Metadata Specifikáció

Verzió: 2.0

(2017. november 30.)

aai@niif.hu

Tartalom

1 Metaadatok előállítása

A metaadatok az entitásokkal kapcsolatos technikai és egyéb információkat tartalmazzák.

Főszabályként az entitásokat a Tagok által felhatalmazott adminisztrátorok a Resource Registry felületen keresztül állíthatják be. A föderációs operátor minden azonosító szervezet egy kapcsolattartója számára megadja a jogosultságot ahhoz, hogy a Resource Registry-ben az intézményéhez tartozó entitásokat adminisztrálja, valamint ezt a jogosultságot tovább delegálja. A felhatalmazás a HEXAA[1] rendszeren keresztül delegálható.

Az intézmény felelős azért, hogy az adminisztrátorai milyen műveleteket hajtanak végre a Resource Registry felületen. A nyilvánvalóan tévesen és/vagy hibásan megadott adatokat a Tag adminisztrátorainak értesítése mellett a föderációs operátor is jogosult javítani.

A Resource Registry az adatbázisában tárolt információk alapján XML állományokat képes előállítani, amelyet a föderációban részt vevő szoftverek felhasználhatnak. (A felhasználás módjáról lásd: Metaadatok használata.) A Resource Registry adatbázisa a föderációban részt vevő entitásokon kívül a Tagok Saját SP-inek az adatait is tartalmazza, ezeket külön XML nézetben képes szolgáltatni.

A Resource Registry által előállított XML állományokat a föderációs operátor digitális aláírással látja el, valamint rendszeresen frissíti. Bővebben lásd: Biztonsági megfontolások.

1.1 Partner entitások

Partnerek nem kapnak adminisztrációs jogosultságot a Resource Registry-ben, így az ő Service Provider entitásaikat a föderációs operátor adminisztrálja a partner kapcsolattartóitól kapott információk alapján. Identity Provider entitás partnerek számára nem regisztrálható.

1.2 Entitás attribútumok

Az OASIS specifikációja[2] alapján az entitásokhoz további háttérinformációk (ún. entitás attribútumok) is társíthatók. A nemzetközi gyakorlatban elterjedtek az entitás kategóriák[3], amelyek célja, hogy használatukkal a SAML föderációk résztvevői között a biztonságos együttműködés egyszerűbb legyen, ezáltal a felhasználók magasabb szintű szolgáltatásokat kaphassanak.

Az eduID.hu az alábbi entitás kategóriákat támogatja[4]:

1 https://hexaa.eduid.hu
2 http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.html
3 http://macedir.org/entity-category
4 A felsorolásban az entitás kategóriák funkciójával kapcsolatos leírás kizárólag a tájékoztatás célját szolgálja, a kategóriák pontos meghatározása a hivatkozott oldalakon érhető el.

- http://eduid.hu/category/registered-by-eduidhu: minden, az eduID.hu föderáció által regisztrált entitás automatikusan megkapja.
- http://www.geant.net/uri/dataprotection-code-of-conduct/v1: olyan SP-k számára beállítható kategória, amelyek jelzik, hogy az EU adatvédelmi irányelveinek maradéktalanul megfelelnek, továbbá az SP-hez tartozó - géppel olvasható - adatvédelmi szabályzatnak hivatkoznia kell a code of conduct specifikációra. A kategória támogatását az IdP entitások is jelezhetik, amellyel az azonosító szervezet jelezheti, hogy az ilyen kategóriával rendelkező SP entitások számára kiadja a szükséges adatokat.
- http://refeds.org/category/research-and-scholarship: olyan SP-k számára beállítható kategória, amely azt jelzi, hogy az SP az oktatási és/vagy a kutatási célú együttműködést szolgálja. A kategória támogatását az IdP entitások is jelezhetik, amellyel az azonosító szervezet jelezheti, hogy az ilyen kategóriával rendelkező SP entitások számára kiadja a szükséges adatokat. A kategória meghatározza az együttműködés során használatos attribútumokat is.
- http://refeds.org/category/hide-from-discovery: olyan IdP-k számára beállítható kategória, amelynek célja, hogy az ilyen entitás ne jelenjen meg a Discovery Service felületeken.

