SWISS NATIONAL GRID ASSOCIATION

SGS11: Swiss Grid School 2011

AAI, Certificates and SLCS

login to the Grid

Andres Aeschlimann SWITCH

Outline

1. AAI
2. X.509 certificates
3. Use of X.509 certificates in Grid technology
4. AAI and Grids
5. Summary

Introduction

- Starting point:
  - Distributed infrastructure

- Problem:
  - How do you manage users?
  - Solution: Authentication and Authorization Infrastructure (AAI)

- Definition of authentication and authorization
  - ***Authentication***: Process of ensuring a credential is valid and belongs to the individual that presents it.
  - ***Authorization:*** Process of checking that a person has the rights to perform an operation. Authorization can be issued based on several criteria, such as, for example,
    - the identity of the person or
    - attributes provided about the person by a trusted third party.

AAI: Authentication and Authorization Infrastructure

AAI solves the old problem of access control to resources

There are various other technologies in use - their usefulness depends on the underlying infrastructure

1. Crusader Castle
2. League of Nations
3. Federated Identity

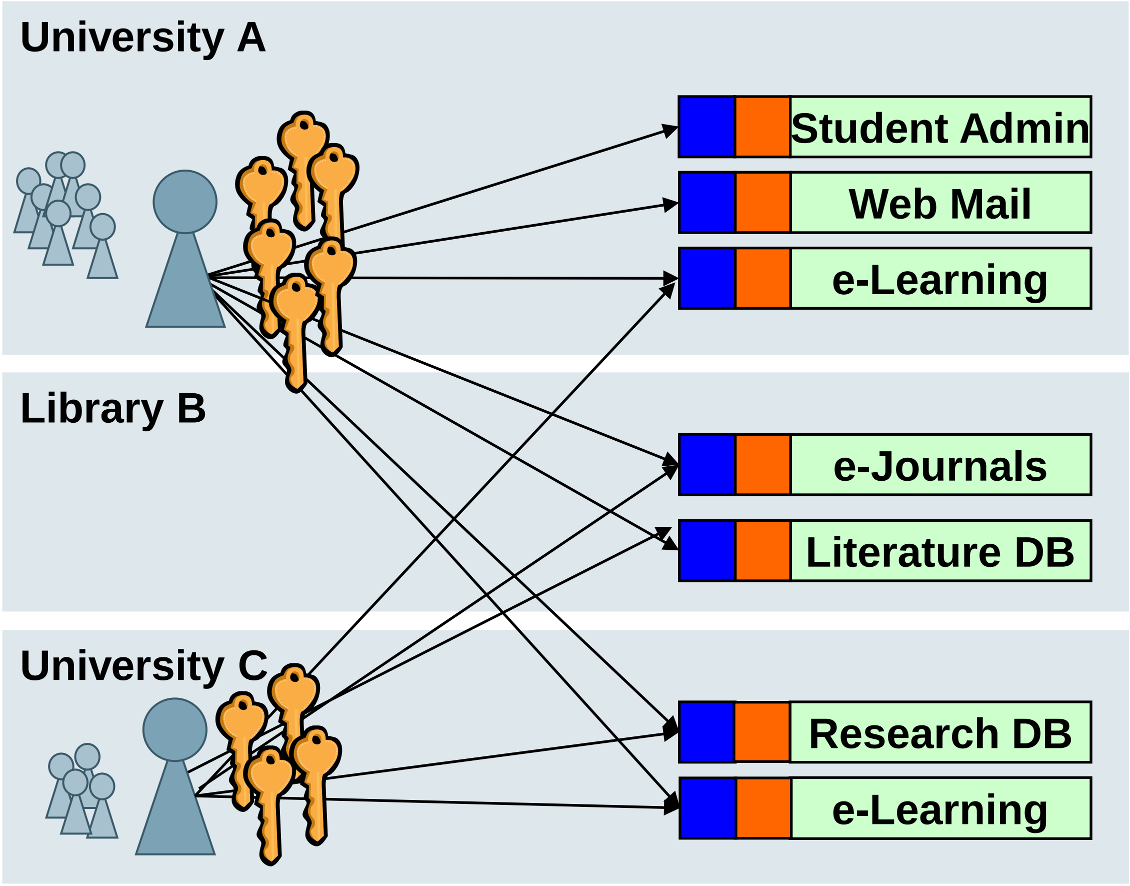
SwiNG

Crusader Castle

Reed Saxon / AP file

Appropriate for few, non-mobile users

Crusader Castle



University A

Student Admin

Web Mail

e-Learning

Library B

e-Journals

Literature DB

University C

Research DB

e-Learning

- Tedious user registration at all resources
- Unreliable and outdated user data at resources
- Different login processes
- Many different passwords
- Many resources not protected due to difficulties
- Often IP-based authorization
- Costly implementation of inter-institutional access

