

AZONOSÍTÁSI RENDSZEREK INTEROPERABILITÁSI KÉRDÉSEI

Absztrakt

A cikk célja az interoperabilitás fogalmi rendezése, azonosítási rendszerek fontos kapcsolódási pontjainak azonosítása, valamint az ezeken felmerülő interoperabilitási problémák felkutatása. Ezek ismeretében néhány jellemző azonosítási eljárásnál a megoldási lehetőségek bemutatása.

The aim of this article is to shed a light upon interoperability, identification of important connection points, as well as searching for interoperability problems emerging at these. Based on all these I am going to show possible solutions for the case of some typical identification processes.

Kulcsszavak: azonosítás, interoperabilitás, információs interoperabilitás, technikai interoperabilitás.

BEVEZETÉS

A felhasználó bizonyíthatóan egyértelmű, hiteles azonosítása az egész informatikai rendszer biztonságának alapvető, és egyik legfontosabb kérdése. Ennek az eljárásnak a sikerén múlik az általunk féltve őrzött információk biztonsága.

Napjainkra a globalizálódási folyamat eredményeképp a különböző szereplők közötti együttműködés, és együttes működés minden szférában egyre nagyobb szerepet játszik. Ennek megfelelően növekszik a szereplők közötti interoperabilitás jelentősége is.

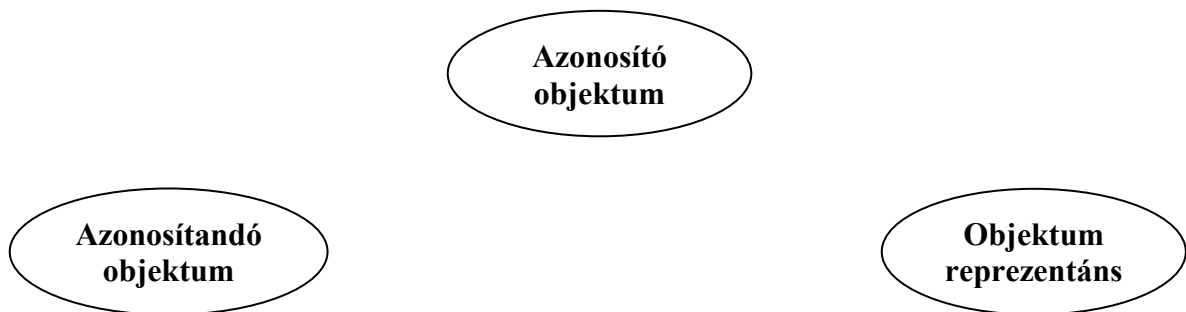
Ezért fontos az azonosítási rendszer kapcsolódó elemeinek elemző vizsgálata, az interoperabilitás szempontjából. Az architektúra ismeretében az egyes rendszerelemek közötti együttműködési nehézségeket, illetve azok helyét fel kell tárni, meg kell érteni az azonosítási rendszer felépítését, az azonosítás folyamatát, illetve ezek ismeretében meg kell határozni az azonosítást végző alrendszerrel szemben támasztott követelményeket.

Az első pontban az interoperabilitás, és az azonosítás fogalmát összegzem. A második pontban rendszerszemlélet szabályainak figyelembevételével, meghatározom az azonosítás rendszer modelljét és az interoperabilitási szempontból fontos kapcsolódási pontokat. A harmadik pontban összegzem az interoperabilitáshoz kapcsolódó alapfogalmakat és elemzem a lehetséges interoperabilitási problémákat. A negyedik pontban e problémák lehetséges feloldási lehetőségeit tekintem át.

1. AZ INTEROPERABILITÁS, ÉS AZ AZONOSÍTÁS FOGALMI ELHELYEZÉSE

Az azonosítás fogalmi alapjainak rendszerezése kapcsán nézzük meg melyek azok a fogalmak melyek a téma tárgyalása során elengedhetetlenek. Nézzük először is az azonosítás meghatározását.

Az *azonosítás* az a folyamat, melynek során az azonosítandó objektum megfeleltetése, és általában hitelesítése is megtörténik egy előre definiált objektum reprezentánsal.



1. ábra Az azonosítás három főobjektuma

Az így keletkezett identitáshoz szolgáltatás igénybevételi jogokat és adat hozzáférési jogosultságokat rendelhetünk. Tehát az azonosítási folyamatnak nem része az identitás felhatalmazása különböző jogosítványokkal.

