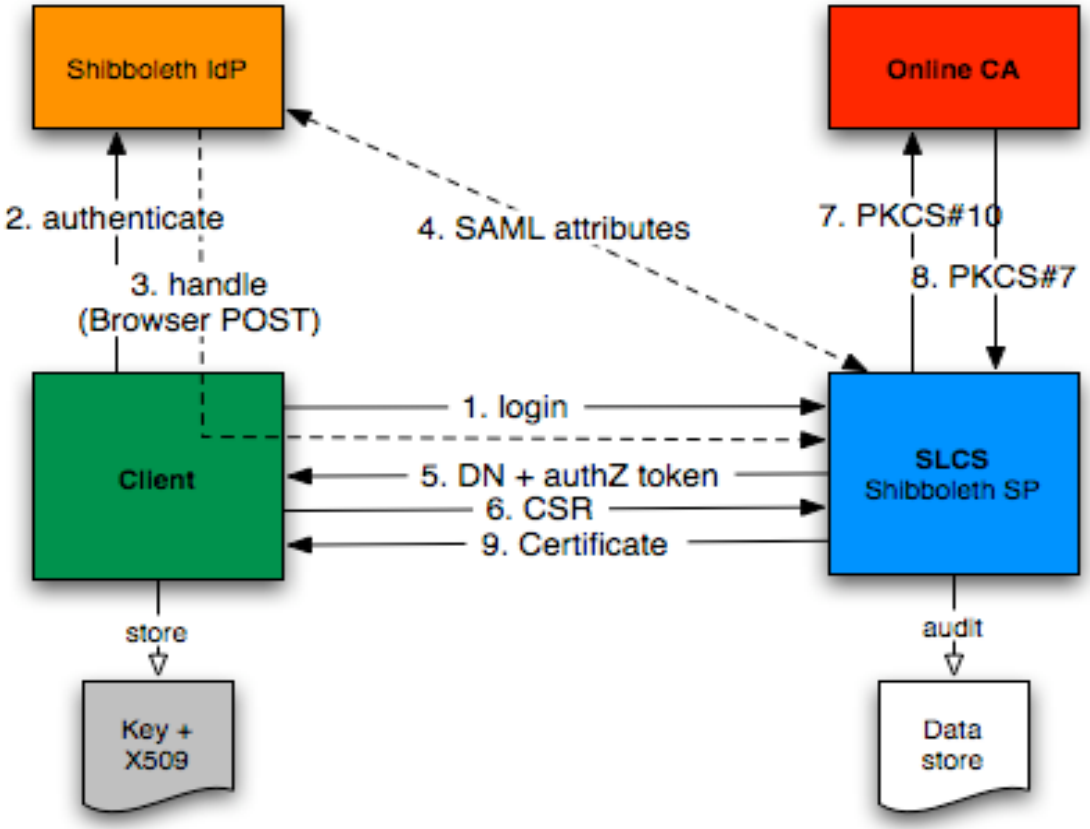
Current Status - Next Steps

SWITCHslcs

SWITCH
The Swiss Education & Research Network

Design goals:

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



Outline

SWITCH
The Swiss Education & Research Network

Introduction

SWITCHslcs Software Design

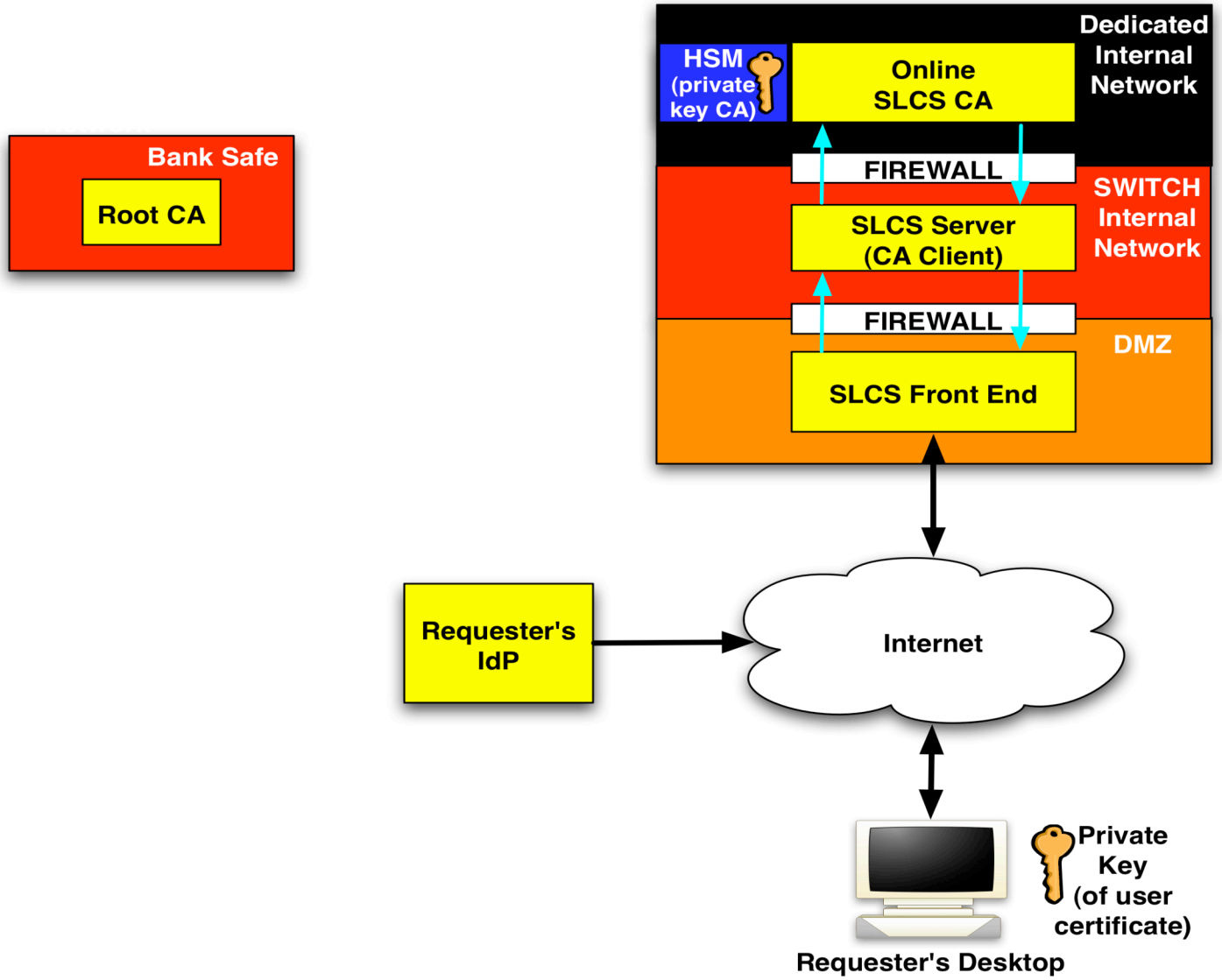
SWITCHslcs Hardware Layout

Registration Procedures and IdP Account Provisioning in SWITCHaai

CP/CPS Highlights

Current Status - Next Steps

SWITCHslcs: CA Setup (1)



SWITCHslcs: CA Setup (2)

SWITCH
The Swiss Education & Research Network

Setup involves three servers in increasingly secure environment (network, physical access)

Front end: Apache with Shibboleth Service Provider

- **In DMZ**

SLCS server:

- **Debian OS**
- **Java + Tomcat + mySQL**
- **Has only Webapp services running**
- **In a highly secure network**

CA Server

- **MSCS**
- **Has only CA relevant services running**
- **In a dedicated network**
- **HSM: nCipher nShield F2 500 (FIPS 140-2 level2)**