User Administration Authentication

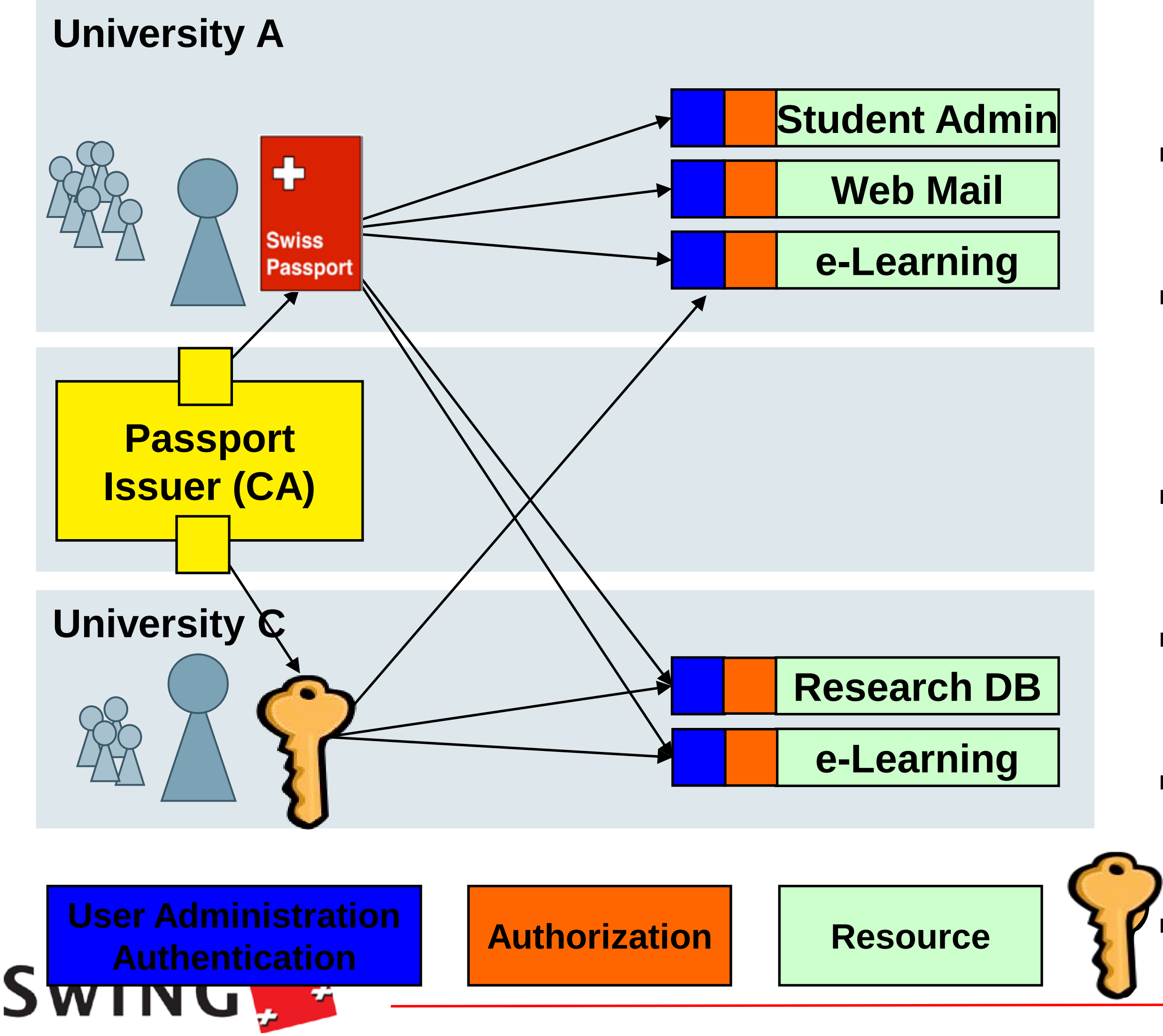
Authorization

Resource

Credentials

League of Nations

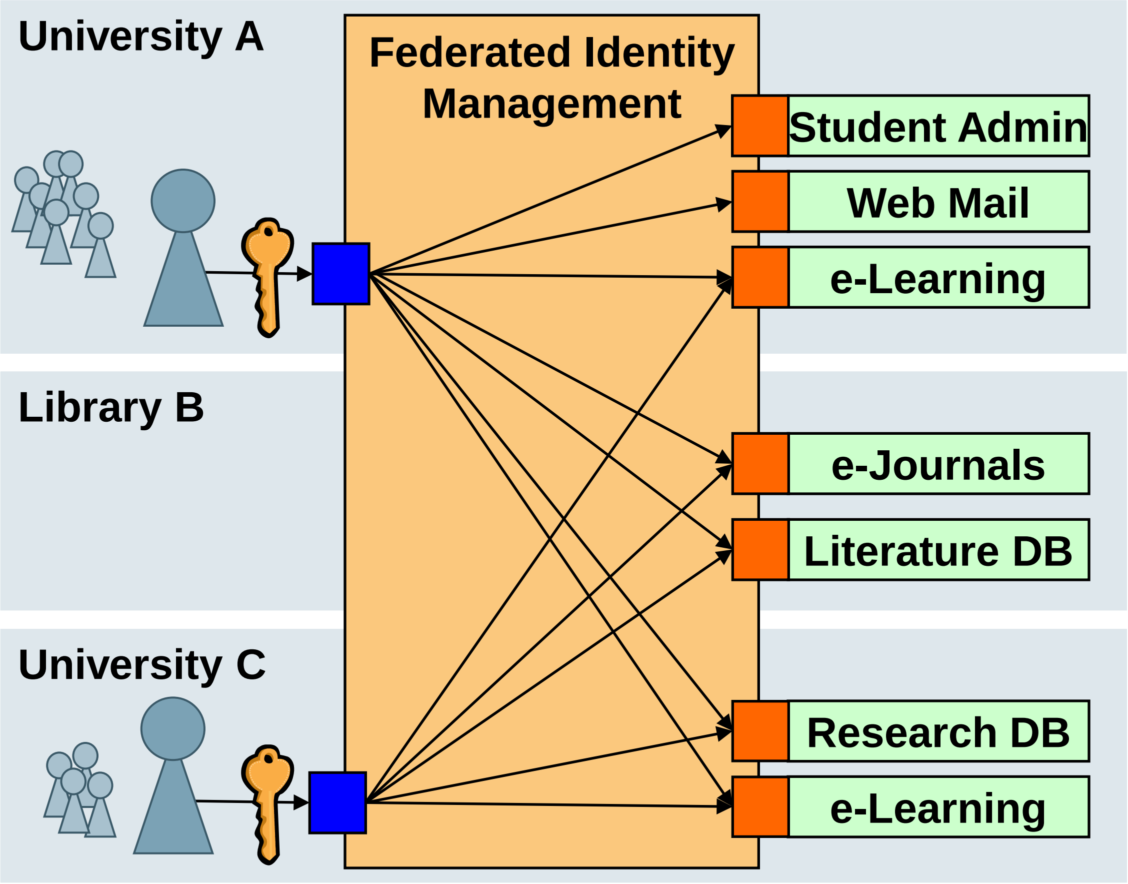
Standardized Credentials (International Conference on Passports 1920)



X.509 credentials

- User registration process with CA
- User has one credential to present to resources
- authN and authZ at resource
- User has to manage credential
- Standard use in grids (IGTF)
- Delegation mechanism

