

1. Jogosultsági viszonyok mind az elektronikus rendszer mind hatósági jogviszony tekintetében	2
1.1. Szerepkör és jogosultság tervezés.....	3
1.2. Munkafolyamat modell forgatókönyv felfogásban	4
1.3. Szerepkör tervezés, szervezés	6
1.4. A hozzáférési és kezelési jogosultsági modell tovább finomítása	7

1. JOGOSULTSÁGI VISZONYOK MIND AZ ELEKTRONIKUS RENDSZER MIND HATÓSÁGI JOGVISZONY TEKINTETÉBEN

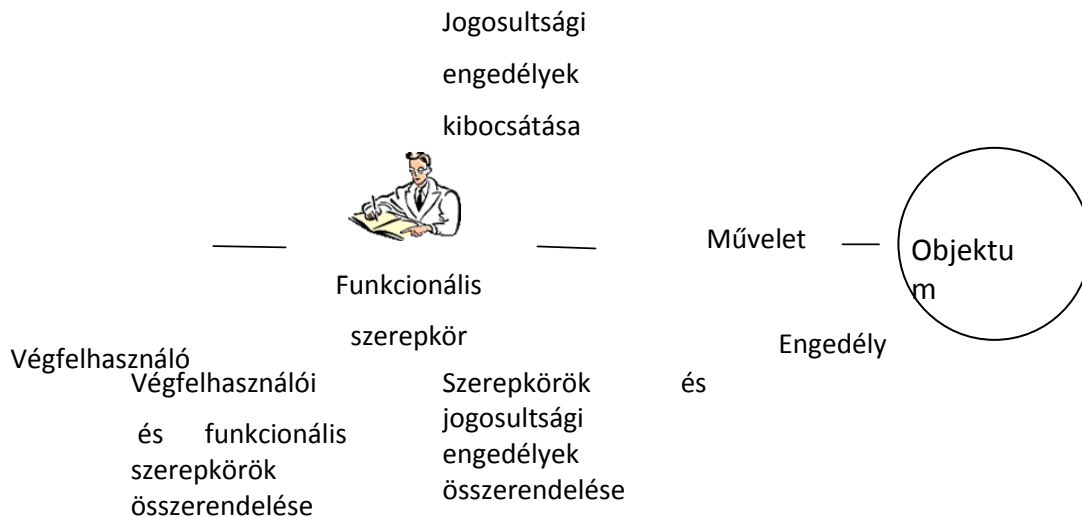
Az ügyintézési rendelkezések megadásánál – mit egy különösen jó reprezentatív elektronikus ügyintézési esetről – a jogosultságok két dimenziója illetve három dimenziója is megjelenik.

A rendszer alapvető szereplői az ügyfél (természetes személy) és hatósági ügyintéző. Megjelenik még egy kibertérben létező szervezet elektronikus megszemélyesítése, mint potenciális szereplő.

Az egyik jogosultsági dimenzió az elektronikus/informatikai hozzáférési jogosultság. A másik az ügyintézési rendelkezés viszonylatában az eljárási cselekménnyel kapcsolatos rendelkezési jog, felhatalmazott, meghatalmazott, saját jogon, önállóan jár el stb.

A rendszerrel érintkezésbe lépő szereplők (ügyfél, meghatalmazott, megbízott, ügyintéző stb.) a kibertérbe átlépve, vagy feladatainak, jogosultságainak leképezése a kibertérben használható fogalmakra a hozzáférési és adatkezelési jogosultsági rendszeren keresztül ragadható meg. E hozzáférési jogosultsági rendszer a kibertér alapfogalmaival dolgozik: adat, e-dokumentum vagy objektum, amelyeken műveletek bizonyos elektronikus adatfeldolgozó tevékenységek elindítása révén hajthatók végre. A hozzáférési jogosultságok leírása alapvetően két bevált módszer áll rendelkezésre a szerepkör alapú és az attribútum (sajátosság, tulajdonság) alapú jogosultsági rendszer. E két rendszer kombinálható is.

A teljes rendszerelemzés és rendszerszervezés feladata a ténylegesen követendő módszer kiválasztása és a jogosultsági rendszer kialakításához szükséges szervezési és tervezési munka elvégzése.



1. ábra A jogosultságok megadásának alapsémája egy elektronikus információrendszer környezetben

1.1. Szerepkör és jogosultság tervezés

Két magas szintű szerepkör modell jelenik meg egy e-kormányzati információrendszerben: funkcionális és strukturális.

