

AAI Attributes



SWITCH

Bea Huber
aai@switch.ch

SWITCHaai Introduction Course
Bern, 1. March 2013

Agenda

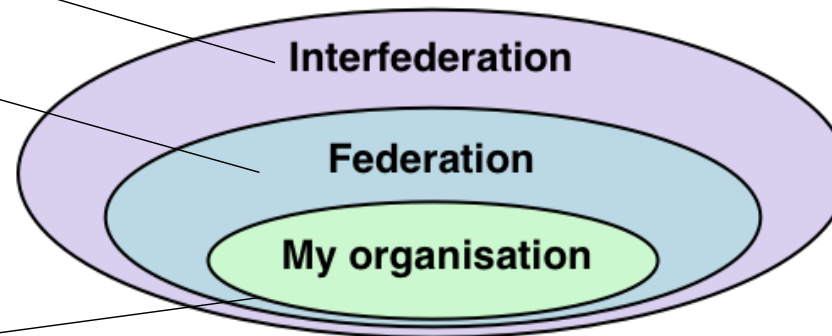
- attribute usage
- attribute scope
- user identifier attributes

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



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

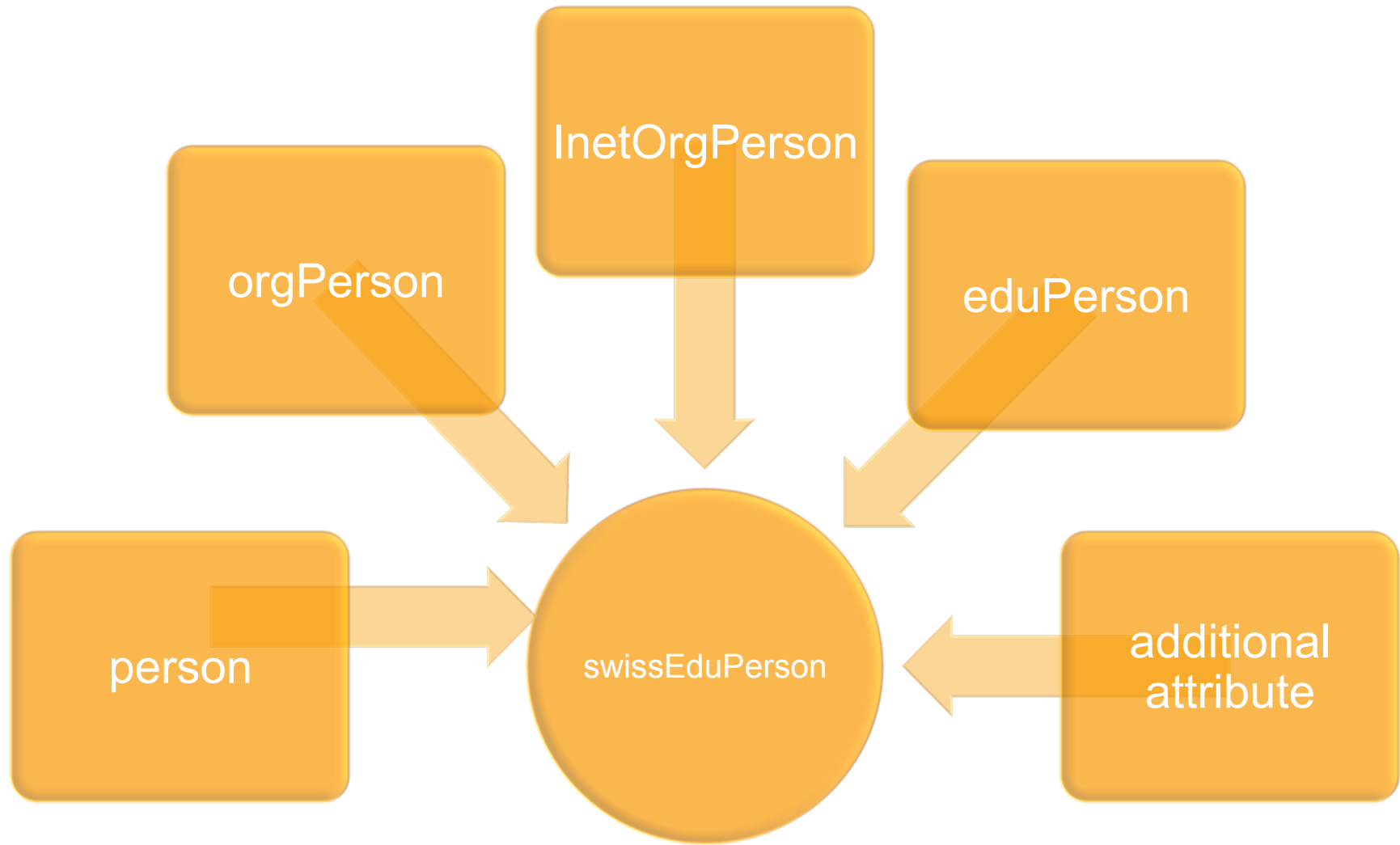
- Home Organization Name
- Home Organization Type
- Affiliation

