HREF metadata specifikáció

A föderációs metaadat célja, hogy a föderációban részt vevő intézmények illetve entitások technikai, bizalmi és adminisztratív adatait egy helyre gyűjtse. A metaadatok formátuma megfelel a SAML2 metaadat szabványnak.

Biztonsági megfontolások

Mivel a metadata tartalmazza a föderációban részt vevő tagok és komponensek technikai információit, ezért a benne tárolt információkkal kapcsolatban figyelembe kell venni a következő biztonsági megfontolásokat:

- Téves vagy kompromittálódott adatok eltávolítása esetén a sérülékenységi ablak megegyezik a metadata gyorstárazhatósági (`cacheDuration`) idejével, **amennyiben a támadó nem képes blokkolni a központi metaadatok elérhetőségét (DOS)**
- Amennyiben a támadó képes blokkolni a központi metaadatok elérhetőségét, a sérülékenységi ablak a legutolsó letöltött metadata állomány érvényességéig (`validUntil` paraméterében meghatározott ideig) tart.
- Amennyiben a metaadatok érvényességi ideje lejár, az entitás nem képes azonosítani a többi föderációs résztvevőt, ezért nem tud föderációs szolgáltatást (pl. IdP esetén azonosítási szolgáltatást) nyújtani.

Metaadatban tárolt információk

- Bizalom a metaadatban
  - a metaadat integritásvédelmét és hitelességét egy digitális aláírás biztosítja.
  - a metaadat visszavonhatóságát a lejárati idő (`validUntil`) biztosítja, ami jelenleg 3 nap.
  - az egyes rendszerek gyorstárazhatják a metaadatot, de legalább naponta egyszer kötelesek a hiteles állományt frissíteni.
  - az aláírási procedúrát a Metaadat_aláírásának_módja fejezet írja le.
- Tanúsítványok
  - kötelező legalább 1024 bites kulcspárt használni
  - az entitások által használt tanúsítvánnyal kapcsolatban a föderáció nem tesz különleges megkötést, sőt: ajánlott hosszú lejáratú self-signed tanúsítványok használata
- További információk

- minden szöveges mezőt legalább két nyelven: magyarul és angolul ki kell tölteni
- kötelezően kitöltendőek az intézményi, adminisztratív információk (`Organization` illetve `ContactPerson` elemek)
- ajánlott megadni egy helpdesk URL-r, ahova hiba esetén a felhasználók fordulhatnak (`errorURL` attribútum)
- SP-k esetén további kötelező elemek
  - `AttributeConsumingService`, ami megadja a kért attribútumokat
    - `RequestedAttributes` - itt az attribútum informális neve is szerepeljen
    - `ServiceName`, `ServiceDescription` az SP szolgáltatás neve és leírása
  - a szolgáltatás elérhetősége, amin a szolgáltatás bemutatkozik (extension)
  - adatkezelési szabályzatra mutató URL (extension)
- IdP-k esetén
  - a scope csak az adott intézmény kezelésében levő domain név lehet (Shibboleth extension)
- lehetőség van további adatok megadására is
  - logó
  - gps koordináták, IP cím tartomány
  - különböző tagek, például a szolgáltatás publikus-e, vagy épp bevezetés alatt áll-e

Metaadat kiterjesztések használata

Ezen kiegészítő adatok tárolására az internet2 szabványtervezetet készít, ennek a sémának a jelenlegi verziója megtalálható itt.

A kiegészítő séma névtere: `urn:oasis:names:tc:SAML:2.0:metadata:ui`. Az alábbi táblázatban ezen névtérben definiált legfontosabb elemeket foglaljuk össze:

element név	szemantika	értékekre vonatkozó megkötések
GeolocationHint	szélesség és hosszúság érték, a + előjel az északi szélességet illetve keleti hosszúságot jelöli	47.47359,19.052891
InformationURL	az entitásról további információkat (pl. helpdesk) szolgáltató oldal.	
PrivacyStatementURL	Az SP adatvédelmi nyilatkozátnak elérhetősége (URL)	Engedélyezett formátumok: HTML, PDF
Logo	Az IdP/SP logójának elérhetősége	Formátummal kapcsolatban lásd Logo
IPHint	(Csak az IdP-knél) az intézmény hálózati tartománya(i). IdP felderítés esetén előválasztás lehetséges ennek alapján.	CIDR, több érték is megadható

element név	szemantika	értékekre vonatkozó megkötések
DomainHint	(Csak az IdP-knél) az intézmény által felügyelt domain név. IdP felderítés esetén előválasztás lehetséges ennek alapján.	Több érték is megadható