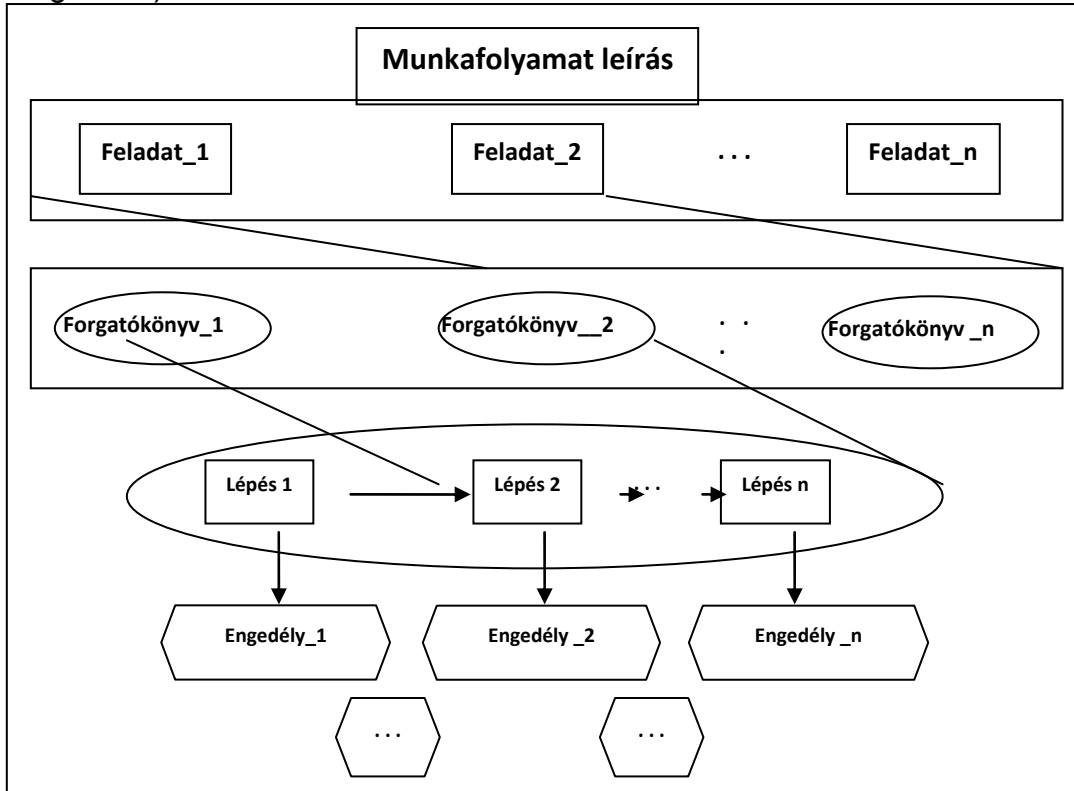
Funkcionális szerepkör azoknak az engedélyeknek a halmazából áll, amelyek egy feladat lefolytatáshoz szükségesek. A funkcionális szerepkör nevek egy-egy jogosultsági engedély csoporthoz kapcsolhatók azért, hogy a végfelhasználók felé történő engedély kiadást leegyszerűsítsék. A jogosultsági engedélyek végső soron ahhoz szükségesek, hogy az adatok, e-dokumentumok (félig-strukturált, strukturálatlan), és funkcionális, információrendszer, Web szolgáltatások tekintetében meghatározza azokat a műveleteket, amelyeket a jogosultsági engedély birtokosa elvégezhet. Ez általában a klasszikus CRUD (LOAT) mátrixban történő e-dokumentum, adatszerkezeti elem (entitás, adattábla stb.) szintű műveleti jogosultság megadását jelenti, a szoftverben megjelenő információrendszer szolgáltatások, funkciók tekintetében pedig a végrehajtási („futtatási”) jogosultságokat. A funkcionális szerepköröket meg lehet adni egy azonosító tanúsítvány végfelhasználói attribútum tanúsítvány formájában, vagy egy jogosultságok és engedélyeik tárolására szolgáló elosztott címtárban lehet megadni (pl. LDAP stb.).

Strukturális szerepkör a szervezet szereplőit a szervezeti hierarchiában helyezi el, annak megfelelően, hogy milyen alkalmazotti kategóriákhoz tartoznak, amelyek egymástól eltérő hozzáférési jogosultsági szinteket jelentenek. A strukturális szerepkör azt jelenti, hogy lehetővé teszi a szerepkörhöz tartozó végfelhasználók számára, hogy részt vegyenek a szervezet munkafolyamatában (elvégezzenek feladatokat), a munkaköri leírásuk, beosztásuk, rangjuk, címük szerint, de nem specifikálja részleteiben a hozzáférési jogosultságokat egyes információ objektumokra vonatkozóan. A strukturális szerepkör lehetővé teszi azt, hogy egy végfelhasználó kapcsolatba léphessen egy információ forrással, de nem adja meg a jogosultsági engedélyeket. Strukturális szerepkörre példa lehet: Főosztályvezető, osztályvezető, ügykezelő stb.

