AAIInterop-OpenSSOShib2

> **Elavult információ**
>
> **Figyelem**: ez a szakasz vagy szócikk elavult információkat tartalmazhat!

OpenSSO IdP - Shibboleth2 SP Interoperabilitás

- IdP: maszat-opensso-idp.xml
- SP: papigw-shibboleth2-sp.xml{.download="papigw-shibboleth2-sp.xml"}

SAML2.0 Single Sign on

- SP oldali SAML2 bindingot támogató AttributeConsumerService-ek:
  - 1: /SAML2/POST urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
  - 2: /SAML2/POST-SimpleSign urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign
  - 3: /SAML2/Artifact urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact
  - 4: /SAML2/ECP urn:oasis:names:tc:SAML:2.0:bindings:PAOS

HTTP-Post

- Működik
- https://papigw.aai.niif.hu/saml2interop/opensso-post/
- SP oldalon

```
<SessionInitiator type="Chaining" Location="/Login" id="maszat-opensso-post"
    relayState="cookie" entityID="https://idp.sch.bme.hu/niif-teszt">
    <SessionInitiator type#"SAML2" defaultACSIndex="1" template="bindingTemplate.html"/>
```

```
</SessionInitiator>
```

HTTP-Artifact

- Az OpenSSO nem figyel arra hogy az SP milyen AttributeConsumerService-t kér, így az IDP oldalon kell konfigurálni az SP tulajdonságait úgy, hogy az alapbeállítás ne a POST legyen.
- TODO - Trust management a back-channel kommunikációnál a tanusítványt ismernie kell az SP-nek.
- JVM beállítása a kliens tanúsítvány használatához - https://opensso.dev.java.net/issues/show_bug.cgi?id=1409

Attribute push

- Gyári buildekkel nem működik, ugyanis az OpenSSO urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified formátumban küldi az attribútumokat, amiket a Shibboleth2 SP nem fogad el.
- Saját patch használata esetén bekonfigurálható az uri típusú NameFormat is, azzal működik probléma nélkül.
  - https://opensso.dev.java.net/issues/show_bug.cgi?id=2775

Attribute pull

- Az OpenSSO-ban nem lehet kikapcsolni az attribute push-t. FIXME

NameIDFormat

- A Shibboleth2 SP által generált metaadatba kézzel be kell illeszteni a NameIDFormat node-ot
- Az OpenSSO támogatja a perzisztens és a tranziens SAML2 azonosítót is.

SAML2.0 Single Log out

- A shibboleth2 nem támogatja (még) a Single Log-out protokollt, lásd: https://wiki.shibboleth.net/confluence/display/SHIB2/SLOIssues

Metaadat problémák

- A Shibboleth2 SP metaadatból el kell távolítani az `<md:Extensions>` node-ot az összes gyerekelemével együtt.
  - Erre nagyon figyelni kell, mert összeomlik tőle az OpenSSO, és csak címtár-módosítással ('hibás' metaadat törlése) állítható helyre.
  - Sajnos nem triviális javítani ezt a viselkedést...
- A metaadatba ágyazott certificate esetén csak a `<ds:X509Certificate>` node szerepelhet, semmi más
  - Ehhez írtam patch-et ami ezt javítja.
  - https://opensso.dev.java.net/issues/show_bug.cgi?id=2985

Változat #2
document-uploader hozta létre 2025-08-07 12:03:10 CEST
cziernorbert frissítette 2026-04-13 15:25:05 CEST