SZÁMHORDOZHATÓSÁGI KÖZPONTI REFERENCIA ADATBÁZIS

TANULMÁNY
A HÍF számára

Készítette:
A Budapesti Műszaki Egyetem
Távközlési és Telematikai Tanszékének
munkacsoportja

Adamis Gusztáv
Csopaki Gyula
Gajdos Sándor

Budapest, 2003. február

Tartalom

1. Bevezető

1.1. A számhordozhatósági központi referencia adatbázis koncepciója

A *számhordozhatósági központi referencia adatbázis* (KRA) a hordozott számokkal kapcsolatos információkat tárolja. Ezek az információk elsősorban a hordozott szám és az ezt a számot éppen kiszolgáló hálózat azonosítása közti kapcsolatot rögzítik, a hívások irányításában a KRA nem vesz részt. A hívások irányítása a szolgáltatók által működtetett *szolgáltatói (üzemi) hívásirányítási adatbázisok* felhasználásával történik.

A KRA nem csupán egy szűken értelmezett adatbázis, amely valamely adatokat meghatározott formában megbízhatóan tárol, hanem az adatokon műveleteket végző funkciók (adatbázis alkalmazás(ok)) rendszere is. A kettőt csak együtt van értelme vizsgálni, azoknak egy konzisztens *információs rendszert* kell alkotniuk.

Több országban is fejlesztenek vagy már létre is hoztak számhordozhatósági központi referencia adatbázist a számhordozás támogatására. Ilyen országok például Finnország, Hollandia, Németország, Norvégia, Hong Kong és az Amerikai Egyesült Államok.

A számhordozhatósági központi referencia adatbázis fontosabb céljai a következők:

1. ha két szolgáltató megállapodik egy számhordozásról, ne nekik kelljen minderről értesíteni a többi szolgáltatót, hanem a változás időpontját és a hordozott számokkal kapcsolatos egyéb járulékos információkat egy központi - minden szolgáltató számára referenciaként szolgáló - adatbázisban minden szolgáltató elérhesse,
2. ha valamely szolgáltatónál megsemmisül az adatbázis, akkor az adatok pótolhatók legyenek,
3. ha megjelenik a piacon egy új szolgáltató, a számhordozhatósági központi referencia adatbázis tudja nyújtani számára a más szolgáltatók között eddig megtörtént hordozásokról az irányítási információkat.

A szolgáltatói adatbázisok a számhordozhatósági központi referencia adatbázisban tárolt információk másolatait tartalmazzák, vagyis az irányításhoz a nemzeti adatbázisban tárolt információkat veszik igénybe – közvetett módon. A számhordozhatósági központi referencia adatbázis és a szolgáltatói adatbázisok ilyen megkülönböztetése azért fontos, mivel

- a számhordozhatósági központi referencia adatbázisnak kis gyakorisággal előforduló ügyleteket kell támogatnia (adatok fel- és letöltése),
- a szolgáltatói adatbázisnak nagy mennyiségű ügyletet kell támogatnia (irányítás),
- a szolgáltatói adatbázis teljesítménye meghatározó egy hálózatüzemeltető szolgáltatásának minőségére nézve, és minden esetben az adott szolgáltató ellenőrzése alatt áll.

A számhordozhatósági központi referencia adatbázis hiányában

- az átvevő szolgáltatónak valamilyen más mechanizmusra lenne szüksége ahhoz, hogy egy szám továbbviteléről tájékoztassa a többi szolgáltatót;
- nem lenne egységes és teljes nyilvántartás a hordozott számokról, ami egy új szolgáltató belépését, illetve az üzemi adatbázisának létrehozását megnehezítené, adott esetben ellehetetlenítené.

A fentiek miatt jelen tanulmányunkban feltételezzük, hogy a számhordozási adatbázis központi és nem elosztott jellegű.