Federated Identity Management



- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Enlarged user communities for resources
- Efficient implementation of inter-institutional access

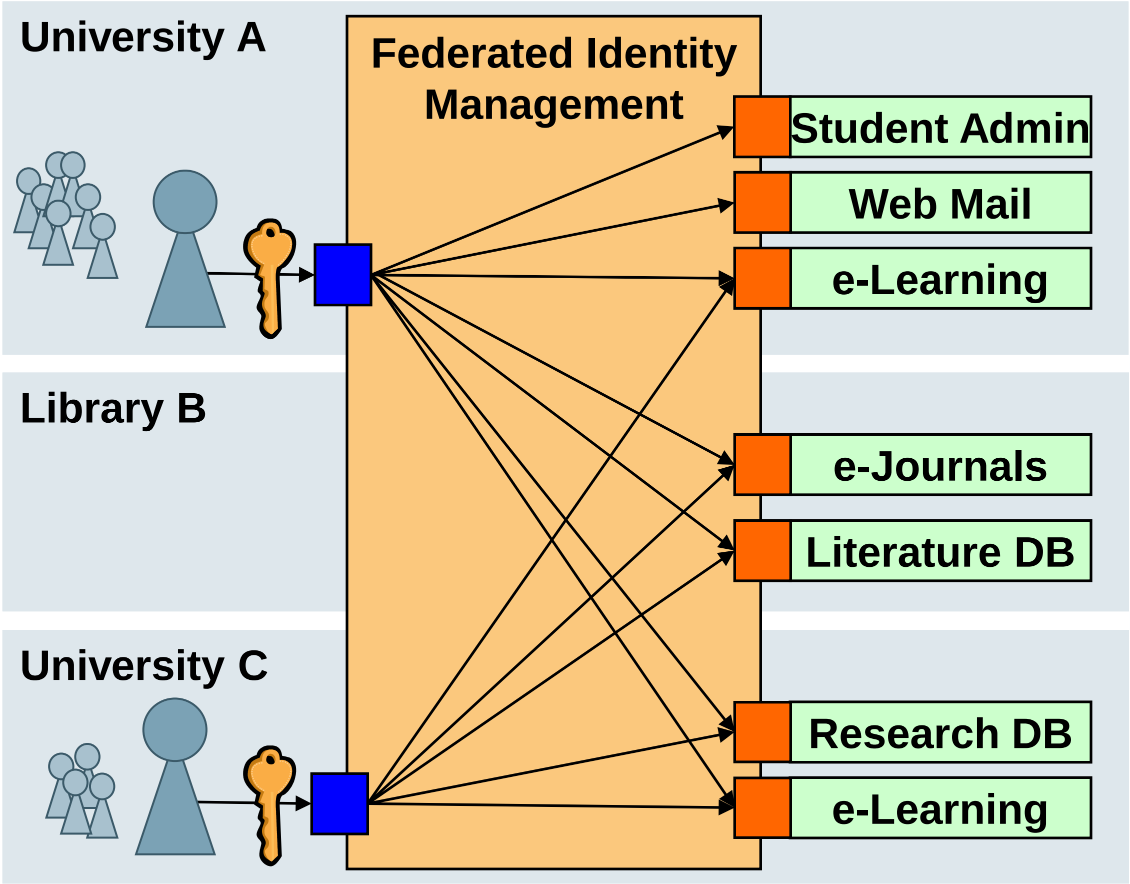
User Administration Authentication

Authorization

Resource

Credentials

Federated Identity Management



Shibboleth

- open source
- internet2
- SAML
- Web-based Single Sign-on
  - authN at Identity Provider
  - authZ at Service Provider based on user’s attributes as provided by IdP
- Privacy

User Administration Authentication

Authorization

Resource

🔑 Credentials

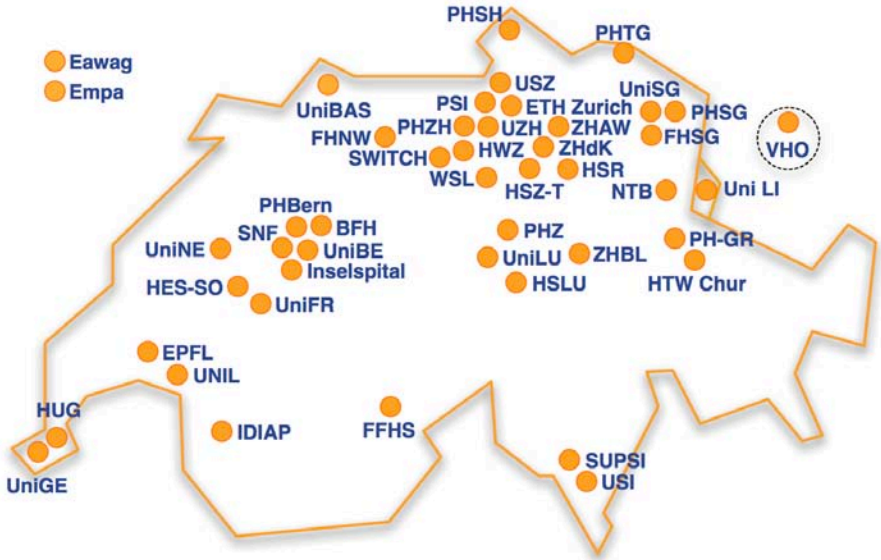
SWITCHaai: Authentication and Authorization Infrastructure of Switzerland

