Shibboleth IdP konfigurációja

> **Elavult információ**
>
> **Figyelem**: a Shibboleth szoftver ezen változata már nem támogatott. Az új verziókhoz a leírások itt találhatók:
>
> • Shibboleth2_IdP
> • Shibboleth2_SP

Az IdP alkalmazást az `idp.xml` állományon keresztül konfigurálhatjuk. Ebben a leírásban feltételezzük, hogy az IdP alkalmazás konfigurációs állományai a `/etc/shibboleth-idp` könyvtárban vannak.

M?köd? példa konfiguráció

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<IdPConfig
        xmlns="urn:mace:shibboleth:idp:config:1.0"
        xmlns:cred="urn:mace:shibboleth:credentials:1.0"
        xmlns:name="urn:mace:shibboleth:namemapper:1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:mace:shibboleth:idp:config:1.0 ../schemas/shibboleth-
idpconfig-1.0.xsd"
        AAUrl="https://idp.niif.hu:8443/shibboleth-idp/AA"
        resolverConfig="file:/etc/shibboleth-idp/resolver.ldap.xml"
        defaultRelyingParty="urn:niif.hu:aai:HREF"
        defaultAuthMethod="urn:oasis:names:tc:SAML:1.0:am:password"
        providerId="https://idp.niif.hu/shibboleth">

        <RelyingParty name="urn:niif.hu:aai:HREF" signingCredential="href_cred">
                <NameID nameMapping="shm"/>
        </RelyingParty>
        <RelyingParty name="urn:geant:niif.hu:niifi:sp:register.ca.niif.hu"
                      signingCredential="href_cred"
```

```
                    forceAttributePush="true">
                <NameID nameMapping="shm"/>
        </RelyingParty>

        <ReleasePolicyEngine>
                <ArpRepository
implementation="edu.internet2.middleware.shibboleth.aa.arp.provider.FileSystemArpRepository">
                        <Path>file:/etc/shibboleth-idp/arps/</Path>
                </ArpRepository>
        </ReleasePolicyEngine>

        <Logging>
                <ErrorLog level="DEBUG" location="file:/var/log/shibboleth-idp/shib-error.log"
/>
                <TransactionLog level="INFO" location="file:/var/log/shibboleth-idp/shib-
access.log" />
        </Logging>

        <NameMapping
                xmlns="urn:mace:shibboleth:namemapper:1.0"
                id="shm"
                format="urn:mace:shibboleth:1.0:nameIdentifier"
                type="SharedMemoryShibHandle"
                handleTTL="28800"/>

        <ArtifactMapper
implementation="edu.internet2.middleware.shibboleth.artifact.provider.MemoryArtifactMapper" />

        <Credentials xmlns="urn:mace:shibboleth:credentials:1.0">
                <FileResolver Id="href_cred">
                        <Key>
                                <Path>file:/etc/httpd/conf/ssl.key/idp.niif.hu.key</Path>
                        </Key>
                        <Certificate>
                                <Path>file:/etc/httpd/conf/ssl.crt/idp.niif.hu.crt</Path>
                        </Certificate>
                </FileResolver>
        </Credentials>
```

```
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.ShibbolethV1SSOHandler">
                <Location>https?://[^:/]+(:(443|80))?/shibboleth-idp/SSO</Location> <!-- regex
works when using default protocol ports -->
        </ProtocolHandler>
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.SAMLv1_AttributeQueryHandler"
>
                <Location>.+:8443/shibboleth-idp/AA</Location>
        </ProtocolHandler>
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.SAMLv1_1ArtifactQueryHandler"
>
                <Location>.+:8443/shibboleth-idp/Artifact</Location>
        </ProtocolHandler>
        <ProtocolHandler
implementation="edu.internet2.middleware.shibboleth.idp.provider.Shibboleth_StatusHandler">
                <Location>https://[^:/]+(:443)?/shibboleth-idp/Status</Location>
        </ProtocolHandler>

