Standardized values for eduPersonEntitlement

Introduction

The attribute **eduPersonEntitlement** indicates a set of rights to specific resources. You might require that a user has a specific value registered in eduPersonEntitlement to allow access to your service or parts of it. This attribute is typically used to assert privileges maintained centrally or remotely rather than within specific (local) application databases. eduPersonEntitlement is a **multivalued** attribute. Each value is a uniform resource identifier (URI) representing a license, permission, right and more to access a resource or service in a particular fashion. Entitlements represent an assertion of authorization to something, computed and asserted by the identity provider. Read the eduPerson Object Class Specification (201310) to get in depth information about the attribute.

> Entitlements are always negotiated between an SP and IdP. It makes little to no sense for an SP to request an entitlement if an IdP is not able or willing to provide such a value.

Using eduPersonEntitlement within SURFconext federation

Within SURFconext we standardize the way the values of this attribute are expressed, because:

- We want to scope the value of the attribute, so it is clear who is authoritative for its value(s) and prevent clashes between attribute values for different SPs (e.g. when two SPs both would need an 'admin' entitlement)
- We want to be able to filter this attribute in our Attribute Release Policy (ARP) so a specific value can be directed to specific SP's. **As SURFconext does not support filtering on URL based attributes, it is recommended to only use URN based attribute values.**
- As it has to be a URI, we want to attach a namespace that is compliant with namespace requirements for Uniform Resource Names (URN's). This will simplify national and international deployment of the attribute and its values.
- We do not want to create something new if in an international context a good alternative already exists.

Technically, eduPersonEntitlement MUST be a **URI**, either **URN (Uniform Resource Name)** or **URL (Uniform Resource Locator)**. In case a URN is used, URN namespacing conventions MUST be applied. For more information on URN namespaces read the documentation as found online and the official RFC will give you more understanding about this. We note that in general using and registering formal namespaces is rather cumbersome. To circumvent the registration problem, while still remaining compliant with RFC3406, we allow x-surfnet to be used within SURFconext as an accepted custom namespace. The namespace is then presented as follows [namespace] = 'x-surfnet:example.org'. Note the added colon ':' as part of [namespace].

Specification

To meet the requirements, values for eduPersonEntitlement for use within SURFconext MUST adopt the formatting specification as depicted.

Generic Format

Example without the use of entitlement name:

```
urn:[namespace]:[servicename]:[entitlementValue]
```

or:

Example with entitlement name:

```
urn:[namespace]:[servicename]:[entitlementName]:[entitlementValue]
```

Example:

- urn:x-surfnet:surf.nl:surfdrive:quota:100
- In this example 'x-surfnet:surf.nl' is the namespace, surfdrive the servicename, quota the entitlementName and 100 the entitlementValue.

Whether or not to include an entitlementName as part of the value is up to the parties involved.

Identity Provider Specific Entitlements

In such a case it is the IdP that defines the entitlement value. In general this is not very convenient, as this means the SP will need to interpret each entitlement value on a per IdP basis.

```
urn:[IdP namespace]:[servicename]:{[entitlementName]}:[entitlementValue]
```

Note that the IdP namespace needs to be formally registered, or a prefix of `x-` needs to be used to signify a custom namespace.
e.g.:

- `urn:mace:exampleIdP.org:demoservice:demo-admin`
- `urn:x-surfnet:surfnet.nl:sab:role:instellingscontactpersoon`

Service Specific Entitlements

The common scenario when using eduPersonEntitlement is that an SP defines the attribute values it needs for its service. Always check if a generic attribute is not already available (e.g. eduPersonAffiliation, UID). Note that even if the SP defines the attributes, the IdP is authoritative for the values being provided!

```
urn:[SP namespace]:[servicename]:{[entitlementName]}:[entitlementValue]
```

Note that the SP namespace needs to be formally registered, or a prefix of `x-` needs to be used to signify a custom namespace.

Examples:

- `urn:mace:example.terena.org:tcs:personal-user`
- `urn:x-surfnet:surfdomeinen.nl:role:dnsadmin`
- `urn:x-surfnet:surf.nl:surfdrive:quota:100`