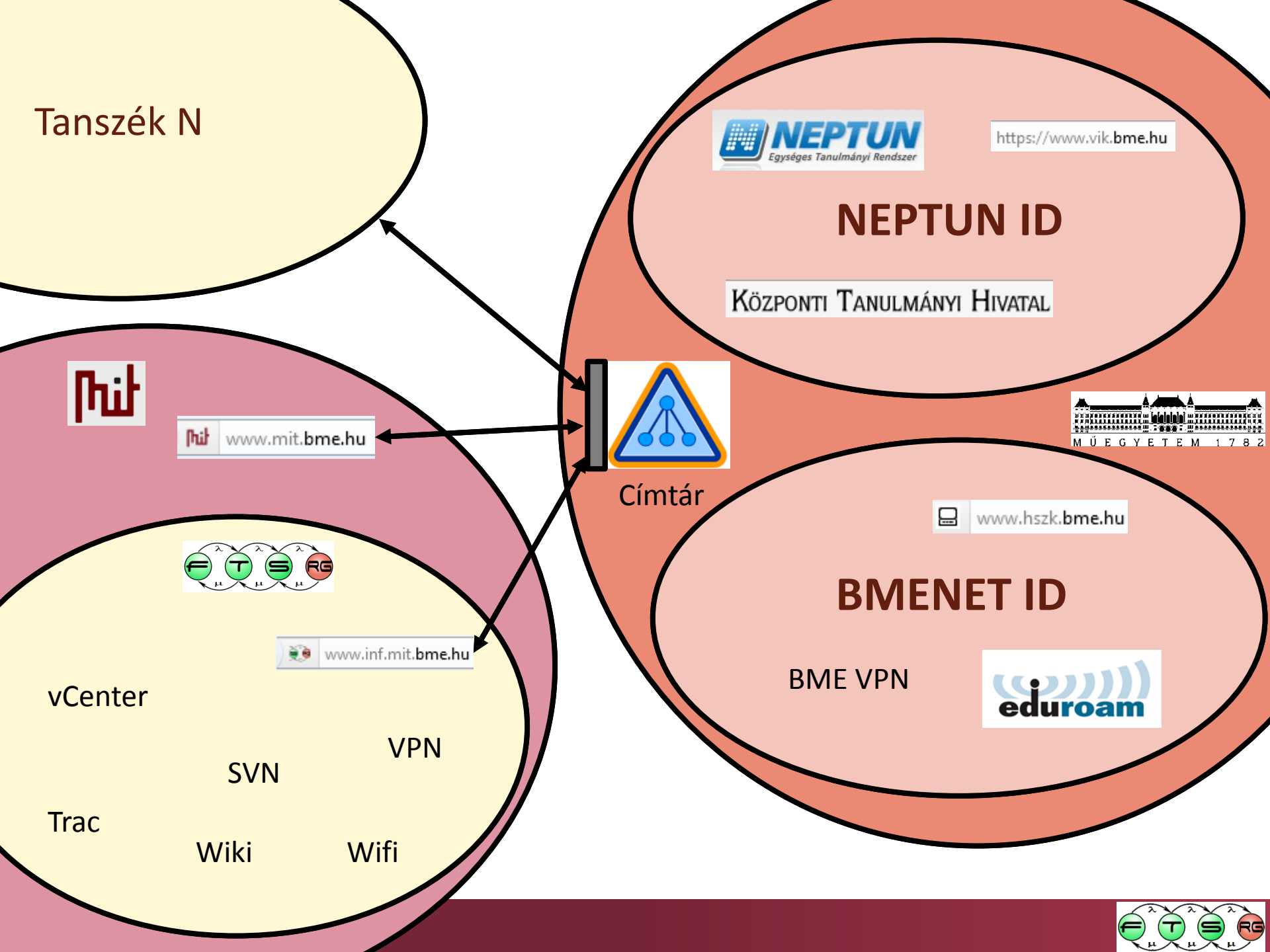
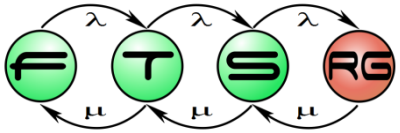

Tanszék N
NEPTUN
Egységes Tanulmányi Rendszer
https://www.vik.bme.hu
NEPTUN ID
Központi Tanulmányi Hivatal
www.mit.bme.hu
Címtár
MŰEGYETEM 1782
www.hszk.bme.hu
BMENET ID
www.inf.mit.bme.hu
BME VPN
eduroam
vCenter
VPN
SVN
Trac
Wiki
Wifi

