Guidelines on expressing group membership and role information

Published Date: 13-06-2017
Revision: 1.0

Work Package: JRA1
Document Code: AARC-JRA1.4A
Document URL: https://aarc-project.eu/wp-content/uploads/2017/03/AARC-JRA1.4A.pdf

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Table of Contents

Table of Tables

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

1 Introduction

Information about the groups a user is a member of is commonly used by SPs to authorise user access to protected resources. Apart from the group information that is managed by the user's home IdP, research communities usually operate their own group managing services. Such services often act as Attribute Authorities, maintaining additional information about the users, including VO membership, group membership within VOs, as well as user roles. It is therefore necessary that all involved SPs and IdPs/AAs can interpret this information in a uniform way. Specifically, the following challenges need to be addressed:

- Standardising the way group membership information is expressed, both syntactically and semantically:
    - Syntactic: Uniform formatting; for example, representing group membership as URNs within a specific namespace and a set of rules for the NSS portion
    - Semantic: Common representation of equivalent concepts; for instance, "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

Harmonisation of naming for groups, hierarchy and use of ontologies within different scientific domains is explicitly excluded from these guidelines.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

2 General guidelines

The guidelines presented in this section, have been defined based on experiences from multiple parties in the AARC project and have subsequently been discussed and tested through the Service Activity 1 Pilots (SA1) attribute management pilot [AARC-SA1-AMP]. Furthermore, it should be noted that a group membership representation scheme following these recommendations has already been adopted to enable cross-infrastructure exchange of group information between the EGI and the ELIXIR AAI.

- **Centralised harmonisation of group membership information**

  Adopt a proxy-based AAI, to delegate to the proxy component the complexity of dealing with different group membership representations that originate from diverse IdPs/AAs. As a result, the end SPs will not have to handle the harmonisation of group membership information as this will be performed in a centralised fashion by the SP proxy.

- **Compatibility with existing group information models**

  Adopt a group representation scheme that can be easily translated to/from standardised or widely used group data models, such as SCIM, VOOT or VOMS, and POSIX systems, if required.

- **Scoping of group membership information**

  Specify the scopes where the identified group membership information is valid. These scopes should include:

  - The authoritative source for each piece of group membership information.
  - The VO associated with the identified group.
  - The entire chain of group components, from the root parent group to the identified child group (in the case of group hierarchies).

  The rationale behind scoping is to prevent clashes between groups that are managed by different VOs/administrative domains. This eliminates the need for syntactic and semantic group information harmonisation among different communities. An added benefit is that scoping allows easy filtering of group values that can be used by SPs for quick authorisation decisions.

- **Use the eduPersonEntitlement attribute**

  When using SAML, different standardised possibilities are available to convey group membership information. Specifically, both the isMemberOf [SWITCH-IMO] and the eduPersonEntitlement attribute [I2-EPE] can be used for representing group membership. However, eduPersonEntitlement values (formatted as URIs, either URNs or URLs) are, in addition, used to indicate rights to resources. In the case of OpenID Connect there is currently no standard claim to carry group membership information. However, the REFEDS OpenID Connect for Research and Education Working Group

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

[OIDCre] is already investigating the standardisation of new claims for expressing the attributes defined in the eduPerson schema [I2-EP].

It should be noted that while eduPersonEntitlement is not part of the REFEDS "Research and Scholarship" (R&S) [REFEDS-RS]) attribute bundle, an SP may request it if necessary [REFEDS-RS-1], without violating compliance with the R&S entity category. However, SPs are still encouraged to stick to the R&S bundle wherever possible.

- **Use of valid URIs, either URLs or URNs, for representing group membership information**

  As of 2015, MACE [MACE] encourages the use of URLs in preference to URNs [MACE-SR].

  Benefits of using URLs instead of URNs include:

  - Legitimate URL values are globally unique if a suitable (sub)domain is used and a delegation model is in place for defining paths under that root domain. No one else has the legal right to create values under that (sub)domain, so any assignments made under that subdomain will be globally unique.
  - If the URLs resolve to web pages, it is possible to make the assigned values self-documenting by posting a definition of the value at that URL.

    In practice, however, the relevant domain that is used for resolvable URLs is often the domain of corporate public relations departments and as such is not easily maintainable by technical staff responsible for the AAI.
  - URLs do not require a formal registration for a subtree, as is required for URNs.

  Benefits of using URNs instead of URLs include:

  - URNs are currently more commonly used for expressing eduPersonEntitlement values by existing IdPs/AAs/federations.
  - URNs can easily support scoping following a hierarchical structure when necessary. Using the namespace identifier registry delegation model, URN values can thus be managed in a distributed fashion by different issuing authorities, communities/VOs, group management systems.

3 Proposed implementation

3.1 Syntax

Based on the guidelines presented in Section 2, an e-infrastructure, research infrastructure or research collaboration could adopt the following eduPersonEntitlement formatting specification for representing group membership information:

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

```
urn:mace:<namespace>:<authority>:group:<group>[:<subgroup>*][:role=<role>]
```

where:

- `<namespace>` is a registered URN namespace ensuring global uniqueness
- `<authority>` is the FQDN of the authoritative source for the entitlement value
- the literal string `"group"` indicates an eduPersonEntitlement value expressing group membership information
- `<group>` is the name of a Virtual Organisation (VO), research collaboration or a top level arbitrary group;
- an optional list of `<subgroup>` components represents the hierarchy of subgroups in the `<group>`;
- the optional `<role>` component is scoped to the rightmost (sub)group; if no subgroup information is specified, the role applies to the top level group/VO

3.2 Semantics

Each eduPersonEntitlement attribute value represents a particular position of the user within a VO, research collaboration or generally a top level arbitrary group. A user may be a member or hold more specific roles within the groups associated to this top level group. Groups are organised in a tree structure, meaning that a group may have subgroups, which in turn may have subgroups, etc.