Az azonosítás és a hitelesítés az informatika világában az esetek többségében szinonimaként használatos. Ez alól azért létezik kivétel, amikor vendégként azonosított objektumot nem hitelesítjük, mert szükségtelen. A hitelesítés során az azonosítás megerősítése történik az azonosítandó objektumtól független hiteles forrásból. Egy hétköznapi példán szemléltetve: egy személy, amikor bemutatkozik, akkor már az azonosítása megtörténik, de csak az igazoltatást követően nevezhető ez az azonosítás hitelesítettnek.

Együttműködő azonosítás esetén az azonosítandó objektum aktívan részt vesz az azonosítás folyamatában. Ebből következően az együttműködést nem igénylő azonosítás esetén az azonosítandó objektum a teljes azonosítási folyamat alatt passzív marad (ilyen például a vonalkódos azonosítás).

Az *objektum reprezentáns* az a rendszer által tárolt leképezése az azonosítandó objektumnak, ahogy „a rendszer látja” az adott entitást. Az identitás egy olyan azonossága az entitásnak, melyhez a felhatalmazó rendszerszolgáltatás igénybevételi, információ hozzáférési lehetőségeket, valamint jogokat rendel.

Ugyanazon azonosítandó objektumhoz különböző rendszerek, illetve ugyanazon rendszer, különböző identitásokat rendelhetnek.

Az azonosítási folyamat során gyakran alkalmazunk technikai eszközt, vagy tárgyat, mely az azonosítandó objektum azonosítását segíti elő.

Az interoperabilitás a hatékony és eredményes együttműködéshez szükséges képességek alapvető összetevőjeként jelent meg 1992-ben az Egyesült Államok hadserege "Informatika a harcok számára" elnevezésű dokumentumában. Az interoperabilitás általánosan megfogalmazható definíciója a következő:

„Az interoperabilitás objektumok között fennálló viszony, az együttműködést támogató, eredményes és hatékony együttes működést biztosító kölcsönös képesség.”¹

Az együttműködési képéségen kívül fontos interoperabilitási kérdés az együttes működés is. Az információs robbanás, és az információs társadalom, ezzel együtt az információs háború hatására napjainkra kiemelt jelentőségű fogalommá lett, hiszen a különböző célú, képességű és fajtájú hálózatok, eszközök, ezek kapcsán információs, és adatbázisok összekapcsolásakor a legfontosabb kérdés a különböző rendszerek együttműködésének kérdése. Más szóval nincs interoperabilitási probléma heterogenitás nélkül. Homogén esetben nem értelmezhető fogalom, mert ebben az esetben a rendszer elemei közt fellépő együttműködési nehézségek a szervezési, a tervezési, illetve kivitelezési hiba tárgykörébe tartoznak. Induljunk ki a heterogenitásból! A heterogenitás három szintre tagolható: az alkalmazott eszközök, hordozók *fizikai* (anyag, technikai) szintje; az *alkalmazott nyelv szintje*, az üzenet- és adatformátumok szintaktikai szintje; végül az *átviendő tartalom*, jelentés szemantikai szintje. Az interoperabilitás a heterogenitás következménye, ezért értelemszerűen az interoperabilitás osztályozása a heterogenitás felosztásából vezethető le.

„Az interoperabilitás alanyai aktív objektumok, amelyek két nagy típusba sorolhatók: tudatosan tevékenykedő entitások, vagy célirányosan, meghatározott rendeltetéssel működő technikai eszközök, rendszerek. Ennek megfelelően megkülönböztethetünk szereplők közötti, illetve eszközök közötti interoperabilitást, amelyeket a katonai szakirodalomban leggyakrabban a (had)műveleti interoperabilitás, illetve a technikai interoperabilitás kifejezésekkel jelölnek.”²

„A (had)műveleti interoperabilitás közös cél megvalósítása érdekében együttműködő szereplők között fennálló viszony, az eredményes és hatékony együttműködést biztosító átfogó, kölcsönös képesség.”³

„A funkcionális területi interoperabilitás együttműködő szereplők között fennálló viszony, az eredményes és hatékony együttműködést egy meghatározott funkcionális területen biztosító kölcsönös képesség.”⁴

Valamennyi funkcionális interoperabilitás az információs és a technikai interoperabilitáson alapul.