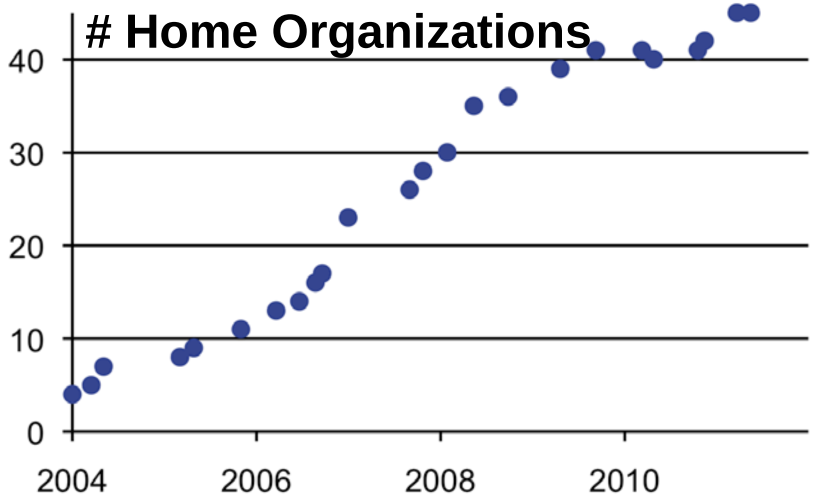
- SWITCHaai: AAI of Switzerland: provides every user of the Swiss academic community an identity that is backed by the user's home organization (i.e. his/her university)

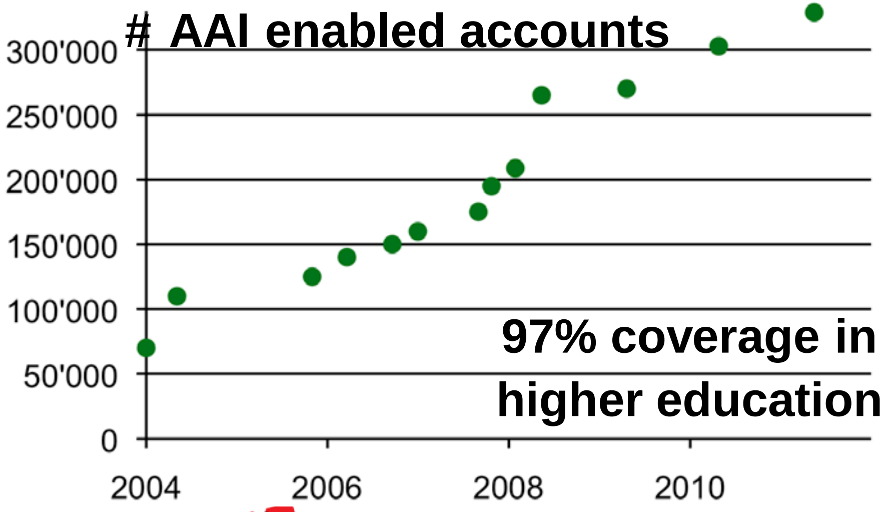
- Today, over 400 services use AAI to authenticate and authorize users

- Every university of Switzerland is member of AAI

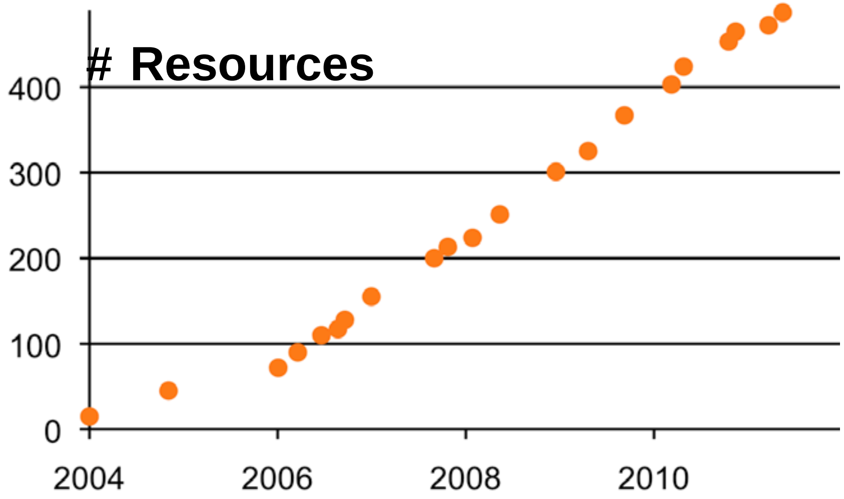
SWITCHaai Federation Spring 2011



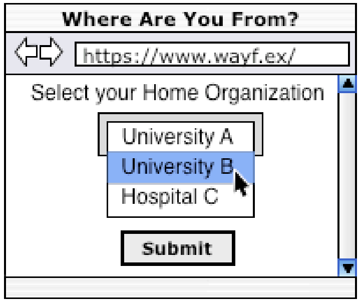

# Home Organizations


# AAI enabled accounts

97% coverage in higher education


# Resources

Demo

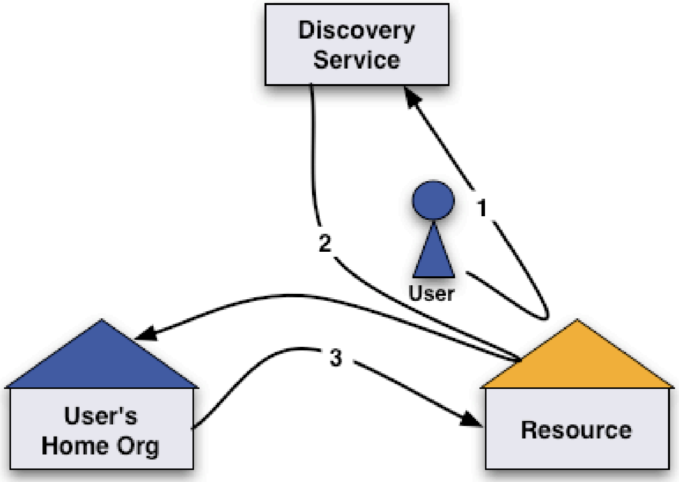


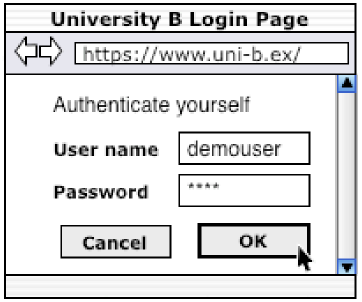
Where Are You From?

https://www.wayf.ex/

Select your Home Organization

- University A
- University B
- Hospital C



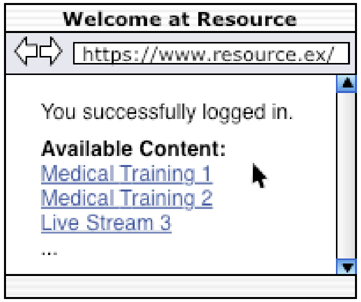


University B Login Page

https://www.uni-b.ex/

Authenticate yourself

User name	demouser
Password	****



Welcome at Resource

https://www.resource.ex/

You successfully logged in.

