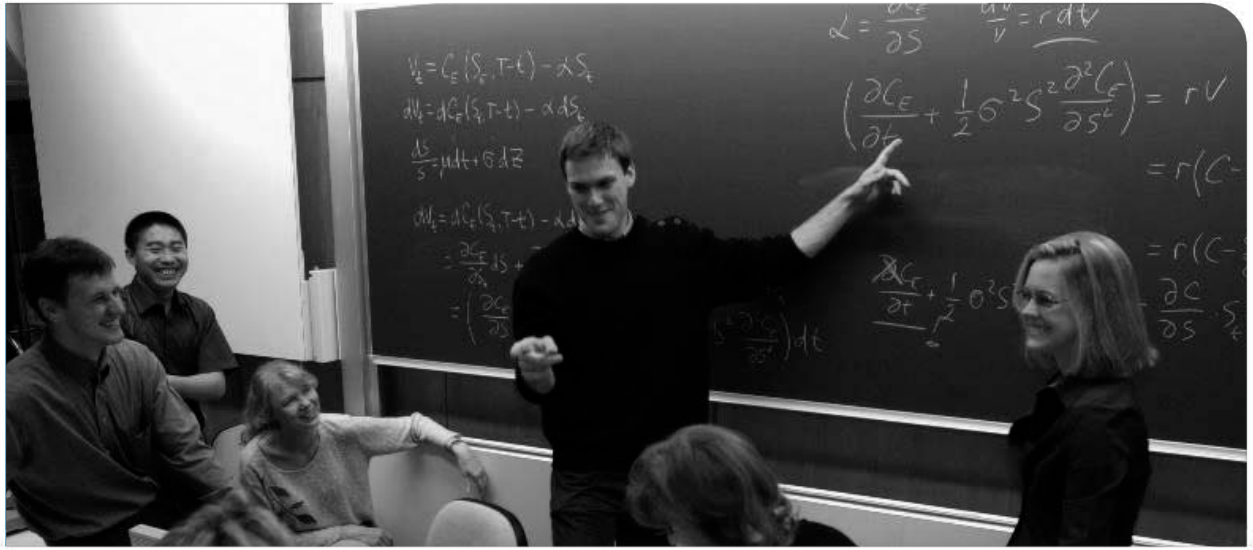
UNIL | Université de Lausanne



AAI Operations Committee Meeting, Tuesday, 15 June 2010

AAA/AAI projects at University of Lausanne

Etienne Dysli, Alexandre Roy

AAA projects at UNIL

1. UNIL.2 : Portail MyUNIL
   - Delegation of authentication in my.unil.ch portal

2. UNIL.3 : AAA-auth
   - Assurance Level
   - Two-factor authentication

3. UNIL.4 : GridUNIL - Phase 2
   - focusing on users needs

Assurance level
Important documents

- “Assurance answers the question, "How sure am I that you are who you say you are?" In other words, how much confidence does a relying party have that the credential presented is in the possession of the person whose identity is being asserted.”

- « OMB M-04-04 defines the required level of authentication assurance in terms of the likely consequences of an authentication error »
  - http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
- « NIST Special Publication 800-63 provides technical guidance to Federal agencies implementing electronic authentication »
  - http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf

- InCommon Identity Assurance Assessment Framework
  - http://www.incommonfederation.org/docs/assurance/InC_IAAF_1.0_Final.pdf
- Identity Assurance Profiles Bronze and Silver
  - http://www.incommonfederation.org/docs/assurance/InC_Bronze-Silver_IAP_1.0.1.pdf
- Incomon site (ass. level): http://www.incommonfederation.org/assurance/

Assurance Level
Aspects to be considered

- Business, Policy and Operational Factors.
- Registration and identity proofing of Applicants.
- Tokens (typically a cryptographic key or password) for proving identity.
- Token and credential management mechanisms used to establish and maintain token and credential information.
- Protocols used to support the authentication mechanism between the Claimant and the Verifier. Security and Management of Authentication Events
- Assertion mechanisms used to communicate the results of a remote authentication if these results are sent to other parties.
- Technical Environment.

