OpenSSO IdP - Shibboleth2 SP

Cél

http://maszat.sch.bme.hu -n futó OpenSSO-n IdP létrehozása, és a https://sandbox.aai.niif.hu/shibboleth alatt futó Shibboleth 2 SP-vel való federáció.

OpenSSO IdP létrehozása

lásd: OpenSSO

Cél Realm: /niif-teszt IDP entityID: https://idp.sch.bme.hu/niif-teszt Legalább a "signing certificate alias" -t állítsuk be

A /opensso/famadm.jsp -> export-entity parancssal tudjuk XML-ként exportálni az létrehozott IDP metaadatát. (Vagy, a /opensso/saml2/jsp/exportmetadata.jsp?entityID=https://idp.sch.bme.hu/niif-teszt&realm=/niif-teszt URL-ről közvetlenül elérhetjük).

Shibboleth 2 SP beállítása

/etc/shibboleth/shibboleth2.xml:

```
...
<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="teszt"
               relayState="cookie" entityID="https://idp.sch.bme.hu/niif-teszt">
  <SessionInitiator type="SAML2" defaultACSIndex="1" template="bindingTemplate.html"/>
</SessionInitiator>
...
<MetadataProvider type="XML" file="maszat-idp.xml"/>
...
```

Shibboleth SP Metadata importálása OpenSSO-ba

A lementett XML-ből töröljük ki az `<md:Extension>` node-ot, mivel a parszolás során hibaüzenetet dob, ami a teljes SAML2Meta konfigurációt megfekteti.

```
ERROR: SAML2MetaManager.getEntityDescriptor
javax.xml.bind.UnmarshalException: Unexpected end of element
{urn:oasis:names:tc:SAML:2.0:metadata}:Extensions
...
```

Ha ez a hiba előjön, akkor a konfigurációs címtárból kell törölni az entity-t, ugyanis ilyenkor teljesen használhatatlan lesz a felület (ez egy bug sajnos)

```
$ ldapmodify ...
dn:
ou=<entityid>,ou=default,ou=OrganizationConfig,ou=1.0,ou=sunFMSAML2MetadataService,ou=services
,
 o=<realm>,ou=services,<basedn>
changetype: delete
```

A problémát az okozza, hogy amikor a metadata xml-t beolvassa a SAX parszer, akkor JAXB-vel mappeli java objektumokra, és ezt marshallolja ki a konfigurációs store-ba. Viszont az Extensions belseje egy teljesen külön névtér és külön séma, ezért arra nincsenek generált osztályok. Ezt úgy veszi a JAXB, hogy egy `<Extensions/>` -t ír ki, ami viszont unmarshal időben nem felel meg már a sémának (ugyanis xsd szerint ott legalább egy elemnek lennie kell).

Egyelőre azt a megoldást javasolták, hogy kézzel szedjem ki az `<Extensions>` -t, aminek továbbra sem örülök az xml aláírás és a kézi hegesztés miatt. Idővel egy olyan javítást fognak készíteni, amivel user osztálykönyvtárat meg lehet adni az opensso-nak, hogy a metaadat bizonyos részeit (pl. extensions belseje) arra mappelje le. Illetve tettem egy olyan javaslatot, hogy ilyen esetben amikor kinullozza a node belsejét a JAXB, akkor a teljes `<Extensions>` node-ot töröljék, így legalább az xml valid marad. Talán azt is javítják, hogy ilyenkor a teljes metaadat rész összeomlik és semmilyen műveletet nem lehet végezni. (

https://opensso.dev.java.net/issues/show_bug.cgi?id=2736)

A ManageNameIDService ill. AssertionConsumerService közé írjuk be a következő node-okat:

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

Ha nem adunk meg NameIDFormat -ot, akkor az OpenSSO IdP vissza fogja utasítani a kérést. Megj. https://opensso.dev.java.net/issues/show_bug.cgi?id=2172 hosszútávon ezt a viselkedést valószínű megváltoztatják.

Ezt a metaadatot a Federation fül Entities -> Import Entity parancssal tudjuk importálni. Itt ki kell választani a /niif-teszt realm-et, és feltölteni az XML-t (vagy megadni az URL-jét). Ezután felül a Circle of Trust-nál hozzá tudjuk már adni a SAML2 SP-t.

Ha mindezt végigcsináltuk, máris működik minden.

Problémák

Ha Shibboleth2 SP-ben külön application-be tesszük a metaadatot, akkor nem találja meg a SAML Response issuer-alapján.

Az OpenSSO nem jelzi a saml attribútum névformátumát (`<saml:Attribute NameFormat="...">`). A Shibboleth pedig csak az urn:oasis:names:tc:SAML:2.0:attrname-format:uri típusú nevet fogadja el.

Emiatt a következő probléma adódik:

```
shibd.log:

2008-05-14 18:33:25 INFO Shibboleth.AttributeExtractor : creating mapping for Attribute
urn:mace:dir:attribute-def:mail
...
<saml:Attribute Name="urn:mace:dir:attribute-def:mail">
   <saml:AttributeValue
          xmlns:xs="http://www.w3.org/2001/XMLSchema"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="xs:string">hege@*********</saml:AttributeValue>
</saml:Attribute>
...
2008-05-14 18:33:31 INFO Shibboleth.AttributeExtractor [1]: skipping unmapped SAML 2.0
Attribute
with Name:  urn:mace:dir:attribute-def:mail, Format:urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecifiedd
```

Itt egy patch OpenSSO-hoz ami megoldja a problémát:

https://opensso.dev.java.net/issues/show_bug.cgi?id=2775 Ezen patch használatával a következő módon kell megadni az IDP attribútum mappelést az IDP > Attribute Processing fülön:

```
# [NameFormat|]SAMLAttributeName=LocalAttributeName
urn:oasis:names:tc:SAML:2.0:attrname-format:uri|urn:mace:dir:attribute-def:mail=mail
```

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:39 CEST
cziernorbert frissítette 2026-04-14 13:23:02 CEST