Műszaki követelmények SP-k számára

Verzió 1.1
(2017. november 30.)

aai@niif.hu

A dokumentum célja

A dokumentum célja, hogy a HREF Föderációhoz csatlakozó SP-k számára elvárásokat és ajánlásokat fogalmazzon meg, melyek a csatlakozáshoz szükséges identitás-menedzsment, valamint üzemeltetési területeket fednek le.

A dokumentumban a **KÖTELEZŐ, TILOS, AJÁNLOTT, NEM AJÁNLOTT** kifejezések értelmezése az alábbiak szerinti:

1. **KÖTELEZŐ** (ill. “köteles”, “kell”) jelentése: a pontban leírtak betartása a föderációba vetett bizalom kiépítéséhez és megtartásához elengedhetetlenül szükségesek, ettől a résztvevők nem térhetnek el;
2. **TILOS** jelentése **KÖTELEZŐ NEM**, azaz a pontban leírtak szerint az üzemeltető szervezet nem járhat el;
3. az **AJÁNLOTT** pontoktól való eltéréseket az üzemeltető szervezetek dokumentálni kötelesek.
4. **NEM AJÁNLOTT** jelentése: amennyiben az üzemeltető szervezet a pontban leírtak szerint jár el, ezt dokumentálni köteles.

1. Identitás-menedzsment

1.1. Az SP-t üzemeltető szervezetnek rendelkeznie kell adatkezelési dokumentummal, és ennek online elérhetőségét köteles a Resource Registry-ben feltüntetni. Az adatkezelési dokumentumnak nyilvánosan elérhetőnek kell lennie.

2. Szolgáltatás-menedzsment

2.1. Az SP-t üzemeltető szervezet **köteles** a föderációs operátorral való kapcsolattartásra megfelelő szerepkört kijelölni.

2.2. SP-t üzemeltető szervezet **köteles** az SP-vel kapcsolatban végfelhasználói támogatást nyújtani, és ezen támogatás elérhetőségéről a felhasználóit tájékoztatni.

3. Üzemeltetési kérdések

3.1. Az AAI infrastruktúra komponensei esetén **kötelező** *legalább 2048 bites* RSA kulcsok, vagy ezzel egyenértékű biztonságot nyújtó egyéb kriptográfiai kulcsok használata.

3.1.1. Biztosítani **kell** a privát kulcsok védelmét.

3.1.2. Amennyiben egy kulcs kompromittálódik, az intézmény **köteles** a föderációs operátort *24 órán belül* értesíteni.

3.1.3. **Ajánlott** hosszú lejáratú, self-signed tanúsítványok használata

3.2. Vonatkozó SAML szabványok

3.2.1. **Kötelező** az *Interoperable SAML 2.0 Web Browser SSO Deployment Profile* (http://saml2int.org) dokumentumban kötelezőnek megjelölt elemek támogatása

3.2.2. **Ajánlott** a SAML2 Single Logout profil támogatása HTTP Redirect illetve SOAP binding felett.

3.3. Az SP-nek **ajánlott** minden SAML végpontját HTTPS (SSL/TLS) protokollok segítségével védeni.

3.4. Az SP minden SAML végpontjának vagy az SP-t üzemeltető szervezet tulajdonában álló DNS domain alatt **kell** lennie, vagy a domain WHOIS adatbázisban megjelölt tulajdonosától a domain a föderációban történő felhasználására írásos felhatalmazással **kell** rendelkezni.