Logo

- formátum: URL egy transzparens hátterű PNG, vagy transzparens hátterű GIF képre
- méretezés
  - javasolt oldalarány 1:1 vagy 16:9
  - maximális méret 200x200px
  - ajánlott egy 16x16px-es verziót is megadni
- attribútumok
  - `xml:lang`: lokalizációs információ
  - `href`: opcionális link
  - `height`: opcionális magasság érték pixelben
  - `width`: opcionális szélesség érték pixelben

Egy IdP példa

```
 <EntityDescriptor entityID="https://idp.niif.hu/shibboleth"
  xmlns:mdui="urn:oasis:names:tc:SAML:2.0:metadata:ui">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol urn:mace:shibboleth:1.0">
   <Extensions>
    <shibmd:Scope>niif.hu</shibmd:Scope>
    <mdui:DiscoHints xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <mdui:GeolocationHint>47.518356,19.055437</mdui:GeolocationHint>
      <mdui:DomainHint>niif.hu</mdui:DomainHint>
      <mdui:DomainHint>iif.hu</mdui:DomainHint>
    </mdui:DiscoHints>
   </Extensions>
   <KeyDescriptor use="signing">
    <ds:KeyInfo>
     <ds:X509Data>
      <ds:X509Certificate>...</ds:X509Certificate>
     </ds:X509Data>
    </ds:KeyInfo>
   </KeyDescriptor>
   <!-- endpoints, nameidformats -->
```

```
   </IDPSSODescriptor>
  <ContactPerson contactType="technical">
   <SurName>NIIF AAI</SurName>
   <EmailAddress>aai@niif.hu</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="support">
   <SurName>NIIF AAI</SurName>
   <EmailAddress>aai@niif.hu</EmailAddress>
  </ContactPerson>
  <ContactPerson contactType="administrative">
   <SurName>NIIF AAI</SurName>
   <EmailAddress>aai@niif.hu</EmailAddress>
  </ContactPerson>
 </EntityDescriptor>
```

