



# HumanolT

IT Tuning

## Identity Management + Role Based Access Control

Hírközlési és Informatikai Tudományos Egyesület Számítástechnikai Szakosztálya, a European Organisation for Quality MNB Informatikai Szakbizottsága, és az ISACA Magyar Fejezete közös rendezvényén - 2010.05.07.

## Mi az IDM?

### ▣ Definíció szerint:

Adminisztratív eszköz (**szoftver**), amely az egyéneket azonosítja egy adott rendszerben (pl. ország, hálózat, vállalat) és szabályozza az erőforrásokhoz való hozzáférésüket ezen rendszeren belül, azáltal, hogy összeköti a felhasználói jogosultságokat és tiltásokat a rendszerben létrehozott identitásokkal.

### ▣ Források

- Források lehetnek: LDAP, AD, OS, ERP-k, CSV fájlok
- Konnektorok a forrásokhoz: gyári vagy fejlesztendő
- Külső források (external resources): mobiltelefon, chipkártya

### ▣ Management rendszer.

- **Nem** végez autentikációt
- **Nem** végez autorizációt

## Két különleges IDM projekt tanulságai

1. **Nagyon sok gép – kevés felhasználó**
2. **Sok felhasználó (3000+ fő) – sok szolgáltatás**

### *Ügyfél elvárás:*

- Komoly testreszabási igények (a rendszer feleljen meg 100%-ban a jelenlegi állapotnak)



- Fejlesztés csak a legvégső esetben!

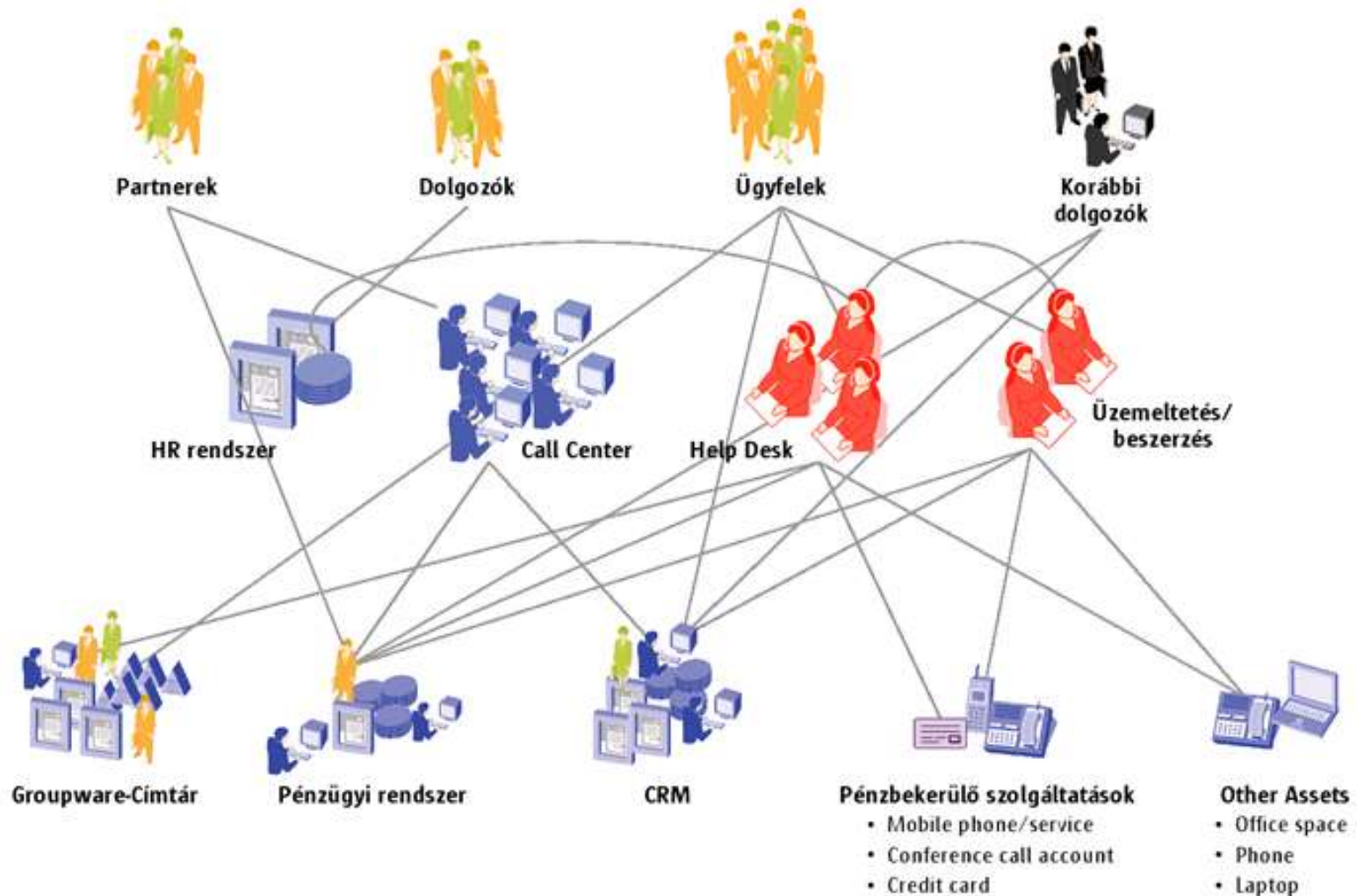
### *Az IDM rendszer:*

- ≠ Sharepoint, Intranet: nehézkes a testreszabása
- Iparági szokványokat támogat