- 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





Attribute examples

SWITCHaai scope:

Affiliation (eduPersonAffiliation)

SAML2 Name:

urn:oid:1.3.6.1.4.1.5923.1.1.1.1

Since 2012:

The member affiliation **MUST** be asserted for people carrying one or more of the following affiliations: faculty or staff or student.

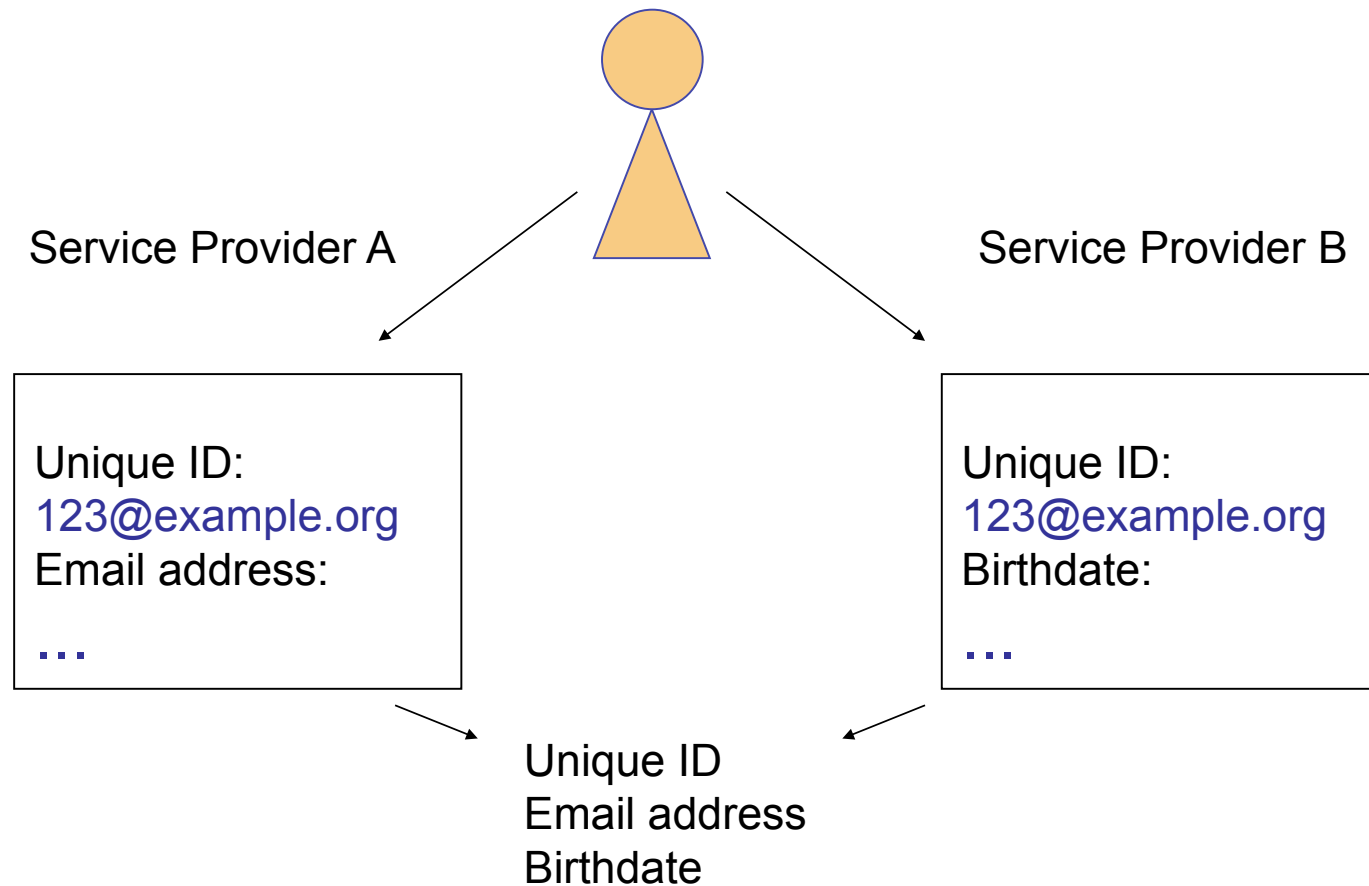
Standardized Attributes

- 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
eduPersonPrincipalName	eduPerson	234cd8z239@switch.ch
schacHomeOrganization	SCHAC	switch.ch
schacHomeOrganizationType	SCHAC	urn:mace:terena.org:schac:home OrganizationType:int:NREN