„Az információs interoperabilitás különböző szereplők kölcsönös képessége információk közös értelmezésén alapuló, a hatékony együttműködéshez szükséges cseréjére.”⁵

¹ Munk Sándor: An analysis of basic interoperability related terms, system of interoperability types; AARMS Volume 1. Issue 1. 2002. (120. o.)

² u. o. (121. o.)

³ u. o. (125. o.)

⁴ u. o. (125. o.)

⁵ Munk Sándor: Role of semantic interoperability in warfare of our age; AARMS Volume 3. No. 4. 2004 (531. o.)

A technikai interoperabilitás tárgykörébe az együtt működő eszközök között felmerülő fizikai, technológiai együttműködési, és együttes működési problémák tartoznak.

Felmerül a kérdés, hogy egy azonosító rendszer tekintetében a fentiek alapján hogy merülhet fel interoperabilitási probléma. A gyakorlatban az azonosító rendszer egyes elemei legtöbb esetben nem egy gyártó termékei. Ez azért van így, mert egyrészt a gyártók szakosodtak, másrészt az azonosító rendszer bizonyos elemei nem csak az adott rendszer elemét képezik. Jellemző, hogy egy azonosító eszközt több rendszerben is felhasználunk azonosításra.

2. AZ AZONOSÍTÁSI RENDSZERMODELL KAPCSOLÓDÁSI PONTJAINAK AZONOSÍTÁSA

A felállított azonosítási rendszermodell elemzése során meg kell keresni az egyes rendszerelemek kapcsolódási pontjait, hogy az interoperabilitási szempontból elemzésre szoruló helyeket lokalizálni tudjuk. Mielőtt ezt megteszem fontos, hogy a rendszer modell egyes elemeit megnevezzük, és definiáljuk funkcióit.

Az azonosítandó objektum egy entitás, ami lehet felhasználó, folyamat, eljárás, vagy tárgy, mely az azonosítási eljárás tárgyát képezi. Az azonosítandó objektumhoz tartozhat az azonosítás bizonyos eseteiben azonosító eszköz, vagy tárgy, mely egyszerűsíti, illetve biztonságosabbá teszi az azonosítást. Ilyen eszköz lehet egy egyszerű vonalkód, vagy akár egy intelligens kártya.

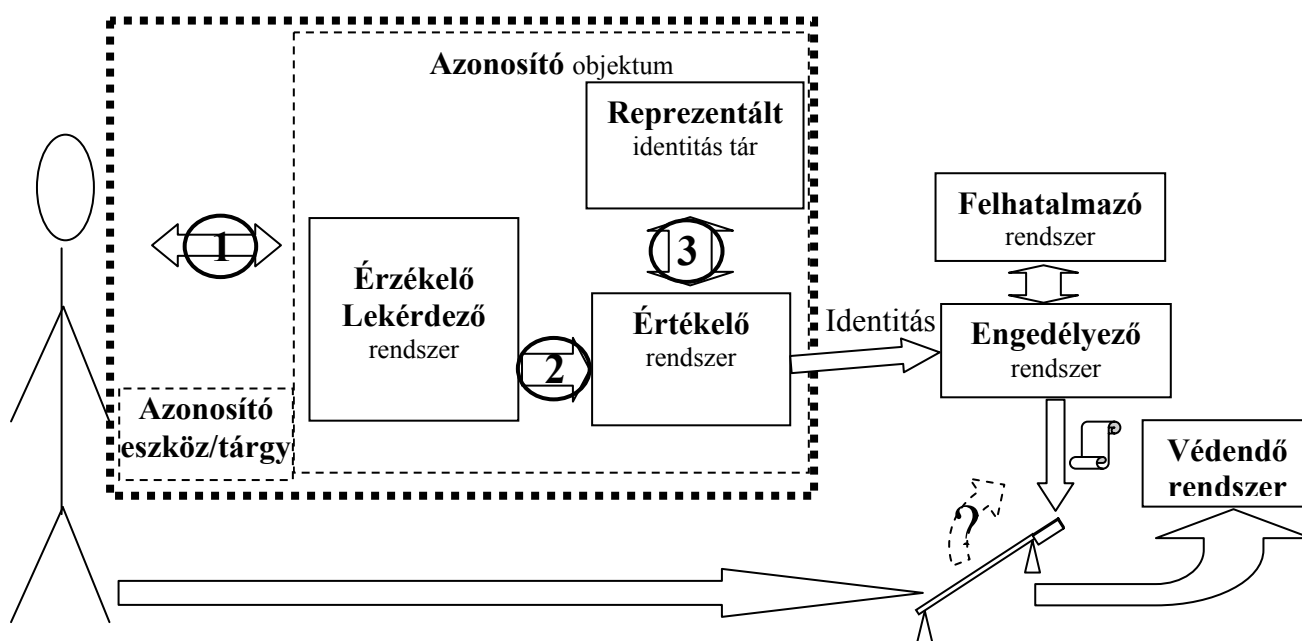
Az azonosító objektum az azonosító rendszer azon része, mely az azonosítandó objektumról „eldönti”, hogy azonos-e azzal az entitással, amiről készült reprezentáns a reprezentált identitás tárban szerepel. Az így azonosított identitás kerül ezt követően egy felhatalmazó-engedélyező rendszer által feljogosításra, és ezen jogok függvényében ez a rendszer teszi lehetővé az entitás számára a védett rendszerhez, annak részeihez, illetve szolgáltatásaihoz a hozzáférést. A felhatalmazó-engedélyező rendszer nem képezi az azonosító rendszer részét. A rendszer modell különböző rendszerlemei nem minden esetben választhatók szét egyértelműen a tényleges megvalósítást követően. Az azonosító objektum három jól elkülöníthető részre tagolható funkcionális szempontból.

