# Transforming Identifiers between OIDC and SAML


- Identifier Properties
- Compatible implementations
  - SAML to OIDC
    - Mapping eduPerson SAML => OIDC public sub claim
    - Mapping eduPerson SAML => OIDC pairwise sub claim
  - OIDC to SAML
    - Mapping OIDC public sub claim => SAML
    - Mapping OIDC pairwise sub claim => SAML


## Identifier Properties

This section investigates identifier properties (non-reassigned, opaque, persistent and unique per service/RP) as describe in the specifications of eduPerson SAML and OIDC Sub claims.

Some of the identifier properties are implementation dependent, if s these are marked with ?.

| **Identifier Properties** | | **Properties** | | | |
|---|---|---|---|---|---|
| | | Non-reassigned | Opaque | Persistent | Unique per Service |
| **eduPerson SAML Identifiers** | | | | | |
| eduPersonPrincipalName | | ✗ | ✗ ? | ✓ | ✗ |
| eduPersonUniqueId | | ✓ | ✓ | ✓ | ✗ |
| eduPersonTargetedID | | ✓ | ✓ | ✓ | ✓ |
| SAML2 Persistent NameID | | ✓ | ✓ | ✓ | ✓ |
| SAML2 transient NameID | | NA | ✓ | ✗ | ✗ |
| | | | | | |
| **OIDC Sub claims** | | | | | |
| Public | | ✓ | ? | ✓ | ✗ |
| Pairwise | | ✓ | ✓ | ✓ | ✓ |

Note: Technically eduPersonPrincipleName may be used in an opaque way, however, this is not common and but this may be unfriendly to enduser as ePPNs may be displayed to endusers

Note: A Pairwise sub may also provide the same sub for "a group of Web sites under single administrative control"

## Compatible implementations

Based on the identifier properties, a mapping can be made on what would be compatible implementations, going between OIDC and SAML eduPERSON

### SAML to OIDC

#### Mapping eduPerson SAML => OIDC public sub claim

SAML identifiers compatibility for creating an OIDC public claim

The table blow marks compatible (GREEN) and Incompatible (RED) mappings. In some cases compatibility can arise from making a specific implementation (YELLOW).

| **Identifier Properties** | | **Properties** | | | | |
|---|---|---|---|---|---|---|
| | | Non-reassigned | Opaque | Persistent | Unique per Service | Remarks |
| **eduPerson SAML Identifiers** | | | | | | |
| eduPersonPrincipalName | | ✗ | ✗ | ✓ | ✗ | OIDC sub may not be reassigned |
| eduPersonUniqueId | | ✓ | ✓ | ✓ | ✗ | |
| eduPersonTargetedID | | ✓ | ✓ | ✓ | ✓ | Public sub must not change per RP |
| SAML2 Persistent NameID | | ✓ | ✓ | ✓ | ✓ | Public sub must not change per RP |

| | | | | | | |
|---|---|---|---|---|---|---|
| SAML2 transient Name ID | | NA | ✓ | ✗ | ✗ | OIDC sub may not be reassigned |
| | | | | | | |
| **OIDC Sub claims** | | | | | | |
| Public | | ✓ | ? | ✓ | ✗ | |

## Mapping eduPerson SAML => OIDC pairwise sub claim

SAML identifiers compatibility for creating an OIDC pairwise claim

The table blow marks compatible (GREEN) and Incompatible (RED) mappings. In some cases compatibility can arise from making a specific implementation (ORANGE).

