Authentic 2 - Bug #9867

Error with the persistent nameID when the nameID format is not given in the authnRequest

03 février 2016 23:59 - Mikaël Ates

Statut:	Fermé	**Début:**	03 février 2016
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

The SP sends an authnRequest with a NameIDPolicy with no Format attribute.
The IdP has a saml options policy for this SP that defines persistent as the default nameID format.

First SSO

When the assertion is built but before fill_assertion():

```
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://id
p.cud.mik.lan:8000/idp/saml2/metadata">_D4C8D87769C774DCDEF6912A0671E1C1</saml:NameID>
```

After fill_assertion()

```
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="http://i
dp.cud.mik.lan:8000/idp/saml2/metadata">_D4C8D87769C774DCDEF6912A0671E1C1</saml:NameID>
```

nid_format is well set as persistent and a federation is created.

Next SSO

The identity dump is built with the correct nameID value :

```
<Identity xmlns="http://www.entrouvert.org/namespaces/lasso/0.0" Version="2">
<lasso:Federation xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0" xmlns:saml="urn:oas
is:names:tc:SAML:2.0:assertion" RemoteProviderID="http://sp.cud.mik.lan:8001/accounts/mellon/metad
ata/" FederationDumpVersion="2">
    <lasso:LocalNameIdentifier>
        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQualifier="
http://idp.cud.mik.lan:8000/idp/saml2/metadata">_D4C8D87769C774DCDEF6912A0671E1C1</saml:NameID>
    </lasso:LocalNameIdentifier>
</lasso:Federation>
</Identity>
```

When the assertion is built but before fill_assertion():

```
<saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" NameQualifier="http://id
p.cud.mik.lan:8000/idp/saml2/metadata">_86897188ED4371C2F35F055FFC0E6837</saml:NameID>
```

After fill_assertion():

```
<saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" NameQuali
fier="http://idp.cud.mik.lan:8000/idp/saml2/metadata">_86897188ED4371C2F35F055FFC0E6837</saml:Name
ID>
```

It seems that the setIdentityFromDump() does not load the dump correctly since a new nameID value is generated.

The get_or_create() then creates a new federation and at the next SSO Authentic raise 'get() returned more than one

LibertyFederation -- it returned 2!'

Historique

#1 - 04 février 2016 00:43 - Benjamin Dauvergne

The bug is because lasso does not know that persistend is required is here so it uses the transient way of creating the NameID event if at the end of fill_assertion() the NameID format is forced to be persistent. I think a fix would be to set the NameID format in the request before the call to login.buildAssertion() so that Lasso will know which format is expected.

#2 - 04 février 2016 15:54 - Mikaël Ates

- Fichier 0001-Set-nameId-format-in-request-when-not-defined.patch ajouté

Indeed, that makes it.

#3 - 04 février 2016 16:04 - Benjamin Dauvergne

NameIDPolicy is not mandatory in an AuthnRequest so name_id_policy could be None.

#4 - 04 février 2016 16:08 - Mikaël Ates

Yes I've seen it in the spec. But if it is not set lasso does not kwow how to handle, it is why I set it in the request, it is what I understood from you comment. What did I miss ?

#5 - 04 février 2016 16:13 - Mikaël Ates

And we still respect the spec since we accept that the SP does not specify it.

```
If omitted, then any type of identifier supported by the identity provider for the requested subject can be us
ed,
constrained by any relevant deployment-specific policies, with respect to privacy, for example.
```

In that case it will be transient if nothing is defined in the options policy.

#6 - 04 février 2016 16:14 - Benjamin Dauvergne

I'm just stating that if name_id_policy is None, you should create it before altering the format:

```
if not name_id_policy:
    name_id_policy = login.nameIdPolicy = lasso.Samlp2NameeIDPolicy()
```

#7 - 04 février 2016 16:44 - Mikaël Ates

- Fichier 0001-Set-nameId-format-in-request-when-not-defined.patch ajouté

- Patch proposed changé de Non à Oui

#8 - 04 février 2016 17:11 - Benjamin Dauvergne

Ack.

#9 - 05 février 2016 10:07 - Mikaël Ates

- Statut changé de Nouveau à Fermé

commit da2c005d33894df8dae078b54c742d52a546eb4d

Fichiers

0001-Set-nameId-format-in-request-when-not-defined.patch	1,14 ko	04 février 2016	Mikaël Ates
0001-Set-nameId-format-in-request-when-not-defined.patch	1,36 ko	04 février 2016	Mikaël Ates