user-attr-edupersonassurance

Jump to:

Overview

`eduPersonAssurance` delivers a set of URIs that expresses a user credential's compliance with specific standards for identity assurance. This multi-valued attribute represents identity assurance profiles (IAPs), which are the set of standards that are met by an identity assertion, based on the Identity Provider's identity management processes and the strength of the binding between those processes and the real world identity of the subject.

`eduPersonAssurance` is defined in the eduPerson LDAP object class.

OID	1.3.6.1.4.1.5923.1.1.1.11
LDAP Syntax	Directory String
# of Values	multi-valued
References	eduPerson

Use in the InCommon Federation

When implementing the REFEDS Assurance Framework (RAF), an identity provider communicates to a service provider in the SAML assertion that the signed-in user meets identity proofing and credentialing assurance requirements using the **`eduPersonAssurance`** attribute.

A user may meet multiple IAP requirements defined in RAF. In these cases, the identity provider should send ALL applicable RAF values.

Applicable Values

See the REFEDS Assurance Framework for specific value definitions.

The REFEDS Assurance Framework defines a range of values to signal varying levels of identity proofing and credential issuance. The Identity Assurance Profile values (sections 2.2), in particular, are hierarchical, i.e., qualifying for a higher level of assurance also qualifies the credential for a lower level. For example, a credential meeting the requirements of `/IAP/medium` also meets the requirements of `/IAP/low`.

When asserting a person's assurance level, the identity provider should send ALL applicable RAF values, not only the highest one. If a credential meets the requirements for `/IAP/medium`, the identity provider should assert `/IAP/medium` AND `/IAP/low`.

Examples

Example 1

In this example:

- the identity management system satisfies the baseline expectations for Identity Providers
- the identity management system has issued the signed-in user a unique identifier value (`/ID/Unique`)
- the user is ID-proofed face-to-face using government-issued photo-ID (`/IAP/medium`)
- the user has access to mission critical enterprise systems (`/IAP/local-enterprise`)

These qualifications means the identity provider should assert the following assurance attribute values:

- `https://refeds.org/assurance`
- `https://refeds.org/assurance/ID/unique`
- `https://refeds.org/assurance/IAP/local-enterprise`
- `https://refeds.org/assurance/IAP/low`
- `https://refeds.org/assurance/IAP/medium`

In SAML 2.0, this looks like:

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

Example 1: IAP assertion

```
<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
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.11"
FriendlyName="eduPersonAssurance">
<saml:AttributeValue xsi:type="xsd:string">https://refeds.org/assurance<
/saml:AttributeValue>
<saml:AttributeValue xsi:type="xsd:string">https://refeds.org/assurance/ID
/unique</saml:AttributeValue>
<saml:AttributeValue xsi:type="xsd:string">https://refeds.org/assurance/IAP
/medium</saml:AttributeValue>
<saml:AttributeValue xsi:type="xsd:string">https://refeds.org/assurance/IAP
/low</saml:AttributeValue>
<saml:AttributeValue xsi:type="xsd:string">https://refeds.org/assurance/IAP
/local-enterprise</saml:AttributeValue>
</saml:Attribute>
...
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```

The remaining examples omit the SAML syntax for brevity.

See Also

- eduPersonAffiliation
- eduPersonScopedAffiliation
- eduPersonEntitlement

Example 2

In this example, the user is a guest. Guests, for the purposes of this example, prove control of an email address and provide self-asserted personal information and so qualify for IAP "low", but are not generally given any access to enterprise systems.

Summarizing:

- the identity management system satisfies the baseline expectations for Identity Providers
- the identity management system has issued the signed-in user a unique identifier value (`/ID/Unique`)
- the user controls an email account and has self-asserted their information (`/IAP/low`)

These qualifications means the identity provider should assert the following assurance attribute values:

- `https://refeds.org/assurance`
- `https://refeds.org/assurance/ID/unique`
- `https://refeds.org/assurance/IAP/low`

Example 3

In this example, the user can login to the Identity Provider via a social identity that masks much of their information and the organization has very little control over or trust in the credential's binding to a person. Furthermore, the IdP is passing through an identifier managed by the social identity source and that may be reassigned.

Summarizing:

- the identity management system satisfies the baseline expectations for Identity Providers
- the identity management system does not possess a reliably unique identifier for the user
- the identity management system does not wish to vouch for any aspect of the processes used by the social identity provider

These qualifications means the identity provider should assert only the following assurance attribute value:

- `https://refeds.org/assurance`

The single value provides no additional confidence in this specific social identity but does indicate to the relying party that the organization is compliant with the REFEDS Assurance Framework and that the absence of additional values is deliberate.