Egy SP példa

```
 <EntityDescriptor entityID="https://rr.aai.niif.hu/shibboleth"
  xmlns:mdui="urn:oasis:names:tc:SAML:2.0:metadata:ui">
 <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol">
  <Extensions>
    <mdui:UIInfo xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <mdui:PrivacyStatementURL>https://rr.aai.niif.hu/privacy-
policy</mdui:PrivacyStatementURL>
      <mdui:InformationURL>https://rr.aai.niif.hu/about</mdui:InformationURL>
    </mdui:UIInfo>
  </Extensions>
  <KeyDescriptor use="signing">
   <ds:KeyInfo>
    <ds:X509Data>
     <ds:X509Certificate>...</ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </KeyDescriptor>
  <KeyDescriptor use="encryption">
   <ds:KeyInfo>
    <ds:X509Data>
```

```
     <ds:X509Certificate>...</ds:X509Certificate>
    </ds:X509Data>
   </ds:KeyInfo>
  </KeyDescriptor>
  <!-- endpoints -->
  <AttributeConsumingService index="1">
   <ServiceName xml:lang="hu">HREF Resource Registry</ServiceName>
   <ServiceName xml:lang="en">HREF Resource Registry</ServiceName>
   <ServiceDescription xml:lang="hu">Resource Registry - a föderáció adminisztrációs
alkalmazása http://rr.aai.niif.hu/</ServiceDescription>
   <ServiceDescription xml:lang="en">Resource Registry - federation administration tool
http://rr.aai.niif.hu/</ServiceDescription>
   <RequestedAttribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3"
isRequired="true"/>
   <RequestedAttribute FriendlyName="surname" Name="urn:oid:2.5.4.4" isRequired="true"/>
   <RequestedAttribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" isRequired="true"/>
   <RequestedAttribute FriendlyName="eduPersonPrincipalName"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" isRequired="true"/>
   <RequestedAttribute FriendlyName="schacHomeOrganizationType"
Name="urn:oid:1.3.6.1.4.1.25178.1.2.10" isRequired="true"/>
   <RequestedAttribute FriendlyName="eduPersonScopedAffiliation"
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.9" isRequired="true"/>
  </AttributeConsumingService>
 </SPSSODescriptor>
 <Organization>
  <OrganizationName xml:lang="hu">NIIF - Nemzeti Információs Infrastruktúra Fejlesztési
Intézet</OrganizationName>
  <OrganizationName xml:lang="en">NIIF Institute - National Information Infrastructure
Development</OrganizationName>
  <OrganizationDisplayName xml:lang="hu">NIIF - Nemzeti Információs Infrastruktúra Fejlesztési
Intézet</OrganizationDisplayName>
  <OrganizationDisplayName xml:lang="en">NIIF Institute - National Information Infrastructure
Development</OrganizationDisplayName>
  <OrganizationURL xml:lang="hu">http://www.niif.hu</OrganizationURL>
  <OrganizationURL xml:lang="en">http://www.niif.hu/en</OrganizationURL>
 </Organization>
 <ContactPerson contactType="administrative">
  <SurName>NIIF AAI</SurName>
  <EmailAddress>aai@niif.hu</EmailAddress>
```

```
</ContactPerson>
<ContactPerson contactType="technical">
 <SurName>NIIF AAI</SurName>
 <EmailAddress>aai@niif.hu</EmailAddress>
</ContactPerson>
<ContactPerson contactType="support">
 <SurName>NIIF AAI</SurName>
 <EmailAddress>aai@niif.hu</EmailAddress>
</ContactPerson>
</EntityDescriptor>
```

Metaadat aláírásának módja

Aláíró kulcs és tanúsítványok

HREF-2011

- Az aláíró kulcsot smart cardon, pin kóddal védve tároljuk.
- Az aláírás on-line történik, a kártya pin kódját az aláíró szoftver indításakor az AAI adminisztrátor adja meg, a jelszó nem kerül tárolásra az aláírást végző rendszeren (sem másutt).

HREF-2020

- 4096 bites, SHA-384 RSA aláíró kulcs.
- Az aláírás on-line történik, több telephelyes tartalékolt infrastruktúrával.

Aláírási folyamat

Az aláíratlan metaadat frissítése:

1. Az aláíratlan metaadat a https://rr.eduid.hu oldalról ütemezetten, minden óra 15. és 45. percében letöltésre kerül.
2. A letöltött metaadat XML séma ellenőrzése ellenőrzése.
3. A metadat feltöltése az objektum tárolóba.

Aláírás ellenőrzése explicit tanúsítvánnyal

A föderáció entitásai a föderációs metaadat hitelességéről a digitális aláírás ellenőrzésével győződhetnek meg. Az explicit ellenőrzés esetén a `[http://metadata.eduid.hu/current/](http://metadata.eduid.hu/current/)` URL-ről kell letölteni a metadata fájlokat.

Ajánlott a tanúsítvány lejárati idejét figyelmen kívül hagyni.

HREF-2011

- A HREF-2011 tanúsítvány a https://metadata.eduid.hu oldalról érhető el.

SHA-1	`FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66`
Serial Number	1
Version	3
C	HU
O	NIIF Institute
OU	eduID Federation Operator
CN	Metadata Signer
emailAddress	aai@niif.hu
Érvényesség kezdete	2011.10.05.
Érvényesség vége	2031.09.30.

HREF-2020

- A HREF-2020 tanúsítvány a https://metadata.eduid.hu oldalról érhető el.