SWITCHslcs: Operation

SWITCH
The Swiss Education & Research Network

- For the user:
  - from the command line: invisible
  - may also access it from the browser (not part of version 1.0)
- For the RA from web-based admin tool:
  - Can enable or disable individual users (only for his institution)
  - 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*)

Outline

SWITCH
The Swiss Education & Research Network

Introduction

SWITCHslcs Software Design

SWITCHslcs Hardware Layout

Registration Procedures and IdP Account Provisioning in SWITCHaai

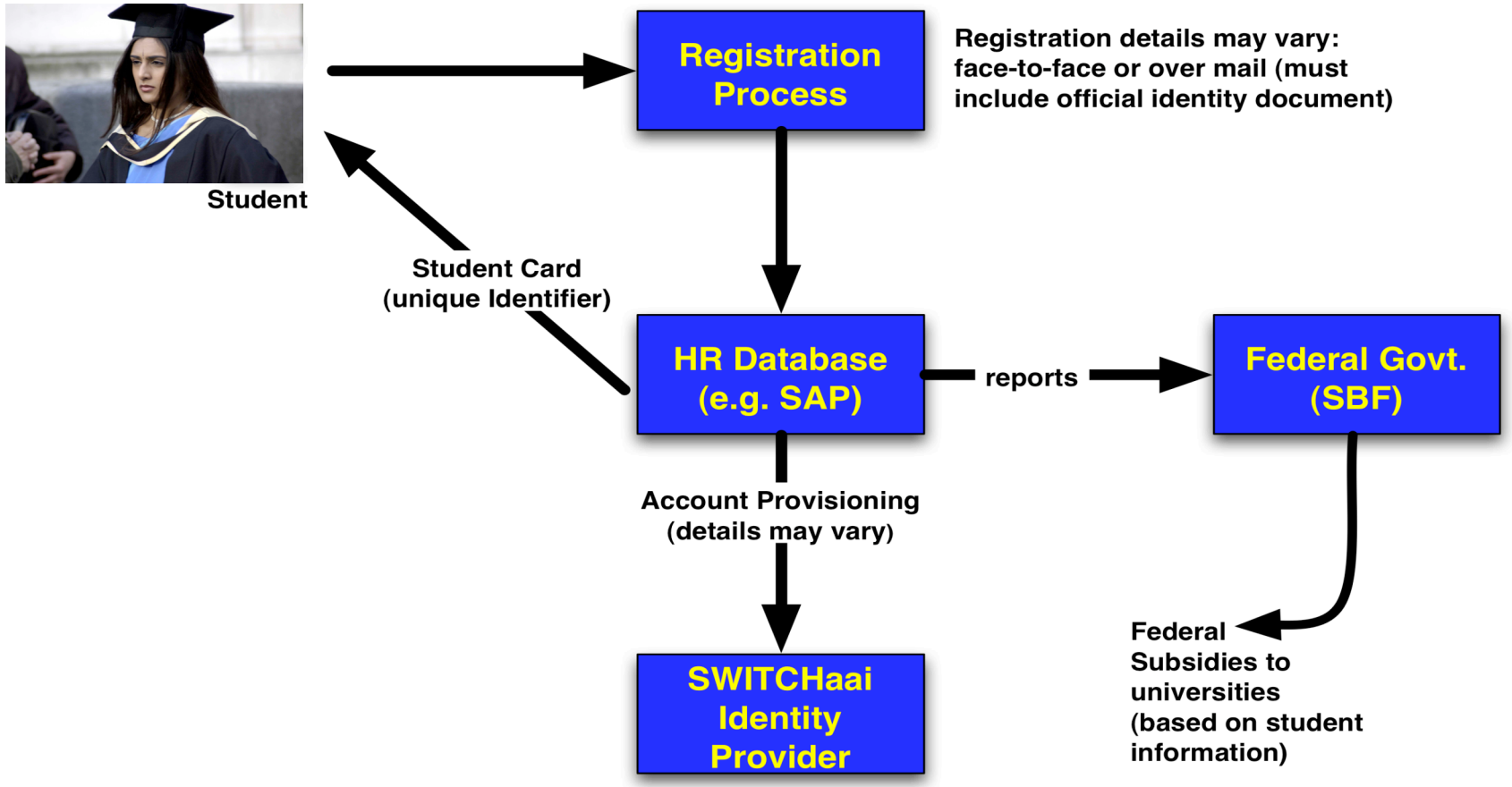
CP/CPS Highlights

Current Status - Next Steps

Registration Procedures (1)

