Authentication and Authorisation for Research and Collaboration

Architecture

Guidelines for the expression of group membership

Nicolas Liampotis

CERN

29 November 2016

Group membership information

- What is it used for:
  - SPs authorise user access to protected resources

- Where does it come from:
  - Home IdP
  - Community-based Attribute Authorities (COmanage, Grouper, HEXAA, Perun, Unity, VOMS, …)

Challenges

- Standardising the way group membership information is expressed:
  - Syntactically: Uniform formatting (e.g. use of URNs within a specific namespace and a set of rules for the NSS portion)
  - Semantically: Common representation of equivalent concepts (e.g. “admin” and “manager” should be communicated to end SPs as “manager”)
- Indicating the entity that is authoritative for each piece of group membership information
- Expressing VO membership and role information
- Supporting group hierarchies in group membership information

Recommendations (I)

- Centralised harmonisation of group membership information → Proxy layer
- Compatibility with existing group information models (SCIM, VOOT, VOMS)
- Scoping of group membership information:
  - Prevent clashes between group name values
  - Allow for easy filtering that can be used by SPs for quick authorisation decisions
- Use of eduPersonEntitlement attribute (vs. isMemberOf) for communicating group membership information:
  - Express more complex info:
    - VO associated with the specified group
    - user's role within that group
    - issuing entity (authority)
  - Compliance with the R&S entity category

Recommendations (II)

- Use of valid URIs, either URLs or URLs:
  - Why URLs?
    - Legitimate URL values are globally unique
    - Easy to delegate their management via use of subdomains
    - Can resolve to actual web pages documenting the values
  - Why URNs?
    - More commonly used by existing IdPs/AAs/Federations
    - Easy to scope using the “@” character which is not reserved in the URN scheme → Services can filter entitlements with minimal parsing and configuration (Shibboleth/SimpleSAMLphp support “@”-based filtering out of the box)

Implementation examples (I)

- Niels' proposal:

  `urn:<namespace>:<service-fqdn>:[<entitlementName>]:[<entitlementValue>]`

  - `<authority-fqdn>`: FQDN of the authoritative source for the entitlement value; either service- or IdP-specific
  - `<service-fqdn>`: name of the service being targeted (RECOMMENDED to be expressed as the service FQDN)
  - `<entitlementName>`: name of entitlement
  - `<entitlementValue>`: value of entitlement
- GN4-1 JRA3 proposal (`anyUri@scope`):

  `urn:<namespace>:<authority-fqdn>:{target}:{service}:[<entitlementName>]:[<entitlementValue>]@[authority-domain]`

Implementation examples (II)

- EGI AAI scheme:

  urn:<namespace>:<authority-fqdn>:[<group>[:<subgroup>:…]]:<role>@<vo>

  - <authority-fqdn>: FQDN of the authoritative source for the entitlement value
  - <vo>: name of the Virtual Organisation
  - <group>: name of a group in the identified <vo> (optional)
  - <subgroup>: the list of <subgroup> components represents the hierarchy of subgroups in the <group> (optional)
  - <role>: the <role> component is scoped to the rightmost (sub)group; if no group information is specified, the role applies to the VO

Thank you

Any Questions?

nliam@grnet.gr

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).