# HREF Key Rollover 2020

# Bevezetés

A HREF új metaadat aláírókulcsra áll át a SAML 2.0 metaadataiban (HREF-2020). A HREF szövetségi tagoknak és partnernek az új aláírókulcshoz tartozó konfigurációkat 2022. január 1.-ig frissíteniük kell az összes eduID.hu-t támogató rendszerükben. Ezt követően a régi - több, mint 6 éves aláírókulcs (HREF-2011) - 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 | href-metadata-signer-2011.crt | 2022.01.01. |
| HREF-2015 | mdx-test-signer-2015.crt | 2022.01.01. |
| HREF-2020 | href-metadata-signer-2020.crt | 2025.06.14. |

## 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` |

| Elnevezés | SHA1 fingerprint |
| --- | --- |
| HREF-2020 | `C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61` |

# Domain név változások

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

# 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-2011" url="https://metadata.eduid.hu/2011/href.xml"
backingFilePath="href-2011.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2011.crt"/>
        <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
    </MetadataProvider>
    <MetadataProvider type="XML" id="href-2020" url="https://metadata.eduid.hu/2020/href.xml"
backingFilePath="href-2020.xml">
        <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.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-2015" ignoreTransport="true" baseUrl="https://mdx-2015.eduid.hu/">
    <MetadataFilter type="Signature" certificate="mdx-test-signer-2015.crt"/>
    <MetadataFilter type="RequireValidUntil" maxValidityInterval="864000"/>
</MetadataProvider>
<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>
```

## Shibboleth 2.X

```
<MetadataProvider type="Dynamic" id="href-2015" ignoreTransport="true">
    <Subst>https://mdx-2015.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="mdx-test-signer-2015.crt"/>
</MetadataProvider>
<MetadataProvider type="Dynamic" id="href-2020" ignoreTransport="true">
    <Subst>https://mdx-2020.eduid.hu/entities/$entityID</Subst>
    <MetadataFilter type="Signature" certificate="href-metadata-signer-2020.crt"/>
</MetadataProvider>
```

# 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-2020.xml"
                  metadataURL="https://metadata.eduid.hu/2020/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2020.crt"/>

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

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</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-2020.xml"
                  metadataURL="https://metadata.eduid.hu/2020/href.xml">

    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
        certificateFile="%{idp.home}/conf/metadata/href-metadata-signer-2020.crt"/>

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

    <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</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-2020.crt"/>

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

    <MetadataQueryProtocol>https://mdx-2020.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-2020.crt"/>

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

    <MetadataQueryProtocol>https://mdx-2020.eduid.hu/</MetadataQueryProtocol>

</MetadataProvider>
```

# SimpleSAMLphp

# MDX

```
//config/config.php
'metadata.sources' => [[=> 'flatfile']('type'), // ez a *-hosted metadata konfiguráció
betöltése miatt szükséges
    [
        'type' => 'mdq',
        'server' => 'https://mdx-2020.eduid.hu',
        /* --- */
        'validateFingerprint' => 'C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61'
    ],
],
```

# 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-2011' => [
          'cron'      => ['hourly'],
          'sources'   => [
              [
                  'src' => 'https://metadata.eduid.hu/2011/href.xml',
                  'validateFingerprint' =>
'FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66',
              ],
          ],
          'expireAfter'       => 777600, // 9 nap
          'outputDir'     => 'metadata/metarefresh-href-2011/',
          'outputFormat' => 'flatfile',
      ],
      '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',
    ],
  ],
];
```

```
// config/config.php
'metadata.sources' => [
    ['type' => 'flatfile'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2011'],
    ['type' => 'flatfile', 'directory' => 'metadata/metarefresh-href-2020'],
],
```

# FAQ /GYIK

Bővítés alatt!

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

---

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:08 CEST
cziernorbert frissítette 2026-04-14 13:24:10 CEST