2. sz. melléklet

Műszaki leírás (igények, követelmények) –

Új felhasználó- és jogosultságkezelő (IDM) rendszer bevezetése

Tartalomjegyzék

I. Előzmények

Az Országgyűlés Hivatala által jelenleg jogosultságkezelésre használt NetIQ Access Governance Suite (AGS) szoftver terméket a Microfocus – stratégiai döntés eredményeképpen – kivezette a termékportfóliójából a korábbi években, így a termék támogatása is megszűnt 2019-ben.

A legköltséghatékonyabb megoldás mindenképpen az, ha a régi Dirxml/IDM rendszerből megmaradt funkciókat fel tudjuk használni, valamint figyelembe vesszük az AGS rendszerünk jelenlegi működését és mindezekkel együtt alakíttatunk ki egy új, hosszútávon támogatott egységes jogosultságmenedzsment rendszert. Ennek a realizálására a legköltséghatékonyabb és egyben legjobb megoldásként az IDM termék jelenleg aktuális (4.8) verziójára esett a választásunk.

Áttekintve a jelenlegi működést mind üzleti, mind műszaki szinten, továbbá figyelembe véve az eddigi tapasztalatainkat és az elmúlt évek során megváltozott igényeket, az új IDM megoldást a következők szerint tervezzük kialakítani:

II. Infrastrukturális és környezeti követelmények

Feladat: egy teszt és egy éles környezet kerül kialakításra közel azonos paraméterekkel a hivatali környezetünkbe. Mindkét környezetbe egy-egy IDM szerver kerül, az éles környezetben további egy úgynevezett eDirectory replika szervert kell létrehozni. A leendő IDM rendszert a korábbi kedvező tapasztaltok alapján SUSE Linux Enterprise Serveren (SLES) kell működtetni. A szerverekre telepíteni kell az operációs rendszert és a szükséges IDM komponenseket. (Megjegyzés: Az IDM által használt, alább tárgyalt Oracle szerver mentésének, monitorozásának, magas rendelkezésre állásának biztosítása az OGYH feladata; az nem része sem a projektnek. Az IDM az Oracle adatbázist egy ponton éri el még akkor is, ha a mögött komplexebb infrastruktúra van.) Az IDM rendszer a naplóállományokat CEF formátumban továbbítja a Sentinel SIEM rendszerbe, ugyanakkor a naplóállományok elemzése, riportok készítése nem része a projektnek.

Az IDM az aktuális felhasználói és jogosultsági adatokat egy eDirectory címtárban tárolja a jelenlegi OGYH metacímtárhoz hasonlóan. Ez az IDM termék része és független az (OGYH-nál elsősorban file és nyomtatómegosztás kapcsán ismert) operatív címtártól, ami szintén eDirectory. A leendő IDM-nek ezen kívül tárolnia kell a munkafolyamatok adatait és az egyéb historikus adatokat, ami egy relációs adatbázisban történik. Az OGYH ehhez környezetenként egy-egy Oracle sémát biztosít a meglévő infrastruktúrájában (dedikált Oracle szerverre nincs szükség).

Az OGYH informatikai környezet jelentős részben a Micro Focus termékeire épül. Bár az OGYH használ MS Active Directory-t is, annak elsősorban a távoli hozzáférés szolgáltatás szempontjából van jelentősége. Ennek megfelelően a munkaállomások túlnyomó többsége nincs AD domain-be léptetve, így továbbra is szükséges az IDM-mel csatolt alkalmazások közötti jelszószinkron. Az IDM felületére történő belépés ennek megfelelően felhasználónévvel és jelszóval kell, hogy történjen. (Vagyis Kerberos authentikáció szükségessége nem merül fel az IDM esetében.)

A felhasználói felületnek magyar nyelvűnek kell lennie legalább azokon a részeken, amikkel az „átlag" felhasználó találkozik. Az alapértelmezett angol nyelv benne maradhat a termékben, de a testre szabott részeket elegendő magyar nyelven elkészíteni, ugyanakkor a rendszer alapbeállítása magyar nyelvű lesz, így a böngésző lokalizációs beállításaiból fakadó problémák elkerülhetők. A csak üzemeltetőknek szánt részeken maradhatnak nem lefordított szövegek, azonban ezek előfordulásának a számát minimalizálni kell.

Az OGYH hivatalos (házon belül támogatott) böngészője a Mozilla Firefox mindig a legfrissebb verziójú ESR kiadása, az új IDM rendszernek legalább ezen a böngészőn kell tudnia helyesen működnie.

A rendszert az OGYH saját szakemberei üzemeltetik az átadást követően saját virtualizációs környezetükben. A Novell PSH Kft. hiba esetén a garanciális időszakban ingyenesen, ezt követő időszakban és a garanciális hibákon túlmutató ügyekben a mindenkori támogatási szerződés szerint nyújt segítséget.