| **Identifier Properties** | | **Properties** | | | | |
|---|---|---|---|---|---|---|
| | | Non-reassigned | Opaque | Persistent | Unique per Service | Remarks |
| **eduPerson SAML Identifiers** | | | | | | |
| eduPersonPrincipalName | | ✗ | ✗ | ✓ | ✗ | OIDC sub may not be reassigned |
| eduPersonUniqueId | | ✓ | ✓ | ✓ | ✗ | OIDC Per service identifier mandatory |
| eduPersonTargetedID | | ✓ | ✓ | ✓ | ✓ | Public sub must not change per RP |
| SAML2 Persistent NameID | | ✓ | ✓ | ✓ | ✓ | Public sub must not change per RP |
| SAML2 transient Name ID | | NA | ✓ | ✗ | ✗ | OIDC sub may not be reassigned |
| | | | | | | |
| **OIDC Sub claims** | | | | | | |
| Pairwise | | ✓ | ✓ | ✓ | ✓ | |

Note:For simplicity it is assumed there is only 1 Web sites under single administrative control

# OIDC to SAML

## Mapping OIDC public sub claim => SAML

SAML identifiers that can be created from an OIDC public claim

The table blow marks compatible (GREEN) and Incompatible (RED) mappings. In some cases compatibility can arise from making a specific implementation (ORANGE).

| **Identifier Properties** | | **Properties** | | | | |
|---|---|---|---|---|---|---|
| | | Non-reassigned | Opaque | Persistent | Unique per Service | Remarks |
| **eduPerson SAML Identifiers** | | | | | | |
| eduPersonPrincipalName | | ✗ | ✗ | ✓ | ✗ | |
| eduPersonUniqueId | | ✓ | ✓ | ✓ | ✗ | |
| eduPersonTargetedID | | ✓ | ✓ | ✓ | ✓ | public sub claim is not issues per SP |
| SAML2 Persistent NameID | | ✓ | ✓ | ✓ | ✓ | public sub claim is not issues per SP |
| SAML2 transient Name ID | | NA | ✓ | ✗ | ✗ | transient properties may be implemented by proxy |
| | | | | | | |
| **OIDC Sub claims** | | | | | | |
| Public | | ✓ | ? | ✓ | ✗ | |

## Mapping OIDC pairwise sub claim => SAML

SAML identifiers that can be created from an OIDC pairwise claim

The table below marks compatible (GREEN) and incompatible (RED) mappings. In some cases compatibility can arise from making a specific implementation (ORANGE).

| **Identifier Properties** | | **Properties** | | | | |
|---|---|---|---|---|---|---|

| | | Non-reassigned | Opaque | Persistent | Unique per Service | Remarks |
|---|---|---|---|---|---|---|
| **eduPerson SAML Identifiers** | | | | | | |
| eduPersonPrincipalName | | ✗ | ✗ | ✓ | ✗ | Technically Opaque pairwise claim can be used,<br><br>but this may be very unfriendly to enduser as ePPNs may be displayed to endusers |
| eduPersonUniqueId | | ✓ | ✓ | ✓ | ✗ | Pairwise sub is unique per RP |
| eduPersonTargetedID | | ✓ | ✓ | ✓ | ✓ | |
| SAML2 Persistent NameID | | ✓ | ✓ | ✓ | ✓ | |
| SAML2 transient NameID | | NA | ✓ | ✗ | ✗ | Transient NameID is Unique per service by definition |
| | | | | | | |
| **OIDC Sub claims** | | | | | | |
| Pairwise | | ✓ | ✓ | ✓ | ✓ | |

An OIDC pairwise sub claim can be mapped to a SAML2 Persistent NameID. For example, consider the following ID token:

**A sample ID token**

```
{
 "iss": "https://server.example.com",
 "sub": "24400320",
 "aud": "s6BhdRkqt3",
 "nonce": "n-0S6_WzA2Mj",
 "exp": 1311281970,
 "iat": 1311280970,
 "auth_time": 1311280969,
 "acr": "urn:mace:incommon:iap:silver"
}
```

Suppose the sub claim in the above ID token is a pairwise sub claim. Then that claim can be mapped to the following SAML2 Persistent NameID:

**A SAML2 Persistent NameID**

```
<saml2:NameID
   Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
   NameQualifier="https://server.example.com"
   >24400320</saml2:NameID>
```

Note that the `saml2:NameID/@SPNameQualifier` XML attribute has been omitted.