Tanúsítványok a föderációban

SAML2 föderációkban az entitásoknak ismerniük kell egymás publikus kulcsát (amelyet X.509 tanúsítványokban osztanak meg egymással) ahhoz, hogy biztonságosan kommunikálhassanak egymással. Eközben a felhasználókkal is interakcióba lépnek, ami miatt könnyű összekeverni a két fajta tanúsítványt:

1. amit az IdP/SP a felhasználó felé használ;
2. amit másik entitások (SP/IdP) felé használ.

A **felhasználók felé** olyan tanúsítványt kell használni, amelyben a felhasználók böngészője megbízik. Ez a tanúsítvány nem szerepel a föderációs metadatában, ellenben a webszerver konfigurációjában hivatkozni kell rá. Jellemzően valamilyen jól ismert CA-val (pl. DigiCert vagy letsencrypt) aláírt tanúsítványt, ami azt is jelenti, hogy rendszeresen cserélni kell őket.

A **föderációs metadatában** szereplő tanúsítványt elsősorban a föderációs alkalmazás (Shibboleth , SimpleSAMLphp) konfigurációjában kell megadni, mert ez az, amivel alá tudja írni az általa küldött üzeneteket, illetve dekódolni tudja a fogadott titkosított adatokat. Ez a tanúsítvány lehetőség szerint hosszú (10+ éves) lejáratú, self-signed tanúsítvány legyen.

- A webszerver (Apache, Jetty) konfigurációban csak akkor szerepeljen a föderációs metadatában szereplő tanúsítvány, ha azt szeretnénk, hogy az IdP támogassa az attribútumok back-channel történő letöltését (a Shibboleth IdP ilyen), esetleg ha valamilyen oknál fogva önálló AttributeAuthority-t építünk. Ha valami fut a szabványos https porton (pl. az IdP SSO szolgáltatása vagy egy SP), akkor az AttributeAuthority szolgáltatást nem tehetjük ide, ezért az jellemzően a 8443-as porton szokott figyelni.

Változat #4
cziernorbert hozta létre 2026-04-14 13:22:25 CEST
cziernorbert frissítette 2026-04-14 13:28:56 CEST