BME címtár elérés Drupal alól

Ujhelyi Zoltán



BME címtár

- Létező felhasználói adatbázis
  - Érzékeny adatok
    - Pl. lakcím, adózási információk
  - Azonosításhoz szűrt nézet
- Technológia
  - Shibboleth v2.0
  - Adatszűrés
    - Szolgáltatásonként
    - Attribútumszinten

Shibboleth architektúra

- Hitelesítés
  - Shibboleth Identity Provider végzi
  - Visszaadja az engedélyezett attribútumokat a szolgáltatásnak
- Autorizáció
  - Shibboleth Service Provider szintjén
  - A kapott attribútumok alapján
    - Engedélyezi a felhasználói műveleteket

Shibboleth és Drupal

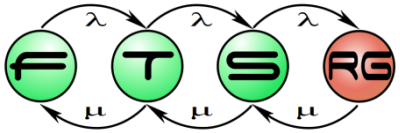
- Shibboleth Apache modul
  - Átirányítható bejelentkezés
  - Shibboleth Identity Provider megadása szükséges
- Drupal
  - Shibboleth attribútumok
    - `$_SERVER` tömbben
  - Szinkronizáció saját felhasználói adatbázissal
    - Új felhasználók létrehozása
    - Hozzárendelés létező felhasználóhoz

DEMO Shibboleth és Drupal

- Shibboleth modul beállítása
- Hitelesítési folyamat
- Visszakapott adatok

Identity Management
– MicroIdM –

Darvas Dániel



ITIL meghatározás

- *Access management* (hozzáférés-menedzsment):

  „Az a folyamat, amely azért felelős, hogy a **felhasználóknak lehetővé tegye az IT-szolgáltatások, adatok vagy más eszközök használatát**. [...] Időnként jogosultság- vagy **identitás-menedzsmentként** is hivatkoznak rá.”

IdM „evolúció”

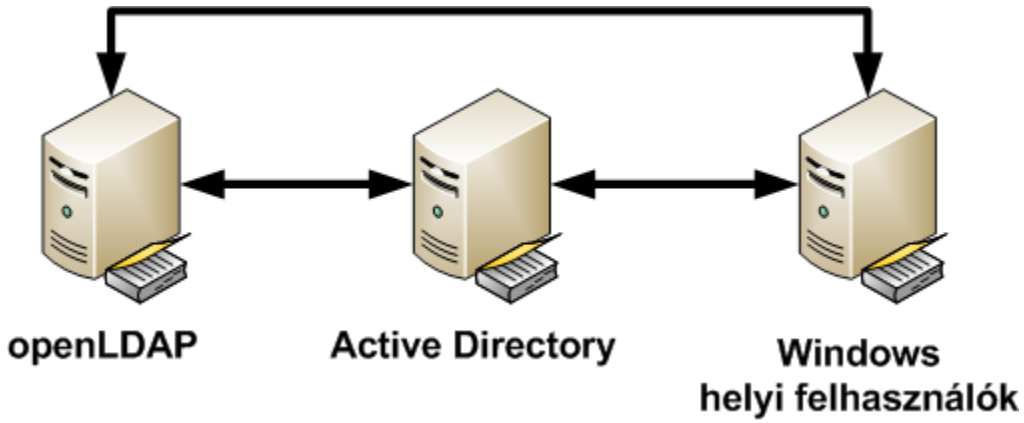
1. Minden rendszer saját maga kezeli a felhasználóit
   - kaotikussá válik
2. Központosítjuk a felhasználókezelést **címtárakba**
   - még mindig létrejöhet több felhasználói siló (heterogén rendszerek)
   - ezek közt ugyanúgy nem biztosított a szinkronitás

