umbrella

Authorisation Models

JF Perrin

How to take benefit of an AAI

"Direct use": restrict access to content and services **based on user attributes**:

- Easy to implement (mod_oauth_openidc, mod_shib, …)

```
<Location /protected>
  AuthType openid-connect
  Require valid-user
  Require claim family_name:Perrin
</Location>
```

- Works for simple cases – you need to have access to users attributes that allow the authorisation decision.
- Typical use case: access to a phonebook, semi-public documents

UmbrellaID attributes

- Up to now, only the EAAH (ID of the user).
- We will soon increase the list of possible attributes.
  - Name
  - Email
  - Affiliation
  - ORCID

https://wiki.geant.org/display/UmbrellaID/Attributes+available+to+Connected+Services

Authorisation based on VO

- Useful for sharing authorisation decision information when working with 3rd parties.
- A VO (Virtual Organisation) has group and sub-group
- Managed by projects or RI, dedicated mgmt. interfaces

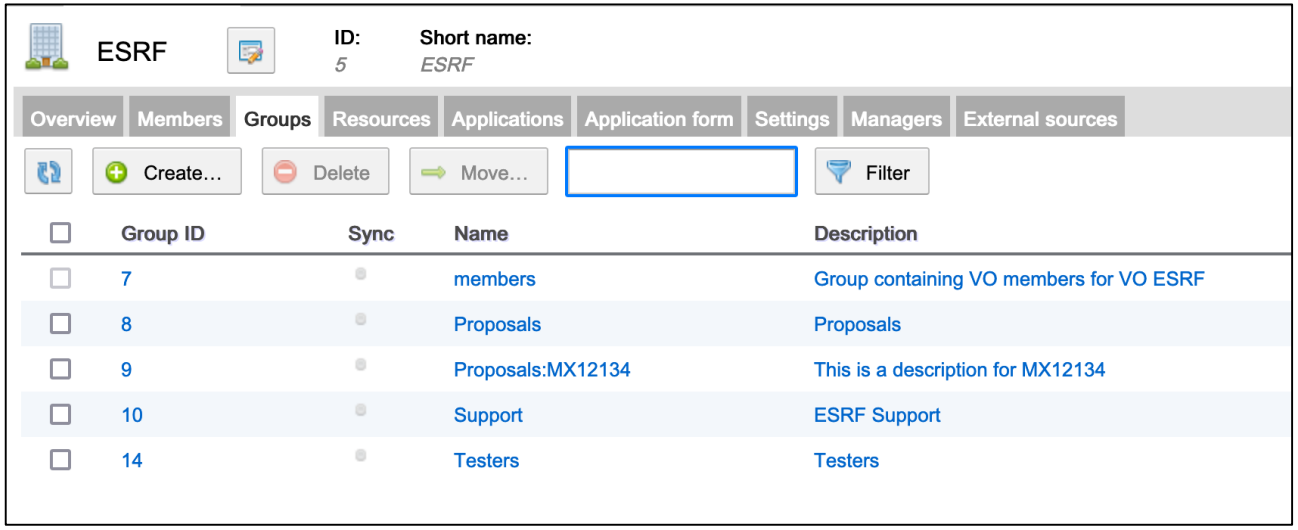
  Proposal: VO = RI
- VO attributes, visible only by services (SP) authorised by the VO manager
- VO is not mandatory

UmbrellaID AAI and Authorization

- The UmbrellaID AAI support a group based architecture that can be used to model authorization structures.
- At the top level there is the Virtual Organization (VO), which is an autonomous group hierartchy with each own organization structure and management.
- One or more VO Managers can manage all aspects of the the VO (e.g. the configuration of the VO, manage the group hierarchy and the VO users)
- The VO can have an arbitary number of nested groups and each group can have each own group admin(s) and application process

