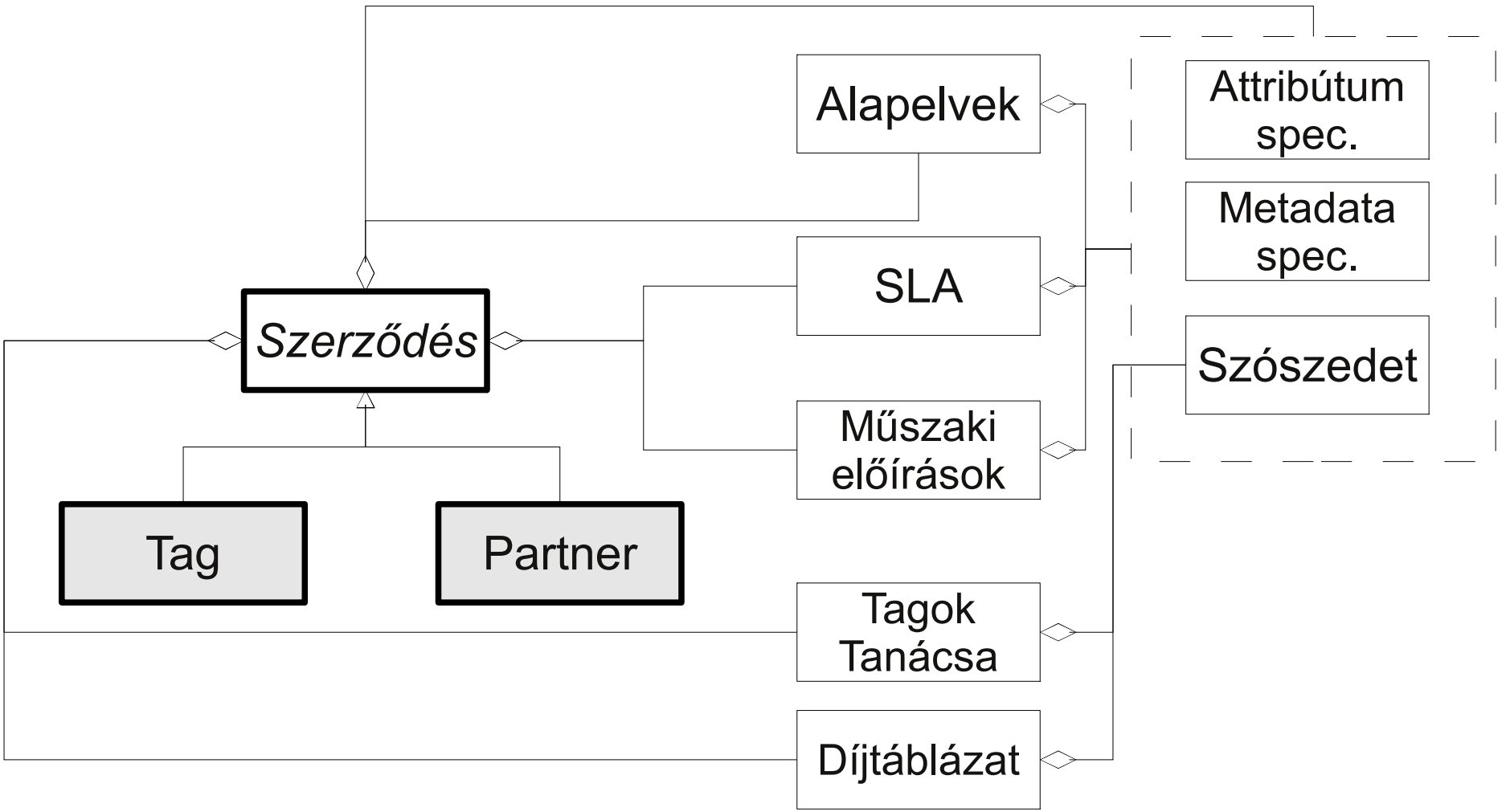
Bajnok Kristóf

HREF Föderáció Policy áttekintés

HBONE ülés,
2010. június 10.