Strukturális szerepkörök azt határozzák meg, hogy mely munkafolyamatban vehet részt az adott végfelhasználó, míg a funkcionális szerepkör definiálja azokat hozzáférési jogosultsági engedélyeket, amelyek lehetővé teszik a különböző bizalmassági fokozatú információk, e-dokumentumok elérését.

1.2. Munkafolyamat modell forgatókönyv felfogásban

A forgatókönyv modell (ld. 2. ábra) a munkaköri leírások, munkafeladatok, forgatókönyvek és azok lépéseit illusztrálja. A jogosultsági engedélyeket az egyes forgatókönyv lépésekhez köti (ennek mikéntjét a szerepkör szervezésé keretében kell megoldani).



2. ábra A jogosultsági engedélyek és forgatókönyvek lépéseinek összekapcsolása munkafolyamat munkafadatain belül

A forgatókönyv alapú szerepkör kialakítás, szervezési eljárás esetében mindegyik tevékenységet és eseményt egy forgatókönyv keretében ábrázolunk. A forgatókönyv lépése mindig egy specifikus hozzáférési művelethez kapcsolódik. Azokat a forgatókönyveket – amelyeket egy előírt sorrendben kell végrehajtani, azért hogy egy adott munkafeladat célját elérjük – a jogosultsági engedélyek kialakításához mint információ források használhatók fel. Egy végfelhasználónak, aki egy bizonyos forgatókönyv szerint folytatja le a tevékenységeket, az összes olyan hozzáférési jogosultsággal rendelkeznie kell, amelyre a forgatókönyv egyes lépéseinek befejezéséhez szüksége van.

Jogosultsági engedély az információ architektúra megfelelő finomságú bontásához illeszkedő szintekhez kapcsolódó „információ építő elemek”-re kell definiálni. Ennek a felbontásnak a finomsága nem lehet sem túl részletes, sem túl nagyvonalú, az információ architektúra hierarchiájában sem túl magas sem túl alacsony. Az 1 a lehetséges hierarchia szinteket mutatja. Kiemeli az aggregált dokumentum szintet, amely interoperabilitás szempontjából a legalacsonyabb hierarchia szintet kívánja jelölni. Az aggregált dokumentum szint egy olyan fogalmi szintű elektronikus információrendszer objektumot vagy funkciót jelöl (pl. Ügyintézési rendelkezési dosszié) amelynek részlet komponenseire már nem utalunk.

1. Táblázat

1.2.1.1. Jogosultsági engedélyek

Tevékenység	Szerepkörök, jogosultságok megtervezés, megszervezése	Szerepkör
Részt vesz	Munkaköri leírás	Strukturális szerepkör
Részt vesz	Ügyfél leírás	
Végrehajt	Feladat	
Végrehajt	Forgatókönyv	
Lefolytat	Lépés	
Létrehoz, Olvas, Aktualizál, Töröl	Aggregált dokumentum szint	Funkcionális szerepkör
Végrehajt	Funkció	Funkcionális szerepkör
Létrehoz, Olvas, Aktualizál, Töröl	Adat entitás, objektum, tábla, dokumentum	
Létrehoz, Olvas, Aktualizál, Töröl	Adatelem	

A rendszer tulajdonosainak, felügyelőinek, adminisztrátorainak, szervezeti architektúra tervezőinek és rendszer gyártóknak, szállítóknak lehetősége van az információ objektumok pontosabb, konkrétabb megragadására, és a saját környezetükben használt információ objektumokra történő leképezésére.

1.3. Szerepkör tervezés, szervezés

A szerepkör tervezés, szervezés alapvető célja az, hogy szabványosított és újra hasznosítható jogosultsági engedélyeket alakítson ki.