User identifier attributes

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



persistent ID (eduPersonTargetedID)

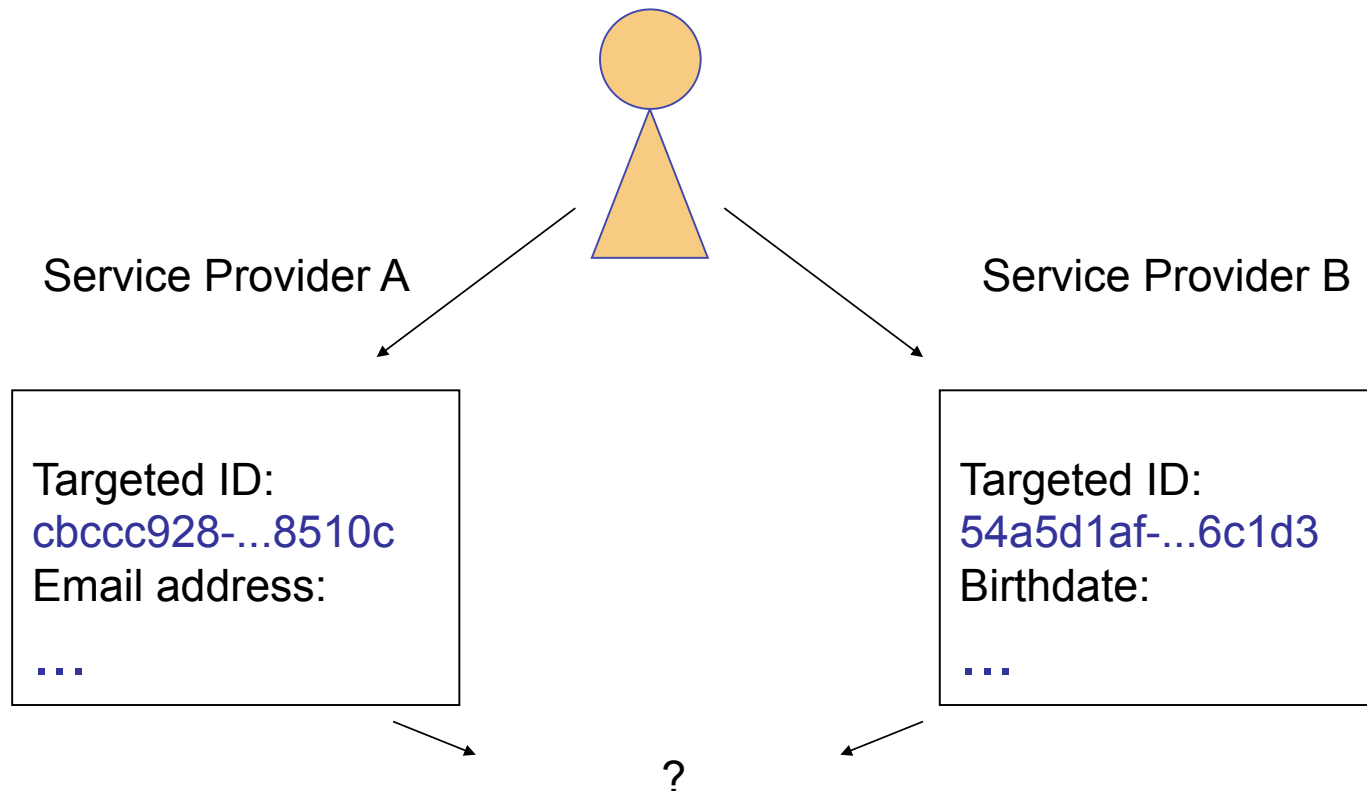


Example persistent ID

`https://idp.example.org/idp/shibboleth!`

`https://sp.example.org/shibboleth!`

`f74698d6-854c-480c-b566-702006318cc3c`



Email vs persistent ID vs Unique ID



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