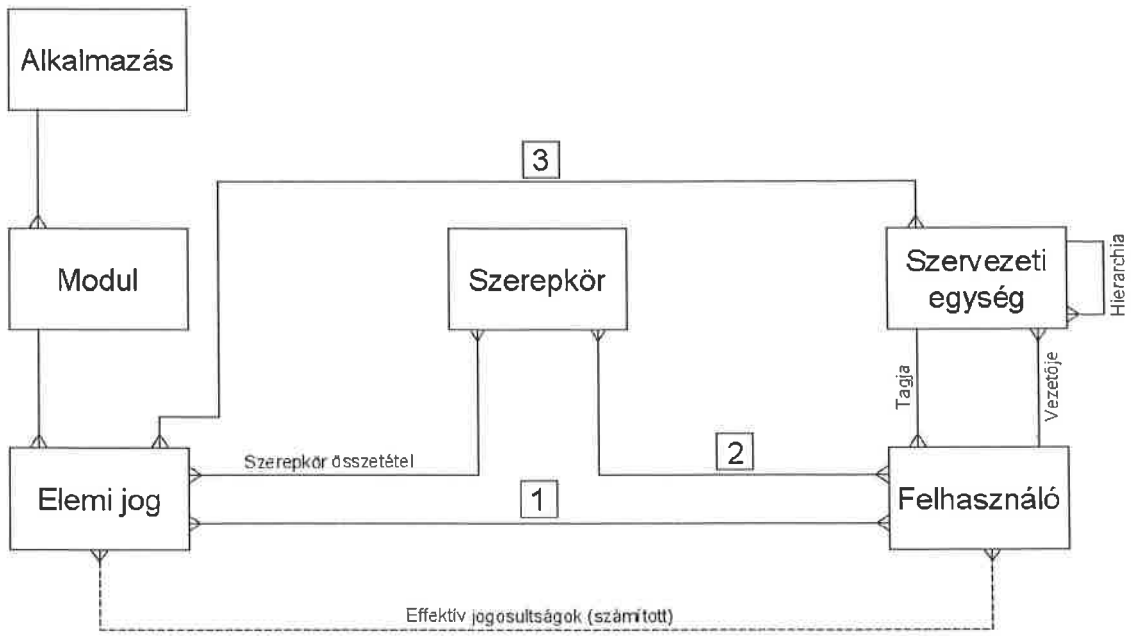
III. Adat- és jogosultságmodell

Az IDM megoldás úgy kerül kialakításra, hogy optimálisan ötvözze az automatikus és a kézi jogosultság kiadás lehetőségét. Ezt szem előtt tartva a következő módokon szerezhetnek informatikai jogosultságokat az egyes felhasználók az IDM által kezelt rendszerekhez:

- **(1) közvetlenül, munkafolyamat segítségével:** A kedvezményezett felhasználónak az igénylő közvetlenül válogatja össze a szerinte szükséges jogosultságokat, amiket egy alkalmazás–modul–jogosultság háromszintű hierarchiából választhat ki. A jóváhagyott jogosultságokat a felhasználó megkapja.
- **(2) szerepkörön keresztül, munkafolyamat segítségével:** A kedvezményezett felhasználónak az igénylő szerepköröket válogat össze egy előre definiált (és az illetékesek által karbantartott) listából. A jóváhagyott szerepkörök jogosultságait (a szerepkörök összetétele alapján) a felhasználó megkapja.
- **(3) szervezeti egységen keresztül, automatikusan:** Az illetékesek minden szervezeti egységhez karbantartanak egy jogosultság listát. A mindenkori HR adatok alapján minden felhasználó, aki ebben a szervezeti egységben van, megkapja azokat a jogosultságokat, amiket a szervezeti egységhez ily módon rendeltek, kivéve azokat, akiknél a Telefonkönyv felületen a nodef(ault) flag be van állítva. .

Megjegyzés: A munkafolyamatokkal kapcsolatos működésbeli követelményekről később esik szó, itt csak a jogosultságszerzés elvét tárgyaltuk.

Az egyes felhasználók mindenkori jogosultságait (effektív jogait) a fenti három lehetséges úton elérhető jogosultságok uniója adja. A megoldáshoz tervezett jogosultság modellt (egyszerűsítve) az alábbi ábra foglalja össze:



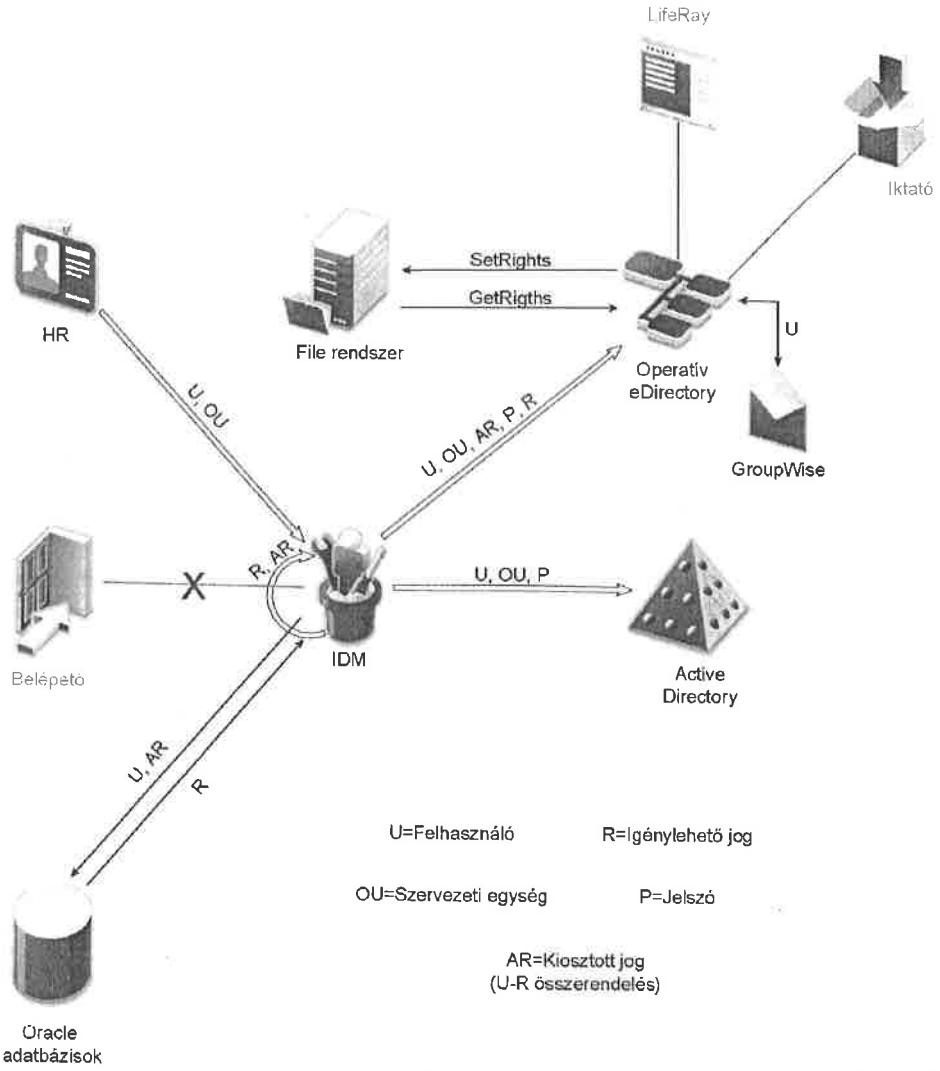
A lehetséges utakon bekövetkező összerendelés-változások hatására az IDM automatikusan újraszámolja az érintett felhasználók effektív jogait és az ebben bekövetkezett változást átvezeti a csatolt rendszerekbe, mely változásról e-mail értesítést küld.