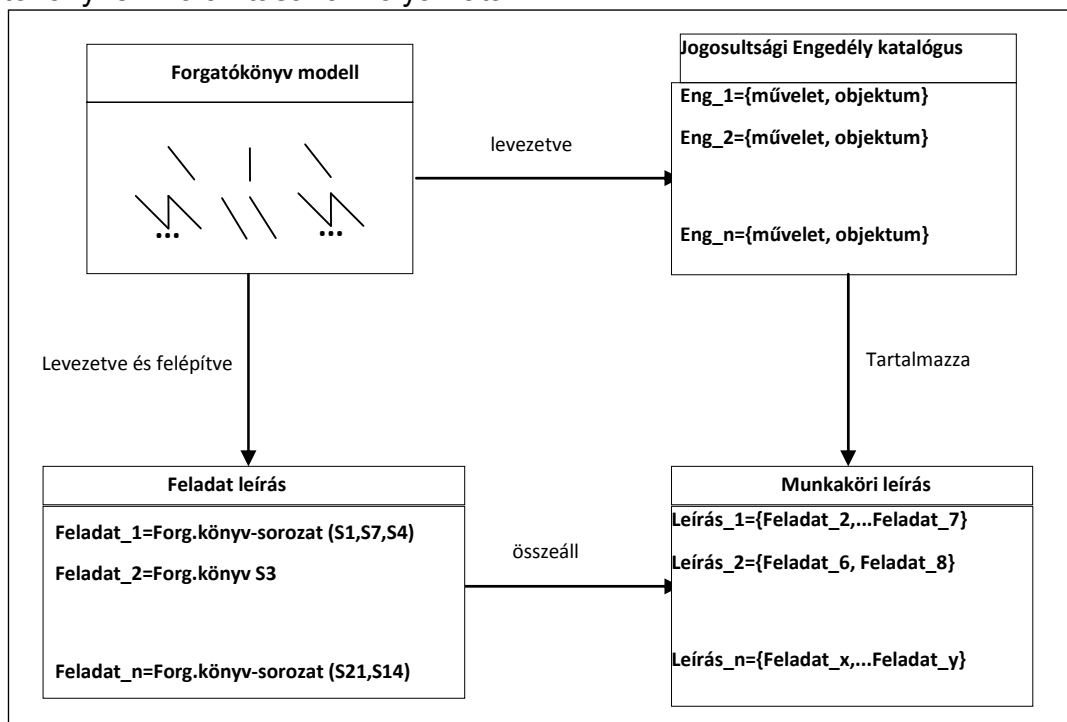
1.3.1. Alapfeltevések

Ahhoz, hogy a részletes jogosultsági engedély rendszer kialakítható legyen a következő előfeltételeknek kell fennállnia:

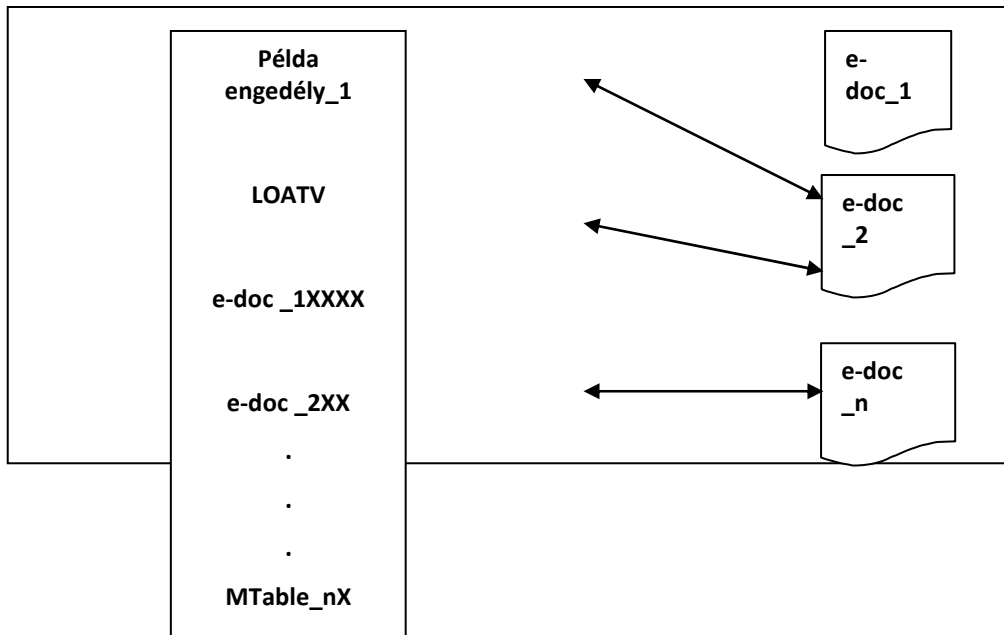
- Feladat egy szervezet munkaköri feladatát tükrözi vissza és felhasználható arra, hogy a jogosultsági engedélyek levezethetők legyenek belőle.
- A strukturális szerepek meghatározzák, hogy a végfelhasználók milyen jogosultságokkal vesznek részt egy munkafolyamatban és hogyan kapcsolódhatnak egyes védett, bizalmas információforrásokhoz.
- Az engedélyek meghatározzák, hogy mely műveletek vannak engedélyezve egyes védett információforrások esetében.
- Az engedélyeket a funkcionális szerepkörökhöz kapcsolják hozzá.
- A szabványosított funkcionális szerepkörök a csoportosított és szabványosított engedélyekből állnak össze, amelyeket úgy definiálnak, hogy támogassák a szervezeten belüli információ áramlást.

