AAI Attributes

Valéry Tschopp, <tschopp@switch.ch>
Directories within a AAI Home Organization

- **Authentication System**
  - any Apache compatible authentication method: LDAP, PAM, RADIUS, TACACS, end-user certificates, Web SSO (e.g. Pubcookie), …
  - any Tomcat compatible authentication method: e.g. Web SSO (CAS)

- **Integration with User Directory via Java APIs**
  - LDAP via JNDI
  - Databases via JDBC

→ Login name is the link between the two parts

SSO = Single Sign On
Authorization Attributes

• AAI transfers user attributes from a Home Organization to a Resource
  • Requires a common understanding of what a value means
  ➔ Authorization Attribute Specification v1.1
    http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf

• A task force selected the attributes for SWITCHaai
  • minimal set to start with
  • attributes with pre-existing ‘common understanding’
  • in line with foreign activities

• Descriptions are LDIF like, but use of LDAP not required
### Authorization Attributes (2)

<table>
<thead>
<tr>
<th>Personal attributes</th>
<th>Group membership</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unique Identifier</td>
<td>• Name of Home Organization</td>
</tr>
<tr>
<td>• Surname</td>
<td>• Type of Home Organization</td>
</tr>
<tr>
<td>• Given name</td>
<td>• Affiliation (student, staff, faculty, …)</td>
</tr>
<tr>
<td>• E-mail</td>
<td>• Study branch</td>
</tr>
<tr>
<td>• Address(es)</td>
<td>• Study level</td>
</tr>
<tr>
<td>• Phone number(s)</td>
<td>• Staff category</td>
</tr>
<tr>
<td>• Preferred language</td>
<td>• Group membership</td>
</tr>
<tr>
<td>• Date of birth</td>
<td>• Organization Path</td>
</tr>
<tr>
<td>• Gender</td>
<td>• Organizational Unit Path</td>
</tr>
</tbody>
</table>

- study branch, study level, staff category are based on SHIS/SIUS
- username and password are missing ⇒ only used locally!
- commonName is missing no common understanding on how to use it
Granting Access

Ueli Kienholz, <kienholz@switch.ch>
Method 1: SWITCHaai Attributes

Login: p.mueller
PW: 4rtz3w

HomeOrg = UniZH
Affiliation = Student
StudyBranch = Medicine
StudyLevel = 34

Access Rule:
HomeOrg = UniZH | UniBE | UniL
Affiliation = Student
StudyBranch = Medicine
StudyLevel >= 20
Method 2: Entitlement

Login: p.mueller
PW: 4rtz3w

Entitlement = http://secure.app.unibe.ch/content

Access Rule:
Entitlement = http://secure.app.unibe.ch/content
Method 3: Definition of additional Attributes

Login: p.mueller
PW: 4rtz3w

Department = IAM

Shibboleth Home Organisation

Web-Application

Shibboleth Component

Access Rule:
Department = IAM
Method 4: Application has it’s own Access Control

Login: p.mueller
PW: 4rtz3w

UniqueID = 235241@ethz.ch

Web Application

Allowed Users

<table>
<thead>
<tr>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:HB5ghl@unibe.ch">HB5ghl@unibe.ch</a></td>
</tr>
<tr>
<td><a href="mailto:235241@ethz.ch">235241@ethz.ch</a></td>
</tr>
<tr>
<td><a href="mailto:Gz58f7@unibe.ch">Gz58f7@unibe.ch</a></td>
</tr>
<tr>
<td><a href="mailto:ktziwlg@unil.ch">ktziwlg@unil.ch</a></td>
</tr>
</tbody>
</table>
Deployment

Valéry Tschopp, <tschopp@switch.ch>
Browser Requirements

- Cookies
- Browser redirect
- SSL
- If no JavaScript: additional click necessary
Supported Servers for Target Installations

