HREF műszaki előírások

A dokumentum célja, hogy a HREF Föderációhoz csatlakozó Tagok és Partnerek 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:

- **KÖTELEZŐ** (ill. **"KÖTELES"**, **"kell"**) jelentése: a pontban leírtak betartása a föderációba vetett bizalom kiépítéséhez és megtartásához elengedhetetlenül szükségesek, ettől a résztvevők nem térhetnek el;
- **TILOS** jelentése KÖTELEZŐ NEM, azaz a pontban leírtak szerint az intézmény nem járhat el;
- az **AJÁNLOTT** pontoktól való eltéréseket az intézmények dokumentálni kötelesek.
- **NEM AJÁNLOTT** jelentése: amennyiben az intézmény 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 igény esetén ezt a dokumentációt a föderáció tagjainak rendelkezésére bocsátani.
- 1.3. Kötelező a felhasználónevek egyediségét biztosítani.
- 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
    - eduPersonPrincipalName
    - eduPersonScopedAffialiation
  - 1.6.3. Az IdP-nek ajánlott megvalósítania az alábbi attribútumokat:
    - displayName
    - mail
    - sn

    - givenName
  - 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, kivéve, ha a tranzakcióban részt vevő SP a teszt felhasználó használatához hozzájárult,
  - 1.7.3. ajánlott ezen felhasználókat a megfelelő homeOrganizationType értékkel megkülönböztetni.
- 1.8. Felhasználói azonosító adatokat (pl. jelszó) publikus hálózaton titkosítatlanul továbbítani (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 és az eduPersonScopedAffiliation attribútum értékében.
  - 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.

2. Szolgáltatás-menedzsment

- 2.1. Az intézmény köteles a föderációs operátorral való kapcsolattartásra megfelelő szerepkört kialakítani. Ajánlott a kapcsolattartáshoz szerep e-mail címet megadni.
- 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 üzemeltett IdP forgalmi adataiból anonimizált, legalább napi felbontású adatokat szolgáltatni a föderációs operátor számára föderációs célú statisztika készítésének céljából.

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 az *Interoperable SAML 2.0 Web Browser SSO Deployment Profile* (http://saml2int.org) dokumentumban kötelezőnek megjelölt elemek támogatása
    - 3.3.2. 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 domainnek, vagy az alatt levő névnek kell lennie.
- 3.6. Az IdP által használt scope-oknak az IdP-t üzemeltető intézmény tulajdonában álló DNS domainnek, vagy az alatt levő névnek kell lennie.

Változat #1
cziernorbert hozta létre 2026-04-14 13:22:05 CEST
cziernorbert frissítette 2026-04-14 13:24:05 CEST