Identification and registration Situation at UNIL

- Regular student
  - Immatriculation process. Documents.
  - Taxes.
  - Validation of postal address (address of record).
- Employee
  - Enrollment process. Documents.
  - In Person Proofing.
  - Validation of postal address (address of record).
- Other persons
  - No registration process.
- Generic identities
  - No binding (or weak binding) to a physical person.
- Strong assurance
  - Strong Identification: In Person Proofing.
  - Two factor authentication.

Project Status

- UNIL.2 SAML Delegation
  - Tried both uPortal's and SWITCH's delegation libraries
  - More SSL issues than metadata/configuration issues

- UNIL.3 Two-Factor Authentication
  - Considering those 2nd factors: our CampusCard (Legic RFID), SMS, USB smartcard (SuisseID?), mobile app

Attributes for external users

- Our group management application allows AAI users as members -> internal LDAP
- IdP on internal LDAP -> replace LDAP query with SAML attribute query
- Publish unilMemberOf attribute for non-UNIL AAI users
- Portal example:
  - User authentication and attributes coming from another institution's IdP
  - Portal makes an additional attribute query to our IdP

Attributes for external users
Service provider

- SP configuration (requires v2.2 or greater)
  - Add a SimpleAggregation AttributeResolver:

```
<AttributeResolver type="Chaining">
  <AttributeResolver type="Query"/>
  <AttributeResolver type="SimpleAggregation" attributeId="Shib-
  SwissEP-UniqueID" format="urn:oid:2.16.756.1.2.5.1.1.1">
    <Entity>https://aai.unil.ch/idp/shibboleth</Entity>
  </AttributeResolver>
</AttributeResolver>
```

  - Bugs
    - Superfluous attribute query when authenticated by our IdP (fixed in 2.4) [1].
    - Some attributes may get duplicate values through aggregation. Your application might choke on this.

Attributes for external users
Identity provider

- IdP configuration
  - Add a PrincipalConnector in attribute-resolver.xml:

```
<resolver:PrincipalConnector xsi:type="Direct"
   xmlns="urn:mace:shibboleth:2.0:resolver:pc" id="saml2uniqueId"
   nameIDFormat="urn:oid:2.16.756.1.2.5.1.1.1" />
```

  - (optional) Avoid attribute value duplication. The following example policy:
    - Only applies to mentioned entities;
    - Prevents the release of UniqueIDs NOT ending with @unil.ch.