1.3 Metaadat halmazok (set)

A Resource Registry a tárolt entitásokat különböző halmazokba (set) képes rendezni úgy, hogy egy entitás több halmazba is tartozhat. A halmazok különböző célokat szolgálnak:

- *href*: a föderációs entitások;
- *href-edugain*: az eduGAIN konföderáció számára publikált eduID entitások (Upstream metadata);
- *intézményi halmaz*: minden entitás, amelyet az intézmény regisztrált, közöttük az intézmény Saját SP-i. Amennyiben létezik saját intézményi halmaz, abban az esetben az intézményhez tartozó IdP entitás(ok) automatikusan a halmazba tartoznak;
- *sulinet*: a Sulinet+ eduID pilot programban részt vevő entitások. Adminisztrációja a Sulinet Dashboard felületen keresztül történik. Az intézményi kapcsolattartó kérésére a föderációs operátor a föderációs résztvevők href halmazban levő SP entitásait publikálja a *sulinet* halmazba is.

Az intézményi adminisztrátorok dönthetnek arról, hogy egy entitás a saját intézményi halmazba, a föderációs entitások közé, vagy a föderáció és az eduGAIN konföderáció számára publikált entitások közé kerüljön.

1.4 Scope-ok használata

Az IdP entitás metaadatai között feltünetett scope biztosítja azt, hogy az ezt támogató attribútumok[5] esetén az információ intézményhez köthető legyen.

A scope formája DNS domain név, amelyet akkor jogosult az intézmény a föderációban használni, ha az az intézmény birtokában van vagy rendelkezésére áll. A scope használatának jogosságát a föderációs operátor a regisztrációkor ellenőrzi. Amennyiben az intézmény nem tulajdonosa a domain névnek, a regisztrációhoz csatolnia kell a tulajdonos írásos jóváhagyását ahhoz, hogy a név az eduID Föderációban scope-ként használható legyen.

A Tag által felhatalmazott adminisztrátor kérése alapján a föderációs operátor a Tag IdP entitásaihoz további scope-okat is rendelhet, amelyek esetében a névhasználati jogosultság ellenőrzése azonos az intézmény regisztrációjakor alkalmazott eljárással.

2 Metaadatok használata

2.1 Statikus metaadatfájlok

A föderáció által biztosított statikus metaadatfájlok olyan SAML Metadata[6] XML állományok, amelyeket a föderációs operátor digitálisan aláírt.

A Resource Registry által kezelt Metaadat halmazok (set) külön-külön XML állományt képeznek, amelyek aláírása egységesen történik. Ezeken kívül az alábbi, nem a Resource Registry-ben kezelt adatforrások is XML metaadat-forrásokat képeznek:

- *edugain*: az eduGAIN konföderációból származó entitások (Downstream metadata);
- *eduid-edugain-sp*: összefoglaló halmaz, amely a föderácóban és az eduGAIN konföderációban megtalálható SP entitásokat tartalmazza (az IdP entitások nélkül, hogy kevesebb erőforrással feldolgozható legyen);

Az entitások adminisztrátorai szabadon választhatnak, hogy mely metaadat-forrásokat kívánják használni, azonban tekintettel kell lenniük a Kölcsönösség elve c. fejezetben leírtakra.

A statikus metaadat-állományok elérhetősége az alábbi:

```
http://metadata.eduid.hu/current/{halmaz_neve}.xml
```

A föderációban részt vevő entitások az alábbi állományban találhatók:

```
http://metadata.eduid.hu/current/href.xml
```

A statikus metaadat-állományok sértetlenségének és aktualitásának ellenőrzése kötelező. Az aláírókulcs ellenőrzéséhez szükséges adatok a Digitális aláíró infrastruktúra c. szakaszban találhatók. Ajánlott a metaadat állományok gyorstárazása az erőforráshasználat korlátozása érdekében, azonban **a gyorstárazás**

5 Pl. eduPersonPrincipalName, eduPersonScopedAffiliation
6 https://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

hossza a 24 órát nem haladhatja meg. A tárolt változat tovább használható a lejárati idő végéig, ha a metaadat-forrás frissítése meghiúsul.

2.2 Dinamikus metaadatok (MDX)

Nagy méretű metaadat források (pl. az eduGAIN) használata esetén a rendszeres letöltés nagy adatforgalmat generál, az XML aláírás ellenőrzése pedig sok memóriát és számítási kapacitást igényel. Ezen problémák kiküszöbölésére alkalmas a Metadata Query Protocol[7], amelyet az elterjedt nyílt forrású middleware megoldások támogatnak. Ennek használata során csak a tranzakcióban érintett távoli entitás metaadatai kerülnek letöltésre[8].

A dinamikus metaadatok kiszolgálója a http://mdx.eduid.hu címen található, az entitásokhoz tartozó SAML metaadat az alábbi címről tölthető le:

```
http://mdx.eduid.hu/entities/{entityID}
```

Ahol az {entityID} paraméter a távoli entitás azonosítója URL kódolt[9] formában.