3. Központosítsuk a központi címtárakat! ☺

Megvalósítási lehetőségek

A. Szinkronizáció a címtárak közt

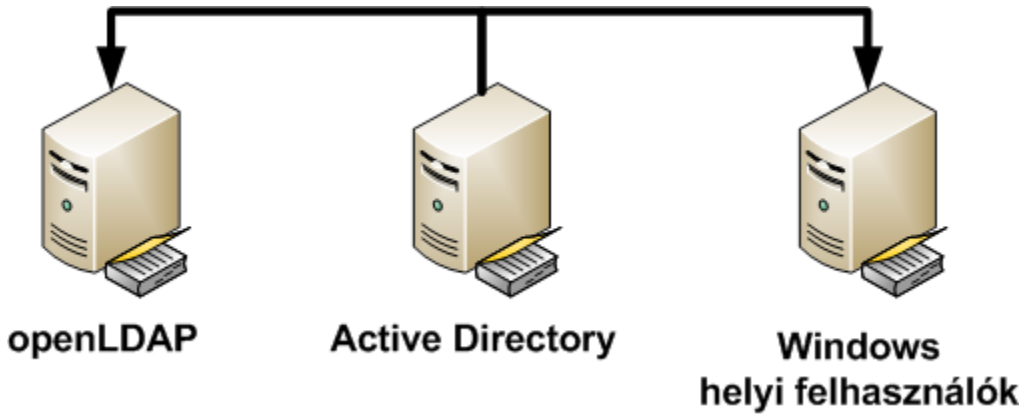
- rengeteg kapcsolat, rengeteg interfész
- minden adat mindenhol módosítható



Megvalósítási lehetőségek

B. „Egy címtár mind felett”

- kevesebb kapcsolat a szerverek közt
- az adatok nem mindenhol módosíthatók
- a szinkronizáció megvalósítása problémás lehet (hogyan lehet kinyerni egy AD-ből a nyílt szövegű jelszavakat?)

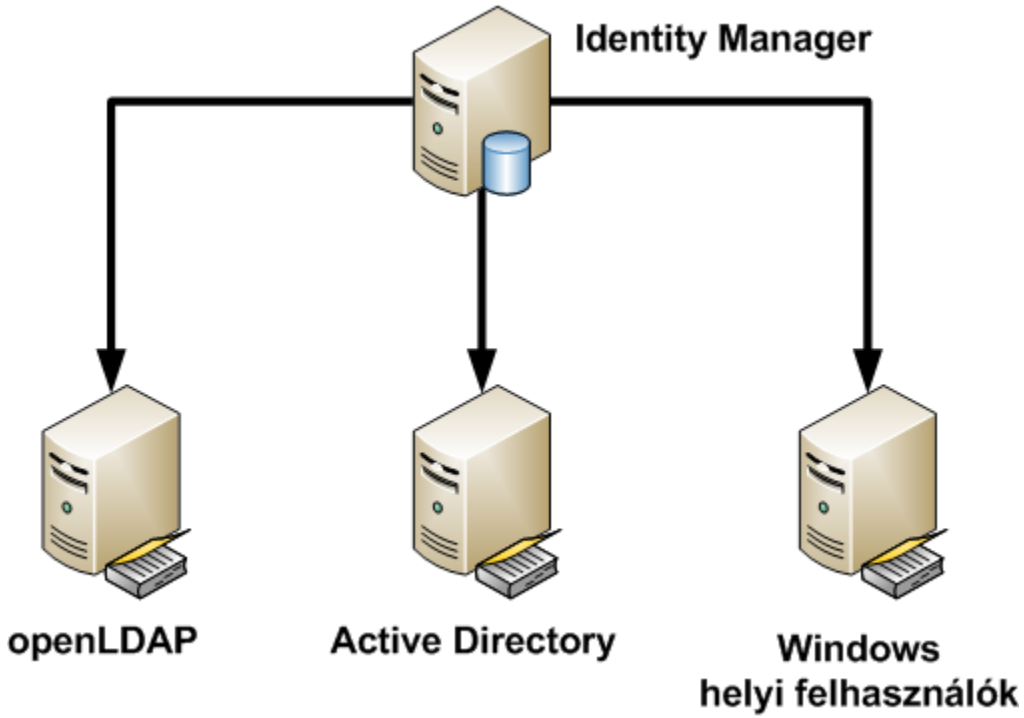


Megvalósítási lehetőségek

C. Identity manager

- új csomópont a rendszerben
- felhasználókezelési szolgáltatást nem nyújt (nem tud hitelesíteni, nem is feladata)

Mi ezt a megoldást választottuk.



Hogyan lehet Identity Managerünk?