Az első az érzékelő-lekérdező rendszer, melynek a feladata az entitás azonosítandó jellemzőit érzékelni, illetve lekérdezni, és ezen jellemzőket megfelelő módon átalakítva bocsátja az értékelő rendszer rendelkezésére.

Amit a második az értékelő rendszer, összehasonlítja az általa a reprezentált identitás tárból kiolvasott mintával. Az összehasonlítás eredményétől függően azonosítja az azonosítandó objektumot, és az így keletkezett identitást átadja a felhatalmazó-engedélyező rendszernek, a jogosultságok hozzárendelése és a hozzáférés biztosítása céljából.

A harmadik a reprezentált identitás tár, mely az azonosítandó objektum azonosítandó jellemzőit tartalmazza, megfelelően átalakított formában. Ez a megfelelően átalakított forma a megvalósítástól függően lehet egy jelszó meghatározott algoritmussal transzformált alakja, vagy egy biometriás esetben az adott jellemző egy adott matematikai modell szerint leképezett mása.

Az azonosítási rendszer modellen számokkal jelöltem, melyek azok a kapcsolódási pontok, amik interoperabilitási szempontból érdeklődésre tarthatnak számot.



2. ábra: Az azonosítás interoperabilitási problémát felvető kapcsolódási pontjai

Az „1” jelű kapcsolódási pont a felhasználó, illetve annak azonosító eszköze és a érzékelő-lekérdező alrendszer között található. Ezen a csatlakozási ponton legalább három markánsan elkülönülő folyamat lebonyolítása történik. Először az azonosítandó objektum azonosítást kezdeményező szándéka jut el az érzékelő-lekérdező rendszerbe. Majd az érzékelő-lekérdező rendszer „felszólítja” az azonosítandó objektumot a megfelelő azonosítási válaszadásra, illetve nem együttműködő azonosítási eljárás esetén leolvassa az azonosítandó jellemzőt, vagy tárgyat. Ezután az azonosítandó objektum, illetve annak az azonosító eszköze, válaszjelet küld a lekérdező rendszernek, illetve nem együttműködő esetben ez nem választható előbbiektől.

A „2” jelű kapcsolódási pont az érzékelő-lekérdező rendszer és az értékelő rendszer között helyezkedik el, ezen a csatornán jut át a feldolgozott válasz-, illetve érzékelt jel.

A „3” jelzéssel ellátott kapcsolódási pont az értékelő rendszer és a reprezentált identitás tár között helyezkedik el, itt zajlik a reprezentált identitás kikeresése a tárból.

Összetett rendszerek esetében az azonosítás azon a rendszeren zajlik, amelyikre az entitás csatlakozik, illetve amelyik rendszer szolgáltatásait először igénybe veszi. A többi kapcsolódó rendszerben általában nem történik az entitás irányában újraazonosítás átjelentkezéskor, illetve szolgáltatás igénybevételekor, csak a már érvényes azonosítás alapján a feljogosításra kerül sor.

3. INTEROPERABILITÁSÁSI PROBLÉMÁK

Az előző részben feltárt kapcsolódási pontokon felmerülő interoperabilitási problémák az alábbiak.

