Inferring and constructing origin-affiliation information across infrastructures

Publication Date	2021-01-12
Editor:	David Groep, *et al.* for the AARC Community
Document Code:	AARC-G057
DOI:	10.5281/zenodo.4433649
Reference as:	https://aarc-community.org/guidelines/aarc-g057
Community:	Policy Area

The work leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme and other sources.

Abstract

Conveying affiliation information from origin providers across infrastructures proxies as defined in G025 is only possible if the origin identity provider releases such information. In case no eduPersonScopedAffiliation is provided, it may be partially reconstructed according to these guidelines. If there is no reliable way to infer origin affiliation, no such affiliation should be asserted by infrastructure proxies.

Table of Contents

1. Introduction

The AARC Guidelines for expressing affiliation information [AARC-G025] defines how affiliation information should be expressed when transported across AARC Blueprint Architecture (BPA) compliant AAIs. In it, two different types of affiliation were distinguished, namely ‘affiliation within the home organisation’ (i.e. the ‘origin’ identity provider) 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, and it designated the *voPersonExternalAffiliation* attribute (hereafter called *vPEA*) as the bearer-attribute for the origin affiliation (the affiliation with the home organisation).

However, G025 does not provide guidance as to what should be conveyed in *vPEA* in case such origin information is lacking. For operational, consistency, and security reasons, for service providers that connect to more than one proxy, it is necessary that all infrastructure proxies act similarly in case of lacking origin affiliation information.

This Guideline defines the conditions and mechanisms governing the inference and (re)construction of origin affiliation information that may be conveyed to service providers connecting to an infrastructure proxy.

In case no *eduPersonScopedAffiliation* is provided by the origin, it may be partially reconstructed according to these guidelines. If there is no reliable way to infer origin affiliation, no such affiliation should be asserted by compliant infrastructure proxies.

This Guideline does not replace any specification or mechanism defined in G025. In case origin affiliation is provided to the infrastructure proxy by the home IdP. such affiliation must thus be conveyed verbatim in the *vPEA* attribute as per the guidance in G025. This Guideline has no influence on the *eduPersonScopedAffiliation* attribute as asserted by an infrastructure proxy.

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].

Where this document states *voPersonExternalAffiliation*, also the (OIDC) claim *voperson_external_affiliation* may be read. Where this document states *eduPersonScopedAffiliation*, also the claim *eduperson_scoped_affiliation* may be read.

2. When to construct origin affiliation

A proxy SHOULD NOT assert *vPEA* unless the service provider requests this attribute. If no origin *ePSA* attribute is provided, and no *vPEA* is requested by the service provider, then a proxy MUST NOT construct a gratuitous *vPEA*.

If a service provider requests *vPEA*, but no *ePSA* is provided by the origin, a proxy SHOULD infer or construct a *vPEA*, and if it does, MUST do so only in accordance with this Guideline.

3. Construction of origin affiliation

Origin affiliation MUST be determined either in an automated way, or by explicitly verified enrolment.

3.1. Automated construction

The origin affiliation, of the form *affiliationtype@scope*, and conveyed by the proxy to service providers in the *vPEA* attribute, MUST be constructed in the following way

1. If the origin provides *eduPersonScopedAffiliation*, its value MUST be used verbatim.
2. If the origin provides *eduPersonAffiliation*, and the scope of the origin provider can be reliably determined, the *vPEA* MUST be constructed by concatenating the value of *eduPersonAffiliation* provided, the "@" (at) sign, and the scope of the origin provider as determined according to the verification rules below.
3. If the origin does not provide any affiliation information, but the scope of the origin provider can be reliably determined, the *vPEA* MUST be constructed by concatenating the string literal "unknown@" and the determined scope of the origin provider.
   The reliable value of scope for the origin provider MUST be determined in accordance with the verification rules below.
   The potential for collision of the value literal "unknown" also being obtained from the origin provider is acknowledged, but this will not change the way the *vPEA* will be constructed.

A reliable value of *scope* for the origin provider MUST be:

a) from the trusted source of meta-data with which the assertion coming from the origin provider is validated, specifically the value of *shibmd:scope* from the eduGAIN meta-data; or

b) from a (verified) *iss* claim; or

c) from the value of the *schacHomeOrganisation* attribute, if that attribute is asserted in the same attribute statement that contains the *eduPersonAffiliation*; or

d) from the *scope* element of another scoped attribute whose scope has been validated against a trusted source, e.g., *eduPersonPrincipalName*; or

e) from matching the attribute signing certificate with that of a public registry of identity providers where the domain-name part of the provider is validated to at least browser-trust domain-control validation standards[1]; or

f) from an explicit validation of the value of scope assigned to that identity provider which confirms its managerial control over the name in the public domain name system corresponding to the *scope* value.

[1] As per https://cabforum.org/baseline-requirements-documents/, or in a registry with reep-like functionality.

3.2. Verified enrolment

The proxy MAY determine the appropriate value of *vPEA* by explicit verification, if all of the following requirements are met:

- The value of scope MUST be determined in accordance with the requirements for reliable in section 3.1
- For asserting the *affiliate* prefix-value for a user for which *vPEA* is to be asserted,
    a) the user MUST be able to prove control of a mailbox whose domain name part of the email address is identical or subordinate to the value of *scope* as determined for its origin provider, by explicit challenge to such an email address; or

    b) the user MUST present a one-time challenge (to the proxy registration service) which has been sent prior to a validated administrative, technical, helpdesk, or billing contact address for the origin provider listed in the eduGAIN meta-data; or

    c) other methods whose strength is equivalent or stronger than one of the methods listed above.
- For asserting *member*, *student, employee*, or *faculty* prefix-value for a user for which *vPEA* is to be asserted, the user MUST be validated in a way that establishes organisational authority over the claim made.
    a) The user MUST present a one-time challenge (to the proxy registration service) which has been sent prior to a source authoritative for the organisation, contacted in a manner that validates the organisation in a verifiable way. This may be sent by phone call or mail to an organisation whose details (e.g. telephone number) are obtained from a Qualified Information Source[2] for the country or region of its establishment, and the affiliation information from an officer responsible for personnel or student affairs; or

    b) the organisational authority - or a designated and authorized representative thereof - explicitly confirms the claim for each of its own end-users, e.g. through managing such claims in the directory used by the proxy; or

    c) other methods whose strength is equivalent or stronger than one of the methods listed above.
- No other prefix-values may be asserted.

For entities where *vPEA* is asserted based on verified enrolment, special care must be taken not to violate the freshness specification requirements of section 4 of G025 (i.e. the https://aarc-community.org/assurance/ATP/vPEA-*period* values). The period stated therein start after each verification of enrolment.

[2] Typical Qualified Information Sources are Chambers of Commerce, Statutory Registries, credit rating agencies, and business registries.

References

AARC-G025	*Expressing affiliation information across infrastructures*, AARC Guideline G025 (11 March 2019); https://doi.org/10.5281/zenodo.3700927
RFC2119	*Key words for use in RFCs to Indicate Requirement Levels* https://www.ietf.org/rfc/rfc2119