understanding-federated-user-identifiers

Jump to:

Introduction | Four characteristics of identifiers | User identifiers used in Federated SSO | Comparison of identifiers users in the Incommon Federation

Introduction

This article compares user identifiers (based on their definitions) in use within the InCommon Federation with five fundamental identifier characteristics to determine when and if an identifier is appropriate to use given any federated SSO scenario.

TL;DR

If you just want to know what identifiers to request without the background discussion, see Cho osing the Right Federated User Identifier.

Four characteristics of identifiers

Privacy-preserving

A *privacy-preserving identifier* prevents a 3rd party from discovering its principal’s (person) identity by examining the identifier’s value. It is REQUIRED to be opaque, having no particular relationship to the principal's other identifiers, such as a username or the individual’s real name. It may also inhibit receiving parties from using this identifier to correlate user information, therefore discovering a person’s identity when it is not intended.

Implementations should consider that releasing non-privacy preserving information (such as email addresses) in combination with these types of identifiers can defeat the privacy protections the IDs are intended to provide.

Unique

A *unique identifier* represents one and only one principal (person) in the system the identifier is issued. An identifier is said to be unique when no two principals can share the same identifier at the same time within an identity system. A *globally unique identifier* introduces additional syntax to guarantee that two identity systems do not issue the same identifier to represent different persons.

Non-reassignable

A non-reassignable identifier is attached to only one Principal (person), i.e., once created, it cannot be repurposed to represent another Principal at any time, even when the Principal associated with the identifier no longer exists in the issuing identity system.

Persistent (long-lived)

A *persistent identifier* is a long-lasting reference to a principal (person) in an identity system. An identifier is said to be persistent if a service can rely on this identifier to point to the same person across multiple interactions.

User identifiers used in Federated SSO

These identifiers are “in play” in the InCommon federated SSO ecosystem. They are either long-established/supported user identifiers, emerging recommendations, or identifiers in use because of common external requests.

See: Navigating federated identifiers

eduPersonPrincipalName (ePPN)

eduPersonPrincipalName is a user identifier attribute defined in the eduPerson LDAP object class. It is a scoped identifier for a person. As this identifier is often used by humans to identify the person it represents, ePPN values are often, but not required to be, human-friendly, and may change as a result of various business processes.

See: eduPerson Object Class Specification (202001) - eduPersonPrincipalName

Choosing the right user identifier

- Why is email address not an appropriate user identifier?
- eduPersonUniqueID
- Why is eduPersonTargetedID deprecated?
- SAML General Purpose Subject Identifier (subject-id)
- SAML Pairwise Subject Identifier (pairwise-id)
- eduPersonPrincipalName (eppn)
- eduPersonTargetedID (eptid)
- Understanding Federated User Identifiers

Related content

- An Introduction to User Data
- R&S Explained in Plain English
- Understanding Federated User Identifiers
- Why is email address not an appropriate user identifier?
- Why is eduPersonTargetedID deprecated?

Get help

Can't find what you are looking for?

help Ask the community

eduPersonTargetedID (ePTID)

eduPersonTargetedID is a user identifier attribute defined in the eduPerson LDAP object class. It is a persistent, non-reassigned, opaque identifier for a principal designed to prevent two relying parties receiving user information from an Identity Provider from correlating user information, thus revealing the user identity when it is not intended.

eduPersonTargetedID is deprecated. It will be marked as obsolete in a future release of the eduPerson Object Class specification.

See: eduPerson Object Class Specification (202001) - eduPersonTargetedID

See: Why is eduPersonTargetedID deprecated?

eduPersonUniqueID (ePUID)

eduPersonUniqueID is a user identifier attribute defined in the eduPerson LDAP object class. It is a long-lived, non-reassignable, omnidirectional identifier suitable for use as a principal identifier by authentication providers or as a unique external key by applications.

See: eduPerson Object Class Specification (202001) - eduPersonUniqueID

SAML V2.0 General Purpose Subject Identifier (subject-id)

The SAML V2.0 General Purpose Subject Identifier is a user identifier attribute defined in the SAML v2.0 Subject Identifier Attributes Profile. It is a long-lived, non-reassignable, omnidirectional identifier suitable for use as a globally-unique external key. Its value for a given subject is independent of the relying party to whom it is given.

See: SAML v2.0 Subject Identifier Profile - General Purpose Subject Identifier

SAML V2.0 Pairwise Subject Identifier (pairwise-id)

The SAML V2.0 General Purpose Subject Identifier is a user identifier attribute defined in the SAML v2.0 Subject Identifier Attributes Profile. It is a long-lived, non-reassignable, unidirectional identifier suitable for use as a unique external key specific to a particular relying party. Its value for a given subject depends upon the relying party to whom it is given, thus preventing unrelated systems from using it as a basis for correlation.

See: SAML v2.0 Subject Identifier Profile - Pairwise Subject Identifier

Email Address

Commercial service providers commonly request the email address as a user identifier in Federated SSO.

See: Why is email address not an appropriate user identifier?

Comparison of identifiers users in the Incommon Federation

	Privacy-preserving	**Unique**	**Non-reassignable**	**Persistent**	**Consistent matching rules**
SAML V2.0 General Purpose Subject Identifier	Poor[1]	Excellent	Excellent	Excellent	Excellent
SAML v2.0 Pairwise Subject Identifier	Excellent	Excellent	Excellent	Excellent	Excellent
ePPN	Poor[2]	Good	Good/Poor[3]	Excellent	Excellent
eduPersonTargetedID[4]	Excellent	Excellent	Excellent	Excellent	Poor
eduPersonUniqueID	Poor	Excellent	Excellent	Excellent	Excellent
Email Address	Very Poor	Poor	Poor	Good	Poor

Notes

1. General Subject Identifier is not required to be opaque. Depending on the implementation of the ID at an institution, the identifier value itself may reveal the identity of the person it represents. The identifier is also correlatable.

2. ePPN is not required to be opaque. Depending on the implementation of the ID at an institution, the identifier value itself may reveal the identity of the person it represents. The identifier is also correlatable.

3. Depending on the implementation at an institution, an ePPN may be reassigned to a different person over time.

4. eduPersonTargetedID has been deprecated. Deployers who currently support eduPersonTargetedID should transition to supporting the SAML v2.0 Pairwise Subject Identifier as a privacy-preserving persistent identifier.