Az „1” jelű kapcsolódási pont esetében az alkalmazott azonosítási módszerek függvényében ezen a kapcsolódási ponton jelentősen eltérő interoperabilitási problémák merülhetnek fel, attól függően, hogy milyen azonosítási eljárást alkalmazunk. A legegyszerűbb esetben ez az eljárás mindössze egy beléptető program (login script) elindítása. Ekkor szinte kizárólag felhasználói, számítógép kezelési hiányosságok, hibák fordulhatnak elő interoperabilitási problémaként. Amennyiben az azonosítás során a felhasználó által birtokolt technikai eszköz, vagy tárgy felhasználására, vagy biometriás jellemzők felhasználására is kerül sor, akkor itt történik meg ezen azonosító eszközök arra alkalmas módon a rendszerhez „csatlakoztatása”, a rendszerszámára hozzáférhetővé tétele. Az említettek alapján a felhasználói kezelési problémák mellett megjelennek a különféle fizikai elhelyezkedésből eredő, vagy technikai jellegű interoperabilitási problémák is. Ezek lehetnek a különféle kártyák, vonalkódok le-, illetve beolvasási problémái, melyek lehetnek hardver vagy szoftver eredetűek.

A „2” jelű kapcsolódási ponton jellemzően protokolláris, és algoritmikus jellegű együttműködési zavar léphet fel, mely a rendszerelemek között fellépő értelmezési, és szabályozásbeli különbségeket jelenti. Ezen a ponton az átalakított válasz/érzékelte jel átalakítása továbbítása zajlik. Ha azonban az azonosítás részét képezi valamilyen biometriás jellemző beolvasása is, akkor a görcsö alá vett biometriás jellemző állandóságával, sérülékenységével, egyéb fiziológiás változás okozta, illetve a leképezési eljárás megfelelőségével kapcsolatos interoperabilitási problémák merülhetnek fel.

A „3” jelzéssel rendelkező pont, ahol a reprezentált identitások tárában keresi ki az értékelő rendszer a beolvasott entitás reprezentánsához tartozó információkat. Ezért ezen a ponton címzési és protokolláris jellegű interoperabilitási problémák fordulhatnak elő elsősorban.

Összetett rendszerek esetében a másik rendszerben azonosított entitás elfogadhatósága merül fel kérdésként.

Általánosságban megemlíthető, mint ahogy az első fejezetben bővebben ismertettem, hogy interoperabilitási probléma nem merülhet fel heterogenitás nélkül. Miből fakadhat az azonosítás során heterogenitás? A különböző azonosítási rendszerelemeket különböző gyártók gyártják, és egy rendszeren belül különböző eszközöket kell használni, esetleg már más rendszerben alkalmazott elemek migrálását kell megoldani. A másik ok az, hogy az azonosítási rendszerelemek készen „dobozosan” kaphatók a kereskedelemben, így a nagy széria miatt lényegesen kedvezőbb ár érhető el az egyedi fejlesztésekkel szemben.

Az alábbiakban a legelterjedtebb azonosítási módszerek esetében veszem sorra az interoperabilitási problémákat.

Jelszavas azonosítás esetén valódi interoperabilitási probléma nem merül fel, a heterogenitás hiánya miatt. Kizárólag a jelszó elfelejtése, kezelő rendszer ismerete, illetve kezeléssel kapcsolatos problémái jelenthetnek problémát.

RF ID azonosítás alkalmazása esetén az „1” jelű kapcsolódási ponton felmerülhet interoperabilitási probléma, hiszen az azonosítást szolgáló Radio Frequency Identification eszköz nem feltétlenül származik ugyan attól a gyártótól, mint a leolvasó eszköz. A „2” pontnál szintén felmerülhet olyan probléma, hogy több érzékelő/lekérdező rendszer kapcsolódik egy értékelő rendszerhez. A „3” jelzéssel rendelkező pont esetében akkor képzelhető el interoperabilitási probléma, ha a reprezentált identitás tár máshol található, mint az értékelő rendszer. Ez első sorban kiterjedt rendszerek központi vezérlése esetén merülhet fel problémaként.

Biometriás azonosítás esetén általában alkalmaznak egy azonosítást szolgáló intelligens technikai eszközt is, mely a jellemzőket tartalmazza, amennyiben nem, úgy az azonosító rendszer tartalmaz minden az azonosításhoz szükséges információt. Az „1” ponton találkozhatunk technikai jellegű interoperabilitási problémával, mely hasonló az RF ID-nál említettekhez. Ezenkívül az azonosítandó biometriás jellemző felismerésével összefüggő problémákkal találkozhatunk. A „2”, és a „3” pont esetében ugyanazok az interoperabilitási problémák jelentkeznek, mint az RF ID alkalmazásakor.