SWITCH
The Swiss Education & Research Network

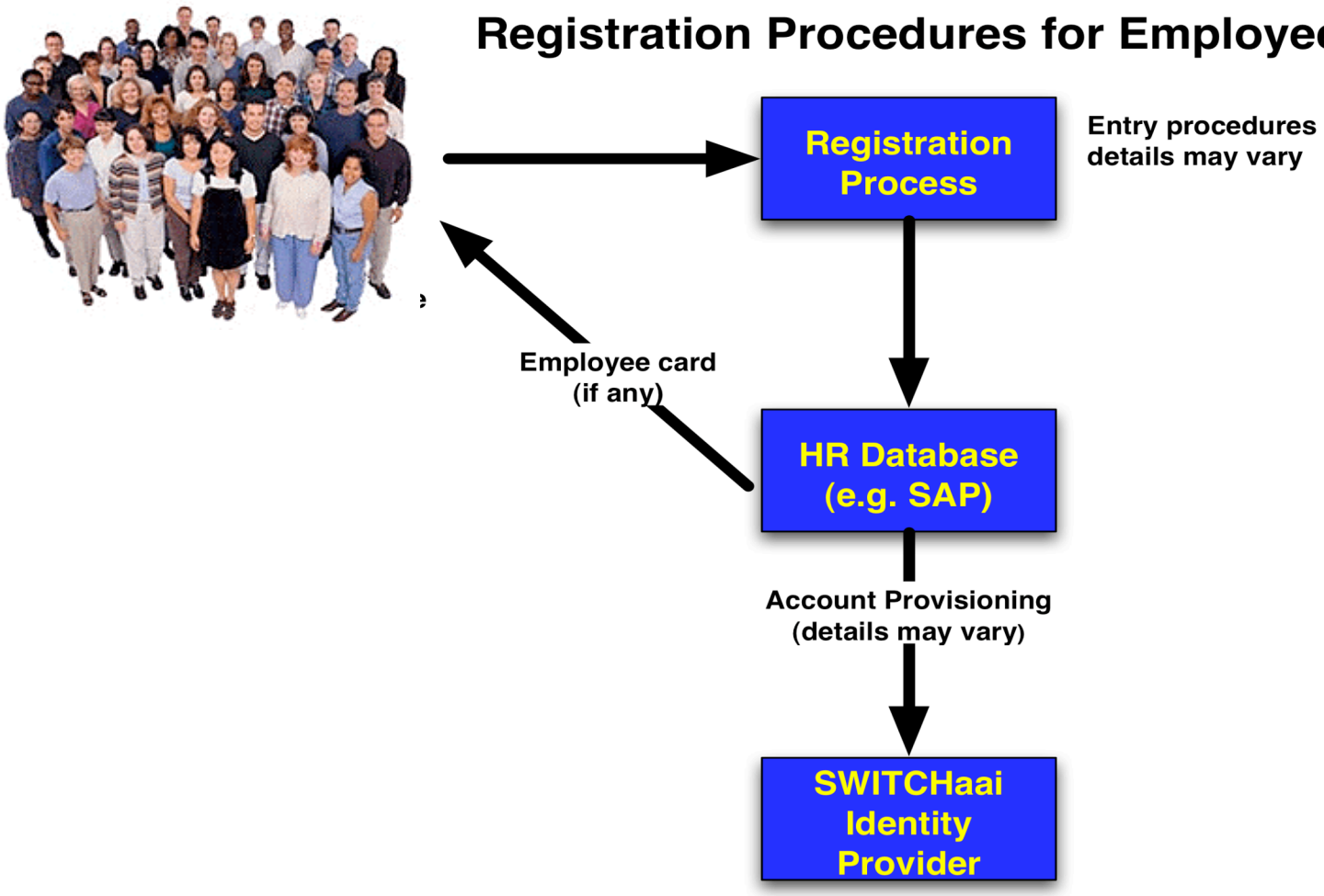
Registration Procedures for Student



MatrikelNummer =
Unique Identifier

Registration Procedures (2)