**Server OS**
- Windows NT, 2000, XP, 2003
- Linux (any blend)
- Solaris

**Web Servers**
- Apache 1.3.x
- Apache 2.x
- IIS 4.x, 5.x, 6.x
Supported Applications

- Static content on Apache or IIS
- Applications (PHP, Perl, ..) running on Apache
- JAVA-web-applications via mod_jk and Apache

* Apple Quicktime Streaming Server
* ArtSTOR
* Blackboard
* CSA
* eAcademy
* EBSCO Publishing
* Elsevier ScienceDirect
* ExLibris – SFX
* EZProxy
* Fedora
* Gale
* Higher Markets
* JSTOR
* Napster
* NSDL
* OCLC
* Ovid Technologies Inc.
* Proquest Information and Learning
* SYMPA
* TWiki
* Web Assign
* WebCT
* Zope4Edu
Useful Information for a Target Deployment

- http://www.switch.ch/aai/deployment.html

With links to:
- Shibboleth Target Deployment Guide (Internet2)
- Compilation and Installation Guide (SWITCH)
- SWITCHaai Configuration Guide (SWITCH)
- SWITCHaai Sample Files (SWITCH)
Server Certificates

Ueli Kienholz, <kienholz@switch.ch>
Why are Server Certificates important?

Can I trust this Resource and send User Attributes to it?

Can I trust this HomeOrg and rely on the User Attributes that were sent to me?

Attribute Request

User Attributes

Resource

HomeOrg

Why are Server Certificates important?
SWITCHpki Service

The SWITCHpki Team
pki@switch.ch
http://www.switch.ch/pki/
Introduction

Motivation for SWITCHpki

- Requirement of AAI Project: server certificates protecting backend communication
- PKI initiatives within our community could benefit from a common service

What happened so far?

- AAI-TF-CA: Taskforce within AAI project
- Produced a CP/CPS draft, recommending SWITCH to make a service out of it
- SWITCH took this up, engaged SwissSign as consultant and potential outsourcing partner and drafted a new CP/CPS
- Result rediscussed in AAI-TF-CA and made into the service being presented today
SWITCHpki - CA Structure

SWITCH CA

SWITCH Server CA

SWITCH Personal CA

Potential additional CAs
CA Structure SwissSign & SWITCHpki

- SwissSign Root
  - SwissSign Bronze
    - SwissSign Silver
      - SwissSign Gold
        - SwissSign Platin
      - SWITCH Server CA
        - RA
      - SWITCH Personal CA
        - RA
  - SWITCH CA
    - Potential additional CAs

The Swiss Education & Research Network
SWITCHpki - CA Structure

SWITCH CA
- signed by ‘SwissSign Silver’
- off-line
- stored in a bank safe
- only used to sign sub-CAs (SWITCH Personal CA & SWITCH Server CA at the moment)
- once in a while used to issue CRL for SWITCH Server CA & SWITCH Personal CA

SWITCH Server CA
- implemented on the SwissSign infrastructure
- online

SWITCH Personal CA
- implemented on the SwissSign infrastructure
- online
- only used for RA personal at the moment
Roles, Entities: Underlying Principles

Correctness of information
- Included information must be correct
- E.g. no nicknames, pseudonyms need to be marked as such

Verifiability of information
- Included information must be verifiable and meaningful
- E.g. organisation names must be registered somewhere

Auditability
- All contents of signed information in certificates must be supported with some form of documentation attainable in reasonable time (e.g. during an audit)
Roles, Entities: The Players

The issuer
- Signs certificate requests issued by the subject
- Registration Authority (RA): entity doing all the checks and paperwork
- Certification Authority (CA): dumb signing engine, following the orders given by its RA

The subject
- Issues certificate signing requests
- Holds the issued certificate

The relying party
- The ones relying on (accepting) a given certificate
- Wants to understand the elements in the cert
Roles, Entities: Signed Information

Organisation names
- Correctness and verifiability: we require evidence of the correctness of organisation names from a trustworthy, official source
- Auditability: we want it on paper