IV. Alkalmazáscsatolók, integráció

Az IDM rendszer központi szerepet tölt be a felhasználók, jogosultságok és egyéb kiegészítő adatok kezelésében, szinkronizációjában. Ennek megfelelően egy csillag topológiájú elrendezés kerül kialakításra, aminek közén az IDM rendszer, oldalágain az egyes csatolt alkalmazások helyezkednek el.

Az alkalmazás csatolók tervezése során általános irányelv (néhány jelölt kivételtől eltekintve), hogy a **felhasználókat az IDM küldi** az alkalmazások felé, a lehetséges (igényelhető) **jogosultságokat az IDM fogadja** az alkalmazások felől, **a kiosztott jogosultságokat** (felhasználóhoz rendeléseket) pedig ismételten az **IDM küldi** az alkalmazások felé. Ezeken kívül még a felhasználók jelszavai és a szervezeti egységek adatai kerülnek szinkronizálásra bizonyos viszonylatokban, továbbá az alkalmazás csatolók bizonyos speciális alkalmazások esetében kiegészítő tevékenységet is végeznek.

A bekötött alkalmazásokat és a szinkronizálni tervezett adatok körét, irányát az alábbi ábra foglalja össze:



Általános követelmény, hogy az egyes alkalmazás csatolók (a HR kivételével) küldjenek e-mail-t a Helpdesk csoportnak, ha felhasználói accountot hoznak létre vagy módosítanak. Jogosultság kiosztásról, elvételről, jelszószinkron eseményről stb. nem kell levelet küldeni.

IV.1. HR rendszer - Telefonkönyv

A HR rendszer az IDM legfőbb adatforrása, nem hagyományos alkalmazásként kerül bekötésre. Az OGYH esetében a Nexon HR rendszer adatait, a frakciók által szolgáltatott adatokat és az Országgyűlési Őrség HR adatait egy, az OGYH telefonkönyv adatbázisában (Oracle) implementált tárolt eljárás aggregálja, majd rendszeres időközönként frissítve, egységes adatbázis nézeteken keresztül publikálja az AGS felé. Az AGS összetett lekérdezésen keresztül az aktuális rekordok felolvasásával frissítette adatbázisát, az IDM eseményvezéreltségéből fakadóan ez változik, a komplex lekérdezést az IDM számára olvashatóan, a változások feltüntetésével kell biztosítani az OGYH-nak. OGYH a felhasználókat csak és kizárólag a Telefonkönyv formon keresztül bocsátja az IDM rendelkezésére, ennek megfelelően az IDM rendszernek nem kell rendelkeznie felhasználó adminisztrációs felülettel.

A szervezeti postafiókok, disztribúciós listák kezelése az új IDM bevezetése után is az eddig megszokott módon, a Telefonkönyv formon fog történni. Megjegyzés: Ennek leváltása és az IDM felületébe integrálása egy másik, későbbi projektben lehetséges igény szerint.

A fentieken túl az NDS csoportok létrehozása is a Telefonkönyv formon történik, ennek menetét az OGYH nem kívánja megváltoztatni.

A Telefonkönyv szolgáltatja:

- a **szervezeti struktúrát**;
- az egyes **felhasználók** HR adatait és a felhasználók besorolását az egyes szervezeti egységekbe;
- a **levelezési listá**kat;
- a **szervezeti postafiók**okat;
- **NDS (eDirectory) csoportok**at.

Ez a kapcsolat egyirányú, az IDM nem ír vissza adatot a Telefonkönyvbe.

A jelenleg használt személyi igazolvány számok a vonatkozó GDPR követelmények miatt az OGYH lecseréli más, egyedi HR azonosítóra. Az IDM rendszernek ezt az új azonosítót kell majd használnia.

Az IDM számára szükséges event táblákat a https://www.netiq.com/documentation/identity-manager-47-drivers/jdbc/data/what-is-event-log-table-in-jdbc-driver.html leírás alapján kell az OGYH-nak elkészítenie. A jelenleg használatos event táblák tartalma szűkebb, mint az AGS esetében, így a táblák, view-k, triggerek bővítése szükséges lehet, melyet OGYH végez el.

IV.2. Beléptető rendszer

A beléptető rendszer vezetői döntés alapján kikerül a csatolt alkalmazások közül. A későbbiekben (egymásik projekt keretében) a csatolás az addigra elkészült IDM-mel újra kialakítható, amennyiben erre szükség lenne.

