Interfederation Attributes

And how to use the Shibboleth Attribute Checker

SWITCH

Lukas Hämmerle
lukas.haemmerle@switch.ch

SP Training, March 2014

Recommended Interfederation Attributes

EduGAIN recommends these attributes for each user:

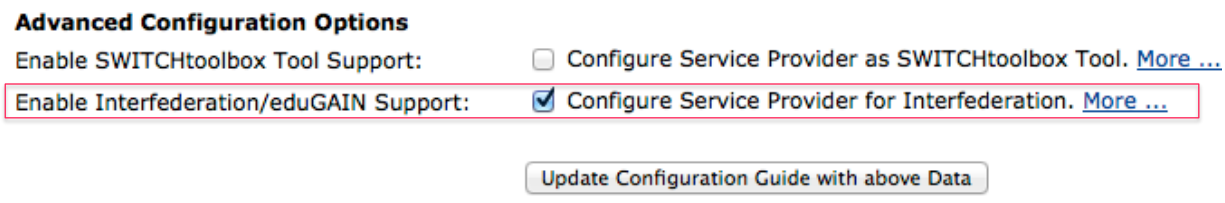
Friendly name	Defined in	Example
displayName	eduPerson	Beatrice Huber
common name (cn)	eduPerson	Beatrice Huber
mail	eduPerson	bea.huber@switch.ch
eduPersonAffiliation **eduPersonScopedAffiliation**	eduPerson	staff staff@switch.ch
eduPersonPrincipalName	eduPerson	234cd8z239@switch.ch
schacHomeOrganization	SCHAC	switch.ch
schacHomeOrganizationType	SCHAC	urn:mace:terena.org:schac:homeOrganizationType:int:NREN
eduPersonTargetedID / Persistent Name ID	eduPerson	https://aai-logon.switch.ch/idp/shibboleth!https://sp.example.org/shibboleth!2389cdhu3e-sda7323

eduGAIN-specific Attributes

- Difference **commonName/displayName**:
  The same but commonName might be multi-valued
- **eduPersonScopedAffiliation**:
  Like eduPersonAffiliation but with domain name appended
- **eduPersonPrincipalName**:
  Like eduPersonAffiliation but with domain name appended
- **schacHomeOrganization**:
  Domain name (like swissEduPersonHomeOrganisation)
- **schacHomeOrganizationType**:
  Not very well defined yet unfortunately...

Make SP eduGAIN attributes

- The attributes in bold blue letters are normally not used in SWITCHaai
- To make SP support them, the attribute-map.xml must be adapted to contain their definition
- SWITCHaai configuration guide can do that for you:
  Choose"Interfederation/eduGAIN Support" during configuration to include definitions automatically



Missing Attributes on SP

- Attribute release in other federations unfortunately is often a manual process
  - Identity Providers in other federations often don't release attributes
  - Not so much an issue in SWITCHaai thanks to Resource Registry
- Consequence: SPs sometimes don't get required attributes
  - Users will get some error from application or SP
- Ideally, application shows an error that tells what attributes are missing
- But Shibboleth SP can do that too

Check Available Attributes

- In `<ApplicationDefaults>` or `<ApplicationOverride>` add the configuration option: `sessionHook="#URL#"`
- User is redirected to this (absolute or relative) URL
  - Done before he is redirected to page requested initially
  - Page should check if all attributes are available and show error if not
  - Page therefore needs access to user's attributes!
- Standard page provided by Shibboleth would be: `sessionHook="/Shibboleth.sso/AttrChecker"`
  - Can use boolean expressions to check attributes

Attribute Checker Example

If condition is not met:

- Shows an error message
- Flushes the Shibboleth session

```
<Handler type="AttributeChecker" flushSession="true"
 Location="/AttrChecker" template="attrChecker.html">
    <OR>
      <Rule require="displayName"/>
      <AND>
        <Rule require="givenName"/>
        <Rule require="surname"/>
      </AND>
    </OR>
</Handler>
```

 https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPHandler

Standard Error Message

- Template is: `/etc/shibboleth/attrChecker.html`
- Ideally mention which attributes are missing