Guidelines for expressing affiliation information

Publication Date:	2019-04-08
Authors:	AARC Consortium Partners;AppInt members;Diego Scardaci (ed.)
Document Code:	AARC-G025
DOI:	
Grant Agreement No.:	730941
Work Package:	JRA1

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

The goal of this document is to define how affiliation information should be expressed when transported across AARC BPA-compliant AAIs. Two different types of affiliation have been identified, namely Affiliation within the Home Organisation, such as a university, research institution or private company; and Affiliation within the Community, such as cross-organisation collaborations. Both affiliation types should be communicated to the service providers that rely on affiliation information in order to control access to resources.

Table of Contents

1. Introduction

After the analysis of several use cases, two different types of affiliation have been identified:

1. **Affiliation within Home Organisation**, such as a university, research institution or private company;
2. **Affiliation within Community**, such as cross-organisation collaborations.

Both affiliation types should be communicated to the service providers that rely on affiliation information in order to control access to resources. Note the use of the word "within," suggesting that the affiliation is not necessarily just membership but could also include the type of membership or role in the organisation.

This document details how this information should be transported across AARC BPA-compliant AAIs and presented to the service providers.

1.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Types of affiliation of information

This chapter describes the types of affiliation information.

2.1. Affiliation within Home Organisation

Each user can be affiliated with one or more Home Organisations (such as, a university, research institution or private company) and the user's affiliations may change over time. The user's Home Organisation expresses affiliation information typically through the eduPersonScopedAffiliation attribute (ePSA) [EPSA] defined in the 200312 version of the eduPerson schema. ePSA is a multi-valued attribute that:

> "specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc. The values consist of a left and right component separated by an "@" sign. The left component is one of the values from the eduPersonAffiliation controlled vocabulary [EPA]. The right-hand component of ePSA is the "scope" whose value MUST be the administrative domain to which the affiliation applies."

The affiliation within the user's Home Organisation is typically used by Service Providers for controlling access to resources, or for accounting purposes[1]. After receiving a scoped attribute

[1] Most services that authorise access based on institutional subscriptions will need to know whether a person is a "member" (as opposed to, say, "affiliate" or "library-walk-in", who would not be authorised to use the service through an institutional subscription.) For "members" (who are authorised), cases have been proposed where the service needed to know whether they were "students" specifically, in order to report the percentage of authorised users who were students.

from the IdP of the Home Organisation, SPs are expected to filter the attribute values by comparing the asserted scope to the scope value(s) in the IdP SAML metadata or to a locally defined list. Therefore, a BPA-compliant proxy SHOULD NOT release affiliation with Home Organisation information using ePSA because the SAML IdP metadata of the proxy typically does not include the scopes of the proxied Home Organisation IdPs. Instead, the proxy SHOULD ensure that the affiliation of the user within their Home Organisation (as released by the Home Organisation through the ePSA attribute) is conveyed to Service Providers via the voPersonExternalAffiliation (vPEA) attribute [VPEA]. The vPEA was defined in version 1.1.0 of the VO Person schema. The syntax and semantics of the vPEA attribute follows the ePSA described above. In particular, vPEA attributes values are scoped, but SPs SHOULD NOT verify the scope value against the list of acceptable scopes as asserted by the proxy in its SAML IdP metadata. As long as vPEA is not used for other purposes, the original authority of the asserted value can be gleaned from the scope of the value. An example flow of the attributes conveying the affiliation within the home organisation is illustrated in Figure 1.

