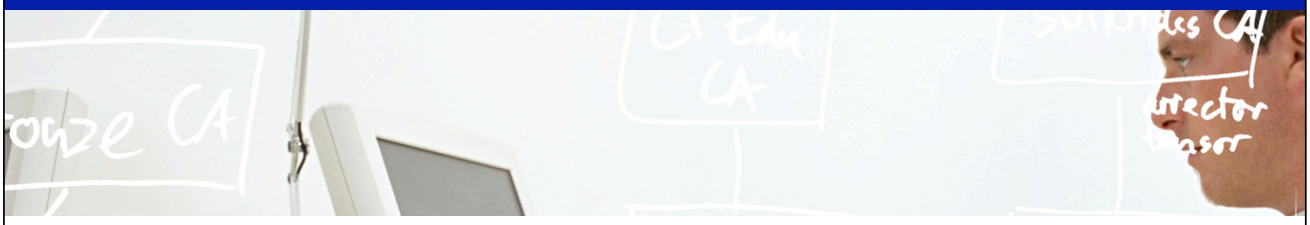
AAI Attributes



SWITCH
Serving Swiss Universities

Beatrice Huber
bea.huber@switch.ch

Basel, 29.August 2012

Agenda

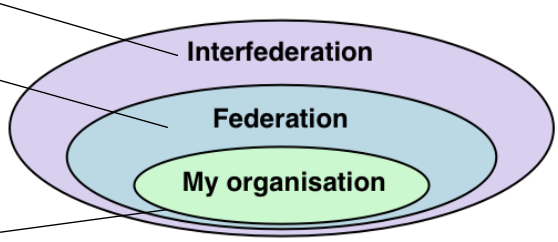
- attribute usage
- attribute scope
- user identifier attributes

Attribute usage

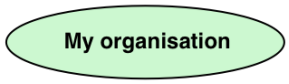
- identification
- authorisation
  - Access decision based on attribute values
  - individual or role based access control
- additional user information
  - Portal personalization e.g. preferred language
- accounting

Attribute scopes

- Standardized
- SWITCHaai
  - Core
  - Other
- Local



Attribute examples



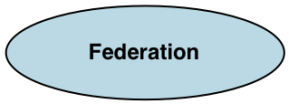
Local scope:

Group membership at the Uni Lausanne

SAML1 Name:
urn:mace:switch.ch:SWITCHaai:unil.ch:unilMemberOf

SAML2 Name:
urn:oid:2.16.756.1.2.5.1.1.1003

Attribute examples



SWITCHaai scope:

Study branch 1 (swissEduPersonStudyBranch1)
Study branch of a student, first level of classification

SAML1 Name:
urn:mace:switch.ch:attribute-def:swissEduPersonStudyBranch1

SAML2 Name:
urn:oid:2.16.756.1.2.5.1.1.6

SWITCHaai Attributes

Federation

Personal

- Unique Identifier
- Surname
- Given name
- E-mail
- Persistent ID
- User ID
- Matriculation number
- Employee number
- Address(es)
- Phone number(s)
- Preferred language
- Date of birth
- Card UID

Group Membership

- Home Organization Name
- Home Organization Type
- Affiliation

- Study branch
- Study level
- Staff category
- Group membership
- Organization Path
- Organizational Unit Path