- **off-the-shelf megoldás**
  - pl. IBM Tivoli Identity Manager,
    MS Forefront Identity Manager
  - igazán nagy rendszerekre van szabva
    - részlet az ITIM felhasználói közül:

- Banca Alpi Marittime
- Banca Nazionale del Lavoro, Gruppo BNP Paribas
- Banca popolare dell'Emilia Romagna
- Banco ABC Brasil
- Banco Bilbao Vizcaya Argentaria
- Banco Bonsucesso
- Banco de Crédito del Peru
- Banco Espirito Santo
- Banco Itaú Argentina
- Banco Pastor S.A.
- Banco Pastor
- Bangchak Petroleum
- Bangkok Hospital Group
- Bank Austria
- Bank DnB NORD
- Bank Hapoalim
- Banking conglomerate
- Banking IT Service Center
- Bank Leumi
- Bank of Communications
- Bank of New Zealand
- BankPlus
- Bank Rakyat Indonesia

Hogyan lehet Identity Managerünk?

- **off-the-shelf megoldás**
  - \+ készen van
  - – gyakran túl komplex egyszerű feladatokra (nehéz beletanulni)
  - – költséges
    MS FF IM 2010 listaára:
    - – 15 000 USD szerverenként és 18 USD felhasználónként
    - – a tanszéki kis rendszerünk így kb. 4-5 millió HUF lenne…

Hogyan lehet Identity Managerünk?

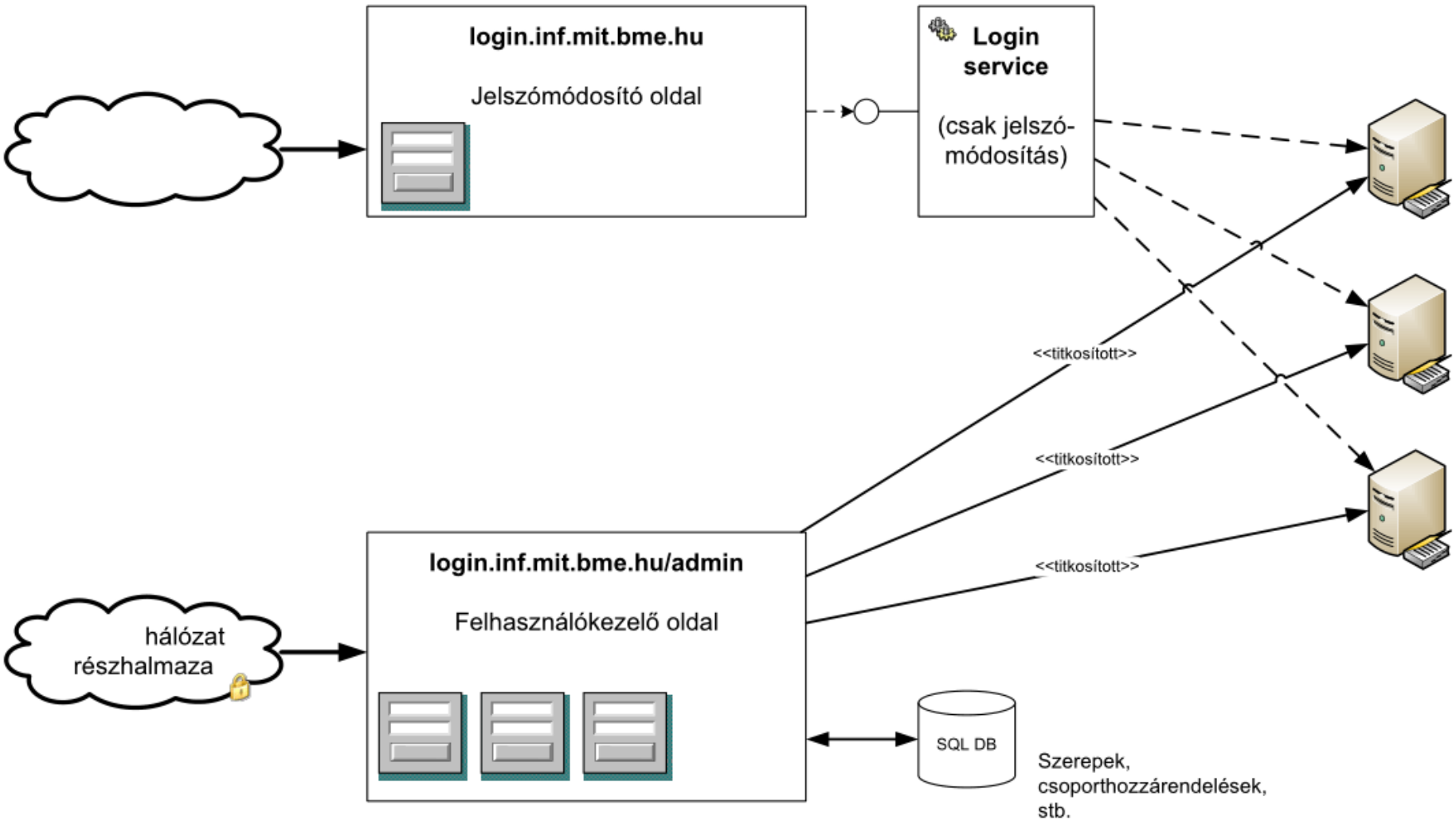
- **saját megoldás**
  - \+ saját igényekre szabható
  - \+ relatíve olcsó
  - – sok-sok munka van vele
  - felhasználható technológiák
    - címtárak interfészének specifikációi alapján teljesen egyedi megoldás
    - .NET System.DirectoryServices (≈ADSI)
    - .NET System.DirectoryServices.AccountManagement
    - …