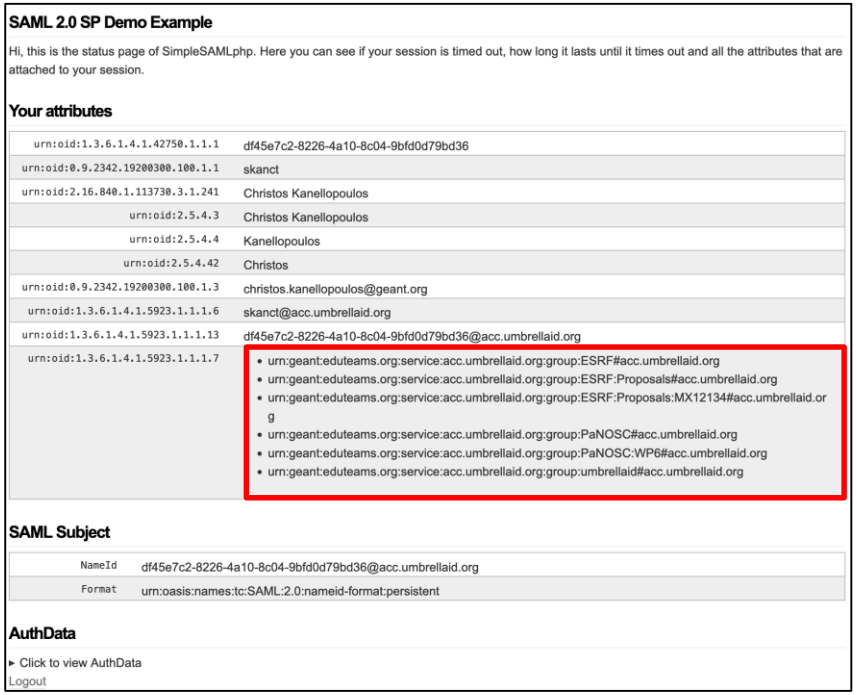
UmbrellaID AAI and Authorization

- For example, ESRF can be modeled as a Virtual Organization with a group structure in it.
- In this example, there are 4 groups: members, Proposal, Support and Testers
- The Proposals group has a subgroup “MX12134” that holds all the users of that project.



UmbrellaID AAI and Authorization

- This information can be used to manage access rights to services and electronic resources



SAML 2.0 SP Demo Example

Hi, this is the status page of SimpleSAMLphp. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that are attached to your session.

Your attributes

urn:oid:1.3.6.1.4.1.42750.1.1.1	df45e7c2-8226-4a10-8c04-9bfd0d79bd36
urn:oid:0.9.2342.19200300.100.1.1	skanct
urn:oid:2.16.840.1.113730.3.1.241	Christos Kanellopoulos
urn:oid:2.5.4.3	Christos Kanellopoulos
urn:oid:2.5.4.4	Kanellopoulos
urn:oid:2.5.4.42	Christos
urn:oid:0.9.2342.19200300.100.1.3	christos.kanellopoulos@geant.org
urn:oid:1.3.6.1.4.1.5923.1.1.1.6	skanct@acc.umbrellaid.org
urn:oid:1.3.6.1.4.1.5923.1.1.1.13	df45e7c2-8226-4a10-8c04-9bfd0d79bd36@acc.umbrellaid.org
urn:oid:1.3.6.1.4.1.5923.1.1.1.7	• urn:geant:eduteams.org:service:acc.umbrellaid.org:group:ESRF#acc.umbrellaid.org • urn:geant:eduteams.org:service:acc.umbrellaid.org:group:ESRF:Proposals#acc.umbrellaid.org • urn:geant:eduteams.org:service:acc.umbrellaid.org:group:ESRF:Proposals:MX12134#acc.umbrellaid.org • urn:geant:eduteams.org:service:acc.umbrellaid.org:group:PaNOSC#acc.umbrellaid.org • urn:geant:eduteams.org:service:acc.umbrellaid.org:group:PaNOSC:WP6#acc.umbrellaid.org • urn:geant:eduteams.org:service:acc.umbrellaid.org:group:umbrellaid#acc.umbrellaid.org

SAML Subject

NameId	df45e7c2-8226-4a10-8c04-9bfd0d79bd36@acc.umbrellaid.org
Format	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