# IDM nélkül

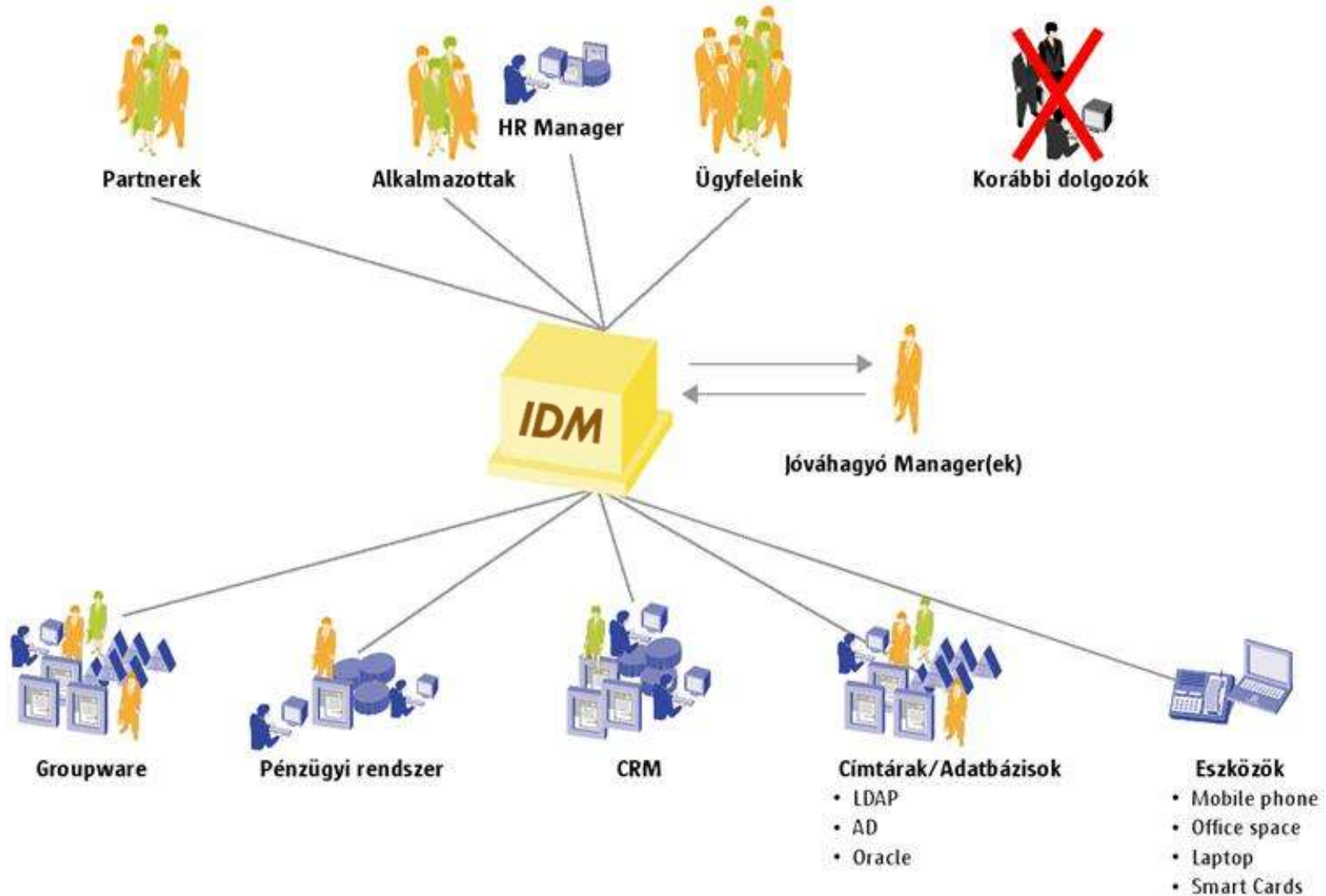
•4

## Anarchia



- IT rendszerek külön fejlődtek
  - így hézagok vagy átfedések keletkeztek.
- Ahány rendszer, annyi felhasználó-felviteli felület
  - (pl.: VPN-kapcsolat, chip-kártya, rendszerjogok), de ezek felhasználó-kezelése rendszerenként független
- A szerepkörök „maguktól” alakultak ki
- Felhasználó-kezelés ad-hoc
  - A szervezeti életút NEM reprodukálható.
- Az egységesítésre tett törekvések (pl. központi LDAP) tovább bonyolították az infrastruktúrát.