SWITCH
The Swiss Education & Research Network



Virtual Home Organisation

SWITCH
The Swiss Education & Research Network

SWITCHaai Resources should also be made available to users

- Whose home institution does not yet operate an identity provider
- Whose home institution is not a member of the SWITCHaai federation

Resource administrator can register these users in the “virtual home organisation” (VHO)

Outline

SWITCH
The Swiss Education & Research Network

Introduction

SWITCHslcs Software Design

SWITCHslcs Hardware Layout

Registration Procedures and IdP Account Provisioning in SWITCHaai

CP/CPS Highlights

Current Status - Next Steps

CP/CPS (1)

SWITCH
The Swiss Education & Research Network

Root CA: SWITCHgrid CA

- Offline in safe
- “standard” CP/CPS (based on J.Jensen’s example)
- Note: no relation to SwissSign
- Long term objective to also use commercial CA

Subject CA SWITCHslcs CA

CP/CPS (2)

SWITCH
The Swiss Education & Research Network

Definition of DN

For member of an IdP institution:

- *DC=ch, DC=switch, DC=slcs*
- *O=<legal name of the institution>, CN=<firstname lastname uniqueID>*

For member of a VHO:

- *DC=ch, DC=switch, DC=slcs*
- *OU=SWITCHaai Virtual Home Organization, CN=<firstname lastname uniqueID>*

uniqueID: makes sure DN is unique (an integer in hex format)

CP/CPS (3)

SWITCH
The Swiss Education & Research Network

Initial Identity Validation

Because registration processes vary in details, we intend not to formulate a procedure, but requirements that the IdP must fulfill to enable access to the SLCS

Requester must contact RA

How: TBD by RA

RA enables access if

1. **User has valid AAI account**
2. **a set of conditions are fulfilled (see next slide)**

Requester can access SLCS

(after successful AAI log-on)

CP/CPS (4)

SWITCH
The Swiss Education & Research Network

Conditions to access SLCS

Account creation was dependent on a process which had one of the following properties:

Issuance of an identity card, which gives its holder monetary benefits

AAI account has direct one-to-one relationship to human resource data, which is used for salary payments

Face-to-face registration with the RA, which included proof of ownership of passport or other official identity card.

(Note: Option 3 corresponds to the “classic” face-to-face registration)

CP/CPS (5)

SWITCH
The Swiss Education & Research Network

Other stipulations:

Logging information at

- CA (MSCS CA)
- SLCS (text files, database)

Certificates have 1 mio sec lifetime

No revocation mechanism

Status

SWITCH
The Swiss Education & Research Network

Software development is finished in January 2007

Accreditation by EuGridPMA in February 2007

Production setup in February/March

Information of home organization administrators March 30th, 2007

Information of RAO April 18th, 2007

Information of potential grid users: April 23, 2007 (email) and May 7th, 2007 (meeting)

More information

SWITCH
The Swiss Education & Research Network

Website: http://www.switch.ch/grid/slcs

SLCS administrator interface https://slcs.switch.ch/SLCS/admin

CP/CPS: http://www.switch.ch/pki/grid/

Contact:

- **For SLCS PKI related questions: pki@switch.ch**
- **For all other questions: grid@switch.ch**

Demo

SWITCH
The Swiss Education & Research Network

1. Obtaining a SLCS certificate

2. SLCS website http://www.switch.ch/grid/slcs

3. SLCS administrator web interface
   https://slcs.switch.ch/SLCS/admin

Q & A