AuthData

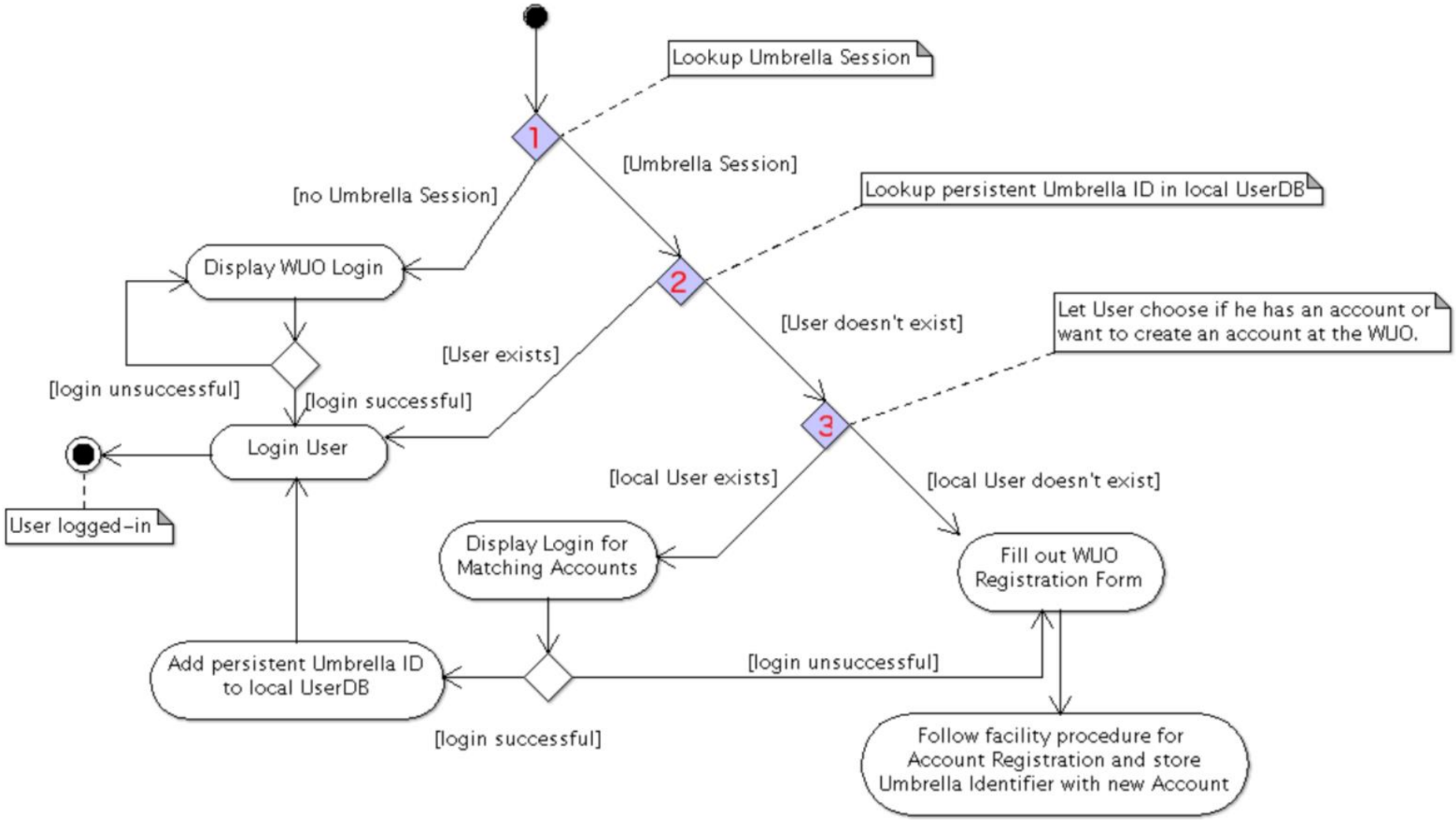
▸ Click to view AuthData

Logout

2nd option: Mapping to local ID

- In your organisation authorisation mechanisms are in place and refer to a local ID
- Mapping the EAAH to a local ID
  - More complex workflow
  - Cumbersome to implement for all applications
  - Use of local SSO (Keycloak) to simplify the set up (Implement the mapping once for all the applications you want to expose).

Mapping workflow



To be discussed this year

Membership Management services

- VO specific **workflows for onboarding members**
- Registry for **user persistent Identifiers**
- Support for **R&S attributes** to maximize interoperability
- Use of **eduPersonEntitlement**(s) to express groups, roles and Service Entitlements
- Choice between **COmanage, HEXAA and Perun**