Vonalkódos azonosításnál az „1” ponton található interoperabilitási probléma. Ez a probléma a vonalkód leolvashatóságára, és értelmezhetőségére vezethető vissza. A leolvashatóságot befolyásolja a vonalkód hordozójának az anyaga, a színe, elhelyezkedése.

*Idegen-barát felismerő rendszer*nél az „1” pontnál különböző interoperabilitási problémák léphetnek fel. Az egyik fajta probléma, hogy különböző szervezetekhez tartoznak az azonosítandó objektumok, valamint az érzékelő/lekérdező rendszer különböző gyártóktól is származhat, ezért különbözhetnek a működési paraméterek, protokollok. A „2” pontnál az esetlegesen a különböző gyártóktól származó rendszerelemek közötti interoperabilitási probléma merülhet fel. A „3” pont esetén alapvető probléma az, hogy a reprezentált identitás tár általában a harcjárműben nem áll rendelkezésre, hanem telekommunikációs csatornán keresztül kell lekérdezni.

4. INTEROPERABILITÁSI PROBLÉMÁK MEGOLDÁSI LEHETŐSÉGEI

Ebben a részben az előző fejezetben felmerült együttműködési nehézségek megoldási lehetőségei a különböző rendszerekben az alábbiak.

RF ID azonosítás alkalmazása esetén az „1” jelű kapcsolódási ponton a különböző gyártóktól származó rendszer elemek alkalmazásakor az egyetlen megoldási lehetőség a kapcsolódási pontok technikai és protokolláris paramétereinek szabványosítása, majd a kiválasztásra kerülő eszközöket, és a működtető szoftvereket e szabványnak való megfelelés alapján választjuk meg. A „2” pontnál a több érzékelő/lekérdező rendszer egy értékelő rendszerhez való alkalmazása esetén szintén a kapcsolódási pont átgondolt technikai és protokolláris szabványosításával oldható meg. A „3” jelzéssel rendelkező pont esetében, amikor a reprezentált identitás tár távol található az értékelő rendszertől, akkor az érzékeny adatok védett formában történő továbbítását is meg kell oldani távközlési csatornán keresztül. Ekkor valamilyen egyedi rejtjelzést alkalmaznak valamilyen szabványos adatkommunikációs protokollba ágyazva, esetleg nyilvános algoritmust alkalmaznak titkos kulccsal, vagy generált valódi véletlen kulccsal.

Biometriás azonosítás esetén, amikor a jellemzőket egy intelligens technikai eszközön kerül tárolásra, akkor ugyanazok az interoperabilitási problémák merülnek fel, mint RF ID alkalmazása esetén. Az „1” ponton ezenfelül felmerülnek az azonosítandó biometriás jellemző leolvasásával összefüggő problémák. Ilyenek az azonosítandó biometriás jellemző térbeli elhelyezkedése, és leolvasáskori állapota. Meg kell oldani, hogy a leolvasó szerkezethez csak közel azonos elhelyezkedéssel lehessen az adott jellemzővel közelíteni. Ki kell oktatni a felhasználókat a berendezés használatáról, mely során fel kell hívni a figyelmüket az adott jellemző állapotának tudatos ellenőrzésére. Itt első sorban az adott jellemző tisztaságára és sértetlenségére kell figyelni. Bizonyos biometriás jellemzők nem csak az adott jellemző fizikai sérülése esetén változik meg valamilyen mértékben, hanem az emberi test más részeinek különböző megbetegedései következtében is. Ilyen elváltozások keletkeznek a reflexzónákon, melyek gyógyítási diagnosztikai eljárások alapját képezik. Emiatt olyan matematikai leképezési eljárást kell kidolgozni, mellyel minimálisra lehet csökkenteni az azonosítás bizonytalanságát. A „2”, és a „3” pont esetében ugyanazok az interoperabilitási problémák és a megoldásaik is, mint az RF ID alkalmazásakor.

