

HREF Key Rollover 2025

Bevezetés

A HREF új metaadat aláírókulcsra áll át a SAML 2.0 metaadataiban (HREF-2025). A HREF szövetségi tagoknak és partnernek az új aláírókulcshoz tartozó konfigurációkat 2025. június 14.-ig frissíteniük kell az összes eduID.hu-t támogató rendszerükben. Ezt követően a régi - több, mint 4 éves aláírókulcs (HREF-2020) - leállításra kerül, és az utolsó aláírástól számított 10. napon a régi metaadat érvénytelen lesz.

Az alábbi táblázatok az átálláshoz szükséges összes adatot tartalmazzák. A konfigurációs példák, olyan megoldásokat kínálnak (ahol ez lehetséges), amelyekkel egyszerre lehet használni a régi és az új metaadatot.

Key Rollover

Elnevezések

Elnevezés	Metaadat aláíró tanúsítvány	Kivezetés tervezett időpontja
HREF-2011	[https://metadata.eduid.hu/certs/href-metadata-signer-2011.crt href-metadata-signer-2011.crt]	2022.01.01.
HREF-2015	[https://metadata.eduid.hu/certs/mdx-test-signer-2020.crt mdx-test-signer-2015.crt]	2022.01.01.
HREF-2020	[https://metadata.eduid.hu/certs/href-metadata-signer-2020.crt href-metadata-signer-2020.crt]	2025.06.14.
HREF-2025	[https://metadata.eduid.hu/certs/href-metadata-signer-2025.crt href-metadata-signer-2025.crt]	2030.06.14.

SHA1 fingerprints

Elnevezés	SHA1 fingerprint
-----------	------------------

HREF-2011	FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66
HREF-2015	91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43
HREF-2020	C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61
HREF-2025	45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE

Domain név változások

Domain	Technikai domain	Kulcs	Állapot
metadata.eduid.hu	metadata.eduid.hu/2011/href.xml	HREF-2011	Prod
	metadata.eduid.hu/2020/href.xml	HREF-2020	Prod
	metadata.eduid.hu/2025/href.xml	HREF-2025	Prod
mdx.eduid.hu	mdx-2015.eduid.hu	HREF-2015	Prod
	mdx-2020.eduid.hu	HREF-2020	Prod
	mdx-2025.eduid.hu	HREF-2025	Prod

Discovery Service változások

URL
https://mdx-2020.eduid.hu/role/idp.ds
https://mdx-2025.eduid.hu/discovery/ds

Shibboleth Service Provider beállítások

<https://wiki.shibboleth.net/confluence/display/SP3/MetadataProvider>

XML

<https://wiki.shibboleth.net/confluence/display/SP3/XMLMetadataProvider>

```

<MetadataProvider type="Chaining">
  <MetadataProvider type="XML" id="href-2020" url="https://mdx-2020.eduid.hu"
backingFilePath="href-2020.xml">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
  </MetadataProvider>
  <MetadataProvider type="XML" id="href-2025" url="https://mdx-2025.eduid.hu"
backingFilePath="href-2025.xml">
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
  </MetadataProvider>
</MetadataProvider>

```

MDX

Shibboleth 3.X

<https://wiki.shibboleth.net/confluence/display/SP3/MDQMetadataProvider>

```

<MetadataProvider type="MDQ" id="href-2020" ignoreTransport="true" baseUrl="https://mdx-
2020.eduid.hu/">
  <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
<MetadataProvider type="MDQ" id="href-2025" ignoreTransport="true" baseUrl="https://mdx-
2025.eduid.hu/">
  <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>

```

példa

apache + shibboleth 3.X - sed segítségével

```

sudo sed 's/mdx-2020.eduid.hu/mdx-2025.eduid.hu/g' /etc/shibboleth/shibboleth2.xml -i
sudo sed 's/href-2020/href-2025/g' /etc/shibboleth/shibboleth2.xml -i
sudo sed 's/href-metadata-signer-2020.crt/href-metadata-signer-2025.crt/g'
/etc/shibboleth/shibboleth2.xml -i
sudo sed 's#https://mdx-202..eduid.hu/role/idp.ds#https://mdx-2025.eduid.hu/discovery/ds#g'
/etc/shibboleth/shibboleth2.xml -i

