MetadataTrust

Ez a szócikk a Metadata bizalmi kérdéseivel foglalkozik. A föderációk üzemeltetéhez hozzátartozik a föderációs metadata állomány karbantartása is. A föderációban való bizalom technikai értelemben megegyezik a metadatába vetett bizalommal, így ezen bizalom fenntartása rendkívül fontos.

További információkkal szolgál a Trust Management oldal a Shibboleth wikin.

Központi metadata bizalmi modellek

Alapvetően kétféle módon lehet biztosítani a metadata hitelességét:

- aláírás + lejárati idő
- hiteles helyről letöltés (SSL/TLS) + gyorstárazási idő

Előbbi módszer esetén a szállítási protokoll biztonsága nem szükséges (tehát a metadata nem hiteles helyről is beszerezhető - pl. http, email, ...), a digitális aláírás ellenőrzésével a hitelesség megállapítható.

A lejárati idő - `validUntil` ebben az esetben kulcsfontosságú, hiszen egy lejárati idő nélküli metadatát nem lehetséges visszavonni (egy rosszindulatú támadó egy régi metadata példányt később bármikor felhasználhat), így az esetleg kompromittált entitások az egész föderáció biztonságát veszélyeztethetik.

Utóbbi módszer használata esetén a föderációs entitások kötelesek a metadatát egy központi helyről, biztonságos csatornán (pl. https megfelelő tanúsítvány-ellenőrzéssel) adott időközönként letölteni. Ezt a frissítési időközt határozza meg a gyorstárazási idő, a `cacheDuration`.

Metadata bizalom a HREF Föderációban

A HREF Föderációban a metadata biztonságát digitális aláírás és 72 órás lejárati idő együttes alkalmazása biztosítja. A metadata óránként generálódik a Resource_Registry-ben, és aláírásra kerül a metadata aláíró kulccsal.

Aláírás ellenőrzése az aláíró kulcs tanúsítványának segítségével

Az aláírás ellenőrizhető a metadata aláíró kulcs tanúsítványának segítségével, mely elérhető a https://metadata.eduid.hu/href-metadata-signer-2011.crt címről.

Shibboleth IdP illetve SP használata esetén a metadata állomány ellenőrzésére az ún. MetadataFilter használatos, mely az aláírást ellenőrzi a tanúsítvány segítségével.

Shibboleth 2 IdP esetén

Metadata provider beállítása:

```
<MetadataProvider id="href" xsi:type="FileBackedHTTPMetadataProvider"
 xmlns="urn:mace:shibboleth:2.0:metadata"
 metadataURL="http://rr.aai.niif.hu/metadata/href-metadata.xml"
 backingFile="/path/to/metadata/href-metadata.xml" >
 <MetadataFilter xsi:type="ChainingFilter">
  <MetadataFilter xsi:type="RequiredValidUntil"
    maxValidityInterval="604800" />
  <MetadataFilter xsi:type="SignatureValidation"
    trustEngineRef="shibboleth.MetadataTrustEngine"
    requireSignedMetadata="true" />
 </MetadataFilter>
</MetadataProvider>
```

Illetve a hozzá tartozó `TrustEngine` konfiguráció:

```
<!-- Trust engine used to evaluate the signature on loaded metadata. -->
<security:TrustEngine id="shibboleth.MetadataTrustEngine"
  xsi:type="security:StaticExplicitKeySignature">
  <security:Credential id="MyFederation1Credentials" xsi:type="security:X509Filesystem">
    <security:Certificate>/path/to/href-metadata-signer-2011.crt</security:Certificate>
```

```
    </security:Credential>
  </security:TrustEngine>
```

Shibboleth 2 SP esetén

```
  <MetadataProvider type="XML"
    url="http://metadata.eduid.hu/current/href.xmll"
    backingFilePath="href.xml">
   <MetadataFilter type="RequireValidUntil" maxValidityInterval="604800"/>
   <MetadataFilter type="Signature" certificate="href-metadata-signer-2011.crt"/>
</MetadataProvider>
```

SimpleSAMLphp esetén

SimpleSAMLphp használata esetén a metarefresh modul használható a metadata időzített letöltésére és ellenőrzésére. Ezzel kapcsolatban további információkat tartalmaz a SimpleSAMLphp HREF integráció fejezet.