Available Content:

Medical Training 1
Medical Training 2
Live Stream 3
...

More about AAI

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

Outline

1. AAI
2. X.509 certificates
3. Use of X.509 certificates in Grid technology
4. AAI and Grids
5. Summary

How do I get a certificate?

1. Create a key pair (using some algorithm)
2. Send the public key to a Certificate Authority
    1. CA must obtain also personal information
    2. CA must perform an identity vetting
3. CA issues certificate with a given lifetime

4. Note:
    1. CA may revoke your certificate (in case of abuse)
    2. Certificate must be renewed once it expires
    3. and ????

YOU MUST PROTECT YOUR PRIVATE KEY

X.509 alias ISO/IEC/ITU 9594-9

- X.509 is ITU Standard:
  - ITU-T Recommendation X.509 (1997 E). Information technology - Open Systems Interconnection - The Directory: **Authentication Framework**
  - Defines a **certificate format**
    - Latest standard: X.509 version 3 certificate format

- X.509 certificate includes:
  - User identification (someone’s subject name)
  - Public key
  - Validity period
  - A “signature” from a Certificate Authority (CA) that:
    - Proves that the certificate came from the CA.
    - Vouches for the subject name
    - Vouches for the binding of the public key to the subject

DEMO: openssl commands

Where do I find more information on how to handle certificates?

http://www.switch.ch/grid/certificates/openssl/

X.509 Certificate Example (1)

```
openssl x509 –in ~/.globus/usercert.pem –text
```

```
Certificate:
   Data:
        Version: 3 (0x2)                                         X509.3 – with extensions
        Serial Number: 199 (0xc7)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=CH, O=CERN, OU=GRID, CN=CERN CA                Issuer CA
        Validity
            Not Before: Sep 25 10:33:05 2008 GMT                 long term certificate
            Not After :Sep 24 10:33:05 2009 GMT
        Subject: O=Grid, O=CERN, OU=cern.ch, CN=Joe User         user identification
        Subject Public Key Info:
       Public Key Algorithm: rsaEncryption                       public key
       RSA Public Key: (1024 bit)
         Modulus (1024 bit): 00:d6:6a:f3:ad:e3:b2:2e:98:32:7f:dd:44:89:38:
       […]
```

X.509 Certificate Example (2)

X509v3 extensions:

X509v3 Basic Constraints: critical   Certificate extensions

CA:FALSE

X509v3 Subject Key Identifier:

71:BC:FC:29:4E:E9:4E:7C:C9:E4:F9:A2:6C:77:4A:E4:55:82:86:53

X509v3 CRL Distribution Points: Certificate Revocation List
URI:http://service-grid-ca.web.cern.ch/service-grid-ca/cgi-bin/getCRL

X509v3 Issuer Alternative Name:

email:service-grid-ca@cern.ch

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.96.10.1.2.1

Netscape Cert Type:

SSL Client, S/MIME, Object Signing   client/user Certificate

Netscape Base Url:

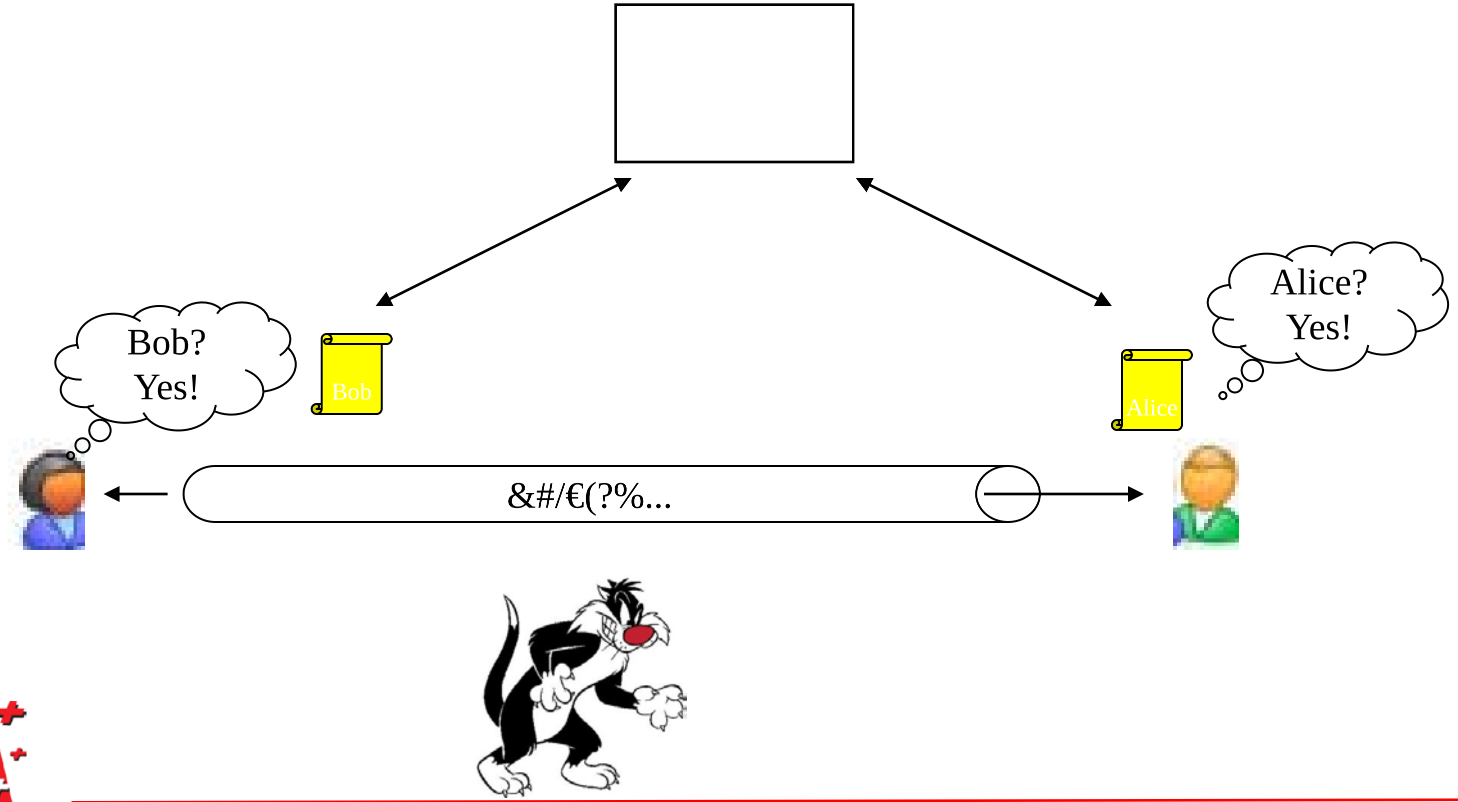
http://service-grid-ca.web.cern.ch/service-grid-ca/

