

MDX

Az MDX, azaz MetaDataeXchange protokolt erőforrás optimalizálás céljából találták ki, hogy ne kelljen egyes IdP-knek és SP-knek indokolatlanul nagy XML fájlokat feldolgozniuk és tárolniuk, mikor a felhasználóiknak jó eséllyel a fájlokban tárolt entitások töredékére van csak szükségük. Ezért az egyes entitásokat be lehet úgy állítani, hogy csak akkor töltsék le az adott entitás metaadatát, mikor arra szükség van (az első letöltés után természetesen helyben tárolódik a metaadat a `cacheDuration`-ben megadott ideig). Az MDX kiszolgáló az alábbi szabvány szerint tudja visszaadni egy-egy entitás metaadatát: `https://mdx.eduid.hu/entities/{urlencoded}$entityID`, pl: `https://mdx.eduid.hu/entities/https%3A%2F%2Fdev.aai.niif.hu%2Fshibboleth`

Dinamikus metadatum kiszolgálás a HREF-ben

Az MDX kiszolgáló a **<https://mdx.eduid.hu>** alatt szolgáltat, és a *href* és az *edugain* metadatum halmazokat tartalmazza.

Mindkét kiszolgáló ugyanazzal a kulccsal írja alá a lekért metaadat-állományt.

- A tanúsítvány letölthető innen: <https://metadata.eduid.hu/certs/href-metadata-signer-2020.crt>
- SHA-1 lenyomata: `C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61` .

Fontos tudnivaló Discovery Service használatával kapcsolatban

Lévéen az MDX-et használó SP-knél nem áll rendelkezésre folyamatosan az összes potenciális IdP listája, így a beépített Discovery Service-ek nem működnek. Ha MDX-et használunk, akkor valamilyen külső Discovery Service-t kell használnunk. A HREF-ben a <https://discovery.eduid.hu> a központi Discovery Service.

Emellett maga az MDX kiszolgáló is biztosít Discovery Service felületet, ehhez akár Shibboleth SP-nél, akár simpleSAMLphp SP-nél a konfigurációban az alábbi URL-t kell megadni, mint Discovery Service: <https://mdx.eduid.hu/role/idp.ds> . Ez a Discovery Service tartalmazza a hazai eduID-ben,

valamint az eduGAIN-ben levő összes IdP-t. (És, ellentétben a hagyományos

<https://discovery.eduid.hu/edugain> szolgáltatással, ez tartalmazza a magyar VHO-t is VHO IdP néven.)

MDX használata kliens oldalon

SimpleSAMLphp

Az 1.14-es kiadástól kezdve a SimpleSAMLphp tartalmazza az dinamikus metadata lekérdezés funkciót, amely mind IdP, mind SP szerepben egységes módon használható. A config/config.php állományban metadata.sources szekcióban kell elhelyezni az alábbi blokkot:

```
'metadata.sources' => array(
    array('type' => 'flatfile'), // ez a *-hosted metadata konfiguráció betöltése miatt szükséges
    array(
        'type' => 'mdx',
        'server' => 'https://mdx.eduid.hu',
        'cachedir' => '/var/simplesamlphp/mdx-cache', //opcionális, de ajánlott
        'cachelength' => 86400, //opcionális,
        'validateFingerprint' => 'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61' //opcionális
    ),
),
```

A dinamikus és a statikus metadataforrások egyidejű használatára egy példa:

SimpleSAMLMixedMetadata

Shibboleth SP

- Le kell tölteni a /etc/shibboleth alá az aláíró tanúsítványát innen:
<https://metadata.eduid.hu/certs/href-metadata-signer-2020.crt>
- Az alábbi blokkot be kell szúrni a `/etc/shibboleth/shibboleth2.xml` fájlba

```
<MetadataProvider type="Dynamic" ignoreTransport="true">
    <Subst>https://mdx.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
```

Shibboleth IdPv3

- Le kell tölteni a `${idp.home}/credentials/` alá az aláíró tanúsítványát innen:
<https://metadata.eduid.hu/certs/href-metadata-signer-2020.crt>
- A `conf/metadata-providers.xml` fájlt kell szerkeszteni az alábbi módon:

```
<MetadataProvider
  xmlns="urn:mace:shibboleth:2.0:metadata"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:metadata http://shibboleth.net/schema/idp/shibboleth-
metadata.xsd"
  id="dynamicMDQ" xsi:type="DynamicHTTPMetadataProvider">

  <!--
    Require a validUntil XML attribute on the EntityDescriptor element
    and make sure its value is no more than 14 days into the future
  -->
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D" />

  <!-- Verify the signature on the metadata file -->
  <MetadataFilter xsi:type="SignatureValidation" requireSignedMetadata="true"
    certificateFile="${idp.home}/credentials/href-metadata-signer-2020.crt" />

  <!-- The MetadataQueryProtocol element specifies the base URL for the query protocol. -->
  <MetadataQueryProtocol>https://mdx.eduid.hu/</MetadataQueryProtocol>
</MetadataProvider>
```

Változat #3

cziernorbert hozta létre 9 április 2025 16:37:31

cziernorbert frissítette 10 április 2025 09:55:27