Motivation for Using AAI

From a web application developer’s point of view

SWITCH

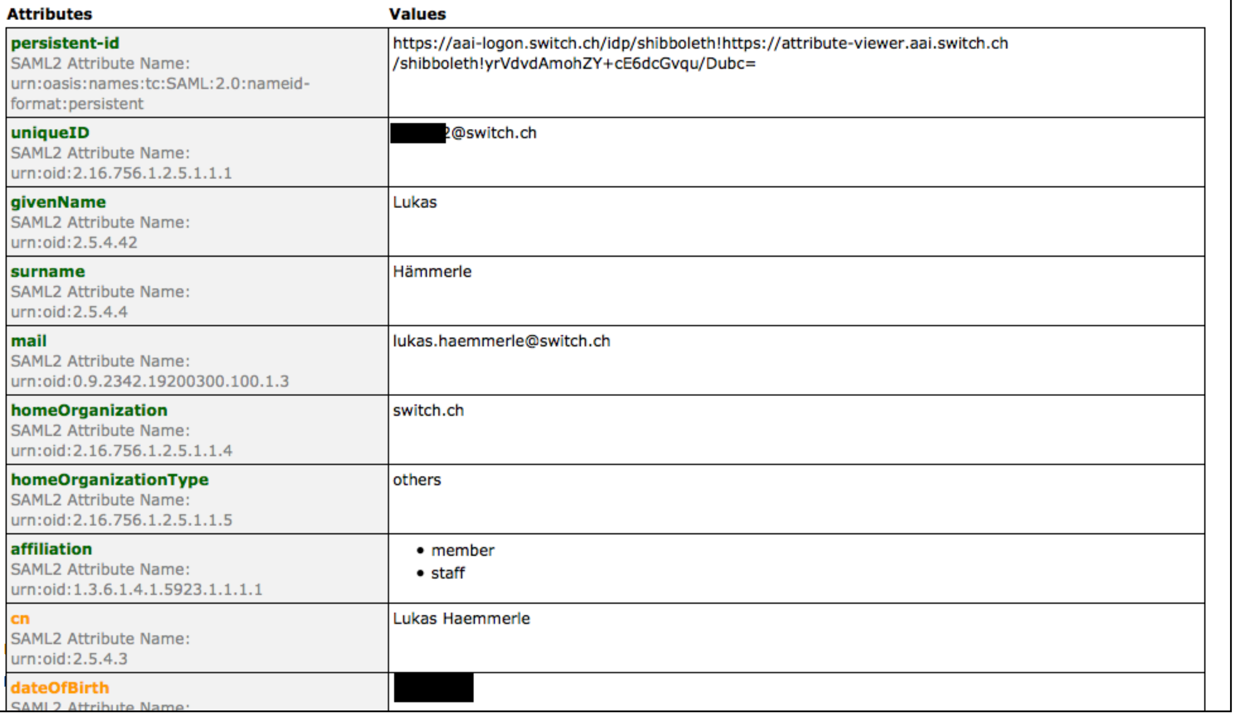
SWITCHaai Team
aai@switch.ch

Why running AAI Services?

- Running a Service Provider requires some effort
  - Understanding non-trivial technology
  - Installing and configuring a SAML Service Provider (SP)
  - (Optionally) install an configure an IdP Discovery Service
  - (Optionally) adapt application or web server configuration
  - Keeping SP software up-to-date
- Why and for what reason do administrators of more than 830 AAI services and additional 960 eduGAIN services run SAML Service Providers?

User Information in Form of Attributes!

Speaker‘s attributes on https://av.aai.switch.ch



Attributes	Values
persistent-id SAML2 Attribute Name: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	https://aai-logon.switch.ch/idp/shibboleth!https://attribute-viewer.aai.switch.ch/shibboleth!yrVdvdAmohZY+cE6dcGvqu/Dubc=
uniqueID SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.1	[redacted]@switch.ch
givenName SAML2 Attribute Name: urn:oid:2.5.4.42	Lukas
surname SAML2 Attribute Name: urn:oid:2.5.4.4	Hämmerle
mail SAML2 Attribute Name: urn:oid:0.9.2342.19200300.100.1.3	lukas.haemmerle@switch.ch
homeOrganization SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.4	switch.ch
homeOrganizationType SAML2 Attribute Name: urn:oid:2.16.756.1.2.5.1.1.5	others
affiliation SAML2 Attribute Name: urn:oid:1.3.6.1.4.1.5923.1.1.1.1	• member • staff
cn SAML2 Attribute Name: urn:oid:2.5.4.3	Lukas Haemmerle
dateOfBirth SAML2 Attribute Name:	[redacted]

Motivation for Running AAI Services

- **User Attributes**
  - Trusted and up-to-date information about user and his organisation
  - Attributes are (typically) verified and set by organisations e.g. when student enrolls or when staff member is hired
  - Self-interest of organisation to keep data up-to-date!
- **Attributes available to services outside organisation**
  - Easier collaboration/sharing of services
- **User has a single account/password**
  - Only one password needed to access AAI services
  - Service in own organisation, SWITCHaai, world-wide via eduGAIN

How Are Attributes Used?

- **User identification**
  Who is user?

- **Authorisation/Access Control**
  Is user allowed to access file or perform action?

Use Attributes for Apache Access Control

```
# Force user to authenticate on protected-directory
<Location /protected-directory>
  AuthType shibboleth
  ShibCompatWith24 On
  ShibRequestSetting requireSession true
  Require shib-attr homeOrganizationType university uas
</Location>
```

Works also in .htaccess files that are processed dynamically.

Use Attributes for Complex Access Control

```
# Complex Shibboleth access control rule
<Host name="sp.example.org">
  <Path name="protected" authType="shibboleth" requireSession="true">
    <AccessControl>
      <AND>
        <OR>
         <Rule require=“uniqueID">23c90324u@ethz.ch</Rule>
         <Rule require="affiliation">student</Rule>
        </OR>
        <OR>
          <Rule require="homeOrganization">ethz.ch</Rule>
          <Rule require="homeOrganization">uzh.ch</Rule>
        </OR>
       </AND>
    </AccessControl>
  </Path>
</Host>
```

Allow ETHZ and UZH students and another user identified by a unique identifier.

Use Attributes in Application

Just read attributes from web server environment and use them.

- No library required
- Same place like REMOTE_USER or REMOTE_ADDR is read from.

```
// PHP Example
$AAIUser->setMail($_SERVER["mail"]);
$AAIUser->setGivenName($_SERVER["givenName"]);
$AAIUser->setSurname($_SERVER["surname"]);

// Java Example
request.getAttribute("uniqueID")
request.getAttribute("homeOrganization")
request.getAttribute("affiliation")
```