Federation 101 Refresher

AuthN/AuthR, User Attributes and Identifiers, HO/IDP, SP, DS

Peter Schober, ACOnet (Austria)

GÉANT SA5 T4 Training

Vienna, April 21st & 22nd, 2015

AuthN, AuthZ/AuthR

Authentication Process of confirming an identity

Authorisation Process of confirming access rights to a specific resource (access control)

AuthN, AuthZ/AuthR

- AuthR *usually* presupposes AuthN
- Sometimes AuthN ≈ AuthR (e.g. SSH, httpd ”valid-user”)
- But AuthN ≠ AuthR, esp. in Federated Identity

Examples

“Unknown user or password incorrect.”

“Access denied”

“Your institutional access to this resource has not been validated. Please ask your librarian […]” (nature.com)

Attributes: Usage examples

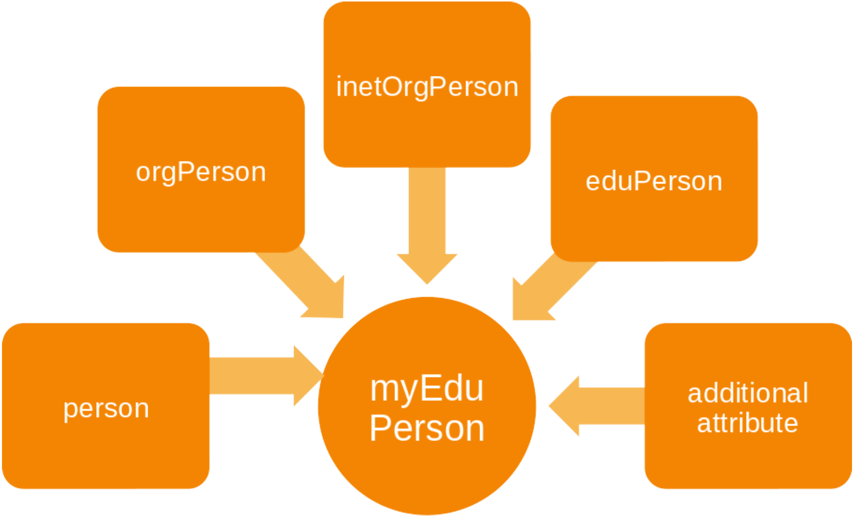
Identification Is subject the same as last time

Authorisation Access decision based on attribute values,
Identity or Role based access control

Profile data Personalisation, identification “for humans”, name,
email address, etc.

Accounting (per subject, per Home Organisation)

Attribute schemas



Common attributes (1)

- Name attributes
  - displayName (`urn:oid:2.16.840.1.113730.3.1.241`)
  - givenName (`urn:oid:2.5.4.42`)
  - sn/surname (`urn:oid:2.5.4.4`)
- Identifiers
  - SAML2 persistent NameID (a.k.a. eduPersonTargetedID, `urn:oid:1.3.6.1.4.1.5923.1.1.1.10`)
  - eduPersonPrincipalName (`urn:oid:1.3.6.1.4.1.5923.1.1.1.6`)
  - mail (`urn:oid:0.9.2342.19200300.100.1.3`)

Common attributes (2)

- Authorisation
  - eduPersonAffiliation ("What I *am*")

    (urn:oid:1.3.6.1.4.1.5923.1.1.1.1)
  - feduPersonScopedAffiliation ("… and where")

    (urn:oid:1.3.6.1.4.1.5923.1.1.1.9)
  - eduPersonEntitlement ("What I *can*")

    (urn:oid:1.3.6.1.4.1.5923.1.1.1.7)
- Organisational data
  - schacHomeOrganization (because 1 IDP ≠ 1 HO)

    (urn:oid:1.3.6.1.4.1.25178.1.2.9)

Common attributes (3)

Examples

displayName: ρεťẹя Ŝçhởьəŗ

eduPersonPrincipalName: `peter@aco.net`

eduPersonScopedAffiliation: `member@aco.net`

eduPersonEntitlement:

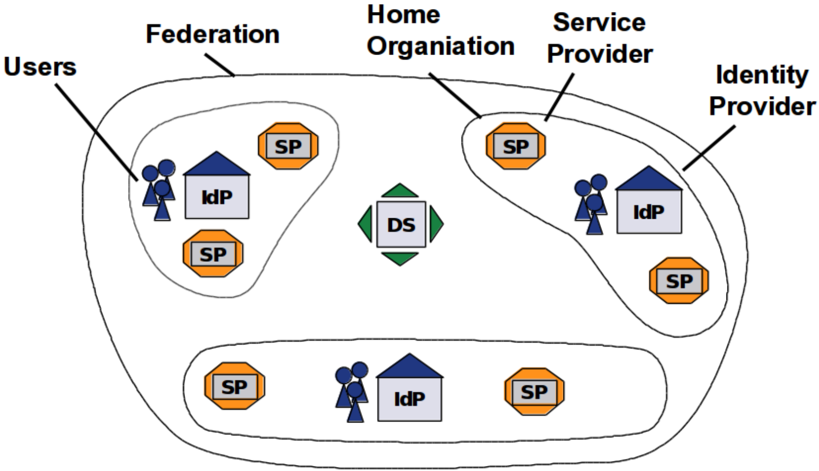
```
 urn:mace:dir:entitlement:common-lib-terms
 urn:mace:terena.org:tcs:personal-user
 http://usi.at/student-discount
```

schacHomeOrganization: `aco.net`

“Players” and Roles

Subject	The “user”, has an affiliation to the HO
HO	Home Organisation, controls the IDP (& own SPs)
IDP	Identity Provider, authenticates Subject and issues data (attributes) about her to SPs
SP	Service Provider, performs access control & provides service based on data from the IDP
DS	(IDP) Discovery Service, lets Subject pick an IDP
Federation	Trusted Third Party, Trust Framework Provider
Metadata	Machine-readable data about IDPs & SPs (mostly)

“Players” and Roles



Federation: Common trust, standards and policies

Questions & Answers

- What examples for authentication and authorisation can you think of, including ones *not involving computers*?
- Where does authorisation happen?
  (At the IDP? The SP? Both?)
- Try to name a few advantages and disadvantages of `eduPersonEntitlement` compared to `eduPerson(Scoped)Affiliation` for authorisation

SAML WebSSO Demo

SWITCHaai Demo Medium