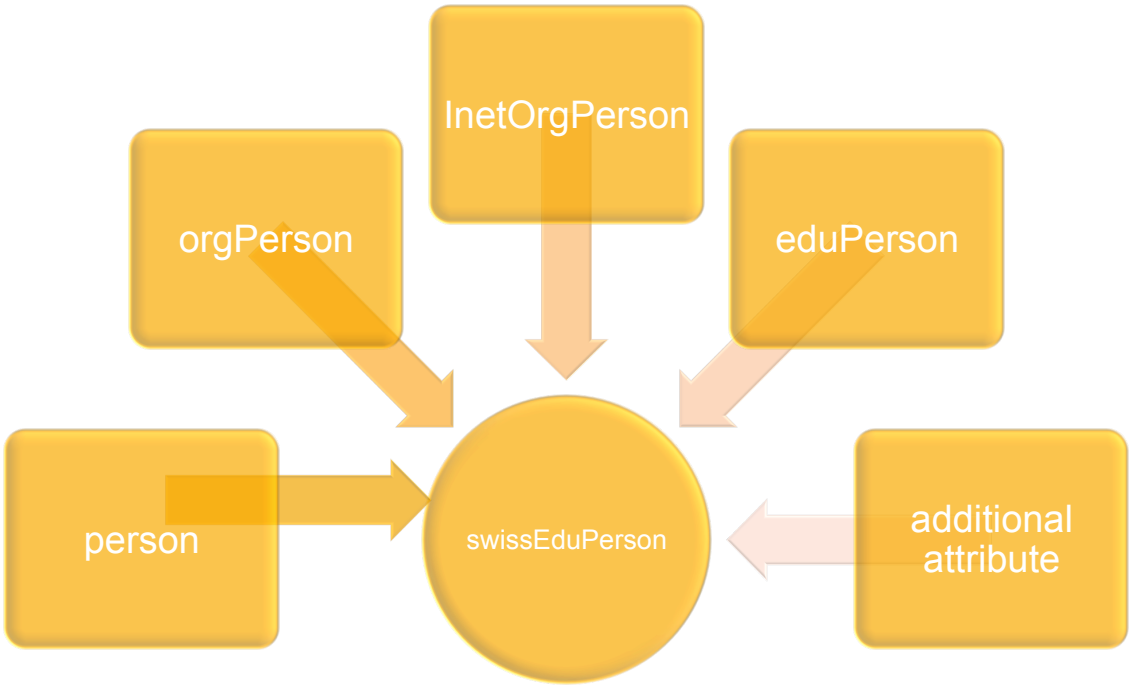
Implementation of Attributes

- Core Attributes
- Other Attributes

AAI Attribute Specification: http://switch.ch/aai/attributes

swissEduPerson definition

Federation



Standardized Attributes

Interfederation

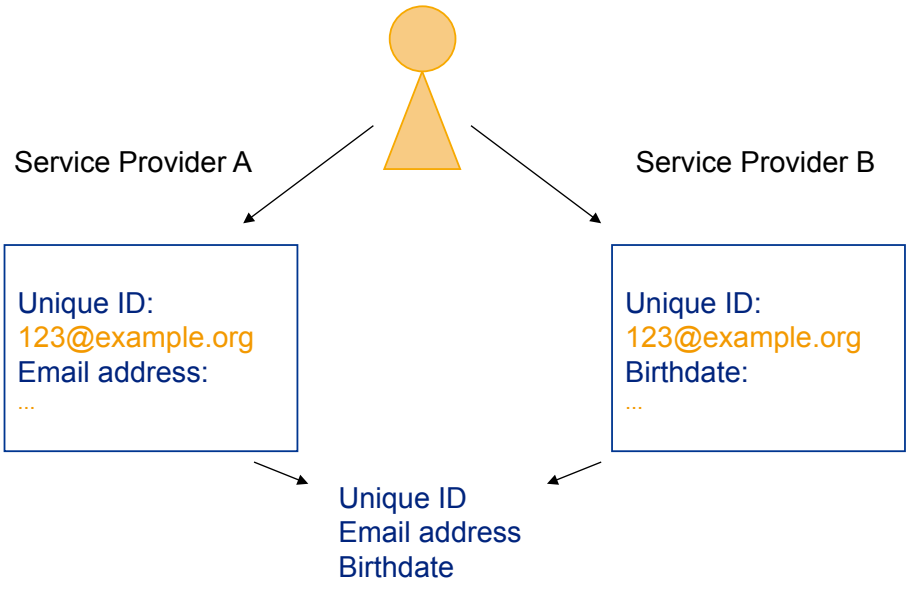
- Relevant for communication with entities from other federation via eduGAIN (or on bilateral basis)

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
schacHomeOrganization	SCHAC	switch.ch
schacHomeOrganizationType	SCHAC	urn:mace:terena.org:schac:homeOrganizationType:int:NREN

User identifier attributes

Federation

- Using account linking, the data is worth even more.

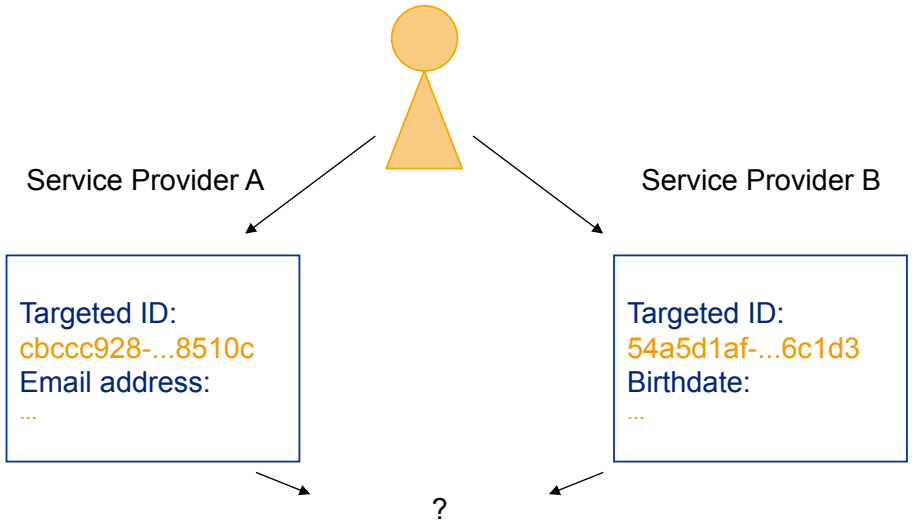


persistent ID (eduPersonTargetedID)

Federation

Example persistent ID

```
https://idp.example.org/idp/shibboleth!
 https://sp.example.org/shibboleth!
 f74698d6-854c-480c-b566-702006318cc3c
```



Email vs persistent ID vs Unique ID

Federation

Properties	Email	Unique ID	persistent ID
scoped	✓	✓	✓
persistent	✓	✓	✓
opaque	×	✓	✓
non-reusable	×	✓	✓
targeted	×	×	✓
revocable	×	×	✓