AAIInterop-Shib2SimpleSAMLphp

!!! bug "Elavult információ"

```
**Figyelem**: ez a szakasz vagy szócikk elavult információkat tartalmazhat!
```

Shibboleth2 IdP - SimpleSAMLphp SP Interoperabilitás

- IdP: papigw-shibboleth2-idp.xml
- SP: papigw-simplesaml-saml2-sp.xml

SAML2.0 Single Sign on

HTTP-Post

- Működik
- A SimpleSAMLphp nem támogatja a NameID titkosítását, csak az egész assertion titkosítását (FIXME)
  - ezért be kell állítani hogy a NameID-t ne titkosítsa az IdP, ugyanígy kényszeríteni kell az Attribute Push használatát is

```
<RelyingParty id="https://papigw.aai.niif.hu/simplesaml"
   provider="https://papigw.aai.niif.hu/idp/shibboleth"
   defaultSigningCredentialRef="IdPCredential">
```

```
   <ProfileConfiguration xsi:type="saml:SAML2SSOProfile"
      encryptNameIds="never" includeAttributeStatement="true"/>
</RelyingParty>
```

- A SimpleSAMLphp SP metaadatába kézzel kell beletenni az aláíró és titkosító publikus kulcsokat, mivel a kiexportált metaadat ezeket nem tartalmazza (ráadásul a php-s konfigurációban szereplő certificate/privatekey paramétereket nem lehet abszolut elérési úttal hivatkozni, mindenképp a cert/ könyvtárban kell lenniük)

HTTP-Artifact

- A SimpleSAMLphp nem támogatja a HTTP-Artifact bindingot (és általában a SOAP-ot használó bindingokat)

Attribute push

- Működik

Attribute pull

- A SimpleSAMLphp nem támogatja az AttributeRequest protokollt (a SOAP binding miatt)

NameIDFormat

- Általában urn:oasis:names:tc:SAML:2.0:nameid-format:transient

SAML2.0 Single Log out

- A SimpleSAMLphp támogatná az SLO-t, de a shibboleth2 IdP nem. A metaadatnál panaszkodik is hogy a Shibboleth metadata nem tartalmaz SingleLogoutService-t.

Változat #1
document-uploader hozta létre 2025-08-07 12:05:54 CEST
document-uploader frissítette 2025-08-07 12:05:54 CEST