Signature Algorithm: md5WithRSAEncryption

54:8b:66:e8:dc:60:cd:e3:dc:43:a7:c9:3a:12:2c:73:05:13:   [...]   **Signature** on the information

CA - Certification Authority

The role of the CA is to manage the certificate life cycle: create, store, renew, revoke



Trusting the CAs

- Nothing hinders you to set up your own CA and issue certificates
  - Getting others to trust you is the hard problem!
- Trust anchors: the CAs that we more or less trust unconditionally
  - Granularity: 1 CA per country
  - Primarily used in production grids for research purposes
- See www.gridpma.org

IGTF

International Grid Trust Federation

AP | EU | TAG

Where are those certificates ?

User certificates:

$HOME/.globus

usercert.pem, userkey.pem

Server certificates:

/etc/grid-security/

hostcert.pem, hostkey.pem

certificates # IGTF bundle, many small files

Scripts:

IGTF as part of the grid software# e.g. rpm, YAIM

fetch-crl # updates the CRLs

How to protect your private key ?

- File permissions on the private key
  - Only readable by owner

- Choose a “good” passphrase
  - Many characters (>14)
  - Not only letters, but also numbers and #@_&%$

- Keep track on which hosts you have put your private key

- Don’t import it into browsers that you don’t use all the time

- Remember: ***Anybody*** with access to your private key can impersonate you

Outline

1. AAI
2. X.509 certificates
3. Use of X.509 certificates in Grid technology
4. AAI and Grids
5. Summary

Single sign-on and delegation

- Jobs require access to **multiple resources**

- To authenticate with your certificate directly you would have to **type a passphrase every time**

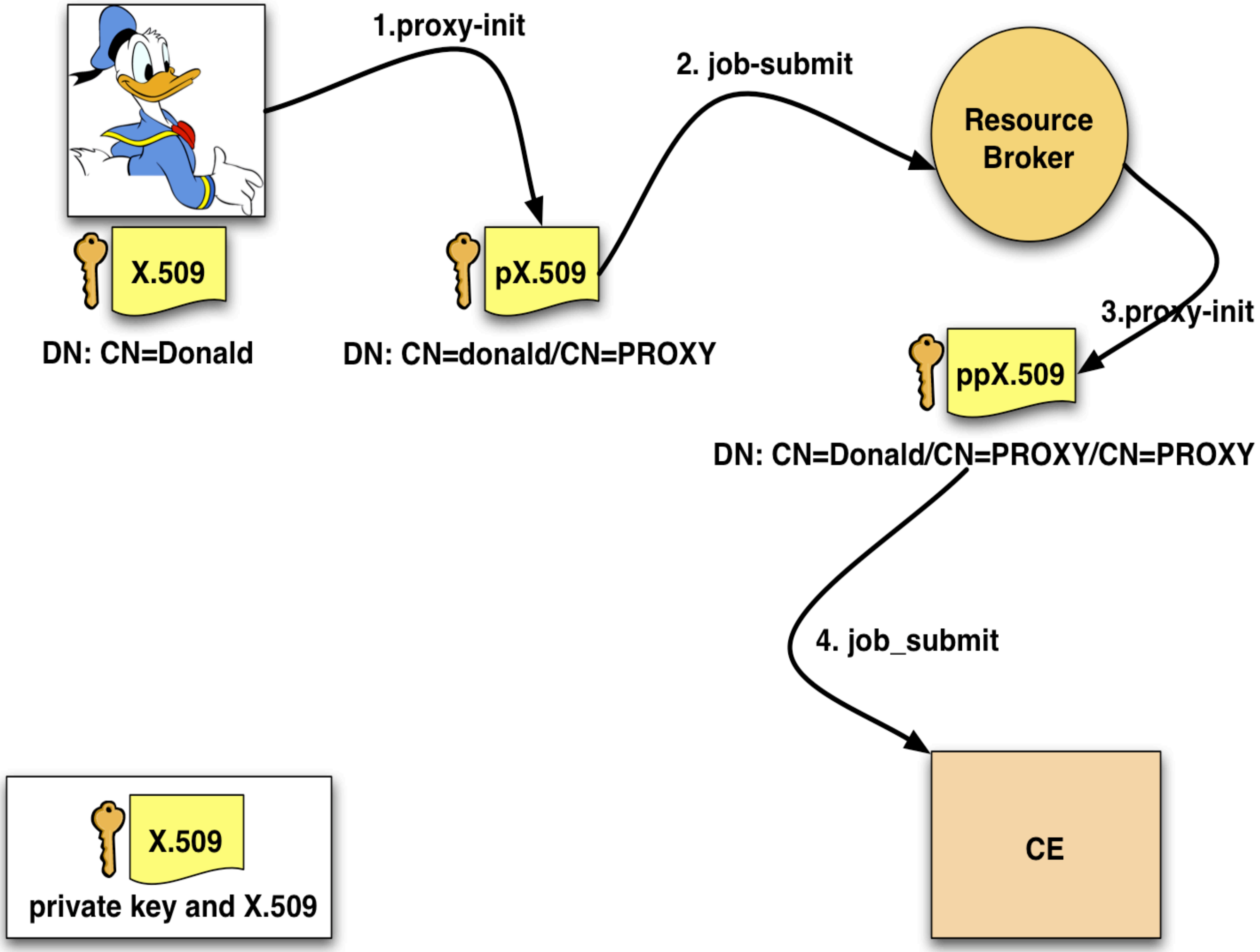
- Need to automate access to other resources: **Authenticate Once**