Az aláíró kulcs visszavonása

A fent leírt modell egyetlen problémája az aláíró kulcs kezelésében rejlik. Az aláíró kulcs visszavonása ugyanis csak a rendszeren kívül történhet, egy új kulcs bevezetéséhez az összes partner rendszerében meg kell változtatni az ellenőrzést. Sőt, az átmeneti időben mindkét kulcs használata szükséges lehet (két különböző metadatán).

Amennyiben az aláíró kulcs kompromittálódik, az azonnali visszavonása és egy új kulcs használata esetén azok a rendszerek, melyek még a régi tanúsítványt használták, a metadata lejárati idő letelte után működésképtelenné válnak.

CA használata

Ezen problémák kiküszöbölhetőek egy CA használatával. Ekkor ugyanis az aláíró kulcs tanúsítványát a CA aláírhatja, a partnerek pedig magát a CA tanúsítványt jelölhetik megbízhatónak.

A metadata aláírásakor ebben az esetben nem elég csak az aláíró tanúsítványt beágyazni (`Signature/KeyInfo/X509Certificate` elembe), hanem a CA tanúsítványát is el kell helyezni az aláírt metadatába.

Tanúsítvány visszavonása

CA használata esetén a tanúsítvány visszavonási listák (CRL) illetve on-line ellenőrzés (OCSP) is alkalmazható az aláíró tanúsítvány érvényességének megállapítására. Ezen kívül - mivel magát a tanúsítványt nem kell külön csatornán eljuttatni a partnerekhez -, alkalmazhatóak rövidebb lejáratú (pár hónap, maximum egy év) tanúsítványok is.

Hitelesség ellenőrzése

A metadata aláírásának ellenőrzése ebben az esetben a beágyazott tanúsítvánnyal történik, az aláírás hitelesítése után pedig megtörténik a megfelelő, megbízhatónak jelölt CA-ra történő PKI ellenőrzés.

Shibboleth IdP esetén

A fenti IdP konfigurációs példában a `TrustEngine` konfigurációt kell megváltoztatni, hogy PKIX validációt végezzen. Fontos, hogy a CRL fájl folyamatosan frissítésre kerüljön, ugyanis a Shibboleth nem ad lehetőséget ezen fájl távoli elérésére.

```
<security:TrustEngine xsi:type="security:StaticPKIXSignature"
  id="shibboleth.MetadataTrustEngine">
 <ValidationInfo xsi:type="PKIXFilesystem" xmlns="urn:mace:shibboleth:2.0:security"
   id="HREFCA" VerifyDepth="1" >
  <Certificate>/path/to/trusted/ca-cert.pem</Certificate>
  <CRL>/path/to/trusted/ca-crl.pem</CRL>
 </ValidationInfo>
</security:TrustEngine>
```

> **Figyelem**
>
> A fenti konfigurációs kódrészlet nem alkalmazható a CRL rendszeres, időzített letöltése és előzetes tesztelés nélkül!

Shibboleth SP esetén

A fenti Shibboleth SP példában a `SignatureMetadataFilter`-t kell módosítani az alábbiak szerint

```
<SignatureMetadataFilter verifyName="false">
 <TrustEngine type="StaticPKIX">
  <CredentialResolver type="File">
   <Certificate>
    <Path>ca-cert.pem</Path>
   </Certificate>
   <CRL>
    <Path>ca-crl.pem</Path>
   </CRL>
  </CredentialResolver>
 </TrustEngine>
</SignatureMetadataFilter>
```

Az újabb Shibboleth SP verziókban lehetőség van a CRL URL-ről történő letöltésére is, ezzel kapcsolatban további információk.

> **Figyelem**
>
> A fenti konfigurációs kódrészlet nem alkalmazható előzetes tesztelés nélkül!

SimpleSAMLphp esetén

> **A szócikk vagy fejezet még megírásra vár**

Külön eszközzel

Az NIIF által fejlesztett metadata aláíró/ellenőrző eszköz támogatja a CA tanúsítványok használatát és a PKI validációt (MDSigner forrás).

Változat #5
cziernorbert hozta létre 2026-04-14 13:22:48 CEST
cziernorbert frissítette 2026-04-17 12:59:37 CEST