Az mdx.eduid.hu szolgáltatás az alábbi statikus metaadat-forrásokat teszi MDQ protokoll szerint elérhetővé:

- *href*: a föderációban regisztrált entitások;
- *edugain*: lásd Downstream metadata.

A dinamikus metaadat-válaszok sértetlenségének és aktualitásának ellenőrzése kötelező. Az aláírókulcs ellenőrzéséhez szükséges adatok a Digitális aláíró infrastruktúra c. szakaszban találhatók. Ajánlott a metaadatok gyorstárazása az erőforráshasználat korlátozása érdekében, azonban **a gyorstárazás hossza a 24 órát nem haladhatja meg.** A tárolt változat tovább használható a lejárati idő végéig, ha a metaadat-forrás frissítése meghiúsul.

2.3 Adatvédelem

A metaadatok funkciójukból fakadóan nyilvánosak.

A föderációs metaadatok személyes adatokat (a kapcsolattartók nevét és e-mail címét) is tartalmazhatnak. A regisztrációt végző adminisztrátor felelős azért, hogy hogy megszerezze az érintett személyek hozzájárulását ahhoz, hogy ezek a személyes adatok a metaadatok között elérhetőek legyenek. A személyes adatok védelmének biztosítása érdekében javasolt a regisztráció során kapcsolattartónak szervezeti egységet kijelölni.

A föderációs metaadatokban található kapcsolattartó adatok kizárólag az alábbi célokra használhatók fel:

- biztonsági incidensek koordinálása;
- az érintett entitással kapcsolatos működési kérdések tisztázása;

7 https://tools.ietf.org/id/draft-young-md-query-saml-07.html, illetve aktuális változata.
8 Egy azonosítási tranzakció esetén az SP entitás az IdP, az IdP entitás az SP metaadatait tölti le.
9 https://tools.ietf.org/html/rfc3986

- felhasználók segítése.

TILOS a metaadatokban található kapcsolattartók adatait egyéb célokra (ideértve különösen a kereskedelmi célú kapcsolatfelvételt) **felhasználni.**

2.4 Kölcsönösség elve

A felhasználók megfelelő föderatív azonosításához elengedhetetlen, hogy az azonosításban részt vevő IdP és SP kölcsönösen ismerje egymás metaadatait, ellenkező esetben a bejelentkezési folyamat a felhasználó számára nehezen értelmezhető hibával megszakad. Ezért minden esetben, amikor egy adminisztrátor egy entitást egy új kör számára tesz elérhetővé, gondoskodnia kell arról, hogy ezen kör entitásainak a metaadatait ismerje.

3 eduGAIN

A GÉANT által üzemeltetett eduGAIN[10] szolgáltatás összekapcsolja a világ föderációit, ezáltal egyszerűsíti a kutatóközösségek és az oktatás résztvevői számára a digitális tartalmakhoz, szolgáltatásokhoz és erőforrásokhoz való hozzáférést.

Az eduGAIN nemzeti föderációktól (mint az eduID.hu föderáció) fogad el metaadatokat, ezeket technikai szempontból ellenőrzi, aggregálja és egyetlen aláírt XML állomány formájában nyilvánosan elérhetővé teszi. Az eduGAIN konföderációnak kizárólag föderációk lehetnek tagjai[11].

Az eduGAIN működését szabályozó dokumentumok a https://technical.edugain.org/documents oldalon érhetőek el. Ezek a dokumentumok a részt vevő föderációk számára tartalmaznak előírásokat és követelményeket; az eduID.hu föderáció tagjai és partnerei számára a csatalkozási, részvételi és működési szabályokat az eduID csatlakozási szerződés és mellékletei már tartalmazzák.

3.1 Upstream metadata

Az eduID föderáció a href-edugain[12] metadata halmazban publikálja azokat az entitásokat, amelyeket az üzemeltető intézmény az eduGAIN konföderáció részévé kíván tenni. Ez a halmaz, bár nyilvánosan elérhető, kizárólag az eduGAIN központi metaadat aggregátora számára készül. A halmazból keletkező XML állományt a föderációs operátor az eduGAIN üzemeltetőivel egyeztetett módon írja alá.

A Resource Registry felületen az intézmények meghatalmazott adminisztrátorai minden entitásról eldönthetik, hogy publikálják-e az entitás adatait az eduGAIN konföderáció számára.

Alapértelmezett módon az sem az IdP, sem az SP entitások adatai **nincsenek publikálva** az eduGAIN upstream metadata halmazban (**opt-in**).

10 https://www.edugain.org
11 A tagok aktuális listája a https://technical.edugain.org/status oldalon található.
12 http://metadata.eduid.hu/current/href-edugain.xml

Kizárólag olyan entitások publikálhatók az eduGAIN-ben, amelyek a föderációs halmazban is benne vannak.

