Föderáció

Az **Identitás Föderáció** olyan intézmények halmaza, amelyek között lehetséges az identitás-információk átadása. Az intézmények - szabályozott keretek között - *megbíznak* a másik intézmény által kiállított identitás-információkban.

A Föderáció a pont-pont bizalmi kapcsolati modell általánosítása. Ekkor nem szükséges egy intézménynek minden egyes társintézménnyel külön megállapodást kötnie, hanem a szövetséghez csatlakozással automatikusan létrejön közöttük a lehetőség az identitás-információk átadására. Általában lehetőség van arra, hogy egy intézmény több Föderációhoz is kapcsolódjon, ill. külön bilaterális megállapodásai legyenek.

Célja

A föderációk célja, hogy az identitás információk egyébként autonóm rendszerek között átjárhatók legyenek. Ez a következő előnyökkel járhat:

- **redundáns felhasználó-adminisztráció elkerülése**: az identitáshoz kapcsolódó adatoknak elegendő egy helyen rendelkezésre állni; nem kell "idegen", "külsős" felhasználókat felvenni az intézményi adatbázisba
- **Single Sign-on**: a felhasználónak elég egyszer megadni az azonosító adatait, a többi rendszer automatikusan megszerzi az identitáshoz kötődő információkat. Ez egyrészt kényelmesebb a felhasználónak, másrészt megkönnyíti a több faktoros (pl. smartcard) azonosítási módszerek bevezetését.

Szerepek

A legtöbb föderációs modell lehetővé teszi azt, hogy egy intézmény egyszerre több szereppel is részt vegyen egy föderációban.

Identitás szolgáltatók (Identity Provider, IdP)

A felhasználók adatait az identitás szolgáltató tárolja. Az identitás szolgáltató funkciói: **Azonosítás**

- Felhasználó azonosítása
- Felhasználó azonosítással kapcsolatos információk átadása a tartalomszolgálatóknak (SP)
- Tartalomszolgáltatóktól érkező azonosítási kérések (AuthRequest) feldolgozása

Attribútumok kiadása

- Felhasználóhoz köthető attribútumok meghatározása
- A tartalomszolgáltató számára hozzáférhető felhasználói adatok átadása a tartalomszolgáltatónak (közvetlenül ill. a felhasználón keresztül)

Felhasználó menedzsment

- Felvétel / törlés
- Attribútumok, role-ok kezelése
- Jelszó ill. adatmódosítás

Tartalom / erőforrás szolgáltatók (Service Provider, SP)

A tartalomszolgáltatók védett tartalmakat szolgáltatnak a felhasználók számára. Általában nincsenek közvetlenül a felhasználókhoz kapcsolatos adataik, ezért nem szükséges a felhasználókat adminisztrálniuk sem.

A tartalomszolgáltató funkciói (a funkciók föderációs modelltől függően ezektől eltérhetnek):

- azonosított kapcsolat létrehozása az identitás szolgáltató segítségével (általában HTTP átirányítás használatával)
- az identitás szolgáltatótól kapott adatok értelmezése
- az identitás szolgáltatótól kapott adatok alapján meghatározni, hogy a felhasználó jogosult-e a művelet végrehajtására (**autorizáció**)

Metadata adminisztráció

A szolgálatókhoz kötődő háttérinformációkat (pl. tanúsítvány, név, scope, stb.) sok esetben a föderációs szoftver számára is elérhetővé kell tenni, ez esetben Metadata használatáról beszélünk. Adminisztrációja általában központilag történik, és *push* vagy *pull* módszerrel jut el a föderációba bevont számítógépekhez.

Speciális szolgáltatás a "Where Are You From?" (WAYF) szolgáltatás, amely a felhasználó számára lehetőséget ad, hogy az identitás szolgáltatóját kiválassza. Ez a szolgáltatás a föderációs metadata állomány(ok)ra épül.

Föderációs alapelvek

1. A föderáció célja, hogy a felhasználók úgy vehessenek igénybe szolgáltatásokat - amennyiben erre jogosultak -, hogy a saját intézményük azonosítja őket.
2. Az IdP és az SP egyértelműen azonosítja magát, amikor üzenetet váltanak egymással.
3. Az IdP csak valós személyeket azonosít (teszt felhasználókat csak meghatározott módon, korlátozásokkal szabad azonosítani)
4. Az IdP csak abban az esetben azonosít egy felhasználót, ha az illető valamilyen - ismert - viszonyban van (volt) az intézménnyel.
5. Az IdP és az SP nem ad meg magáról hamis, félrevezető információt.
6. Az IdP minden tőle telhetőt megtesz annak érdekében, hogy a kiadott információ a lehető legpontosabb legyen. Az SP tisztában van vele, hogy bizonyos információkat a felhasználók maguk is szerkeszthetnek.
7. Az IdP gondoskodik róla, hogy a felhasználót azonosító információk (pl. jelszó) védett módon legyenek tárolva, ill. a felhasználók ezt biztonságosan adhassák meg.
8. Az SP csak a működéséhez minimálisan szükséges adatmennyiséget igényli a felhasználóról.
9. Az SP nem kérheti a felhasználót, hogy adja meg az IdP-nél érvényes jelszavát. Jelszó az SP-nek nem adható ki (kivéve speciális esetben egyszer használatos vagy rövid lejáratú jelszavak).
10. Az SP az IdP-től származott információt harmadik félnek nem adja tovább.
11. Felhasználói visszaélések esetén az IdP és az SP együttműködik egymással.
12. Az IdP és az SP az informatikai rendszereit az elvárható gondossággal üzemelteti.

Technológiák

- Föderációs modellek

Szabályozás

A lazán csatolt modellek (pl. az OpenID) nem igényelnek központi szabályozást, de a magasabb biztonság-igényű, nagy bizalmat igénylő modellek esetén szükséges az, hogy a föderációban résztvevő intézmények kidolgozzák (esetleg szerződésbe is foglalják) az együttműködés feltételeit.

A megállapodás pl. az alábbi területeket érintheti

- Felhasználó-kezelés (pl. lejárt azonosítók inaktívvá tétele, password policy)
- Felhasználói adatok védelme (privacy követelmények)
- Felhasználó-azonosítási technológiák, ezek elnevezése
- Scope-ok kiosztása

- Felhasználói attribútumok használatának a feltételei (pl. milyen feltételekkel mondhatja egy intézmény XY-ról, hogy ő egy *oktató*?)
- Metadata információk karbantartása
- Új intézmény csatlakozásának feltételei (IdP, ill. SP szerepben)
- Audit, nemmegfelelőségi szankciók
- Költségviselés szabályai
- stb.

Változat #3
cziernorbert hozta létre 9 április 2025 16:36:56
cziernorbert frissítette 10 április 2025 09:54:52