This hierarchical structure implies that if someone is member of a subgroup, then they are also member of the parent group. For example:

```
parent-group:child-group
```

implies membership in parent-group, i.e.:

```
parent-group
```

Ownership of any role always implies membership in that particular (sub)group. However, holding a more specific role in a subgroup does not imply the same role in the parent group. For example:

```
parent-group:child-group:role=manager
```

implies plain membership in both child-group and parent-group, but NOT:

```
parent-group:role=manager
```


The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

3.3 Example mappings with existing group representation standards

Standard	Original value	Mapped value
VOMS FQAN [VOMS-FQAN]	/vo.example.org	urn:mace:<namespace>:<authority>:group:vo.example.org
	/vo.example.org/Role=NULL	urn:mace:<namespace>:<authority>:group:vo.example.org
	/vo.example.org/Role=manager	urn:mace:<namespace>:<authority>:group:vo.example.org:role=manager
	/vo.example.org/thegroup/thesubgroup/thesubsubgroup	urn:mace:<namespace>:<authority>:group:vo.example.org:thegroup:thesubgroup:thesubsubgroup
	/vo.example.org/thegroup/thesubgroup/thesubsubgroup/Role=NULL	urn:mace:<namespace>:<authority>:group:vo.example.org:thegroup:thesubgroup:thesubsubgroup:role=manager
	/vo.example.org/thegroup/thesubgroup/thesubsubgroup>/Role=manager	urn:mace:<namespace>:<authority>:group:8878ae43-965a-412a-87b5-38c398a76569
SCIM [SCIM] / VOOT [VOOT]	{ "id": "8878ae43-965a-412a-87b5-38c398a76569", "displayName": "Project on group APIs" }	urn:mace:<namespace>:<authority>:group:8878ae43-965a-412a-87b5-38c398a76569
VOOT	{ "id": "e01eafb1-5f1c-4992-fcd5-ab0160c7ad24", "displayName": "Course M.201 Mathematics at University of Oslo", "membership": { "basic": "member", }	urn:mace:<namespace>:<authority>:group:e01eafb1-5f1c-4992-fcd5-ab0160c7ad24:role=member

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

Standard	Original value	Mapped value
	}	
	{ "id": "e01eafb1-5f1c-4992-fcd5-ab0160c7ad24", "displayName": "Course M.201 Mathematics at University of Oslo", "membership": { "basic": "admin", } }	urn:mace:<namespace>:<authority>:group:e01eafb1-5f1c-4992-fcd5-ab0160c7ad24:role=admin

Table 3.1: Example mappings with existing group representation standards

4 References

[AARC-SA1-AMP] Attribute Management Pilot wiki https://wiki.geant.org/display/AARC/AttributeManagementPilot

[I2-EPE] eduPersonEntitlement description http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonEntitlement

[MACE] MACE website https://www.internet2.edu/communities-groups/middleware/middleware-architecture-committee-education-mace/

[MACE-SR] "Information for organisations requesting a delegated namespace" https://www.internet2.edu/products-services/trust-identity/mace-registries/#service-registries

[OIDCre] REFEDS OpenID Connect for Research and Education Working Group https://wiki.refeds.org/display/GROUPS/OIDCre

[REFEDS-RS] REFEDS web page: Research and Scholarship Entity Category https://refeds.org/category/research-and-scholarship

[REFEDS-RS-1] REFEDS wiki page: "Are SPs allowed to request attributes other than R&S attributes?" https://wiki.refeds.org/display/ENT/Research+and+Scholarship+FAQ#ResearchandScholarshipFAQ-AreSPsallowedtorequestattributesotherthanR&Sattributes?

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).

[SCIM]	System for Cross-domain Identity Management https://tools.ietf.org/html/rfc7644
[VOOT]	VOOT http://openvoot.org/datamodel/
[SWITCH-IMO]	isMemberOf description https://www.switch.ch/aai/support/documents/attributes/ismemberof/index.html
[VOMS-FQAN]	VOMS Fully Qualified Attribute Name: https://www.ogf.org/documents/GFD.182.pdf

5 Glossary

AA	Attribute Authority
AAI	Authentication and Authorisation Infrastructure
EGI	European Grid Infrastructure
FQDN	Fully Qualified Domain Name
IdP	Identity Provider
MACE	Middleware Architecture Committee for Education
NSS	Namespace Specific String
OIDCre	OpenID Connect for Research and Education
POSIX	Portable Operating System Interface
REFEDS	Research and Education FEDerations group
R&S	Research and Scolarship
SCIM	System for Cross-domain Identity Management
SP	Service Provider
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
URN	Uniform Resource Name
VO	Virtual Organization
VOMS	Virtual Organization Membership Service
VOOT	Virtual Organization Orthogonal Technology

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965 (AARC).