3.2 Downstream metadata

Az eduGAIN az előállított metaadatokat a föderációkkal egyeztetett helyen és aláírási módon teszi elérhetővé a föderációk számára. Ez az állomány a föderációk aláíró infrastruktúrája számára készül, és nem a föderációkban részt vevő entitások számára.

A föderációs operátor által üzemeltett eduID.hu aláíró infrastruktúra a központi eduGAIN aláírásokat ellenőrzi, majd az alábbi műveleteket végzi:

1. Eltávolítja a halmazból az eduID.hu föderáció által regisztrált entitásokat;
2. Eltávolítja a halmazból azokat az entitásokat, amelyeket a föderációs résztvevők számára (technikai vagy egyéb okokból) nem kíván elérhetővé tenni. Az így eltávolított entitások aktuális listáját a föderációs operátor kérésre a föderációs kapcsolattartók rendelkezésére bocsátja.
3. A halmazt aláírja és az eduID.hu föderáció entitásai számára elérhetővé teszi.

A föderációs operátor az eduGAIN downstream metadata állományt **ugyanazzal az aláírókulccsal írja alá**, mint a föderáció többi metaadat állományát.

A föderációs operátor az eduGAIN downstream metadata állományban található entitások helyes működését nem tudja garantálni, de - garancia vállalása nélkül - segítséget nyújt abban, hogy a részt vevő entitások sikeresen együttműködhessenek.

4 Biztonsági megfontolások

4.1 Digitális aláíró infrastruktúra

A metaadatok integritásvédelmét és hitelességét – mind a statikus-, mind a dinamikus metaadat-kiszolgálás esetén – digitális aláírás biztosítja.

A **statikus metaadatokat** aláíró digitális kulcs adatai:

Elérhetőség	https://metadata.eduid.hu/2011/href-metadata-signer-2011.crt
Tulajdonságok	2048 bites RSA kulcs, hardver tokenen tárolva
SHA-1 ujjlenyomat	FE:AE:0B:E8:FB:59:ED:F7:CB:7F:69:DF:19:4F:8B:6D:C7:F6:96:66
SHA-512 ujjlenyomat	6C:45:36:18:3D:79:A0:60:D5:57:24:7B:17:0A:59:E2:06:3C:E6:9F:A8:58:6A:86:98:77:2B:2F:3A:93:F6:6C:63:41:93:37:E4:1F:9B:BB:51:1C:5E:4F:DC:2E:D0:EA:63:E9:46:55:07:90:9C:2F:59:19:CA:60:DC:27:9B:8F
X.509 DN	C=HU, O=NIIF Institute, OU=eduID Federation Operator, CN=Metadata Signer/emailAddress=aai@niif.hu
Lejárat	Sep 30 08:18:46 2031 GMT

A **dinamikus metaadatokat** aláíró digitális kulcs adatai:

Elérhetőség	https://metadata.eduid.hu/2011/mdx-signer-2015.crt
Tulajdonságok	2048 bites RSA kulcs, szoftver tokenen tárolva
SHA-1 ujjlenyomat	91:81:AD:2B:F1:C1:4E:47:93:A2:9D:49:34:B7:77:62:4F:2F:98:43
SHA-512 ujjlenyomat	E4:0D:7C:C1:5A:A1:99:F2:3F:78:BC:AA:C6:C7:F1:C4:AE:72:C7:78:B0:DA:6F:2D:ED:20:AD:CA:8C:B0:ED:A4:85:8F:F3:B9:D7:33:A5:87:82:D7:DF:B1:79:2D:11:C0:D1:51:A0:C7:1E:36:CD:26:DF:42:3E:BD:FF:98:AC:9E
X.509 DN	C=HU, ST= , L=Budapest, O=NIIFI, OU=AAI, CN=eduID MDX metadata signer/emailAddress=aai@niif.hu
Lejárat	Dec 12 11:19:40 2034 GMT

4.2 Érvényességi idők

Változtatásra szoruló, hibás vagy kompromittálódott adatok esetén a sérülékenységi ablak megegyezik a metaadatok gyorstárazási idejével, amennyiben a központi metaadatok elérhetősége biztosított. A metaadatok javasolt gyorstárazási ideje a `cacheDuration` attribútumból olvasható ki. A metaadatok a `validUntil` paraméterben megadott ideig használhatók fel.

Az egyes metaadat-forrásokhoz tartozó gyorstárazási és érvényességi idők az alábbiak:

	Statikus	**Dinamikus**
Érvényességi idő	10 nap	7 nap
Gyorstárazási idő	5 óra	5 óra
Időzített frissítés	óránként	óránként