Tartalom

- Dokumentum struktúra
- Aktorok
- Alapelvek
- Szerződés
- Műszaki előírások
- SLA
- Attribútumok
- Metadata


Alapelvek
Attribútum spec.
Metadata spec.
SLA
Szerződés
Szószedet
Műszaki előírások
Tag
Partner
Tagok Tanácsa
Díjtáblázat

Aktorok

- Tag
  - ~ tagintézményi szerződéssel rendelkezők
  - felhasználói igénybe vehetik más Tagok és Partnerek szolgáltatásait
  - a tagok köre nincs kőbe vésve!
    - a Tagok Tanácsa később változtathat/pontosíthat
- Partner
  - ~ bárki
  - szolgáltatásokat nyújthat a felhasználóknak
- Föderációs Operátor

Alapelvek

- A föderáció „alkotmánya”
  - alapvető feltételezések, amelyek a bizalmi szövetség kialakításához szükségesek
  - a felek „jó szándékának” rögzítése
    - üzemeltetési,
    - adatvédelmi,
    - adatkezelési szempontból
- (Aktorok leírása)

Szerződés

- Jelenleg: szolgáltatási szerződés
  - metadata
  - discovery service
  - SLA: VHO, Resource Registry
- Nincs benne, mert nem konkrét:
  - támogatás
    - segédletek
    - fejlesztések
  - jelentkezők felkészítése és elbírálása
  - nemzetközi kapcsolattartás, stb
- ***Cél****: lehetőleg ne kelljen többször aláírni*

Szerződés

- 3. Jogok és kötelezettségek
- 4. Szolgáltatási díj
  - mindenkinek 0 forint (egyedi kedvezmények adhatók :))
  - a díjszabás változtatásába van beleszólásuk a tagoknak
  - ***cél**: a finanszírozási körülmények kisebb-nagyobb változásai ne követeljék meg feltétlenül a szerződés módosítását*
  - külön dokumentum tartalmazza

Szerződés

- 5. Dokumentumok módosításának rendje
  - FedOp konzultál a résztvevőkkel
    - személyesen, e-mailen, stb
  - FedOp meghirdeti a változást
  - 30 nap áll rendelkezésre a tiltakozásra
    - BUG!
  - Ha a tagok több, mint fele tiltakozik, nem léphet hatályba

Szerződés

- 6. Szerződés megszüntetése
  - (közös megegyezés, rendes felmondás)
  - szerződésszegés = bizalom/biztonság veszélyeztetése
    - FedOp kötelessége a többiek érdekében eljárni
    - felfüggesztés, ha nincs érdemi válasz 3 napon belül
  - súlyos szerződésszegés: szándékosság vagy súlyosan gondatlanság feltételezhető
    - azonnali felfüggesztés lehetősége
  - FedOp hibája esetén is alkalmazható
- 7. Egyéb rendelkezések
  - logóhasználat, stb

Műszaki követelmények

- Követelmény
  - kötelező megfelelni (csatlakozáskor és folyamatosan)
- Ajánlás
  - az eltérést dokumentálni kötelező

Műszaki követelmények

- Témakörök
  - Identitás-menedzsment
  - Szolgáltatás-menedzsment
  - Üzemeltetési előírások
- ***Cél****: biztonságosságot garantáló, de megvalósítható követelmények*
- Módosítások lehetségesek!
  - de ehhez feedback szükséges!

Identitás menedzsment

- Kötelező dokumentálni a folyamatokat
- Ha van külső adatbázis, szinkronizálni kell
  - normál: 30 nap
  - affiliation: 7 nap ! (kilépés)
- Tilos:
  - egy személyhez több identitás
  - felhasználónevek újra kiosztása
- Nem személyhez kötődő bejegyzések
- Jelszó erősség (SSL kötelező)

Szolgáltatás menedzsment

- Kötelező végfelhasználói támogatást nyújtani
- Kötelező statisztikai adatokat szolgáltatni
  - anonim módon, csak aggregált adatok

Üzemeltetés

- Logok: 30 napig kötelező megőrizni, utána törölni kell (személyes adat)
- SSL tanúsítvány: ajánlott
  - IdP ↔ felhasználó: „jól ismert” tanúsítvány
  - IdP ↔ SP: self-signed
  - kötelező: min. 2048 bites kulcsok, kompromittálódás esetén azonnal visszavonni
- Metadata: kötelező min. 24 óránként frissíteni, aláírást ellenőrizni

Üzemeltetés

- SAML2 HTTP-POST/HTTP Redirect Binding kötelező, Artifact megengedett (de nem kötelező)
- Ajánlott a Single Logout támogatása
- SSL végpontok (vagy EncryptedAssertion)
  - IdP esetén SSL kötelező!

Adatvédelmi felelős

- IdP köteles megnevezni
- Attribútum igényeket jóváhagyja
  - 7 napon belül
  - Automatikus jóváhagyás lehetősége?
    - opcionális?