Domain names
- Correctness and verifiability: we require evidence from the domain name holder, that the domain names are correct
- Auditability: we want it on paper

Subject information
- Correctness and verifiability: we require some evidence about the subject from a trustworthy, official source
- Auditability: we want it on paper
Roles, Entities: Who is doing what? (1)

Site/Organisation contact:

– Gets clearance from the represented organisation and relevant domain name holders to issue certificates linking each other and lets SWITCH-RA know about it

– Acts as primary contact to SWITCH regarding SWITCHpki services

– Checks the correctness of presented personal identification (e.g. student/staff card), takes copies and checks whether they link to the certificate requestor

– Checks whether the requestor is entitled to get a certificate for the service or server in question (assuming local procedures exist, probably linked to DNS maintenance)

– Decides whether the represented organisation wants to grant this certificate request (cost issues, other local policies)

– Discard the request or forward it to SWITCH-RA with supporting documentation

⇒ primarily checks the correctness of the documentation
Roles, Entities: Who is doing what? (2)

SWITCH-RA

- Checks authenticity of incoming certificate request from site contacts
- Checks whether the elements fit together (site contact - organisation name - domain name)
- Checks completeness of provided information
- Approves or denies certificate requests

⇒ primarily checks the completeness of the documentation
Participants in SWITCHpki

Participating Organisations

As stated in 3.2.2 of the CP/CPS the authentication of an organization identity has to be proven. Academic organisations are not necessarily listed in the Central Business Names Index (Zefix), therefore participating organisations must be listed in the table below.

In addition, the relevant 'O = ' subject entry is listed as well, based on 3.1.4 'Rules for interpreting various name forms' of the CP/CPS.

| ETH Swiss Federal Institute of Technology Zurich | 0 = ETH Swiss Federal Institute of Technology Zurich |
| Fachhochschule Aargau Nordwestschweiz | 0 = Fachhochschule Aargau Nordwestschweiz |
| SWITCH - Teleinformatikdienste für Lehre und Forschung | 0 = SWITCH - Teleinformatikdienste fuer Lehre und Forschung |
| Universität Bern | 0 = Universität Bern |
| Université de Fribourg - Universität Freiburg | 0 = Université de Fribourg - Universität Freiburg |
| Universität de Lausanne | 0 = Universität de Lausanne |
| Universität Zürich | 0 = Universität Zürich |

current list available at: http://www.switch.ch/pki/participants.html
<table>
<thead>
<tr>
<th>Site</th>
<th>Contact Person(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH</td>
<td>Dolores Parravicini</td>
</tr>
<tr>
<td></td>
<td>Brigitte Malacarne</td>
</tr>
<tr>
<td>Fachhochschule Aargau</td>
<td>Martin Sorg</td>
</tr>
<tr>
<td>Universität Bern</td>
<td>Christian Heim</td>
</tr>
<tr>
<td></td>
<td>Roland Trummer</td>
</tr>
<tr>
<td></td>
<td>Peter Geiser</td>
</tr>
<tr>
<td>Université de Fribourg</td>
<td>Bruno Vuillemin</td>
</tr>
<tr>
<td>Université de Lausanne</td>
<td>Alexandre Roy</td>
</tr>
<tr>
<td>Universität Zürich</td>
<td>David Meier</td>
</tr>
<tr>
<td></td>
<td>Jann Forrer</td>
</tr>
<tr>
<td></td>
<td>Luzian Scherrer</td>
</tr>
<tr>
<td></td>
<td>Roberto Mazzoni</td>
</tr>
</tbody>
</table>
Request a Certificate

http://www.switch.ch/aai/certificates.html
http://www.switch.ch/pki/manage.html
Documents & further information

CP/CPS, detailed slides
- Certificate Policy and Certification Practise Statement (CP/CPS)
  http://www.switch.ch/pki/SWITCH_CP-CPS200401.pdf