



Metadata specifikáció

Verzió: 1.1

(2011. szeptember 14.)

aai@niif.hu

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 lejáratási 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 készíti, ennek a sémának a jelenlegi verziója megtalálható [itt](#).

A kiegészítő séma névtére: `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 nyilatkozatnak 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	CIDR, több érték is megadható

	lehetséges ennek alapján.	
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 háttérű PNG, vagy transzparens háttérű 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

Metaadat aláírásának módja

Aláíró kulcs és tanúsítványok

- 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).

Aláírási folyamat

- Aláíratlan metaadat frissítése
 - az aláíratlan metaadat a <https://rr.aai.niif.hu> oldalról ütemezetten (5 perc) letöltésre kerül. A letöltés során az rr.aai.niif.hu tanúsítványa explicit módon ellenőrzésre kerül.
 - a letöltött metaadat formai ellenőrzése
 - az ellenőrzött entitások egy verziókövető rendszerbe kerülnek, az esetleges változásról e-mail értesítés készül ([href-metadata-changes](#)nevű levelezőlistára)
- Az aláíró szoftver rendszeresen (1-2 percenként) ellenőrzi a metaadatot a verziókövető rendszerben, és változás esetén új aláírt metaadatokat készít
 - amennyiben nincs változás, fix időközönként (naponta legalább egyszer) új aláírt állományok készülnek

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/> URL-ről kell letölteni a metadata fájlokat, például: <http://metadata.eduid.hu/current/href.xml>.
- A tanúsítvány a <https://metadata.eduid.hu> oldalról érhető el.
 - DN-je EMAILADDRESS=aai@niif.hu, CN=HREF Metadata Signer 2010, OU=AAI, O=NIIF Institute, O=NIIF CA, C=HU
 - SHA1 09:C2:8B:09:AB:9E:C2:9B:A5:71:37:E7:36:C6:10:FF:96:9F:D7:FE
- Ajánlott a tanúsítvány lejáratát figyelmen kívül hagyni.
- A tanúsítványcsere koordinálása out-of-band módszerrel történik (a href-tech levelezőlista segítségével).

Aláíró kulcs cseréje

- A föderációs metadata aláíró kulcsa 2-3 évente kerül megújításra.
- A föderációs entitások számára ajánlott a tanúsítvány lejáratát idejének figyelmen kívül hagyása.
- A kulccsere koordinálása a href-tech levelezőlistán keresztül történik.
- Kulcs visszavonásakor (kompromittálódás gyanúja esetén) a régi aláíró kulcs azonnal eltávolításra kerül, kontrollált kulccsere 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}/\\${metaadata_forras}.xml](http://metadata.eduid.hu/${alairo_kulcs_kibocsatas_eve}/${metaadata_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 tesztrendszeri. Bármely, föderációban részt vevő intézmény tehet be teszt-entitást ebbe a halmazba, ezért ezen metaadat-forrás csak tesztelési célra használható.
- href-edugain.xml: a HREF föderációból az [eduGAIN](#) konföderációba kijánlott 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.
- `edugain-test.xml`: az [eduGAIN](#)konföderáció teszt metaadata, a HREF aláíró kulccsal aláírva.
- intézmény-specifikus metaadat fájlok, melyeket a föderáció kérésre biztosítja, tetszőleges entitások halmazba gyűjtésével.

Metaadat nézetek

A föderációs operátor külön kérésre speciálisan transzformált metaadat nézeteket is szolgáltat. Ezek a nézetek XSLT transzformációval állnak elő a mindig aktuális metadata állományból. A nézetek speciális URL-en keresztül érhetőek el (csak HTTPS

felett): [https://metadata.eduid.hu/\\${nezet}/\\${relativ_metadata_fajl}](https://metadata.eduid.hu/${nezet}/${relativ_metadata_fajl}).

Néhány példa:

- <https://metadata.eduid.hu/entities/current/href.xml> - entitás azonosítók listája (mindig az aktuális aláíró kulcs használatával).
- <https://metadata.eduid.hu/php-ds-idp/current/href.xml> - SWITCH-féle Discovery Service-hez konfigurációs állomány.