IV.3. Oracle adatbázisok

Az Oracle adatbázisok eléréséhez szükséges felhasználó és jogosultság szinkronizáció kétirányú kapcsolat kiépítésével valósul meg. A kapcsolat JDBC-n keresztül kerül kialakításra.

- Az Oracle alkalmazások **felhasználói**t az IDM rendszernek kell azokat létrehoznia.
- Az Oracle **jogosultságok** adatbázis szerepkörök (role-ok), amik átadása az IDM felé az OGYH által fejlesztett adatbázis komponensek segítségével fog történni, továbbá az event táblák kialakítása is az OGYH feladata. Ezek a szerepkörök (nem összetévesztendő az IDM szerepkörökkel) igényelhető jogosultságként jelennek meg az IDM-ben.

- A **kiosztott jogosultságok** az IDM effektív jogok alapján, felhasználó-szerepkör összerendelések formájában jelennek meg az Oracle oldalon. (Ennek hatása ekvivalens az Oracle oldalon kiadott megfelelő GRANT ROLE és REVOKE ROLE parancsokkal.)

Az integráció kialakításához az OGYH adatbázissal foglalkozó munkatársai segítséget nyújtanak, elkészítik az esetlegesen szükséges adatbázis oldali fejlesztéseket.

IV.4. Operatív eDirectory

Az IDM címtára, valamint az operatív címtár közötti felhasználó és jogosultság szinkronizáció kétirányú kapcsolat kiépítésével valósul meg. A kapcsolat kifejezetten erre a célra készült csatoló segítségével kerül kialakításra.

Az operatív címtár elsődleges célja a file és nyomtatási szolgáltatásokkal összefüggő, illetve egyéb LDAP alapú rendszerek számára authentikációs és authorizációs forrás biztosítása. Az IDM–operatív címtár csatolás kialakításával valamennyi, az operatív címtárba bekötött alkalmazás, szolgáltatás IDM integrációja megvalósulhat.

- Az eDirectory **felhasználói**t az IDM rendszernek kell létrehoznia az operatív eDirectory-ban a telefonkönyv adatok által megjelölt helyen és felhasználónévvel. A jelszószinkron kétirányú lesz a két eDirectory között.
- A **jogosultságok** eDirectory csoportokat az IDM hozza létre a Telefonkönyv formon rögzített CN-nel és meghatározott helyen. Ezen csoportok tagsága az IDM-en keresztül válik igényelhetővé.
- A **kiosztott jogosultságok** az IDM effektív jogok alapján, csoporttagság formájában jelennek meg az operatív címtár oldalon.
- A **levelezési listá**kat és **szervezeti postafiók**okat a csatoló az operatív címtár meghatározott konténerébe szinkronizálja.
- A Telefonkönyv formon rögzített **csoportok**at a csatoló létrehozza, átnevezi, továbbá fájlrendszerbeli csoportok esetén a GetRights csatoló által írt adatokat az IDM felé ellentétesen szinkronizálja.

Ennek a csatolónak a kialakítása során megtartásra kerül az operatív címtárat a GroupWise levelező rendszerrel összekötő csatoló (szinkronizációs és ezáltal változtatási igény csak a személyes postafiókok kvótájának és láthatósága terén fogadható be a projekt keretében). A filerendszerrel kapcsolatos háttérműveletekért felelős SetRights és GetRights csatolók módosítás nélkül kerülnek felhasználásra, működésbeli módosításra a projekt keretében nincs lehetőség.

A jelenlegi operatív címtár struktúra kis mértékben módosul: az egyes konténerek a jelenlegi helyükhöz képest egy szinttel lejjebb kerülnek annak érdekében, hogy a címtár fa érdemi része egy LDAP base DN-nel kijelölhető legyen. Ezt a változtatást az OGYH végzi el a leendő IDM projektet megelőzően, szükség esetén támogatást NPSH support szerződés keretében nyújt.

Szintén a csatoló feladata lesz a Telefonkönyvön keresztül HR rendszerből átvett szervezeti adatok alapján az operatív címtár konténereinek létrehozás a fa megfelelő pontján. Névváltozás esetén a konténereket át is kell vezetni. Egység vagy részfa mozgatása esetén a konténerek automatikus mozgatására nincs lehetőség, ezt a funkciót a csatoló technikailag nem támogatja.

IV.5. Active Directory

Az IDM címtára, valamint az Active Directory címtár között csak felhasználó szinkronizáció kerül kialakításra az AD felé. Csoportok, jogosultságok (a jelenlegi AGS alapú megoldástól eltérően) nem lesznek szinkronizálva. A kapcsolat kifejezetten erre a célra készült csatoló segítségével kerül kialakításra.

Az Active Directory címtár elsődleges célja az OGYH-nál a távoli hozzáférésekkel kapcsolatos felhasználói authentikáció lehetővé tétele. Ennek megfelelően az operatív címtárhoz hasonlóan minden felhasználót ide is át kell szinkronizálni. Ezek a felhasználók csak Domain User csoporttagságot kapnak, ami a felhasználók létrehozásával automatikusan megtörténik. Ennél szofisztikáltabb jogosultság kezelésre az IDM részéről nincs szükség az AD-ban.

A jelszószinkron egyirányú lesz az IDM eDirectory-ja és az Active Directory között, tehát az IDM az operatív címtárban/IDM felületen beállított jelszót juttatja automatikusan érvényre az AD-ban.

Az AD konténerstruktúrája (egy meghatározott ponttól) meg fog egyezni az operatív címtáréval, ezért a felhasználókat ugyanúgy a telefonkönyvtől kapott információk alapján kell elhelyezni a fában és a konténerstruktúrát ugyanúgy kell karbantartani a csatoló segítségével.