SHA-1	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`
Serial Number	80:21:EF:F0:BA:16:04:BD
Version	1
C	HU
ST	Budapest
L	Budapest
O	Governmental Agency for IT Development
OU	eduID Federation Operator
CN	Metadata Signer
emailAddress	info@eduid.hu

SHA-1	`C3:72:DC:75:4C:FA:BA:65:63:52:D9:6B:47:5B:44:7E:AA:F6:45:61`
Érvényesség kezdete	2020.06.13.
Érvényesség vége	2025.06.14.

Aláíró kulcs cseréje

- A kulccsere koordinálása a `href-tech` levelezőlistán keresztül történik.
- Kulcs visszavonásakor (kompromittálódás gyanúja esetén) a régi aláíró kulcs azonnal eltávolításra kerül, kontrollált kulcscsere esetén az aláírás párhuzamosan történik a régi és az új kulccsal.

Metaadat elérése

A HREF föderációban többféle metaadat-forrás áll rendelkezésre, melyeket a http://metadata.eduid.hu -ról lehet elérni. Fontos megemlíteni, hogy a metadata letöltésénél nem indokolt az SSL használata, ezért - amennyiben lehetséges -, érdemes a metadata URL-eket nem titkosított HTTP protokoll segítségével letölteni.

A metadata elérés URL-je a következő:
`http://metadata.eduid.hu/${alairo_kulcs_kibocsatas_eve}/${metadata_forras}.xml`.

A metadata források jelenleg a következők lehetnek:

`href.xml`	**Az éles föderációban részt vevő, és a föderáció kritériumait teljesítő entitások.**
`href-test.xml`	A HREF föderáció tesztrendszerei. Bármely, a föderációban részt vevő intézmény tehet be teszt-entitást ebbe a halmazba, ezért ezen metaadat-forrás csak tesztelési célra használható.
`href-pending.xml`	A HREF föderáció "előszobája". Az újonnan csatlakozó intézmények IdP-je először itt lesz elérhető.
`href-edugain.xml`	A HREF föderációból az eduGAIN konföderációba kiajánlott entitások. Ide csak olyan entitások kerülhetnek be, melyek megfelelnek a föderációs kritériumoknak, és képesek az eduGAIN konföderációval való együttműködésre. Ezen entitások be kell hogy olvassák az eduGAIN metaadatot is.
`edugain.xml`	Az eduGAIN konföderáció metaadata, a HREF aláíró kulccsal aláírva.

`href.xml`	**Az éles föderációban részt vevő, és a föderáció kritériumait teljesítő entitások.**
`intézmény-specifikus`	Az intézmény-specifikus metaadat fájlok (pl.: bme.xml, ceu.xml, stb.), melyeket a föderáció kérésre biztosítja, tetszőleges entitások halmazba gyűjtésével.

MDX-alapú elérés

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 tároldóik a metaadat a `cacheDuration`-ben megadott ideig).

A HREF föderációban teszt jelleggel működik és elérhető MDX-kiszolgáló: http://mdx.eduid.hu. A megfelelő beállításokhoz itt érhető el segédlet.

Az MDX kiszolgáló eltérő kulcsot és tanúsítványt használ. Jelenleg az MDX elérés még csak teszt jelleggel működik, az élesüzemre váltáskor a HREF-2020 tanúsítvánnyal fog működni.

A jelenlegi tanúsítvány innen tölthető le: http://metadata.eduid.hu/current/mdx-test-signer-2015.crt

HREF-2015

SHA-1	`91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43`
Serial Number	AA:90:7C:D9:0C:D5:64:8D
Version	3
C	HU
ST	-
L	Budapest
O	NIIFI
OU	AAI
CN	eduID MDX metadata signer
emailAddress	aai@niif.hu
Érvényesség kezdete	2015.10.13.
Érvényesség vége	2034.12.12.

Változat #1
document-uploader hozta létre 2025-08-07 12:06:01 CEST
document-uploader frissítette 2025-08-07 12:06:01 CEST