Authentic 2 - Bug #8061

mimecast support

17 août 2015 13:37 - Nickolas Grigoriadis

Statut:	Fermé	**Début:**	17 août 2015
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	

Description

Hi I want to authenticate mimecast as a service provider.

I'm using authentic2==2.1.20

Mimecasts SAML support is a bit weird, as they provide no metadata file, just give you some manual things to do.
I have built what I think *should* be a valid SP metadata document:
Note that the entityID is not a URL, And this causes some confusion in the Admin interface.

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"  entityID="console-za.mimecast.com.CSA54A58">
    <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://console-za.mimecast.com/mimecast/admin?action=sso" index="0" />
    </md:SPSSODescriptor>
</md:EntityDescriptor>
</md:EntityDescriptor>
```

Thing is, I get a 500 Internal error, and when looking at the debug info I get:

```
  File "/opt/isid2/lib/python2.7/site-packages/authentic2/idp/saml/saml2_endpoints.py", line 465, in sso
      logger.debug('nameID policy is %s' % name_id_policy.dump())
AttributeError: 'NoneType' object has no attribute 'dump'
```

But this confuses me, as I explicitly set the nameIdPolicy to Email?

What more information should I provide?

Demandes liées:

Lié à Authentic 2 - Bug #7612: NameIDPolicy is optional	**Fermé**	**17 juin 2015**

Historique

#1 - 17 août 2015 13:57 - Frédéric Péters

- Statut changé de Nouveau à En cours

This was a bug in authentic when the request didn't contain a nameidpolicy (#7612), this has been fixed in commit 66e4d0f, unfortunately it's not yet part of any release and can't be cherrypicked automatically.

This patch (not tested) could maybe work:

```
--- a/src/authentic2/idp/saml/saml2_endpoints.py
+++ b/src/authentic2/idp/saml/saml2_endpoints.py
@@ -462,10 +462,10 @@ def sso(request):
                 AUTHENTIC_STATUS_CODE_MISSING_DESTINATION)
     # Check NameIDPolicy or force the NameIDPolicy
     name_id_policy = login.request.nameIdPolicy
-    logger.debug('nameID policy is %s' % name_id_policy.dump())
-    if name_id_policy.format and \
+    if name_id_policy and name_id_policy.format and \
             name_id_policy.format != \
                 lasso.SAML2_NAME_IDENTIFIER_FORMAT_UNSPECIFIED:
+        logger.debug('nameID policy is %s' % name_id_policy.dump())
         nid_format = saml2_urn_to_nidformat(name_id_policy.format)
         logger.debug('nameID format %s' % nid_format)
         default_nid_format = policy.default_name_id_format
@@ -483,7 +483,6 @@ def sso(request):
         logger.debug('no nameID policy format')
         nid_format = policy.default_name_id_format or 'transient'
         logger.debug('set nameID policy format %s' % nid_format)
-        name_id_policy.format = nidformat_to_saml2_urn(nid_format)
     return sso_after_process_request(request, login, nid_format=nid_format)
```

Can you test and confirm?

#2 - 17 août 2015 13:57 - Frédéric Péters

- Lié à Bug #7612: NameIDPolicy is optional ajouté

#3 - 17 août 2015 14:14 - Nickolas Grigoriadis

Now getting:

```
  File "/opt/isid2/lib/python2.7/site-packages/authentic2/idp/saml/saml2_endpoints.py", line 487, in sso
    return sso_after_process_request(request, login, nid_format=nid_format)
  File "/opt/isid2/lib/python2.7/site-packages/authentic2/idp/saml/saml2_endpoints.py", line 667, in sso_after
_process_request
    if login.request.nameIdPolicy.format == \\
AttributeError: 'NoneType' object has no attribute 'format'
```

#4 - 17 août 2015 14:20 - Frédéric Péters

Ok, it's probably more effective to simply update your checkout to 66e4d0f. Alternatively I'll see next week if we could get a new version out (Benjamin, te maintainer, is currently away).

#5 - 17 août 2015 14:22 - Nickolas Grigoriadis

Changing line 667 to:

```
    if login.request.nameIdPolicy and login.request.nameIdPolicy.format == \
```

stops the error from happening.

It redirects back to mimecast but I now get some error from mimecast:
"Invalid user name or permissions. Error Code: 8946"
And that means nothing to me...

I'll apply those fixes to my own instance of Authentic2 for now, but I plan to keep this ticket open until mimecast actually works.

Thanks for the help.

#6 - 28 août 2015 17:20 - Benjamin Dauvergne

In authentic logs verify that an emailAddress NameID was effectively sent as part of the AuthnResponse.

#7 - 31 août 2015 07:59 - Nickolas Grigoriadis

Hi Benjamin

I found out that that error means the certificate failed to validate. I then checked and determined that I needed to define the certificate prepending SAML_ to SIGNATURE_PUBLIC_KEY and SIGNATURE_PRIVATE_KEY. Once we got past that and signed the assertion, I now get an error message of:
java.lang.NullPointerException

Looking in the local logs it actually looks correct (once again to my understanding), and mimecast logs says that it has identified the correct user. I have asked mimecast support to try and find out why it is hitting an NPE...

#8 - 31 août 2015 10:22 - Benjamin Dauvergne

- Statut changé de En cours à Fermé

It it was just misconfiguration I will close the ticket, feel free to open a new one refering to this one if there is a new problem.