1.3.2. Modellek közötti kapcsolat

A használat kialakítása érdekében először a forgatókönyv modellt kell kifejleszteni. Az 3. ábra mutatja azt, hogy hogyan kapcsolódik össze a szerepkör tervezés és forgatókönyvek kialakításának folyamatai.



3. ábra A forgatókönyv és az engedély modell közti kapcsolatok



4. ábra Példa engedély katalógusra

1.4. A hozzáférési és kezelési jogosultsági modell tovább finomítása

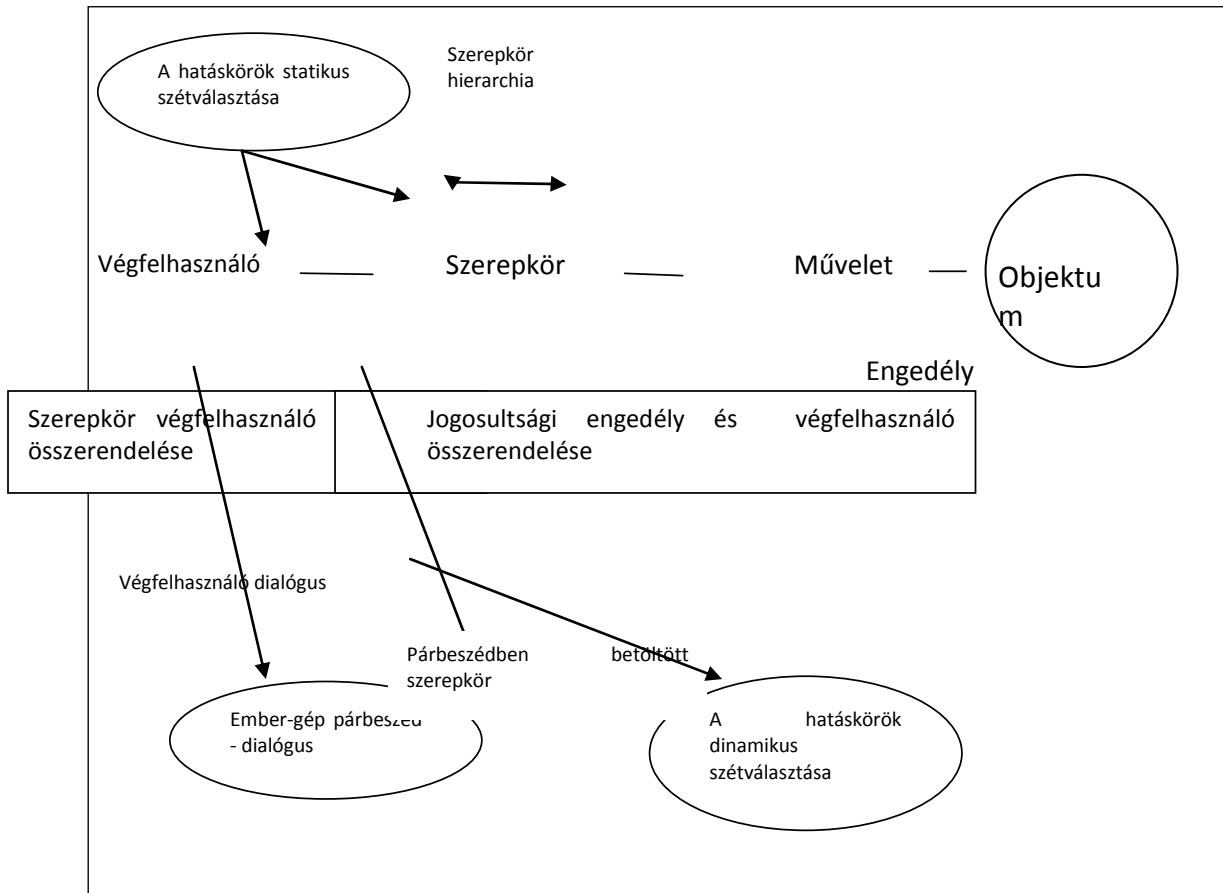
A szerepkör hierarchia egy öröklődési relációt definiál azért, hogy a rendszeradminisztrációs terheket csökkentse. Két fajta szerepkör hierarchia definiálható, egy általános szerepkör hierarchia és egy korlátozott szerepkör hierarchia. Az öröklődési hierarchia azt jelenti, hogy az engedélyek örökölhettek. Ez egy parciális rendezéshez vezet az engedélyek között.

