Hálózati azonosság kezelése, biztonsági és alkalmazás fejlesztési aspektusai

A Sun Microsystems a digitális azonosítás problémakörének megoldására igen régóta kínál különféle tecnológiai komponenseket, sok esetben az adott terület szabványainak kialakításában is jelentős szerepe volt (és van a mai napig) a cégnek. Felismertük, hogy napjaink vállalatainak, szervezeteinek egyik legfontosabb problémája éppen a digitális azonosítók kezelésének módja a különböző rendszerek között, ezen azonosítók kezelése azok teljes életciklusa alatt illetve az informatikai folyamatok harmonizálása a vállalati, szolgáltatás folyamatokhoz. Természeseten az adatok mit sem érnek önmagukban, így biztosítani kell az adathoz történő hozzáférést illetve azt, hogy ezen adatok felhasználásával nyújtsunk szolgáltatásokat az egyéb rendszerek irányába (authentikáció, authorizáció, SSO, identity federáció stb.).

A Sun Microsystems által kialakított identity menedzsment koncepció szerint a megoldásnak alapvetően három területet kell lefednie. A három terület:

- Felhasználói adatok biztonságos tárolása
- Felhasználói adatok létrehozása, karbantartása, szinkronizálása a különböző rendszerek (adatbázisok) irányába és azok között
- Különböző informatikai rendszerekben történő authentikáció, authorizáció, rendszerek közötti egyszeres belépés (SSO) megvalósítása

A fentiekben vázolt mindhárom terület valamilyen mértékben jelen van szinte minden vállalat szervezet esetében, azonban sok esetben bizonyos területekre már született megoldás, melyekkel a különböző szervezetekben az identity management területén felmerülő tipikus problémákat lehet kezelni. A legfontosabb problémák a következők (a teljesség igénye nélkül):

- Különböző informatikai rendszerekben létrehozott felhasználók azonosítói nincsenek szinkronizálva egymással
- A különböző informatikai rendszerekben a felhasználókat nem egységesen kezelik, a felhasználók digitális azonosságának életciklus kezelése alapvetően manuális tevékenység
- Hiányzik az identity provisioning-et (digitális azonosító létrehozását és karbantartását) a szervezet működésére leképező folyamatmodell (workflow)
- A rendszerek közötti egyszeres belépés (SSO) nem működik
- A különböző rendszerekben tárolt felhasználói adatok kezelési módja, az adatokhoz való hozzáférés nem minden esetben szabályozott, előfordulat, hogy az adatkezelés nem felel meg törvényi, jogszabályi előírásoknak.
- A felhasználók informatikai “önkiszolgálása”, self adminisztációja nem megoldott
- A különböző informatikai rendszerek adminisztrációjának szabályozott delegálása nem biztosított
- A digitális azonosítókban (digitálisan tárolt felhasználói adatokban) történt változtatások nyomonkövetése nem megoldott
- A digitálisan tárolt felhasználói adatok megfelelése (megfeleltetése) a szervezeti szabályozáshoz nem minden esetben biztosított, alapvetően manuális folyamat.
- A rendszer bővítését (új felhasználói csoportok felé történő megnyitását) illetve új alkalmazások bevezetését, integrálását megnehezíti a jelenlegi azonosítás kezelés.

- Az informatikai munkatársak idejük jelentős részét olyan (támogatási) tevékenységgel töltik, amelyekre automatizált megoldások léteznének

A probléma kör kezelése kiterjedt biztonsági és fejlesztési elvek szerinti rendzser, alkalmazás építését követeli meg. Egyetlen rendszer sem követelhet meg egyedi felhasználói menedzsement kialakítását, hanem egyszerűen integrálhatónak kell lennie a komplex környezetben kialakított azonosság kezelő rendszerhez