- Important for complex applications that need to use Grid resources
  - Enables easy coordination of varied resources
  - Enables automation of process
  - Allows remote processes and resources to act on user’s behalf - also known as **delegation**

In the Grid Security Infrastructure today, this is solved by *‘proxy certificates’*

- ***A temporary key pair***
- ***In a temporary certificate signed by your ‘long term’ private key***
- ***Valid for a limited time (default: 12 hours)***

Delegation



1.proxy-init

2. job-submit

Resource Broker

X.509

DN: CN=Donald

pX.509

DN: CN=donald/CN=PROXY

3.proxy-init

ppX.509

DN: CN=Donald/CN=PROXY/CN=PROXY

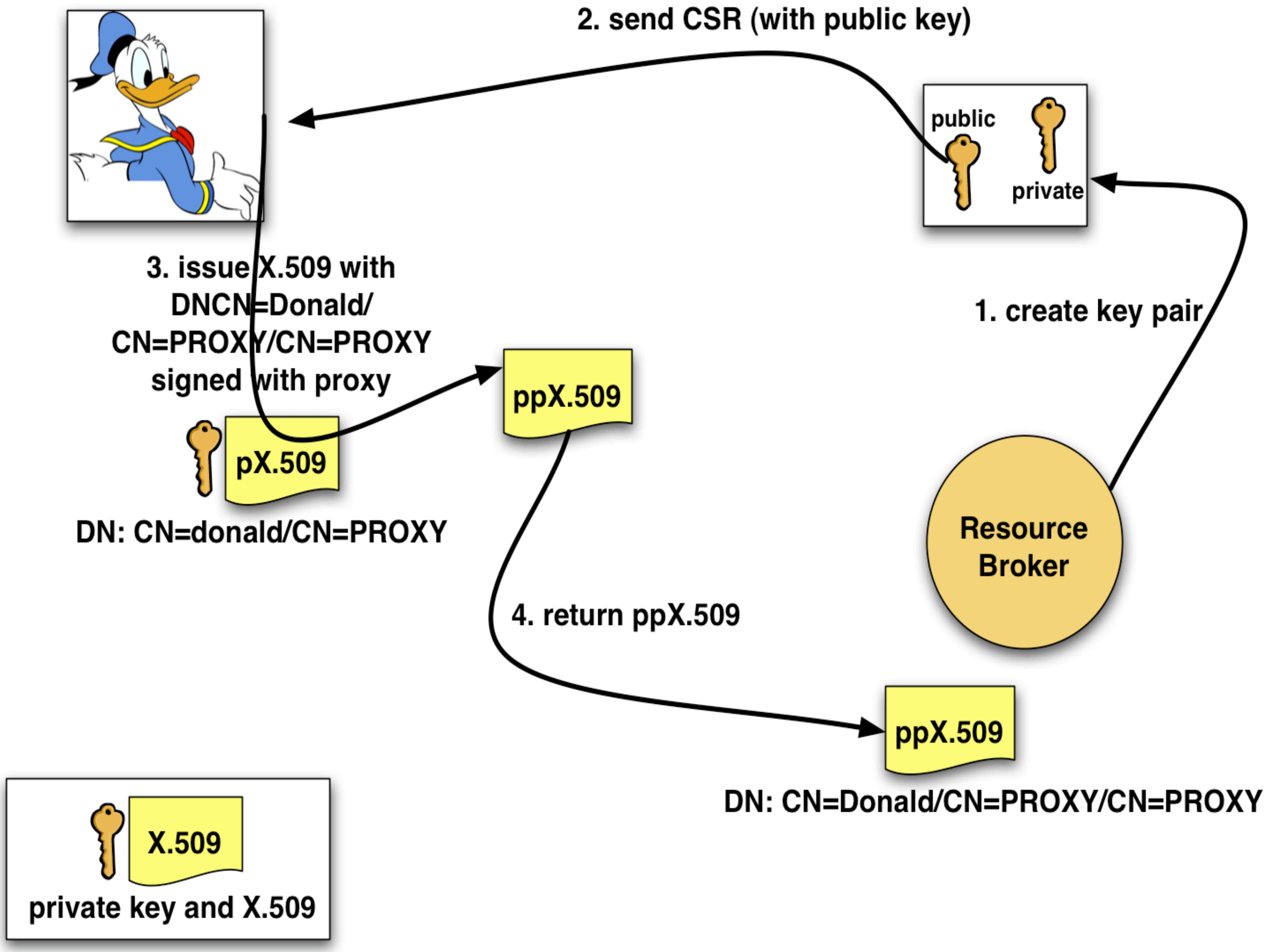
4. job_submit

CE

X.509

private key and X.509

Proxy Certificates



Delegation and limited proxy

Delegation = remote creation of a (second level) proxy credential

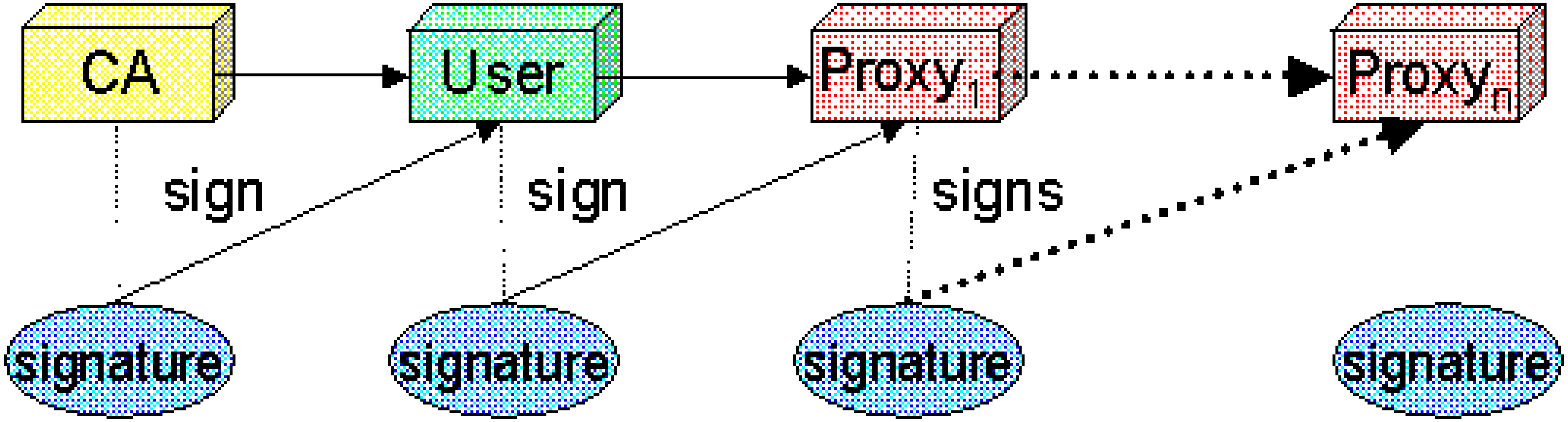
- Agents and brokers act on behalf of users
- with (a subset of) their rights
- This leads to a push model with proxies
  - you don't know beforehand where your task will end up

Allows remote process to authenticate on behalf of the user

- Remote process "impersonates" the user

The client can elect to delegate a "limited proxy"

- Each service decides whether it will allow authentication with a limited proxy



Proxy renewal

Proxy has limited lifetime (default is 12 h)

- Bad idea to have longer proxy

However, a grid task might need to use a proxy for a much longer time

- Grid jobs in HEP Data Challenges on LCG last up to 2 days

A dedicated service can **renew** automatically the proxy

But

Something is missing……

VO information

Remember: user acts as member of a VO

VO may also add information

- Group memberships
- Roles

Example: VO PlatypusLovers

- Groups: HavePlatypus, BeenInAustralia
- Role: FinancialOfficer, PlatypusCaretaker

De-facto Standard: VOMS

- Virtual organization membership service
- One VOMS instance per VO

VO Information in VOMS

Groups and role information is issued as an Attribute Certificate (AC) that is put as an extension into the user’s proxy certificate

All groups are listed, ordering matters

Role information is present *only if the users requests it*

AC contains list of “fully qualified attribute names “ FQAN

Example:

/vo_name/group1/Role=administrator

/vo_name/group2