A korlátozott szerepkör hierarchia esetében az engedélyek parciális rendezése azt jelenti, hogy egy gráf elméleti erővel állunk szemben, amelyet invertált fák halmaza alkot. Ez lehetővé teszi az erőforrások megosztásának leírásához szükséges engedélyezési rendszert.

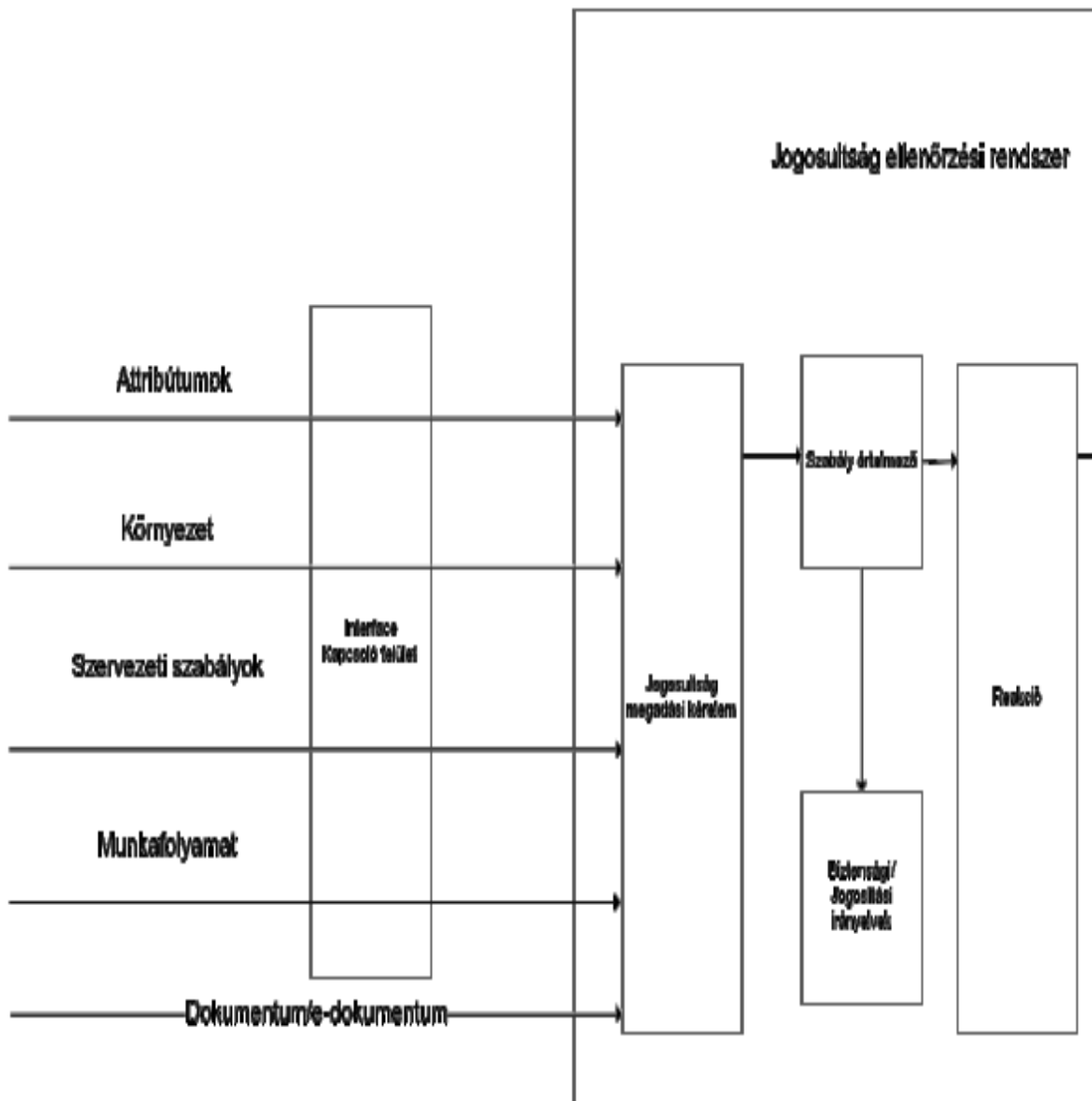
Attribútum alapú hozzáférési jogosultság megadására is lehetőség van. Ez sokkal rugalmasabb, az igényekhez könnyebben illeszthető megoldás, de számítási komplexitása lényegesen nagyobb, a szóba jöhető attribútumok kettő hatványával arányos.

