Subject Identifiers in the UK federation

Jon Agland

Trust and Identity, Jisc

Jisc

Subject Identifiers in the UK federation

- Background (What are they, existing, the new standard, problems)
- Supporting the new standard as IdP (first)
- Supporting the new standard as SP (later)
- Supporting the new standard as a federation operator

What are Subject Identifiers?

Subject - a person or thing that is being discussed, described, or dealt with.

Identifier - a person or thing that identifies someone or something.

Existing Subject Identifiers in the federation

From the eduPersonSchema [1]

eduPersonTargetedID is an abstracted version of the SAML V2.0 Name Identifier format of "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"

eduPersonPrincipalName is a scoped identifier for a person. It should be represented in the form "user@scope" where 'user' is a name-based identifier for the person. Each value of 'scope' defines a namespace within which the assigned identifiers MUST be unique

[1] **https://wiki.refeds.org/display/STAN/eduPerson**

Further identifiers in the federation

eduPersonNamePrincipalPrior

- multi-valued
- only one SP has this a Requested Attribute

eduPersonUniqueID

- appeared in 2013, low take-up
- indication that 59 SPs have Requested Attributes for this
- Only one of those directly registered in the UK federation.

- **[1] https://wiki.refeds.org/display/STAN/eduPerson**

Jisc

Requested Attribute as an indicator

Requested Attributes as a (bad!) indicator of attribute usage...

eduPersonTargetedID - 674

eduPersonPrinicpalName - 1269

- Federation default policy – advises release of both these by IdPs to SPs
- Only 378 of 1731 SPs in the UK federation have Requested Attributes in their metadata.

Existing Subject Identifiers in SAML

Name Identifiers

- Some commonly used NameIDs
  - `urn:oasis:names:tc:SAML:2.0:nameid-format:`**`persistent`**
  - `urn:oasis:names:tc:SAML:2.0:nameid-format:`**`transient`**
  - `urn:oasis:names:tc:SAML:1.1:nameid-format:`**`emailAddress`**
- An IdP in the UK federation will typically release
  - Transient in the Subject
  - Persistent in a SAML Attribute (eduPersonTargetedID)

Email Address as an Identifier

- Not guaranteed unique to a subject
  - e.g. service@ukfederation.org.uk
- Maybe be re-assigned
  - e.g. vc@camford.ac.uk
  - e.g. joe.bloggs@camford.ac.uk
- Life events or affiliation may change it
- Not always assigned by institution
- May not be validated
- https://spaces.at.internet2.edu/display/federation/why-is-email-not-an-appropriate-user-identifier
- Here our war story!

New Standard – SAML Subject Identifiers

Two new SAML Attributes defined in a new standard [1]

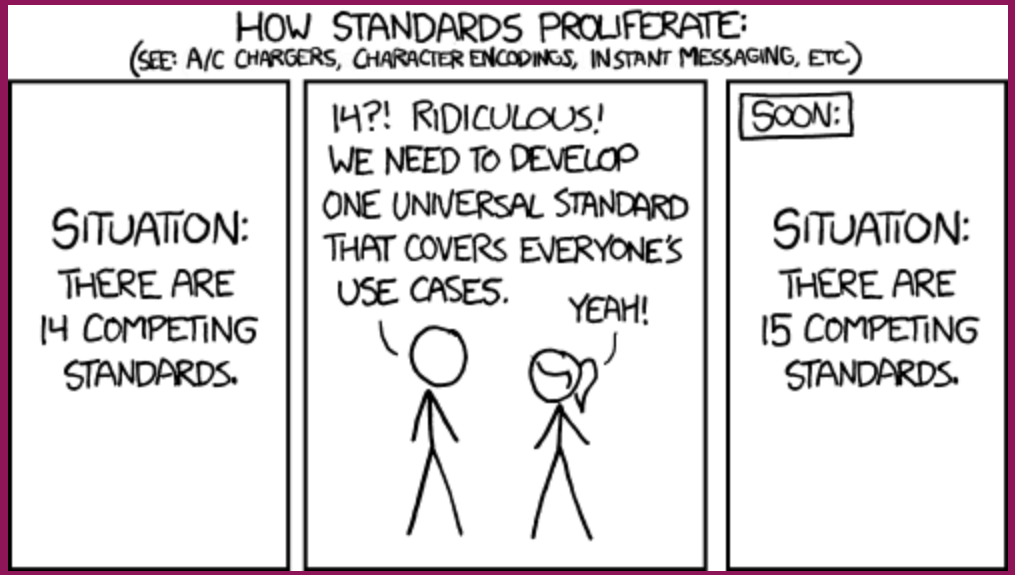
- **urn:oasis:names:tc:SAML:attribute:subject-id**
  - bob123132@example.ac.uk
  - Alignment with **eduPersonUniqueID**
- **urn:oasis:names:tc:SAML:attribute:pairwise-id**
  - NVSXE2DNMFZWIZ3BONSGO2DBONSGOCQ=@example.ac.uk
- Hang on this looks familiar? SAML1/eduPerson mace-dir/eduPersonTargetedID.old
- Review the problem statement in the standard.

