Guidelines for expressing community user identifiers

Publication Date:	2021-06-14
Authors:	Marcus Hardt, Jens Jensen, Ivan Kanakarakis, Christos Kanellopoulos, Nicolas Liampotis (ed.), Mikael Linden, Mischa Sallé
Document Code:	AARC-G026
DOI:	10.5281/zenodo.5504407
Reference as:	https://aarc-community.org/guidelines/aarc-g026
Working Area:	Architecture

Abstract

This document provides guidelines for expressing Community User Identifiers (CUIDs) such that the identifier values can be transported in an interoperable way across AARC Blueprint Architecture (BPA) compliant Authentication & Authorisation Infrastructures (AAIs). The CUID is a subject identifier, where the subjects are generally but not exclusively natural persons. The community user identifier is an attribute of the subject's digital identity which is managed by the Community AAI. The guidelines specify how the CUID is communicated from the Community AAI to its connected services, i.e. infrastructure services (accessible through Infrastructure Proxies), generic and community services.

Table of Contents

1 Introduction

This document provides guidelines for expressing Community User Identifiers (CUIDs) such that the identifier values can be transported in an interoperable way across AARC Blueprint Architecture (BPA) compliant Authentication & Authorisation Infrastructures (AAIs). The CUID is a subject identifier, where the subjects are generally but not exclusively natural persons. The community user identifier is an attribute of the subject's digital identity which is managed by the Community AAI **[AARC-G045]**. This Community Identity typically includes additional attributes such as profile information, group membership and role information. The guidelines specify how the CUID is communicated from the Community AAI to its connected services, i.e., infrastructure services (accessible through Infrastructure Proxies), generic and community services **[AARC-G045]**. This specification imposes requirements that must be implemented by the Community AAI and the Infrastructure Proxy. These requirements may serve as best practices for other services.

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 [**RFC2119]**.

2 Identifier concepts

Identifiers can generally be described by the following properties (see also **[SHIB-NameIdentifiers]**):

- **persistent** - denotes an identifier intended to be used for an extended period of time across multiple sessions. Conversely, an identifier intended to be used for a relatively short period of time that need not span multiple sessions is called a **transient** identifier.

- **permanent** - denotes a subject identifier that persists over the entire lifetime of the subject's relationship with the issuer of the identifier[1]. A permanent identifier is also a persistent identifier.
- **opaque** - denotes a privacy-preserving identifier that by itself provides no information about the subject (e.g., a UUID Version 4). An identifier that can be used to identify the subject is called a **transparent** identifier (e.g., an email address).
- **targeted** (or **pairwise**) - denotes an identifier intended for a specific relying party (or group of parties) and not for anyone else. An identifier that is not targeted is a **shared** (or **public**) identifier.

3 General guidelines

This section provides general guidelines for expressing community user identifiers that can be transported across AARC BPA-compliant AAIs. The community user identifier:

- MUST be unique within the issuing system and is therefore globally unique when combined with either an identifier of the issuing system or scope of the community
- MUST be assigned so that no two values created by distinct identity systems could collide when identifying different subjects.
- SHOULD be opaque

[1] A permanent identifier which is not scoped to the IdP or community might be transferred to another IdP/community if the user changes their community and the applicable policies permit it. Typically, this will require the user to request the transfer and prove their “ownership”.

- once assigned, MUST NOT be reassigned to another subject
- SHOULD be permanent
- MUST be persistent
- MUST be shared; if there are privacy and regulatory requirements that need to be met, the proxy may not release this community user identifier to specific relying parties; for instance, to prevent them from using the identifier as a basis for correlation.

4 Considerations for different federated identity protocols

This section discusses protocol-specific considerations for communicating CUIDs.

4.1 Security Assertion Markup Language 2.0 (SAML)

The community user identifier MUST be communicated using the `voPersonID` attribute defined in voPerson schema version 2.0 (draft) **[voPerson-v2.0]**. Other types of identifiers that may become available to relying parties are out of scope of this specification.

4.1.1 NameID considerations

The use of the voPersonID attribute is meant as a replacement of the `<saml:NameID>` element as a means for identifying users. However, <saml:NameID> identifiers MAY need to be supported for compatibility reasons but their use MUST NOT be required (see also **[SAML2int-v2.0]**).

4.2 OpenID Connect (OIDC) and OAuth 2.0

The community user identifier MUST be communicated using the `voperson_id` claim defined in voPerson schema version 2.0 (draft) **[voPerson-v2.0]**. The `voperson_id` claim MUST be present in the UserInfo Response and in the ID Token.

5 Considerations when communicating community user identifiers across AAI services

The infrastructure proxy SHOULD forward the community user identifier unless specific privacy or regulatory policies need to be met.

6 References

[AARC-G045] AARC Blueprint Architecture 2019 (AARC-G045); https://aarc-community.org/guidelines/aarc-g045/

[**RFC2119]** Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, https://www.rfc-editor.org/info/rfc2119

[SAML2int-v2.0] SAML V2.0 Deployment Profile for Federation Interoperability, Dec 2019, https://kantarainitiative.github.io/SAMLprofiles/saml2int.html

[SHIB-NameIdentifiers] Shibboleth Consortium, "Name Identifiers", v. 24, Jan 10, 2018; https://wiki.shibboleth.net/confluence/pages/viewpage.action?pageId=4358265

[voPerson-v2.0] Oshrin, B., Koranda, S., and J. Basney, "voPerson v2.0”, Draft, May 6, 2021; https://github.com/voperson/voperson/blob/draft-2.0.0/voPerson.md