/vo_name/group2/subgroup2

First FQAN is primary FQAN → special role in job handling

Outline

1. AAI
2. X.509 certificates
3. Use of X.509 certificates in Grid technology
4. AAI and Grids
5. Summary

Problems of Certificates

- Certificates have their drawbacks:
  - Provisioning certificates to the user is cumbersome
  - Certificates require a lot of knowledge from the user
  - Private keys must be properly secured

- Conclusion from a usability point of view:

Easiest is to hide the certificates from the user !

Issuing Certificates based on AAI

Idea:

As every student of Switzerland already has an AAI credential, issue certificates based on AAI
→ identity vetting is already been done by the university

Consequence: user friendly way to obtain certificate

- No special identity vetting needed
- Certificates simply expire once they are no longer used

Short-lived credential service (SLCS): issues Grid certificates to a member of SWITCHaai based upon successful authentication at his/her home organization

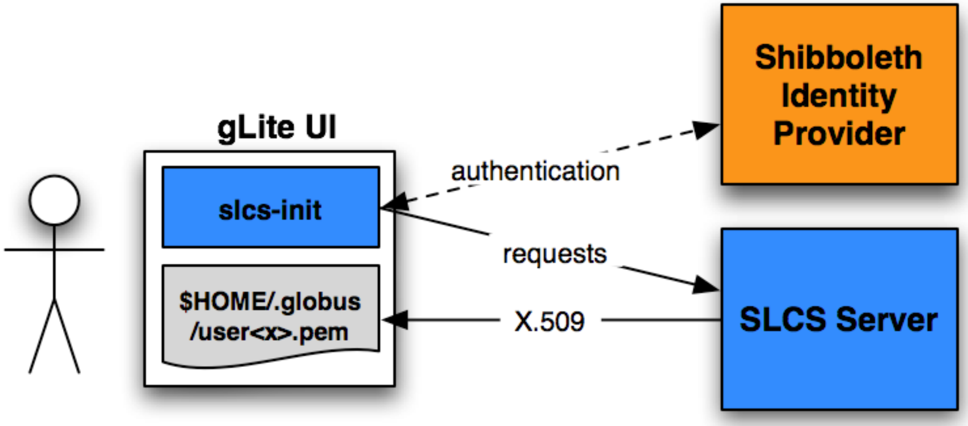
Easy grid access: SLCS Certificates

Online CA issuing short-lived X.509 certificates based upon authentication at Shibboleth Identity Provider

Shibboleth attributes used in DN

In production and accredited by EuGridPMA

SLCS Certificates based on AAI



Certificate lifetime < 1 mio sec (~ 11 days)

Easy generation from the command line based on authentication to AAI

Certificates simply expire after 11 days and can reissued many times → easy to use for the user

SLCS service is operated by SWITCH – see http://www.switch.ch/grid/slcs

Outline

1. Introduction
2. Virtual Organizations
3. A sloppy introduction into cryptography
4. X.509 certificates
5. Use of X.509 certificates in Grid technology
6. AAI and Grids
7. Summary

Summary

Basics of cryptography

Access to the Grid through proxy certificates

VO Information:

- groups and roles
- Issued as attribute certificate (AC) containing FQANs

Delegation mechanism

Issuance of SLCS certificates through AAI authentication

Links, references

PKI and general internet security:
C.Kaufmann, R.Perlman, M.Speciner: Network Security, Prentice Hall

Certificate handling:
http://www.switch.ch/grid/certificates/openssl/

SLCS certificates: http://www.switch.ch/grid/slcs

EGEE security architecture:
https://edms.cern.ch/file/935451/2/