IV.6. Iktató rendszer

A Fiksz10 iktatórendszer vezetői döntés alapján egyelőre kikerül a csatolt alkalmazások közül. A későbbiekben (másik, későbbi projekt keretében) a csatolás IDM-mel újra kialakítható. Viszont, amennyiben az Iktató rendszer operatív címtár alapon képes authentikációt és authorizációt végzeni, úgy az eDirectory csatolóval a rendszer csatolása is megoldottnak tekinthető.

IV.7. LifeRay

A Liferay alkalmazás képes LDAP alapú hitelesítést és hozzáférésvezérlést végezni, így az operatív címtárral teljeskörűen integrálható. Az integráció elvégzése a Hivatal feladata, melynek határideje a projekt zárását megelőző harmadik hónap vége.

IV.8. IDM rendszer

Az IDM rendszer a saját belső jogosultságait is a többi csatolt alkalmazáshoz hasonlóan kezeli. Ezeket az információkat úgynevezett loopback csatolók alakítják csoporttagságokká. Felhasználó szinkronizációra értelemszerűen nincs szükség. Az IDM authentikáció és authorizáció az IDM címtárában (eDirectory) történik az operatív címtárhoz hasonló módon.

Ilyen jogosultság például az IDM adminisztrátor, a riportokhoz való hozzáférés vagy az egyes alkalmazások adatgazdái és egyéb döntéshozók a munkafolyamatokban. Ezeket a jogosultságokat a kezdeti adatfeltöltés után ugyanúgy meg kell igényelni, mint más csatolt alkalmazások jogosultságait. Megjegyzés: Ugyanakkor lehetnek olyan döntéshozói pontok a munkafolyamatokban (pl. vezetői jóváhagyás), amik nem IDM jogosultságok, hanem HR adatok alapján kerülnek felhasználókhoz rendelésre.

Jelszó szinkronizáció a fentebb leírtak szerint történik az IDM címtára és más címtárak, esetleg adatbázisok között.

Tágabb értelemben ide tartoznak azok a belső logikát megvalósító komponensek, amik szintén loopback csatolókkal vagy az IDM eDirectory-ja és Oracle adatbázisa közötti szinkronizációval kerülnek megvalósításra.

V. Munkafolyamatok, felhasználói felületen végezhető tevékenységek

Az IDM rendszerben a legtöbb felhasználói tevékenység, így a jogosultság igénylés-visszavonás ugyanúgy munkafolyamatokon keresztül valósul meg, mint a különböző adatok karbantartása. Az egyszerűbb, csak adatrögzítést igénylő munkafolyamatokban nincsenek jóváhagyói pontok, de az ezekkel végzett tevékenység is naplózásra kerül. A bonyolultabb folyamatok akár több jóváhagyói pontot is tartalmazhatnak, a velük végzett változtatások csak a folyamat sikeres lefutását követően (az utolsó jóváhagyás után) lépnek életbe.

Az egyes munkafolyamatok az IDM egyik kezdő képernyőjén elhelyezett csempék segítségével indíthatók. Az IDM-beli jogosultságok és egyéb adatok alapján csak azok a csempék jelennek meg a felhasználók számára, amelyek mögött álló funkciók eléréséhez a felhasználóknak joguk van.

Általános követelmény, hogy kapjon e-mail értesítést az a felhasználó, akinek feladata van az IDM rendszerben. Továbbá ha egy jóváhagyói pontot is tartalmazó munkafolyamat véget ért, kapjon értesítést az igénylő és a kedvezményezett a folyamat eredményéről.

V.1. Alkalmazás, modul és elemi jog törzsadat karbantartó

A jogosultság hierarchia karbantartására három hasonló munkafolyamat készül. Ezek rendre a fentebb vázolt jogosultság hierarchia elemeinek (alkalmazások, modulok, elemi jogosultságok) felvételére, módosítására (átszervezés is), inaktiválására szolgálnak. Csak olyan adatok szerkeszthetők, amiket nem csatolók hoznak át más rendszerekből, továbbá az OGYH csak és kizárólag rendszerjogosultságok nyilvántartására kívánja használni az IDM-et.

Ezeket a munkafolyamatokat az IDM adminisztrátorok futtathatják. Jóváhagyás nem történik, az elvégzett változtatások azonnal életbe lépnek.

Az IDM rendszer kialakításának és a tárgyi projektnek csak az AD, Oracle és NDS címtár integrált rendszerek központi jogosultságkezelésének megvalósítása a feladata.

Az Alkalmazáskarbantartó az alábbi funkciókat biztosítja:

- Új, NDS címtárbeli alkalmazás felvétele (később integrációra kerülő rendszerek egyszerűbb adminisztrációja végett)
- A felület az alkalmazások alábbi paramétereinek szerkeszthetőségét teszi lehetővé:
  - Megnevezés
  - Adatgazda (szervezeti egység)
  - Jóváhagyó (felhasználó/csoport/szervezeti egység vezető)
  - Státusz
  - Igényelhetőség (annak max időtartama)
  - Végrehajtó csoport (későbbiekben beállítást végző csoport)

Az IDM terminológiájában modulként rögzített objektumok szerkesztése a Modulkarbantartó felületen keresztül történhet. A modulok paraméterei megegyeznek az alkalmazásokéval, a Végrehajtó csoport és Adatgazda viszont ezen a szinten már nem jelenik meg.

A jogosultságok tekintetében a beállítási lehetőségek megegyeznek a modulokéval.