```

```
sudo systemctl restart shibd.service apache2.service
```

Shibboleth 2.X

```
<MetadataProvider type="Dynamic" id="href-2020" ignoreTransport="true">
  <Subst>https://mdx-2020.eduid.hu/entities/$entityID</Subst>
  <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
<MetadataProvider type="Dynamic" id="href-2025" ignoreTransport="true">
  <Subst>https://mdx-2025.eduid.hu/entities/$entityID</Subst>
  <MetadataFilter type="Signature" certificate="href-metadata-signer-2025.crt"/>
</MetadataProvider>
```

Shibboleth Identity Provider beállítások

XML

Shibboleth 4.X

<https://wiki.shibboleth.net/confluence/display/IDP4/FileBackedHTTPMetadataProvider>

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
  backingFile="%{idp.home}/metadata/href-2025.xml"
  metadataURL="https://metadata.eduid.hu/2025/href.xml">

  <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
    certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2025.crt"/>

  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

  <MetadataFilter xsi:type="EntityRoleWhitelist">
    <RetainedRole>md:SPSS0Descriptor</RetainedRole>
  </MetadataFilter>

</MetadataProvider>
```

Shibboleth 3.X

<https://wiki.shibboleth.net/confluence/display/IDP30/FileBackedHTTPMetadataProvider>

```
<MetadataProvider id="RemoteMetadataAggregate" xsi:type="FileBackedHTTPMetadataProvider"
    backingFile="%{idp.home}/metadata/href-2025.xml"
    metadataURL="https://metadata.eduid.hu/2025/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSS0Descriptor</RetainedRole>
    </MetadataFilter>

</MetadataProvider>
```

MDX

Shibboleth 4.X

<https://wiki.shibboleth.net/confluence/display/IDP4/DynamicHTTPMetadataProvider>

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
    connectionRequestTimeout="PT2S"
    connectionTimeout="PT2S"
    socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2025.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

Shibboleth 3.X

<https://wiki.shibboleth.net/confluence/display/IDP30/DynamicHTTPMetadataProvider>

```
<MetadataProvider id="DynamicEntityMetadata" xsi:type="DynamicHTTPMetadataProvider"
    connectionRequestTimeout="PT2S"
    connectionTimeout="PT2S"
    socketTimeout="PT4S">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/credentials/href-metadata-signer-2025.crt"/>

    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P9D"/>

    <MetadataQueryProtocol>https://mdx-2025.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

SimpleSAMLphp

MDX

```
//config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'], // ez a *-hosted metadata konfiguráció betöltése miatt szükséges
    [
        'type' => 'mdq',
        'server' => 'https://mdx-2025.eduid.hu',
        /* --- */
        'validateFingerprint' =>
'45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE'
    ],
],
```

metarefresh

https://simplesamlphp.org/docs/stable/simplesamlphp-maintenance#section_3

https://github.com/simplesamlphp/simplesamlphp-module-metarefresh/blob/master/docs/simplesamlphp-automated_metadata.md

```

// config/config-metarefresh.php
$config = [
    'sets' => [
        'href-2020' => [
            'cron'      => ['hourly'],
            'sources'   => [
                [
                    'src' => 'https://metadata.eduid.hu/2020/href.xml',
                    'validateFingerprint' =>
'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61',
                ],
            ],
            'expireAfter'      => 777600, // 9 nap.
            'outputDir'        => 'metadata/metarefresh-href-2020/',
            'outputFormat' => 'flatfile',
        ],
        'href-2025' => [
            'cron'      => ['hourly'],
            'sources'   => [
                [
                    'src' => 'https://metadata.eduid.hu/2025/href.xml',
                    'validateFingerprint' =>
'45:B2:33:96:7C:4F:7E:42:86:8D:CC:CF:CC:0E:3E:1C:2E:24:C2:DE',
                ],
            ],
            'expireAfter'      => 777600, // 9 nap.
            'outputDir'        => 'metadata/metarefresh-href-2025/',
            'outputFormat' => 'flatfile',
        ],
    ],
];

```

```

// config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2020'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2025'],
],

```

FAQ /GYIK

Bővítés alatt!

- Miért cserél KIFÜ kulcsot?
- IdP-t érinti?
- Mi a helyzet az eduGAIN-t használó IdP-ekkel?
- Mi a helyzet az eduGAIN-t használó SP-ekkel?
- Hogyan tudom ellenőrizni, hogy jó kulcsot használok?

Változat #1

document-uploader hozta létre 2025-08-07 12:04:06 CEST

document-uploader frissítette 2025-08-07 12:04:06 CEST