user-attr-epuid

Overview

eduPersonUniqueID is a long-lived, non re-assignable, omnidirectional identifier suitable for use as a principal identifier by authentication providers or as a unique external key by applications.

This identifier is scoped and of the form `uniqueID@scope`.

The `uniqueID` portion MUST be unique within the context of the issuing identity system and MUST contain only alphanumeric characters (a-z, A-Z, 0-9). The length of the uniqueID portion MUST be less than or equal to 64 characters.

The `scope` portion MUST be the administrative domain of the identity system where the identifier was created and assigned. The `scope` portion MAY contain any Unicode character. The length of the scope portion MUST be less than or equal to 256 characters. Note that the use of characters outside the seven-bit ASCII set or extremely long values in the scope portion may cause issues with interoperability.

See also: Scope in InCommon metadata

OID	1.3.6.1.4.1.5923.1.1.1.13
LDAP Syntax	Directory String
# of Values	single-value
References	eduPerson

Use in the InCommon Federation

eduPersonUniqueID is supported in the InCommon Federation. It is widely used in InCommon as well as in global R&E federations.

eduPersonUniqueID satisfies the REFEDS Research & Scholarship (R&S) entity category's requirement for a shared user identifier.

Although an **eduPersonUniqueID's** formatting resembles that of an email address, an relying party receiving an **eduPersonUniqueID** MUST NOT treat this identifier as an email address for the principal. It is unlikely for it to be valid for that purpose.

IdP organizations MUST NOT use existing email address values as values for this identifier unless the email address meets ALL (long-lived, non-reassigned, syntax constraints, etc.) of the requirements of the **eduPersonUniqueID**.

SAML Response Example

Working with user data

- Additional user data handling recommendations
- Handling User Data Exchange in SAML
- Getting user data to manage access control
- Person characteristics and contact information
- eduPersonEntitlement
- eduPersonAssurance
- Common name (cn)
- displayName
- givenName
- Surname (sn)

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

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                ID="..." Version="2.0" IssueInstant="2020-07-17T01:01:48Z"
                Destination="...." InResponseTo="...">
 ...
 <saml:Assertion ...>
  ...
   <saml:AttributeStatement>
    <saml:Attribute xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:
attribute:X500"
                    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
                    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.13"
                    FriendlyName="eduPersonUniqueID"
                    x500:Encoding="LDAP">
      <saml:AttributeValue xsi:type="xsd:string">ae4017bf0980@example.edu<
/saml:AttributeValue>
   </saml:Attribute>
   ...
   </saml:AttributeStatement>
 </saml:Assertion>
</samlp:Response>
```

See Also

- eduPersonTargetedID
- eduPersonPrincipalName
- SAML General Purpose Subject Identifier (subject-id)
- SAML Pairwise Subject Identifier (pairwise-id)
- Understanding Federated User Identifiers