        <MetadataProvider
type="edu.internet2.middleware.shibboleth.metadata.provider.XMLMetadata"
                uri="file:/etc/shibboleth-idp/href-metadata.xml"/>
</IdPConfig>
```

XML elemek magyarázata

IdPConfig

Az IdPConfig elem attribútumai közül az xmlns: és xsi: attribútumokat nem szabad megváltoztatni, de van néhány, amit kötelező:

- *defaultRelyingParty*: ez adja meg, hogy melyik RelyingParty-t kell használni, ha a request alapján nem állapítható meg. Ha nincs ehhez tartozó RelyingParty elem, akkor az IdP nem indul el.
- *providerID*: ez adja meg az IdP egyedi azonosítóját a föderációban. Általában URN vagy URL formában adjuk meg.
- *resolverConfig*: az attribútum feloldás konfigurációs állományát adja meg.

- *AAUrl*: az Attribute Authority elérhetősége. (Erre csak a Shibboleth 1.1-el való kompatibilitás megőrzése érdekében van szükség. Nem biztos, hogy kötelező megadni...)

Általában nem szükséges megadni:

- *authHeaderName*: itt kell megadni, ha az SSO Handler más változóban kapja meg a felhasználó azonosítóját (principal), mint a REMOTE_USER szerver változó
- *defaultAuthMethod*: megadható, hogy az elkészített SAML Assertion milyen autentikációs metódust tartalmazzon. A lehetséges értékek a SAML 1.1 specifikáció 7.1-es szakaszában találhatók. Ha nincs megadva, akkor az értéke `urn:oasis:names:tc:SAML:1.0:am:unspecified`. A `defaultAuthMethod` értéke RelyingParty szintjén felülbírálható
- *maxSigningThreads*: az üzenet aláírására és egyéb műveletekre indított thread-ek maximális száma. Az IdP teljesítménye hangolható ezzel.
- *passThruErrors*: boolean változó, amely azt szabályozza, hogy a hibákat az IdP továbbadja-e az SP felé

Az IdP konfigurációban a többi XML Element az IdPConfig gyereke.

RelyingParty

Egy IdP tetszőleges mennyiségű RelyingParty-t kezelhet.

A legfelső szintű alapértelmezett beállításokon kívül minden egyes RelyingParty-ra beállíthatjuk az alábbi értékeket:

- *name* (kötelező): a RelyingParty neve. Ha nem egyezik meg az SP által küldött providerId-vel, akkor az IdP a metadata segítségével próbálja megállapítani, hogy az SP-re melyik RelyingParty definíció vonatkozik.
- *providerId*: az a providerId, amelyet az IdP használ a RelyingParty-k felé.
- *signingCredential*: az Assertion-ök és az SSL sessionben használt SSL kulcsokra vonatkozó FileResolver elem ID-jét adhatjuk meg itt.
- *AAUrl*: az Attribute Authority elérhetősége.
- *defaultAuthMethod*: megadható, hogy a RelyingParty számára elkészített SAML Assertion milyen autentikációs metódust tartalmazzon. A lehetséges értékek a SAML 1.1 specifikáció 7.1-es szakaszában találhatók. Ha nincs megadva, akkor az értéke az IdPConfig element-nél megadott érték, ill. `urn:oasis:names:tc:SAML:1.0:am:unspecified`.
- *passThruErrors*: boolean változó, amely azt szabályozza, hogy a hibákat az IdP továbbadja-e az SP felé. Alapértelmezett érték: false
- *signAssertions*: boolean változó, amely azt szabályozza, hogy az IdP aláírja-e a kiállított Assertion-öket. Leginkább akkor van rá szükség, ha az Assertion-t más alkalmazásnál is fel akarjuk használni. Alapértelmezett érték: false

- *forceAttributePush*: boolean változó, ennek segítségével ki lehet kényszeríteni az Attribute Push használatát. Alapértelmezett érték: false

A RelyingParty element NameID gyermeke segítségével állítható be a használt NameID kezelés.

ReleasePolicyEngine

Itt adhatjuk meg az attribútum kiadás implementációját (ezt általában nem kell változtatni) és az ARP állományok elérhetőségét.

Logging

A Logging element szabályozza a naplózási szintet, ill. a naplófile-ok helyét. Részletesebb beállításokra a Log4J-t is használhatjuk. (Lásd még: Értelmes naplóüzenetek (IdP))

NameMapping

Ebben az elemben adható meg a NameMapper implementációja, illetve az assertionökben használt azonosító (Subject Identifier) formátuma.

- Az alapértelmezett értékek az esetek többségében megfelelők, csak akkor módosítsd, ha tudod, mit csinálsz!

Attribútumok:

- *id*: egyedi név, erre lehet hivatkozni a NameID elementben.
- *format* (URI): ez határozza meg a Subject Identifier formátumát. Tetszőleges URN használható, amiben az IdP és az SP megegyezik. Néhány gyakrabban használt formátum:
  - `urn:mace:shibboleth:1.0:nameIdentifier`: alapértelmezett Shibboleth azonosító (tranziens, átlátszó)
  - `urn:oasis:names:tc:SAML1.1:nameid-format:X509SubjectName`: X.509 tanúsítvány DN. A GridShib használja ezt a formátumot.
  - `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`: email-cím, használata nem javasolt
  - `http://schemas.xmlsoap.org/claims/UPN`: MS UPN, az ADFS integrációhoz használható
- *class*: a NameMapper implementációjának a javaclass útvonala. (HAShib használatához módosítani kell.)
  A további attribútumok csak az alapértelmezett implementáció esetén értelmezhetők.
- *handleTTL*: azt határozza meg, hogy az IdP mennyi ideig őrizze a Session Cache-ében a kiosztott azonosítókat. (Csak `urn:mace:shibboleth:1.0:nameIdentifier` formátum esetén értelmezhető.) Ezt követően erre az azonosítóra történő hivatkozás már nem lesz

megengedett, a felhasználónak esetleg újra kell azonosítania magát.

- *type*: azt adja meg, hogy az SSO Handler és az Attribute Authority között milyen formában utazzanak az azonosítók. Lehetséges értékek:
  - `CryptoHandleGenerator`: szimmetrikus kódolással titkosított azonosítók használata
  - `Principal`: az SSO Handler-től megkapott azonosító átadása az Attribute Authority-nek
  - `SharedMemoryShibHandle`: (alapértelmezett) megosztott, memóriában tárolt session cache. Ha az SSO Handler és az Attribute Authority egy konténerben futnak, ezt érdemes használni.

ArtifactMapper

Itt adható meg az ArtifactMapper implementációja. HAShib használata esetén át kell állítani.

Credentials

Ebben az elemben adhatók meg a használt titkos kulcsok és tanúsítványok. Több is megadható, az *id* attribútum értékével hivatkozhatunk rájuk, pl a RelayingParty konfigurációban.

ProtocolHandler

Itt adhatók meg az egyes handler servletek elérhetőségei. Általában nem szükséges felülírni!

Forrás

** Shibboleth Wiki**

- IdP fő konfiguráció
- Relying Party konfiguráció
- NameMapping

Változat #2
document-uploader hozta létre 2025-08-07 12:07:17 CEST
cziernorbert frissítette 2026-04-10 12:46:13 CEST