- [1] http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html

Drivers – SAML Subject Identifiers

- New standard has been ratified for over two years.
  - Use cases are coming...
- eduPerson 2020-01 marks existing identifier as deprecated
  - *eduPersonTargetedID is DEPRECATED and will be marked as obsolete in a future version of this specification.*
- New REFEDS Research and Scholarship v2.0 entity category
  - Nearing consultation, will require the new SAML Subject Identifier.
  - Research intensive organisations, may need to support the new standard sooner.

eduPersonTargetedID is dead, long live eduPersonTargetedID



https://xkcd.com/927/

One existing problem - Case sensitivity

- Existing Identifiers may be using case sensitive values
- Existing Shibboleth IdPs, Base64, ComputedID StoredID.
- How does an SP handle this scenario?

```
https://idp.example.ac.uk/idp!https://sp.example.org/sp!bWVyaG1hc2RnYXNkZ2hhc2RnCg==
```

```
https://idp.example.ac.uk/idp!https://sp.example.org/sp!BWVYAG1HC2RNYXNKZ2HHC2RNCG==
```

- New(er) Shibboleth IdPs deployers should use Base32.
- SPs can test with the UK federation Test IdP (accounts Yanny and Laurel) [1]

[1] https://www.ukfederation.org.uk/content/Documents/TestIdP

Two questions for IdPs? (a poll)

- How are you deriving **eduPersonTargetedID**?
  - (what is the source attribute)
- How are you deriving **eduPersonPrincipalName**?
  - (what is the source attribute)?

Supporting the SAML subject identifiers - IdPs

A fresh start?

- If your existing ComputedID connector uses Base64, then you should.
- Change to Base32
- Change source attribute
  - `ObjectGUID`, `ObjectSid` – these tie you heavily to Microsoft Active Directory, Binary Attributes tricky to handle
  - `uid`, `sAMAccountName`, `userPrincipalName`, `cn`, `mail` – all potentially affected by changes of name, affiliation
  - **employee and student number** – on the face of it, a great choice as a source `pairwise-id`
  - What source for `subject-id`?

Two more questions for IdPs (another poll!)

- What source attribute would you use for **subject-id**?
  - `(urn:oasis:names:tc:SAML:attribute:`**`subject-id`**`)`
- What source attribute would you use for **pairwise-id**?
  - `(urn:oasis:names:tc:SAML:attribute:`**`pairwise-id`**`)`

Signalling

We talked about Requested Attributes..

- SPs signalling what attributes they support/require using Requested Attributes
- Existing Requested Attributes are another problem
  - Can't say "*I'd like one of* `eduPersonPrincipalName`, `eduPersonTargetedID` *or* `mail` *(Email address) please?*"
  - Can only say "these are required, these are not required/optional"
- New entity category has options of `pairwise-id`, `subject-id`, `any` or `none`
- How do IdP operators feel about `subject-id` being auto released?
  - Will you being using an attribute containing personal information?
  - Quick poll..

entityIDs vs scopes

- Existing SAML attributes are tied based on entityID - another problem!
- Deployment of the new Subject Identifiers
  - Will eventually free us from the tie of the entityID
  - Will tie us instead to the scope
  - In the meantime, we will be tied to both?
  - Aren't we already?
- Scopes
  - A single scope can be asserted by multiple IdPs
  - IdPs can assert multiple scopes (depending on their software/configuration)
  - Scopes and the domains they represent are verified for compliance with our metadata registration practice statement [1]

[1] https://docs.ukfederation.org.uk/mdrps/

Jisc

Shibboleth IdP configuration

(examples from Shib IdP 4.1.0)
attribute-resolver.xml

```
<!-- Schema: SAML Subject ID Attributes -->
<AttributeDefinition xsi:type="Scoped" id="samlSubjectID" scope="%{idp.scope}">
    <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}"/>
</AttributeDefinition>

<AttributeDefinition xsi:type="Scoped" id="samlPairwiseID" scope="%{idp.scope}">
    <InputDataConnector ref="computed" attributeNames="computedId"/>
</AttributeDefinition>
```