Attributes for external users
Example attribute filter policy

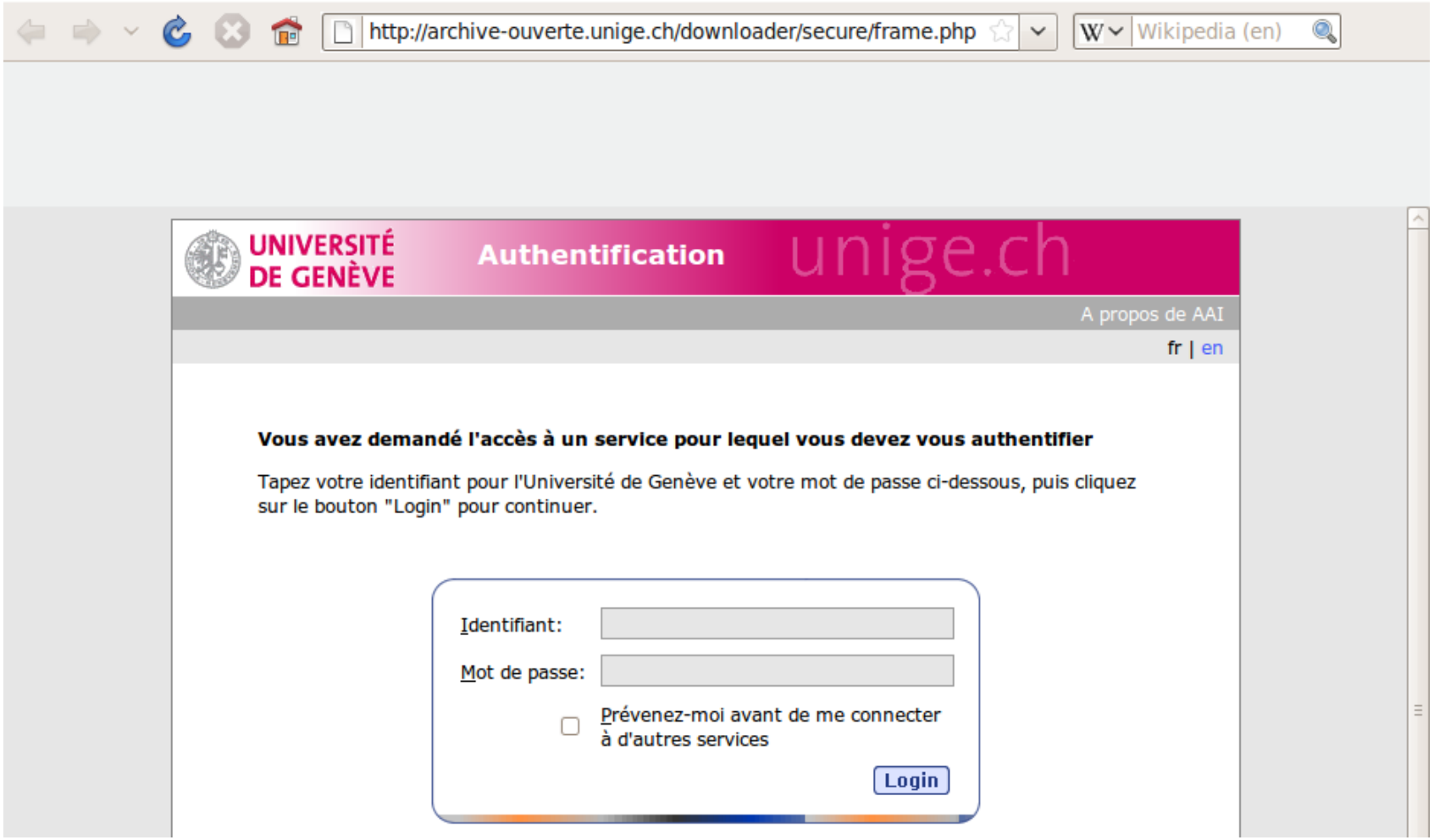
```
<AttributeFilterPolicy id="afp_for:externalUniqueID">
  <PolicyRequirementRule xsi:type="basic:AND">
    <basic:Rule xsi:type="saml:AttributeRequesterInEntityGroup" groupID="urn:mace:switch.ch:SWITCHaai" />
    <basic:Rule xsi:type="basic:OR">
      <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://xenos.unil.ch/shibboleth" />
      <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://my.unil.ch/shibboleth" />
      <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://mydev.unil.ch/shibboleth" />
      <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://mytest.unil.ch/shibboleth" />
    </basic:Rule>
  </PolicyRequirementRule>
  <AttributeRule attributeID="swissEduPersonUniqueID">
    <DenyValueRule xsi:type="basic:NOT">
      <basic:Rule xsi:type="basic:AttributeValueRegex" attributeID="swissEduPersonUniqueID"
   regex=".*@unil\.ch$"/>
    </DenyValueRule>
  </AttributeRule>
</AttributeFilterPolicy>
```

Clickjacking Protection for the IdP (1)

- Clickjacking [2]:
  - Hijacking mouse clicks on a web page.
  - User clicks on an invisible object that lies on top of what he sees.
  - Abused to trigger actions on a site where the user is logged in.
  - Your site could be vulnerable if it can be displayed in a frame or iframe.

- Why protect the IdP?
  - Login form could be abused
  - Framed login page example [3]
  - "Next Generation Clickjacking" at BlackHat Europe 2010 featured some scary examples [4]

Framed login page example



Clickjacking Protection for the IdP (2)

- X-Frame-Options HTTP header
  - Designed by Microsoft; supported by IE8, Safari 4, Chrome 2 and NoScript (Firefox extension)
  - JSP example:

```
<% response.addHeader("X-Frame-Options","deny"); %>
```

- JavaScript
  - Frame buster example:

```
if (top!=self) {
  top.location.replace(self.location.href);
}
```

  - Can be circumvented [2,4]

References

1. https://bugs.internet2.edu/jira/browse/SSPCPP-213

2. http://www.owasp.org/index.php/Clickjacking

3. http://archive-ouverte.unige.ch/downloader/secure/frame.php

4. Stone, Paul. Next Generation Clickjacking. BlackHat Europe 2010. http://www.blackhat.com/html/bh-eu-10/bh-eu-10-archives.html#Stone