Saját rendszer: **MicroIdM**

- Micro Identity Manager (MicroIdM) 

  - csak a saját céljainkra szükséges funkcionalitást szeretnénk beletenni
  - .NET DirectoryServices alapú
  - támogatott címtárak: AD, WinNT local users, openLDAP
  - működési logika: pass-through
    - minden módosítást azonnal replikálunk
    - lényegében csak olyan adatokat tárolunk, amik nem következtethetők ki bármelyik címtárból
    - nem tárolunk jelszavakat (biztonsági megfontolás)

MicroIdM architektúra



A .NET megoldások összevetése

DirectoryServices	DirectoryServices. AccountManagement
alacsony szintű • DirectoryEntry objektum szöveges indexeléssel • Invoke-ok	magas szintű, elegáns kódot eredményez • User és Group objektumok .NET property-kkel
pontosan ismerni kell az alatta fekvő implementációt	elrejti az implementációs különbségeket
támogatott rendszerek: AD, WinNT local users, LDAP, IIS, Novell NDS	támogatott rendszerek: AD, WinNT local users

Technológiai heterogenitás

- pl. felhasználókezelés

LDAP	AD	WinNT
Felhasználónév megadása		
cn=john	cn=john	john
Felhasználó típusa		
inetOrgPerson, posixAccount	user	user
Hivatkozás egy felhasználóra		
LDAP://server/cn=john, dc=domain,dc=local	LDAP://server/cn=john, dc=domain,dc=local	WinNT://server/john,user
DirectorySearcher		
támogatott	támogatott	nem támogatott

„Példakód”

- pl. felhasználó engedélyezése AD-ben

```
private void EnableUser
    (DirectoryEntry user)
{
  int val = (int)user.Properties
    ["userAccountControl"].Value;

  user.Properties["userAccountControl"].
    Value = val & ~0x0002;
  user.CommitChanges();
}
```