## Anarchia helyett



## ·7 Az idő függvényében

40%

- Felmérés

20%

- Role management,
- Role mining

10%

- Workflow implementálás
- Felület testreszabás

20%

- Betöltés, éles üzembe állítás

10%

- Projektzáró tevékenységek



# 1. Lépés

## Felmérés

- ▣ Interjúk a forrásgazdákkal
- ▣ Folyamatok felmérése
  - Rendszerezettek-e
  - Működnek-e
  - Dokumentáltak-e

---

***Eredménytermék:***

Megvalósítási rendszerdokumentáció



## 2. Lépés

•9

### Role Management = szerepkörök kezelése

- ▣ **Általános Role Management:** a szerepkörök kezelésével, élelciklusával foglalkozik
- ▣ **Role Mining:** szerepkör-bányászat, ami a role management része lehet.

#### Céljai:

- Szerepkörök összevonhatóságának vizsgálata
- Szerepkör-anomáliák kutatása
- Szerepkör-anomáliákra intézkedési terv kidolgozása

# 3. lépés

•25

## Workflow implementálás, felület-testreszabás

- A felmért workflow-k rendszerbe építése
- A workflow-k implementálásának főbb szempontjai:
  - Eszkalációs pontok
  - Jogok delegálása (helyettesítés esetére)
  - Jóváhagyások
  - Jogok időbeli lejáratának kezelése (előtte figyelmeztetés, meghosszabbítási lehetőség, eszkaláció stb.)
- A felületen a használt funkciók megjelenítése, fejlesztések

# 4. lépés

## Betöltés - Az igazság pillanata...

### Fejlesztői rendszer

- Csak a HumanolT fejlesztői dolgoznak benne
- A munkáról dokumentáció készül, mely a tesztelést segíti

### Tesztrendszer

- Az ügyfél szakemberei dolgoznak benne, a HumanolT szakértői támogatásával
- A fejlesztői dokumentációk szükség esetén módosíthatók

### Éles rendszer

- A dokumentációk alapján az ügyfél szakemberei állítják be.
- A dokumentációk módosítása csak Change Management folyamaton keresztül

# 5. lépés

## Projektzárás

- Dokumentáció véglegesítés
  - Oktatás
  - Online dokumentációk készítése:  
az oktatás ezzel még gyorsabban megvalósítható
- 



- Üzemeltetés támogatás
- Road-map

- **A rendszert folyamatosan karban kell tartani:**
  - Új felhasználókat könnyen kezelhetjük
  - Átszervezéssel, bővüléssel új szerepkörök keletkeznek: folyamatos role
  - Új rendszerek bevezetése után azok is forrásul szolgálhatnak, szerepkörök jogosultságait bővíthetik
  - Törvényi változásokkal módosulhatnak a workflow-k, szerepkörök (pl. jóváhagyás esetén)

- **Jelszó management** - A helpdesk idejének 30-70%-a telik jelszavak visszaállításával\* – Beállítási lehetőségek: biztonsági kérdések száma, elfogadás módja
- **Self-servicing** – a felhasználók saját maguknak, beosztottaiknak igényelhetnek, vonhatnak vissza jogokat
- **Workflow** - jogosultság létrehozására, engedélyezésére, terítésére, jóváhagyásra, visszavonásra, eskalációra)
- **Provisioning** – online változás-terjesztés, meghatározható terjesztési iránnyal

- **Teljes körű megfelelés**
  - Központosított szabályozási és ellenőrzési funkciók (egyszerű auditálhatóság pl.: PSZÁF)
- **Nagyobb biztonság**
  - Strukturált erőforrás menedzsment
- **Javuló szolgáltatás minőség (Komfortosabb felhasználói rendszerek)**
  - Mérőpontok, átláthatóság
  - Önkiszolgáló funkciók (gyorsabb, biztonságosabb)
  - Átruházási funkciók
- **Üzlet és IT hatékony együttműködése**
  - Üzleti folyamatok és rendszerek integrációja
  - Címtár-szinkronizáció



### ▣ **Segít a bevezetéskor:**

- A forrásokhoz tartozó konnektorok megléte
- Jól kidolgozott folyamatok
- Jól dokumentált folyamatok

### ▣ **Az IDM rendszer lehetőségei:** Egyes IDM gyártók licenz-skálájában szerepelnek 10 milliós felhasználói körre ajánlott licenzcsomagok

# Köszönjük a figyelmet!



Humanoit Kft.

## ▣ **Hollósi Gábor**

- Rendszermérnök, szakértő
- gabor.hollosi@humanoit.hu

## ▣ **Fazekas Éva**

- Account manager
- eva.fazekas@humanoit.hu