Add a new/different Computed connector?

```
<DataConnector id="computed" xsi:type="ComputedId"
    excludeResolutionPhases="c14n/attribute"
    generatedAttributeID="computedId"
    salt="%{idp.persistentId.salt}"
    algorithm="%{idp.persistentId.algorithm:SHA}"
    encoding="BASE32">

    <InputDataConnector ref="myLDAP" attributeNames="%{idp.persistentId.sourceAttribute}" />

</DataConnector>
```

Shibboleth IdP configuration

attribute-filter.xml

(per 3.5.1 of the new standard)

```
<AttributeFilterPolicy id="subject-identifiers">
    <PolicyRequirementRule xsi:type="ANY" />

    <AttributeRule attributeID="samlPairwiseID">
        <PermitValueRule xsi:type="OR">
            <Rule xsi:type="EntityAttributeExactMatch"
                attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req"
                attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                attributeValue="pairwise-id" />
            <Rule xsi:type="EntityAttributeExactMatch"
                attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req"
                attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                attributeValue="any" />
        </PermitValueRule>
    </AttributeRule>

    <AttributeRule attributeID="samlSubjectID">
        <PermitValueRule xsi:type="EntityAttributeExactMatch"
            attributeName="urn:oasis:names:tc:SAML:profiles:subject-id:req"
            attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            attributeValue="subject-id" />
    </AttributeRule>
</AttributeFilterPolicy>
```

Shibboleth SP configuration

(default in a new installation of Shib SP 3)

shibboleth2.xml

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
    REMOTE_USER="eppn subject-id pairwise-id persistent-id"
```

attribute-map.xml

```
<Attribute name="urn:oasis:names:tc:SAML:attribute:subject-id" id="subject-id">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>

<Attribute name="urn:oasis:names:tc:SAML:attribute:pairwise-id" id="pairwise-id">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>
```

Shibboleth SP configuration

(default in a new installation of Shib SP 3)

shibboleth2.xml

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
    REMOTE_USER="eppn subject-id pairwise-id persistent-id"
```

attribute-map.xml

```
<Attribute name="urn:oasis:names:tc:SAML:attribute:subject-id" id="subject-id">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>

<Attribute name="urn:oasis:names:tc:SAML:attribute:pairwise-id" id="pairwise-id">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder" caseSensitive="false"/>
</Attribute>
```

Supporting the SAML subject identifiers - SP

- No personalisation, no worries?

- Possibly one, reporting may show more unique users.

Supporting the SAML subject identifiers - SP

Maintaining Personalisation

- Problem of mapping X to Y in a lot of cases
  - `https://idp.example.ac.uk/idp!https://sp.example.org/sp!bWVyaG1hc2RnYXNkZ2hhc2RnCg==`
  - `NVSXE2DNMFZWIZ3BONSGO2DBONSGOCQ=@example.ac.uk`
- Will likely need co-ordination between IdP and SP
- Might need to share and log the most recent **Assertion ID** to aid this process.
- Attribute priority might need to be done per customer, rather than per service?
  - In the Shibboleth SP REMOTE_USER vs Attribute itself

Supporting the SAML subject identifiers - SP

Building a new SP

- If I was deploying an SP today and required personalisation attributes..
- `urn:oasis:names:tc:SAML:attribute:subject-id` fallback to `eduPersonPrincipalName`
- `urn:oasis:names:tc:SAML:attribute:pairwise-id` fallback to `eduPersonTargetedID`
- `urn:oasis:names:tc:SAML:attribute:pairwise-id` fallback to `eduPersonPrincipalName`
  - Handy if your end application can't handle `SPentityID!IdPentityID!value`

Supporting the SAML subject identifiers – UK federation

- **What do we need to do?**
  - Build the new entity category support into our tooling, so that SPs can signal their support
  - Setup IdP test accounts that release `pairwise-id` and `subject-id`
  - Test SP and attribute viewer
    - Might be additional entityIDs based on the four values of the entity attribute
  - Guidance/documentation for Shibboleth IdP and SP operators
  - Your thoughts and feedback?

Jisc

Thank you!

Jon Agland

Technical Services Manager, Trust and Identity, Jisc

---

service@ukfederation.org.uk

T: 0300 300 2212, option 2

customerservices@jisc.ac.uk

jisc.ac.uk