



Műszaki követelmények IdP-k számára

Verzió: 1.0

(2011. szeptember 27.)

aai@nif.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 intézmény **köteles** adatkezelési elveit dokumentálni, azt a felhasználókkal megismertetni.
- 1.2. Az intézmény **köteles** a felhasználóiról általa ismert adatok forrását, karbantartásának módját, illetve ezen adatok becsült adatminőségét dokumentálni, és ezt a dokumentációt a föderáció rendelkezésére bocsátani.
- 1.3. Felhasználónevet újra kiosztani **tilos**.
- 1.4. Egy természetes személyhez **nem ajánlott** több felhasználói azonosítót rendelni.
- 1.5. **Nem ajánlott** szerep felhasználók (dékán, igazgató) használata.
- 1.6. Attribútumok használata:
 - 1.6.1. A megvalósított attribútumokat az IdP-nek az Attribútum Specifikációban leírt módon **kell** megvalósítani
 - 1.6.2. Az IdP-nek **kötelező** megvalósítania az alábbi attribútumokat:
 - eduPersonTargetedID
 - eduPersonScopedAffiliation
 - schacHomeOrganizationType
 - eduPersonPrincipalName
 - 1.6.3. Az IdP-nek **ajánlott** megvalósítania az alábbi attribútumokat:
 - displayName
 - mail
 - eduPersonEntitlement
 - 1.6.4. Az IdP-nek **kötelező** biztosítania, hogy az eduPersonTargetedID és az eduPersonPrincipalName attribútumok ne legyenek újra kioszthatók
- 1.7. Teszt felhasználók az alábbi megkötések mentén használhatóak:
 - 1.7.1. minden teszt felhasználót egyértelműen azonosítani és dokumentálni **kötelező** (az érte felelős munkatárssal együtt),
 - 1.7.2. teszt felhasználóval valós tranzakciót kezdeményezni **tilos**,

- 1.7.3. **ajánlott** ezen felhasználókat a megfelelő schacHomeOrganizationType értékkel megkülönböztetni.
- 1.8. Felhasználói azonosító adatokat (pl. jelszó) publikus hálózaton titkosítatlanul továbbítani (pl. felhasználótól bekérni, adatbázisszerver felé kommunikálni) **tilos**.
- 1.9. A felhasználói jelszavakat **ajánlott** nem elektronikus formában kiosztani (pl. személyesen, vagy postai úton).
- 1.10. A felhasználók intézményhez fűződő viszonyában bekövetkezett változásokat 7 napon belül **kötelező** megjeleníteni az IdP adatbázisában.
 - 1.10.1. Amennyiben az intézmény külső adatforrást (tanulmányi- ill. bérügyi rendszert) használ a felhasználói adatok tárolására, úgy ez a 7 napos korlát a hiteles adat elsődleges rendszerben történő megváltozásától számítandó.
 - 1.10.2. Hallgató kilépése esetén lehetőség van arra, hogy a jogviszony megszűnte után ún. 'alum' státuszban továbbra is használható maradjon a szolgáltatás. A 'student' illetve 'member' jelző ilyenkor már nem használható.
 - 1.10.3. Oktató illetve alkalmazott kilépése esetén a 'staff', 'employee', 'faculty', 'member' értékeket törölni **kell**.

2. Szolgáltatás-menedzsment

- 2.1. Az intézmény **köteles** a föderációs operátorral való kapcsolattartásra megfelelő szerepkört kialakítani.
- 2.2. IdP-t üzemeltető intézmény **köteles** az IdP-vel kapcsolatban végfelhasználói támogatást nyújtani, és ezen támogatás elérhetőségéről a felhasználóit tájékoztatni.
- 2.3. Az intézmény **köteles** az általa üzemeltetett IdP napi felbontású anonimizált forgalmi statisztikáit a föderációs operátor rendelkezésére bocsátani. Ezen statisztikai adatok a következők:
 - 2.3.1. egyedi felhasználók száma,
 - 2.3.2. egyes föderációs szolgáltatások felé indított tranzakciók száma,
 - 2.3.3. összes bejelentkezési tranzakció száma.

3. Üzemeltetési kérdések

- 3.1. A személyes adatokkal kapcsolatos tranzakciókról **kötelező** naplóállományt készíteni, és azt legalább 30 napig megőrizni.
 - 3.1.1. Az intézmény ezeket a naplókat **köteles** a hatályos adatvédelmi szabályokkal összhangban kezelni.
- 3.2. Az AAI infrastruktúra komponensei esetén **kötelező** legalább 2048 bites kulcsok használata.
 - 3.2.1. Biztosítani **kell** a privát kulcsok védelmét.
 - 3.2.2. Amennyiben egy kulcs kompromittálódik, az intézmény **köteles** a föderációs operátort 24 órán belül értesíteni.
 - 3.2.3. **Ajánlott** hosszú lejáratú, self-signed tanúsítványok használata.
- 3.3. Vonatkozó SAML szabványok
 - 3.3.1. **Kötelező** a SAML2 Web Browser SSO profil támogatása HTTP-POST binding felett;
 - 3.3.2. A Web Browser SSO profil támogatása HTTP-Artifact binding felett **ajánlott**.

- 3.3.3. **Ajánlott** a SAML2 Single Logout profil támogatása HTTP-Redirect illetve SOAP binding felett.
- 3.4. Az IdP **köteles** minden végpontját HTTPS (SSL/TLS) protokollok segítségével védeni.
- 3.5. Az IdP minden SAML végpontjának az IdP-t üzemeltető intézmény tulajdonában álló DNS domain alatt **kell** lennie.
- 3.6. Az IdP által használt scope-oknak az IdP-t üzemeltető intézmény tulajdonában álló DNS domain alatt **kell** lennie.