V.2. Szerepkörök és összetételük kezelése

Különböző elemi jogosultságok (akár több alkalmazásból) szerepkörökbe szervezhetők, így ezek egyben oszthatók ki és vonhatók vissza a jogosultság modellben leírtaknak megfelelően. Ebben a munkafolyamatban van lehetőség új szerepkörök felvételére, meglévők módosítására (név, leírás

módosítása, a szerepkör tulajdonosának – későbbi jóváhagyó – és a szerepkörben foglalt jogosultságok listájának szerkesztése, igényelhetőség) és inaktiválására is.

Ezt a munkafolyamatot az IDM adminisztrátorok futtathatják. Új jogosultság felvételekor, illetve a szerepkör összetételének bővítésekor a szerepkör adatgazdája és a bevont jogok adatgazdája hagyja jóvá a változtatást. Jogosultság szerepkörből való elvételét elegendő a szerepkör adatgazdájának jóváhagynia.

V.3. Szervezeti egységekhez rendelt jogosultságok kezelése

A különböző elemi jogosultságok (akár több alkalmazásból) szervezeti egységekhez és munkakörhöz rendelhetők. Így ezek a jogosultságok automatikusan oszthatók ki és vonhatók vissza a jogosultság modellben leírtaknak megfelelően aszerint, hogy a felhasználók az adott szervezeti egységben és/vagy munkakörben foglalnak-e helyet. Ebben a munkafolyamatban van lehetőség az egységekhez és munkakörökhöz rendelt elemi jogosultságok listájának szerkesztésére. (A szervezeti egységeket a HR rendszer adja át, így azok adatai itt nem módosíthatók, a munkakörök listáját vagy a Telefonkönyv formon keresztül kapja meg az IDM, vagy fix listaként – nem felületi kivezetéssel – kerülnek karbantartásra. Az ületi és működési szempontok figyelembe vételével az 1. megoldás az elsődlegesen támogatott, az adatbázis megfelelő előkészítés és fejlesztése OGYH feladata.)

Ezt a munkafolyamatot az IDM adminisztrátorok futtathatják. Új jogosultság felvételekor (a szervezeti egység alapértelmezett jogainak bővítésekor) a szervezeti egység vezetője és a bevont jogok adatgazdája hagyja jóvá a változtatást. Jogosultság szervezeti egységről való levételét elegendő az egység vezetőjének jóváhagynia.

V.4. Jogosultság és szerepkör igénylése felhasználóknak

Az IDM fő funkciója a jogosultság igénylés lehetőségében jelenik meg a felhasználók többsége számára. Ennek a munkafolyamatnak a segítségével kérhetők a felhasználók részére azok a jogosultságok, amik nem automatikusan kerülnek kiosztásra.

Igényelni egyszerre egyetlen felhasználónak lehet elemi jogosultságo(ka)t és/vagy szerepkör(öke)t, ugyanakkor az IDM lehetőséget biztosít hozzáférés irányból is igénylés kezdeményezésére (egy hozzáférés – legyen az szerepkör vagy jogosultság – kiválasztása után több felhasználó is választható). Továbbá egy felhasználó számára, másik felhasználó aktuális jogosultságai alapján is indítható igénylés. A felhasználók kiválasztásánál szűrési paramétereket biztosít a rendszer (pl: szervezeti egység), a pontos paraméterek a tervezési fázisban kerülnek meghatározásra. Minden felhasználó saját magának, a vezetők ezen felül közvetlen és közvetett beosztottjaiknak adhatnak fel igénylést. Minden felhasználónak igényelhetnek jogot a Helpdesk munkatársak és az IDM adminisztrátorok.

- Első jóváhagyó a kedvezményezett (akinek a jogot kérték) közvetlen felettese abban az esetben, ha az igénylő magának kérte a jogot vagy Helpdesk/IDM adminisztrátori igénylés történt. Egyébként (ha a közvetlen vagy egy közvetett felettes adta fel az igényt, akkor) kimarad.
- Második jóváhagyó a kért jogosultság jóváhagyója vagy szerepkör tulajdonosa.

Ha bármelyik ponton elutasítják az igényt, az a teljes folyamat elutasítását jelenti. Jóváhagyottnak akkor minősül az igény, ha azt minden ponton jóváhagyták.

Nem szükséges a folyamatot jóváhagynia annak a személynek, aki az igényt indította (ha ő jóváhagyó is lenne). Továbbá nem szükséges egy személynek többször jóváhagyni az igényt (amennyiben az illető több minőségében is érintett a folyamatban). Ilyenkor a rendszer a felesleges lépéseket átugorja, mintha a jóváhagyás megtörtént volna.

V.5. Jogosultság és szerepkör visszavonása felhasználóktól

Az igénylés és jóváhagyás logikája szerint kerül kialakításra a visszavonás. Visszavonni egyszerre egyetlen felhasználótól is lehet elemi jogosultságo(ka)t és/vagy szerepkör(öke)t, illetve egy hozzáférés – szerepkör/jogosultság – kiválasztása után több embertől is visszavonható a kiválasztott tétel.

Minden felhasználó indíthat visszavonást saját magára, a helpdesk munkatársak és az IDM adminisztrátorok pedig minden felhasználóra. Ezekben az esetekben a közvetlen vezető jóváhagyását igényli a folyamat.

A vezetők ezen felül közvetlen és közvetett beosztottjaiknak indíthatnak visszavonást. Ebben az esetben nincs szükség jóváhagyásra.

V.6. Felhasználókezelés

Kialakításra kerül egy egyszerű munkafolyamat, amivel a felhasználók adatai megtekinthetők, illetve egyes adatai szerkeszthetők.

A vezetők a közvetlen és közvetett beosztottjaik adataihoz férnek hozzá, míg a Helpdesk/IDM adminisztrátorok és riport adminisztrátorok az összes személyéhez. A helyettesítés beállítására ezen formon keresztül nyílik lehetőség.