Adatvédelmi követelmények

- Adatok kiadása alapvetően a felhasználó jóváhagyását igényli
  - uApprove vagy SSP Consent module kötelező
  - kivéve:
    - oktatáshoz szükséges (felsőoktatási tv. alapján)
    - egyéb törvényi felhatalmazás
  - intézményen belül: nem szólunk bele

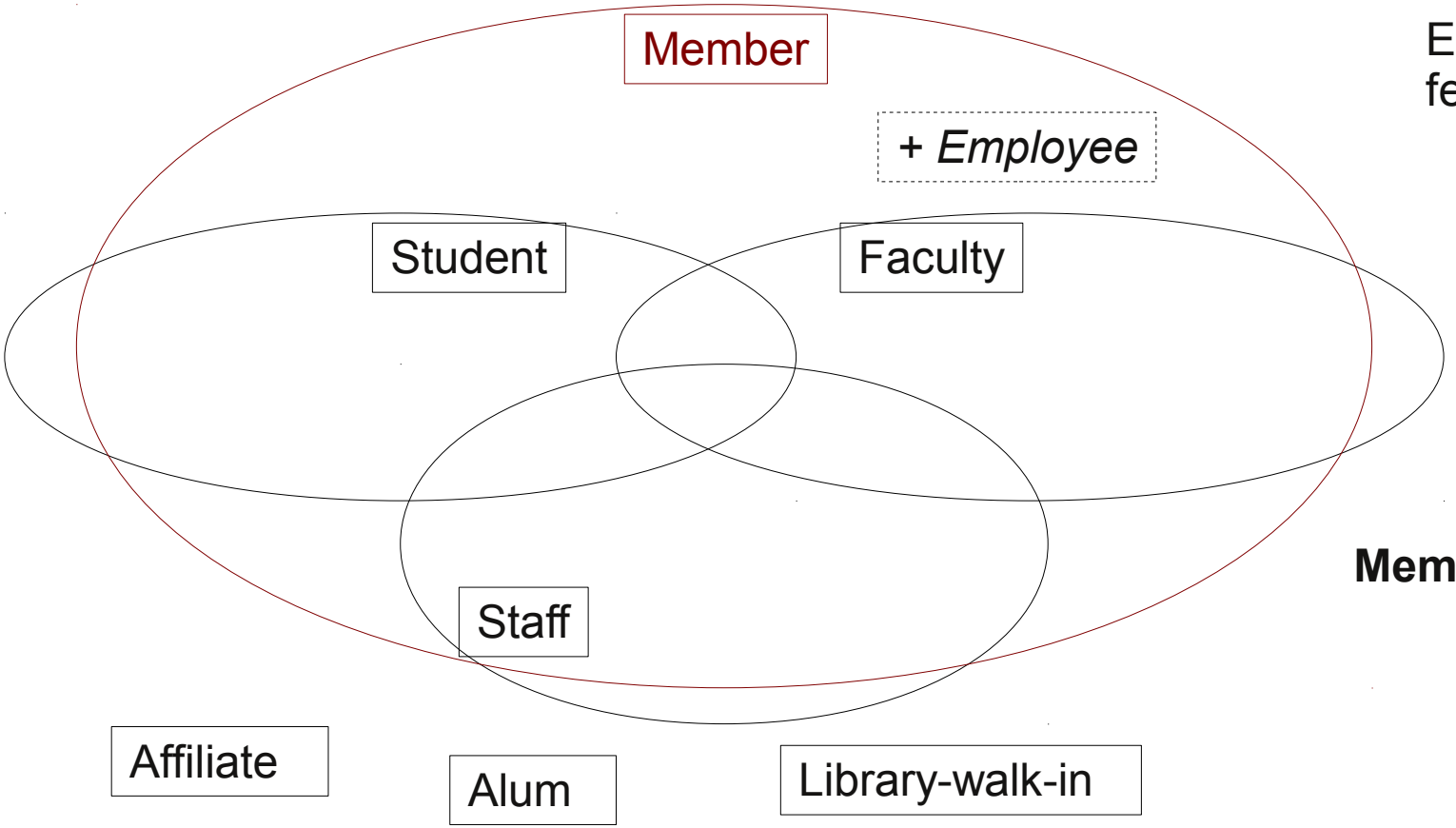
Attribútumok

- Kötelezően implementálandó attribútumok:
  - eduPersonTargetedID
  - eduPersonPrincipalName
  - eduPersonScopedAffiliation
  - schacHomeOrganizationType
- Ajánlott:
  - displayName
  - mail
  - eduPersonEntitlement
  - eduPersonOrgUnitDN

NameID

- Kötelező implementálni valamilyen opaque állandó azonosítót
- Minimum: ComputedID
  - pl. eduPersonTargetedID
    - nem lehet scope-os hash (SSP default)
- Ajánlott: StoredID
  - adatbázist igényel
  - visszavonható

Affiliation



Employee: csak belső felhasználásra javasolt

Member értéket ki kell adni!