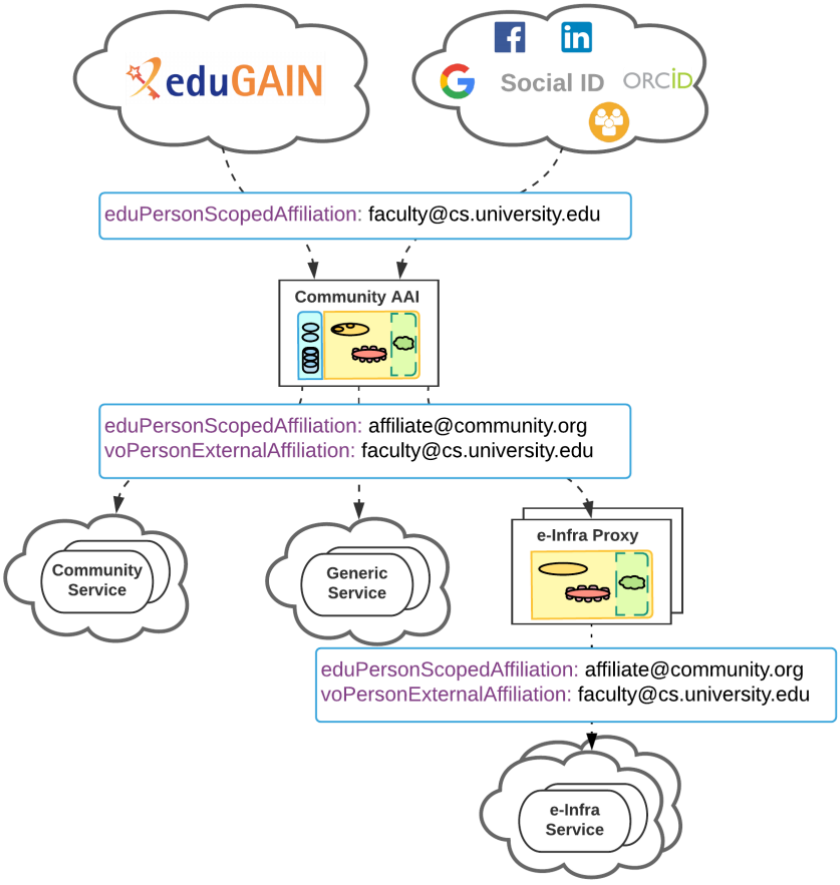

Figure 1. Flow of affiliation information across AARC-BPA compliant AAIs: Affiliation with Home Organisation is typically released to the BPA-compliant proxy of the community/research infrastructure/collaboration by the IdP of the Home Organisation through the eduPersonScopedAffiliation attribute. Services connected to the community SP-IdP-Proxy consume the Affiliation with Home Organisation information through the voPersonExternalAffiliation attribute. The Affiliation within Research Infrastructure can also be made available through the eduPersonScopedAffiliation attribute.

2.2. Affiliation within Community

Communities typically grant their members access to services and resources as expressed through each member's community identity [AARC-G045]. The SP-IdP-proxy that is serving the Community SHOULD release the affiliation within the Community using the eduPersonScopedAffiliation attribute [EPSA]. To allow the SPs behind the IdP proxy to consume the ePSA attribute values, the security domain(s) of the Community should be included as allowed scope values in the IdP proxy metadata. An example flow of the attributes conveying the affiliation within the community is illustrated in Figure 1.

3. Representation of affiliation information

This chapter specifies how the types of affiliation information presented in Chapter 2 shall be represented using federated identity protocols.

3.1. Security Assertion Markup Language 2.0 (SAML)

In SAML, affiliation information is represented as follows:

1. Affiliation within Home Organisation is represented using the multi-valued voPersonExternalAffiliation attribute, as defined in voPerson [VPEA].
2. Affiliation within Community is represented using the multi-valued eduPersonScopedAffiliation attribute, as defined in eduPerson [EPSA].

See Appendix A for examples.

3.2. OpenID Connect (OIDC)

In OIDC, affiliation information is represented as follows:

1. Affiliation within Home Organisation is represented using the multi-valued voperson_external_affiliation claim, as defined in voPerson [VPEA], following the naming conventions specified in [OIDCRE].
2. Affiliation within Community is represented using the multi-valued eduperson_scoped_affiliation claim, as defined in eduPerson [EPSA], following the naming conventions specified in [OIDCRE].

See Appendix A for examples.

4. Expression of affiliation information freshness

This document has adopted the definition of freshness from version 1.0 of [RAF] which defines hierarchical values for expressing the "freshness" of affiliation information. "Freshness" here does not mean the actual freshness of the attribute, i.e. the time when the home organisation validated it, but rather the target *time window* within which the published value must change

following a change in the user's affiliation. Specifically, when asserting `$RAF-PREFIX$/ATP/ePA-1d` for a given user, `$RAF-PREFIX$/ATP/ePA-1m` MUST also be asserted. Note that RAF is limited to the eduPersonAffiliation, eduPersonScopedAffiliation and eduPersonPrimaryAffiliation attributes defined in [EP]. Additionally, the freshness of the attribute is further limited by the RAF specification to apply only to the following attribute values: "faculty", "student" and "member". Other values and attributes are out of scope of the RAF specification. Therefore, this document introduces the following additional values for expressing the freshness of affiliation information, which have no restriction on the values of the ePSA attribute. If the ePSA value is one of the values covered by the RAF specification (i.e. the left component of the value is one of "faculty", "student" or "member"), the affiliation freshness values MAY be expressed by asserting both the AARC and the RAF values. Note that the AARC values (listed in Table 1) are expressed as URIs which have the following prefix:

`$AARC-PREFIX$=https://aarc-community.org/assurance`

Value	Description
$AARC-PREFIX$/ATP/ePA-1m	eduPersonScopedAffiliation (SAML) / eduperson_scoped_affiliation (OIDC) (if populated and released to the RP) reflects user's departure from the Community within[2] 31 days time. If the value of affiliation is one of "faculty", "student" and "member" then $RAF-PREFIX$/ATP/ePA-1m MAY be asserted in addition to $AARC-PREFIX$/ATP/ePA-1m.
$AARC-PREFIX$/ATP/ePA-1d	eduPersonScopedAffiliation (SAML) / eduperson_scoped_affiliation (OIDC) (if populated and released to the RP) reflects user's departure from the Community within one day. If the value of affiliation is one of "faculty", "student" and "member" then $RAF-PREFIX$/ATP/ePA-1d MAY be asserted in addition to $AARC-PREFIX$/ATP/ePA-1d.
$AARC-PREFIX$/ATP/vPEA-1m	voPersonExternalAffiliation (SAML) / voperson_external_affiliation (OIDC) attributes (if populated and released to the RP) reflect user's departure from the Home Organisation within 31 days time. $AARC-PREFIX$/ATP/vPEA-1m SHOULD only be released if a) the Home Organisation released the eduPersonScopedAffiliation value within the same authentication session and b) the HO follows procedures in line with the $RAF-PREFIX$/ATP/ePA-1m policy, which is asserted by the HO to the proxy either via the release of the $RAF-PREFIX$/ATP/ePA-1m or by other means).
$AARC-PREFIX$/ATP/vPEA-1d	voPersonExternalAffiliation (SAML) / voperson_external_affiliation (OIDC) attributes (if populated and released to the RP) reflects user's departure from the Home Organisation within one day. $AARC-PREFIX$/ATP/vPEA-1d SHOULD only be released if a) the Home Organisation released the eduPersonScopedAffiliation value within the same

[2] Since we need to follow RAF's definition of freshness, we have adopted the wording from the RAF specification. The use of the word "within" is ambiguous as it can suggest past or future, but the use here copies the usage in RAF. The intended meaning is that if at some point there is an event that leads to the user no longer being entitled to the attribute as originally published, this change is reflected by the attribute being changed accordingly, or removed, after at most 31 days following the event.

	authentication session and b) the HO follows procedures in line with the $RAF-PREFIX$/ATP/ePA-1d policy, which is asserted by the HO to the proxy either via the release of the $RAF-PREFIX$/ATP/ePA-1d or by other means).

Note that the term departure is used according to the definition from Section 2.3 in version 1.0 of [RAF].

References

AARC-G045 AARC Blueprint Architecture: Community-first approach; https://aarc-project.eu/guidelines/aarc-g045/

EP eduPerson Object Class Specification (201602); http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html

EPA eduPersonAffiliation attribute definition; http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html#eduPersonAffiliation

EPSA eduPersonScopedAffiliation attribute definition; http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html#eduPersonScopedAffiliation

OIDCRE REFEDS White Paper for implementation of mappings between SAML 2.0 and OpenID Connect in Research and Education; https://wiki.refeds.org/download/attachments/38895621/20181011-OIDC-WP.pdf?version=2&modificationDate=1539611807924&api=v2

RAF REFEDS Assurance Framework; https://refeds.org/assurance

VPEA voPersonExternalAffiliation attribute definition; https://github.com/voperson/voperson/blob/1.1.0/voPerson.md#vopersonexternalaffilation-attribute-definition

Appendix A. Examples

The table below lists example values for the different types of affiliation information:

Description	SAML attribute	OIDC claim	Example value
Affiliation within Community	eduPersonScopedAffiliation	eduperson_scoped_affiliation	affiliate@lifescienceid.org
Affiliation within Home Organisation	voPersonExternalAffiliation	voperson_external_affiliation	member@example.org