A felületen keresztül az aktuálisan beállított szűrési paraméterekkel (szervezeti egység, HR státusz, informatikai státusz) rendelkező felhasználók exportálhatók csv formátumba, melynek tartalma: felhasználó törzsszáma, felhasználóneve, teljes neve, szervezeti egységének neve; valamint a HR szerinti státusza (aktív, távollévő, kilépett) és informatikai státusza, tehát, hogy tiltott-e a belépése. Az export tényleges tartalma a rendszertervezés fázisában kerül pontosításra, kiegészítésre.

A személy adatlapján az AGS-ben fő adatlapon kivezetett adatok jelennek meg, továbbá:

- Amennyiben a folyamatot indító személy Helpdesk és IDM adminisztrátori csoportba tartozik, jelszóvisszaállítási kérelmet tud gombnyomásra elindítani. A felületen az új jelszó a jelszószabályoknak megfelelően generálásra kerül, továbbá intruder unlock és grace login paraméterek változtathatók. Az új jelszó az IDM-ben, az operatív eDirectory-ban és az Active Directory-ban, esetleg további bekötött adatbázisokban, címtárakban jut érvényre.
- A meghatározott csoportok (később kerül tisztázásra) tagjai számára elérhető egy, az összes rendszerben inaktivitást kiváltó „Azonnali tiltás", úgynevezett piros gomb.
- A tartós távolléten lévő személyek ideiglenes aktivációját egy, az összes rendszerre érvényes „Tartós távolétről aktivál" gombon keresztül érhetik el a vezetők és IDM adminisztrátorok. A Telefonkönyv formról kikerül ennek lehetősége.

A felületen adatok beállítására nincs lehetőség, kizárólag a felhasználókezelés kapcsán felmerült – fent részletezett – igények kielégítése és az adatok tájékoztató jelleggel történő feltüntetése a célja.

VI. Riportok

Az IDM rendszerben a következő riportokat tervezzük kialakíttatni. A riportok lekérésére csak meghatározott jogosultság birtokában van lehetőség. Bizonyos szűrőket a rendszer beépítetten alkalmaz, míg más szűrő feltételek opcionálisan beállíthatók. A lekérdezés technikailag egy munkafolyamat indítás, rendszer a riport generálást a háttérben végzi el. Az elkészült riportok CSV-ben vagy PDF-ben tölthetők le az IDM felületén, mintha az egy jóváhagyási lépés lenne egy munkafolyamatban.

VI.1. Effektív jogosultságok lekérdezése

A rendszer a jelenben vagy egy adott múltbéli időpontban megmutatja a felhasználók effektív kiosztott jogait.

- **Hatáskör:** A felhasználók saját magukra, vezetők az alattuk elhelyezkedő szervezeti részfára futtathatják a riportot. Az információbiztonsági felelős, a helpdesk, a riport adminisztrátor és az IDM adminisztrátor minden felhasználó minden jogosultságát lekérdezheti.
- **Paraméterek:** Megadható az időpont, valamint szűrni lehet szervezeti egységre, felhasználóra, alkalmazásra, modulra és/vagy jogosultságra. (Megjegyzés: Nem értelmezhető minden lekérdezőre az összes szűrési lehetőség. A szűrési lehetőségek részleteit a rendszertervezés fázisában dolgozzuk ki.)
- **Adatok:** Megjelenik a felhasználó törzsszáma, felhasználóneve, teljes neve, szervezeti egységének neve; valamint az alkalmazás, modul, elemi jog neve, a hozzárendelés forrása (automata/egyedi igényből fakadó).

Megjegyzés: A riport nem érzékeny arra, hogy az effektív jogosultság milyen (akár több) úton állt elő (lásd a jogosultság modellt), amennyiben több úton is jár a jogosultság, priorlista alapján tünteti fel a összerendelés forrását.

VI.2. Effektív jogosultságok változásának lekérdezése

A rendszer egy múltbéli időintervallumra megmutatja a felhasználók effektív kiosztott jogainak változásait.

- **Hatáskör:** A felhasználók saját magukra, vezetők az alattuk elhelyezkedő szervezeti részfára futtathatják a riportot. Az információbiztonsági felelős, a helpdesk, a riport adminisztrátor és az IDM adminisztrátor minden felhasználó minden jogosultságának változását lekérdezheti.
- **Paraméterek:** Megadható az időintervallum, valamint szűrni lehet szervezeti egységre, felhasználóra, alkalmazásra, modulra és/vagy jogosultságra. (Megjegyzés: Nem értelmezhető minden lekérdezőre az összes szűrési lehetőség. A szűrési lehetőségek részleteit a rendszertervezés fázisában dolgozzuk ki.)
- **Adatok:** Megjelenik a felhasználó törzsszáma, felhasználóneve, teljes neve, szervezeti egységének neve; valamint az alkalmazás, modul, elemi jog neve és az elemi jog szöveges leírása. Szintén megjelenik a hozzárendelés időtartama (kezdő-végdátum).

Megjegyzés: A riport nem érzékeny arra, hogy az effektív jogosultság milyen (akár több) úton állt először elő és milyen út szűnt meg utoljára (lásd a jogosultság modellt),), amennyiben több úton is jár a jogosultság, priorlista alapján tünteti fel a összerendelés forrását.

VI.3. Szervezeti jogosultságok lekérdezése

A rendszer a jelenben megmutatja az egyes szervezeti egységekhez/munkakörökhöz rendelt jogosultságokat.