A szerepkör és attribútum alapú megközelítés kombinálható.

A tényleges engedélyek kiadása a „legalacsonyabb privilégium” elve alapján történik meg.

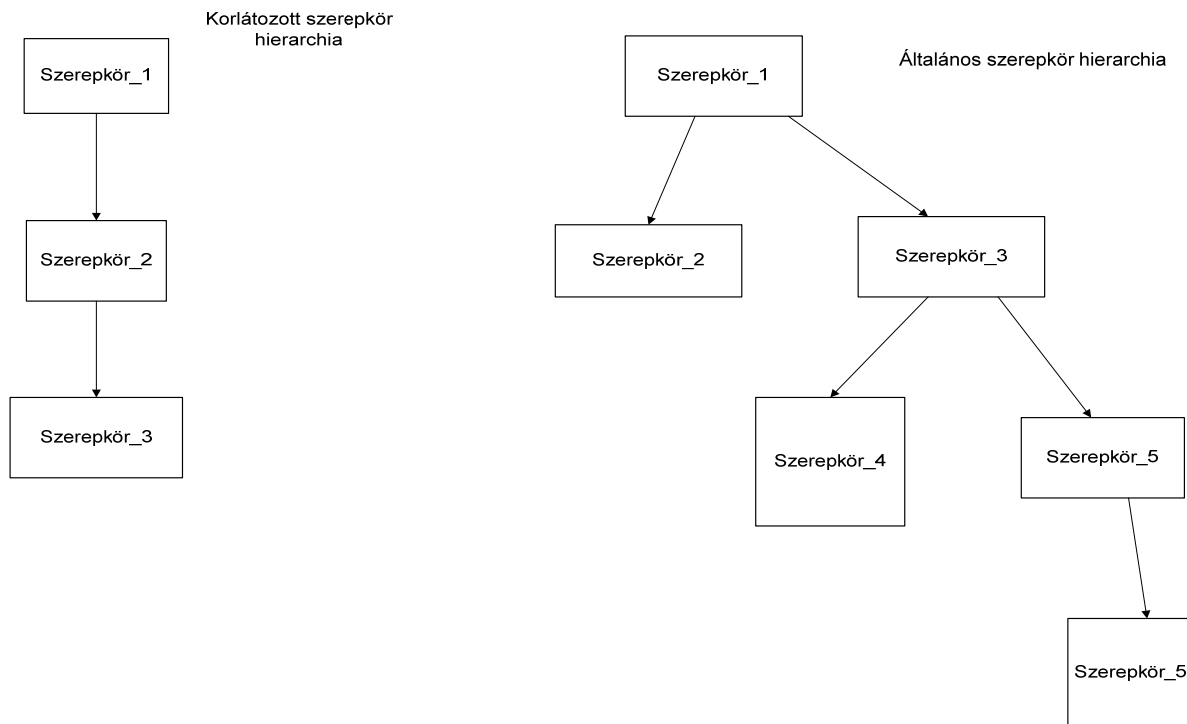


5. ábra Az ember-gép párbeszéd dinamikusan változó jellegének figyelembe vétele egy elektronikus információrendszer környezetben



