IDP 4 include-RandS-reassigned-ePPN

REFEDS R&S and reassigned ePPN attributes

Note if your deployment of the eduPersonPrincipalName (ePPN) attribute allows for reassigning ePPN values from one person to another that R&S v1.x requires you to also release a SAML 2.0 persistent NameID then. Because SAML 2.0 persistent NameIDs prohibit reassignment also releasing those enables R&S Service Providers (that care and do the work) to detect ePPN reassignments by always looking at the combination of ePPN and persistent NameID (instead of just at the ePPN): If one day a known ePPN arrives together with a different/unknown persistent NameID that’s a sign that the ePPN likely has been reassigned to a different person and that access to data held at the SP from/about the former ePPN-NameID combination should be denied.

Of course that assumes that you can and do support proper SAML 2.0 persistent NameIDs and that you create those from source data that itself is not reassigned from one person to another. (If you don’t have any such data and you also cannot mint it on the fly, as illustrated in our IDP attribute resolver documentation, you cannot produce spec-conformant persistent NameIDs and therefore also cannot support REFEDS R&S v1.)

Also note that if you don’t have the (old, deprecated) eduPersonTargetedID (ePTID) attribute configured in your IDP then the Shibboleth IDP attribute filter rules given above may not be sufficient to conform to R&S v1: Technically (proper) SAML 2.0 persistent NameIDs are not “attributes” and consequently cannot be released using the Shibboleth IDP’s attribute filter configuration (contrary to ePTID attributes, which wrap a persistent NameID in an attribute, but which are deprecated and their use should be phased out). Unless a REFEDS R&S Service Provider also signals that it wants to receive SAML 2.0 persistent NameIDs in its SAML Metadata using the NameIDFormat element (which other federations don’t even support and many SPs simply don’t currently do) the above attribute filter snippet is insufficient to satisfy the R&S 1.x requirements – if your ePPN values may be reassigned and you don’t have ePTID available.

So (only) if all of the following 3 criteria apply to your deployment:

- ePPN attribute values may be reassigned from one person to another, over time,
- You have some other (internal) data available (or can mint it on the fly, as illustrated in our IDP attribute resolver documentation) that can serve as a basis for conformant (i.e., not-reassigned) attributes and persistent NameIDs,
- You don’t have the (old, deprecated) eduPersonTargetedID (ePTID) attribute configured in your IDP,

then you’d need to amend your IDP’s relying-party.xml configuration with a “relying party override” like the one shown below, forcing the NameIDFormat to “persistent” for all REFEDS R&S Service Providers (just in case those SPs don’t already request that NameID format in their metadata):

Shibboleth IDP relying-party.xml

```xml

<util:list id="shibboleth.RelyingPartyOverrides">
  <bean parent="TagCandidate" c:name="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
</util:list>

N.B.: If your Shibboleth.DefaultRelyingParty setting includes other properties on the bean with parent="SAML2.SSO" you should also include /repeat them here, e.g. p:postAuthenticationFlows="attribute-release".

Of course that’s overly complex (or plain crazy) which is exactly why ePPN, ePTID, persistent NameIDs and even R&S v1 are all more or less in the process of being replaced or phased out for newer, simpler replacements. For existing services relying on these standards, attributes and NameIDs, though, the above may be needed for proper support by the IDP.