- **Hatáskör:** A vezetők az alattuk elhelyezkedő szervezeti részfára futtathatják a riportot. Az információbiztonsági felelős, a helpdesk, a riport adminisztrátor és az IDM adminisztrátor minden szervezeti egység minden jogosultságát lekérdezheti.
- **Paraméterek:** Szűrni lehet szervezeti egységre.
- **Adatok:** Megjelenik a szervezeti egység neve; (ha van, akkor munkakör neve), valamint az alkalmazás, modul, elemi jog neve.

VII. Egyéb projekttevékenységek

VII.1. Projektvezetés

Szállító projektvezetője a projektvezetői tevékenységeket a projekt időtartama alatt ellátja.

Projektvezetői tevékenységek közé sorolandó:

- VIII. fejezetben fel nem tüntetett minden egyéb dokumentum készítése.
- személyesen vagy elektronikusan, telefonon/levelezésben folytatott kommunikáció (ide tartozik minden projekttel kapcsolatos szervezési és menedzsment tevékenység, válaszadás).
- OGYH kérése alapján dokumentumok, anyagok (például megbeszélés emlékeztetők, státuszok) készítése, véleményezése.

VII.2.Tervezés

A tervezési fázis célja a későbbi implementációs feladatok olyan szintű definiálása, hogy a fejlesztés a lehető legkisebb Megrendelői bevonással teljesíthető legyen. A feladatok ellátása során OGYH a szükséges mértékben biztosítja a szakembereket a minél pontosabb igényfelméréshez. A fázis eredményterméke a Rendszerterv dokumentum.

VII.3.Tesztelés

Szállító a fejlesztések alatt egység- és integrációs teszteket végez. A tesztelésről jegyzőkönyv nem készül, Szállító a rendszert a Hivatal által elvégzendő tesztekre csak akkor adja át, ha a saját fejlesztői környezetén a tesztek sikeresen lefutottak.

Megrendelő a Szállító által átadott tesztelési forgatókönyv alapján végzi el az UAT teszteket. A teszteléshez Megrendelő szakembert biztosít tesztkoordinátori feladatok ellátására. A tesztkoordinátor feladata, hogy a tesztelés alatt jelzett hibákból a felhasználói hibákat kiszűrje, ezáltal Szállító felé a tényleges rendszer hibák jussanak csak el. Amennyiben a Szállítóhoz beérkező bejelentések több, mint 10%-a felhasználói hibából fakad, azt jelzi Megrendelő felé, aki a tesztkoordinátor felelősségre vonásáról gondoskodik.

VII.4.Élesítés

Szállító az élesítés kapcsán adattisztítást nem végez, a tervezési fázisban meghatározott adattisztítási koncepció mentén a betöltőállományokat a Hivatal biztosítja. Az élesítés előtt megtörténik a Rendszerterv aktualizálása. Az ősfeltöltést az NPSH végzi, OGYH a betöltések megfelelőségét IDM felületen ellenőrzi, illetve a szimulált események (például automata kiosztások) kapcsán szükséges áttekintéseket megteszi. Az éles indulás után NPSH 3 munkanapig távoli munkavégzéssel 1 fő személyt kiemelten készenlétben tart.

VIII. Eredménytermékek, dokumentációk

A fő leszállítandó eredménytermék az IDM rendszer bevezetési projekt kapcsán maga az új 4.8-as verziójú IDM rendszer, amely az OGYH éles környezetében hibátlanul működik és a kezdeti adatokkal fel van töltve.

Az átadott rendszer részét képzik azok a forráskódok, amik kifejezetten ennek az IDM rendszernek kialakítása során állnak elő. (Ide nem tartozik az egyébként zárt forráskódú, licence-elt IDM termék és azok a Novell PSH Kft. által fejlesztett komponensek, amik általános céllal készültek.)

Ezeken kívül a következő dokumentációk elkészítése és átadása szükséges:

- **Felhasználói kézikönyv:** A felhasználók által használt felületek és a munkafolyamatok működésének bemutatása.
- **Üzemeltetési kézikönyv:** Az üzemeltetők által végzendő feladatok bemutatása, a gyakoribb hibák kezelésének leírása.
- **Tesztelési forgatókönyv:** Megrendelő által üzemeltetett Redmine-ba betölthető formátumban.
- **Rendszerterv:** A rendszer architektúrája és implementációs leírás. A kezdeti terveket követően, a projekt végén aktualizálásra kerül a kezdeti tervekhez képest végzett változtatásokkal és az implementáció során meghatározott műszaki paraméterekkel.

IX. Ütemezés

Az IDM bevezetési projekt az alábbi mérföldkövek szerint kerül ütemezésre.

Mérföldkő	Megjegyzés	Mérföldkő hossza	Határidő	Napszám
0. Szerződéskötés		-	x	
1. Tervezés	• Ügyfél oldali igények felmérése • Adattisztítás tervezése • Rendszer technikai tervezése • Rendszerterv dokumentum	2 hónap	x + 60 nap	177 nap
2.Implementáció	• Infrastruktúra telepítése • Fejlesztések elvégzése elfogadott Rendszerterv alapján • Tesztelési fogatókönyv • Felhasználói kézikönyv dokumentum • Tesztelésre alkalmas környezet	3 hónap	x + 150 nap	
3. Tesztelés, élesítés	• Rendszerterv aktualizálása • Megrendelő oldali tesztelés • Üzemeltetési dokumentum • Adattisztítás fogadása • Ősfeltöltés, éles indulás • Helyszíni támogatás induláskor	3 hónap	x + 240 nap	80 nap

A projekt hossza – az előzetes felméréseink alapján – előreláthatóan 9 hónap, amennyiben a Megrendelő által elvégzendő feladatok (pl.: tesztelés, adattisztítás, infrastruktúra biztosítása) a mindenkori projektütemezés alapján határidőre elvégzésre kerülnek.