Vonalkódos azonosításnál az „1” ponton a leolvashatóságot főként a vonalkód hordozójának az anyaga, a színe, elhelyezkedése befolyásolja. Mivel a vonalkódos azonosítás széles körben elterjedt tárgyak (árúk, eszközök, berendezések...) nyilvántartására, ezért sokféle anyagú, és színű hordozón található vonalkódot, valamint léteznek automatikus, illetve kézi leolvasó rendszerek, ezek megnehezítik a kód sikeres leolvasását. A leolvasási probléma csökkentése érdekében több, egymással különböző szöveget bezáró leolvasó egységet integrálnak egy olvasó fejbe, így javítva a sikeres leolvasás valószínűségét. Főként automatikus rendszerek esetén törekszenek a csomagolási egységek, és az azokon szereplő vonalkódok elhelyezkedésének szabványosítására, így segítve a leolvasás pozicionálását. A másik jelentős probléma a kódgenerálás, hiszen tetszőlegesen sok, egymástól független szervezetnél, és helyen állítanak elő vonalkódot. Amennyiben ezeket egy rendszerben kívánjuk feldolgozni, akkor vagy sikerül az eredeti kóddal integrálni rendszerünkbe egyszerűen felvéve azt, vagy ha már ugyanazon kódhoz mást rendeltünk rendszerünkben, akkor újra kell kódolnunk az integráláshoz. Természetesen saját kódrendszert is kialakíthatunk.

*Idegen-barát felismerő rendszer*nél az „1” pontnál szervezeti interoperabilitási problémák feloldása komoly szervezési és bizalmi problémát jelent. Ez a probléma több nemzetiségű haderő együttes bevetése kapcsán merült fel igazán élesen, hiszen olyan rendszer kialakítására volt szükség, mely egyszerre kielégíti a nemzeti egységek adatainak egyedi, nemzetbiztonsági szempontokat, megvalósító védelmét, és a szövetséges egyértelmű csapatok azonosítását. A különböző gyártóktól származó rendszerelemek együttműködése a szövetségen belüli szabványosítással oldható meg, mely részletesen leírja a technikai, a protokolláris, és a szervezeti adatok feltöltési rendszerét. A „2” pontnál a különböző gyártóktól származó rendszerelemek közötti interoperabilitási probléma az adott szervezeten belüli szabványosítással oldható meg. A „3” pontnál a reprezentált identitás távoli elhelyezkedése következően a védett távközlés problémáját kell a szervezeten belül megoldani.

ÖSSZEFOGLALÁS

Napjainkban, mikor az információs társadalomba való átmenet korszakát éljük, életünk minden területét behálózzák a különböző informatikai rendszerek, adatainkat számtalan adatbázisban tartják nyilván, mozgásunk során különböző beléptető rendszereken haladunk át, távközlési-, és banki szolgáltatásokat veszünk igénybe gyakorlatilag földrajzi megkötöttség nélkül. Ezeket a korábban elképzelhetetlen szabadságot, adó szolgáltatásokat egyebek mellett a különböző azonosítási módszerek és rendszerek, és a különböző rendeltetésű rendszerek összekapcsolásai tették lehetővé. Ezek az összetett rendszerek igen komoly feladatok elé állították a szakembereket, hogy az információs rendszerek integrálásával egy időben megőrizhessék az információk bizalmasságát, az informatikai rendszerek biztonságát.

Ebben a cikkben először összegeztem az azonosítás, és az interoperabilitás fogalom rendszerét. Az azonosítás rendszermodelljét elemezve azonosítottam az interoperabilitási szempontból fontos kapcsolódási pontokat. Ezt követően néhány jellemző azonosítási módszer esetében megállapítottam az interoperabilitási problémákat, melyekhez a cikk végén megadtam a lehetséges megoldási lehetőségeket. A munka során az azonosítási rendszerek interoperabilitási elemzéséhez teremtettem meg az alapokat, hogy az azonosítást biztosító technikai eszközök további kutatásához kiépítendő szempont rendszer részét képezze.

FELHASZNÁLT IRODALOM

- Dr. Munk Sándor (2002): An analysis of basic interoperability related terms, system of interoperability types; AARMS Volume 1. Issue 1.
- Dr. Munk Sándor (2004): Role of semantic interoperability in warfare of our age; AARMS Volume 3. No. 4.
- Dr. Munk Sándor (1992): Az informatika eszközzrendszere; ZMNE jegyzet, (J-1082), Budapest.
- Dr. Munk Sándor (2003): Katonai informatika III, A katonai informatika eszközzrendszere; ZMNE jegyzet, Budapest.