6. ábra Hozzáférési jogosultság ellenőrzési rendszer

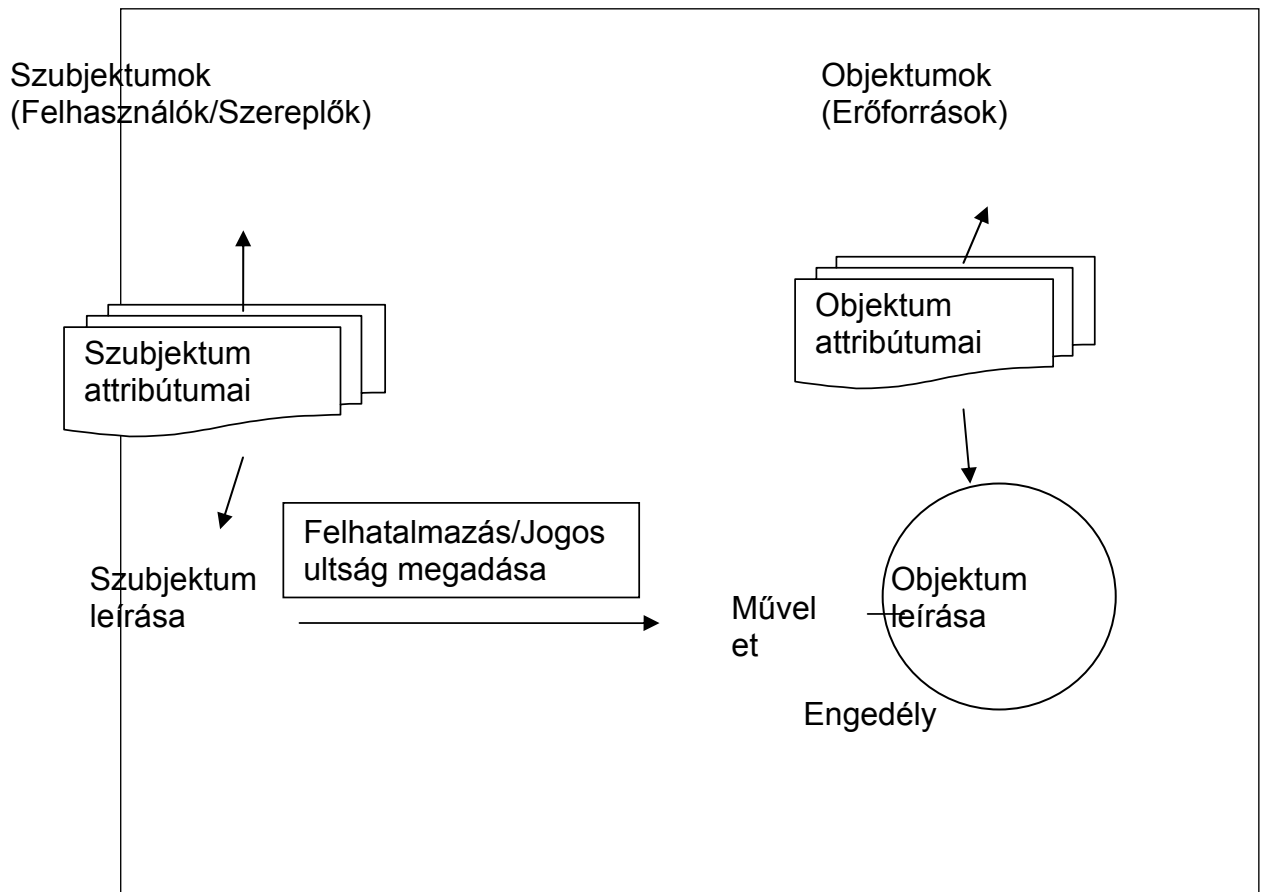
1. Környezet- a környezeti tényezőktől függő állapot,
 - a. idő korlátok használatra megengedett időablak;
 - b. biztonsági szint: kibertér védelmi riasztási szint.
2. Dokumentum –
 - a. A konkrét dialógusban dinamikusan megjelenő adattartalom
 - b. Kérdőívre adott válaszok
3. Szervezeti szabályok –testre szabható szervezeti előírások
4. Munkafolyamat előrehaladásának fázisai, munkafeladatai



7. ábra Szerepkör hierarchiák- Általános és korlátozott

Az attribútum alapú hozzáférési jogosultságnak az alapelve az, hogy a felhasználó/szobjektum és az objektum/erőforrás között nem definiál közvetlen kapcsolatot, hanem az aktuális attribútum értékeket használja fel a jogosultság meghatározására. A felhasználók/szobjektumok attribútumai lehetnek statikus jellegűek, pl. munkakör, beosztás a szervezetben. De lehetnek dinamikus jellegű attribútumok is pl. az alany kora, pillanatnyi földrajzi vagy kibertéri helyzete, vagy éppen megszerzett jogosultsága.

Az objektumok attribútumai a meta-adatok lehetnek, pl. egy dokumentum tárgy,cím attribútuma. Mind a szobjektumok mind az objektumok az attribútumok egy halmazával jellemezhetők. Az engedélyek az objektum leíró adatokból, amelyek az attribútumok és feltételek egy halmazával írhatók le – pl olyan feltételekből állnak össze mint „kora > 18” vagy „Meghatalmazott=IGEN” –, az adott objektumon megengedett műveletekkel. A jogosultságot a szobjektum leírója és az objektumra vonatkozó engedélyek együtt alkotják. E jogosultsági feltételek kiegészíthetők további feltételekkel, pl. a szobjektum attribútumai és az objektum attribútumainak összehasonlítása révén (feltételek előírása nélkül, csak konstans értékekkel történhet meg összehasonlítás).



8. ábra Attribútum alapú jogosultság kezelés