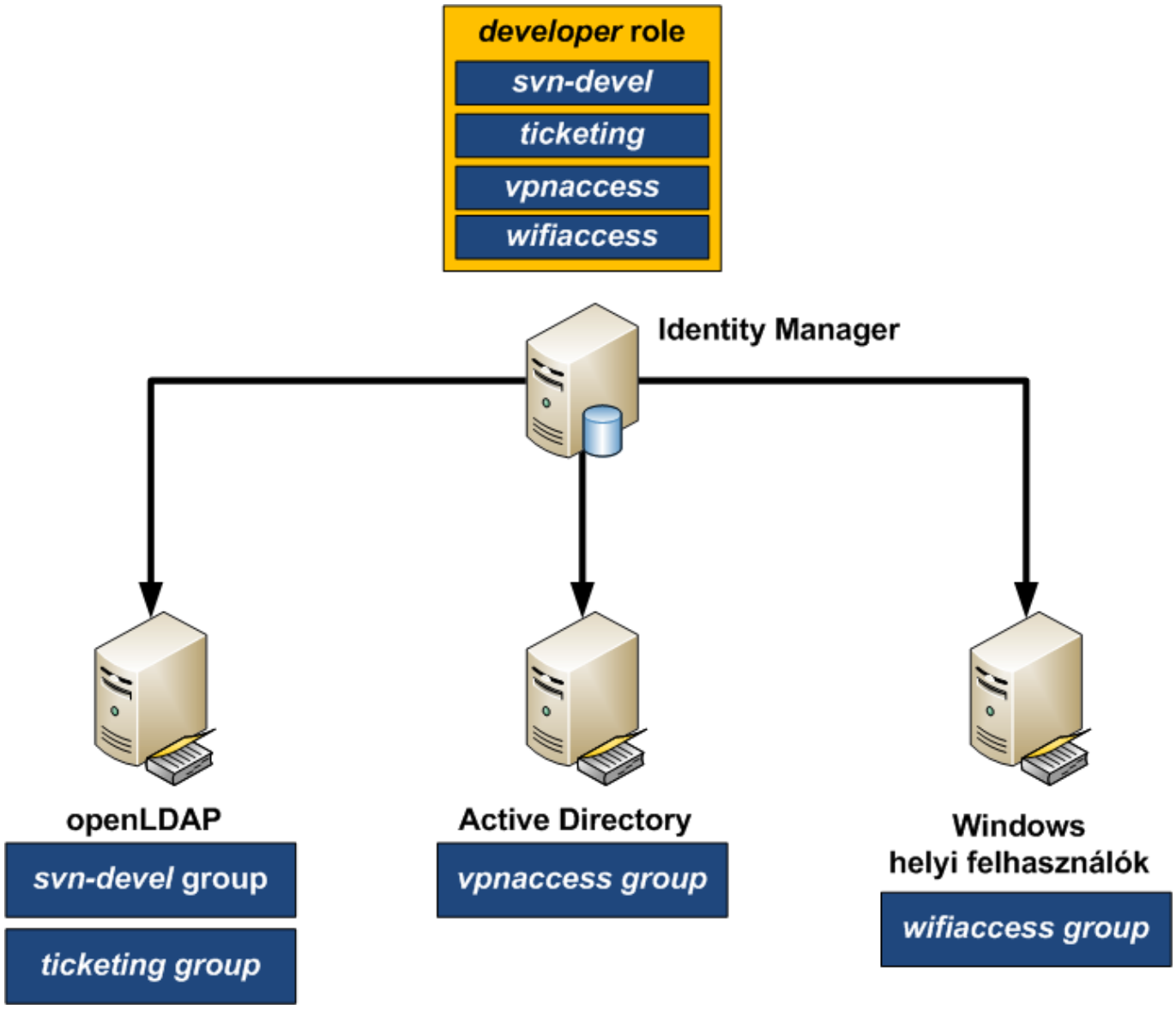
Csoportok

- nem elég a felhasználók szinkronitásával foglalkozni
- szeretnénk **egységes csoportmenedzsmentet** is
- **RBAC**
  - a jogosultságokat szerepekhez rendeljük
  - a felhasználókhoz szerepeket rendelünk

RBAC több siló esetén

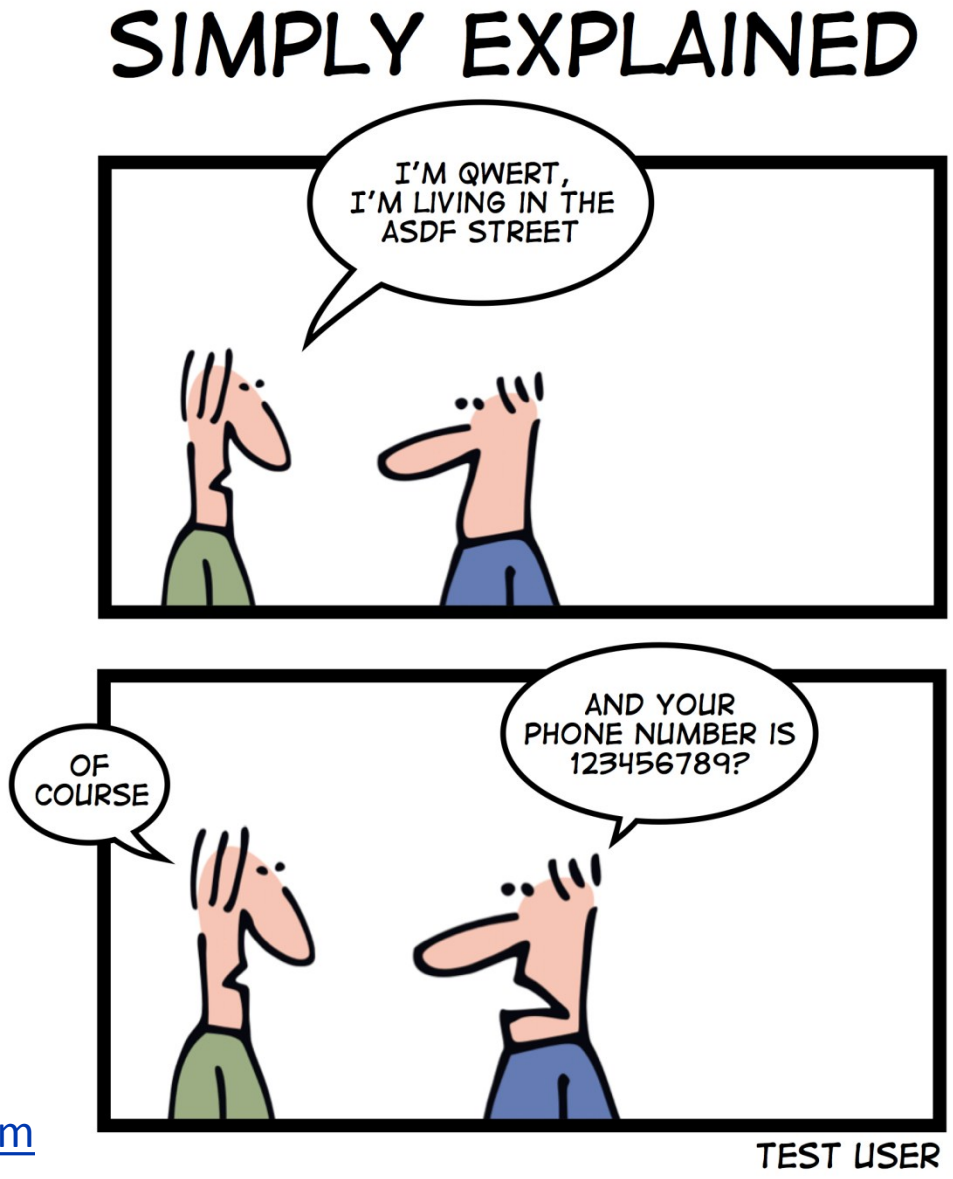
- *Példa:* Egy szoftverfejlesztőnek osztunk jogosultságokat. Kell, hogy legyen:
  - írási joga a verziókezelő dev könyvtárára,
  - írási joga a hibajegykezelő rendszerhez,
  - csatlakozási joga egy VPN-szerverhez,
  - csatlakozási joga egy RADIUS-os WiFi AP-hoz.
- **Mi itt egy szerep?**
  - ha ez 4 külön szerep, a jogosultságok is „szétszinkronizálódnak”
  - ha ez 1 szerep, mi a helyzet a több silóval?

„Metaszerepek”



DEMO MicroIdM

- Az előzőek után talán furcsa, de *képes működni*.
- *Példa*:
  Felhasználó létrehozása három külön címtárban .NET-ből



http://geekandpoke.typepad.com

Felhasználó létrehozása – WinNT

```
newUser = root.Children.Add(loginName
    + "_local", "user");
newUser.Invoke("SetPassword", new
    object[] { "12345Abcd#" });
newUser.CommitChanges();
newUser.Close();
```

Felhasználó létrehozása – LDAP

```
newUser =
    root.Children.Add(string.Format(
    "CN={0}", loginName),"inetOrgPerson");
SetProperty(newUser, "givenName", "Given
    Name " + loginName);
SetProperty(newUser, "sn", "SN " +
    loginName);
SetProperty(newUser, "cn", loginName);
SetProperty(newUser, "uid", loginName);
newUser.CommitChanges();
newUser.Close();
```

Felhasználó létrehozása – AD

```
newUser = root.Children.Add(string.Format("CN={0}",
    loginName), "user");
SetProperty(newUser, "SAMAccountName", loginName);
SetProperty(newUser, "userPrincipalName",
    loginName);
SetProperty(newUser, "givenname", "Given name of "
    + Name);
newUser.CommitChanges();
newUser.Invoke("SetPassword", new object[] {
    "12345Abcd#" });
newUser.CommitChanges();
newUser.Close();
```