1.2. Adottságok

A számhordozhatóság megvalósításának kereteit néhány körülmény és az ezeket tükröző dokumentumok 2003. elejére alapvetően meghatározták. Ezek közül a legfontosabbak:

1. Hírközlési törvény (Hkt), különösen a 18. § (1) valamint 106. § (6) [1],
2. Kormányrendelet tervezet a számhordozhatóság alkalmazásának szabályairól [2],
3. A szolgáltatók egyeztetett javaslata a hazai számhordozhatóság megvalósításának egyes kérdéseiről (2002. júl. 26.) [[3]]

Azt az általános szempontrendszert, amely a műszaki megoldás kialakítását alapvetően meghatározza, [3] foglalja össze:

1. feleljen meg az EU szabályoknak,
2. legyen versenysemleges,
3. nemzetközi szabványokon alapuljon,
4. minél kevesebb Magyarországra specifikus kiegészítést tartalmazzon,
5. legyen egyaránt alkalmas a földrajzi, nemföldrajzi és mobil számok hordozásának támogatására,
6. költségkímélő legyen, azaz ne tartalmazzon átmeneti megoldásokat és az igényeknek megfelelő ütemben fokozatosan kiépíthető legyen.

1.3. A számhordozás elvi folyamatai

Egy telefonszám hordozásának két szakasza van:

1. a szám átadása az átadó szolgáltatótól az átvevő szolgáltatónak,
2. a többi szolgáltató tájékoztatása a szám átadásáról.

A számhordozás folyamatát az előfizető kezdeményezi az 1. szakaszban, amikor az igényét bejelenti az átvevő szolgáltatónál. Eközben ugyanott előfizetői szerződést kell kötnie. A számhordozás megvalósulása érdekében az átvevő szolgáltató köteles eljárni az átadó szolgáltatónál és végrehajtani az ehhez szükséges lépéseket. Az átvevő szolgáltató 3 munkanapon belül értesíti az igényről az átadó szolgáltatót, aki további 3 munkanapon belül válaszol a megkeresésre és jóváhagyja vagy elutasítja a kérést. Az előfizetőt az igénybejelentéstől számított 8 munkanapon belül kell értesíteni az átadásra felajánlott időpontokról és időablakokról, melyek közül az előfizető választhat. Az időablak hossza nem lehet több 12 óránál. A teljesítés időpontja nem lehet későbbi, mint az igénybejelentéstől számított 15 nap, hacsak az előfizető ezt nem kéri. [2]

A számhordozhatósági központi referencia adatbázis megléte a második szakaszban elengedhetetlen. Az átvevő szolgáltató (ld. [2] 8.§ (3)) a hordozás folyamata során "frissíti a referencia adatbázist". A frissítés eredményeként a többi szolgáltató képes lesz arra, hogy hozzájusson a számhordozási információkhoz. Ennek érdekében minden szolgáltató rendszeres időközönként, például naponta (vagy akár naponta többször, például a számátadási időablakok végén) kapcsolatba lép az adatbázissal, melynek eredményeként olyan naprakész információkat kap, melyeket saját üzemi adatbázisának frissítésére használ.

Megjegyzések:

1. A [8], [10] tanulmány írásakor még az volt az elképzelés, hogy a számhordozhatósági központi referencia adatbázis egyik fő funkciója lesz a számhordozási folyamat szolgáltatók közötti ügyintézésének támogatása is. A HÍF szakértőivel történt konzultáció során kapott információ alapján [4] **azóta eldőlt, hogy a számhordozhatósági központi referencia adatbázisnak semmiképp nem kell a számhordozási folyamat szolgáltatók közötti ügyintézését támogatnia** (azaz az 1. fázist), erre a szolgáltatóknak más csatornákat kell kialakítaniuk.
2. A hívások irányításán túlmenően az KRA információira számlázási célból is szükség lehet. Ennek segítségével kívánja a HÍF meghatározni azt az összeget, amelyet az átvevő szolgáltatónak kell fizetnie a szám használatáért, illetve azt a díjvisszatérítést, amely a számblokk szolgáltatót illeti.
3. Jelen tanulmány írásának időpontjában még nem ismert, hogy az átvevő szolgáltató pontosan milyen adattartalommal (bár ennek egy minimumhalmaza természetesen ismert), milyen gyakorisággal/milyen feltételek mellett és milyen szabályok szerint (protokoll) frissíti a referencia adatbázist. Úgyszintén hasonló megállapításokat lehet tenni a KRA lekérdezésére. Ezeket a kérdéseket [2] nem specifikálta, hanem a HÍF hatáskörébe utalta. Így jelen tanulmány arra korlátozódik, hogy szempontokat fogalmazzon meg ezeknek a nyitott kérdéseknek a lehető legjobb megválaszolásához, illetve esetenként feltételezésekre is kellett építeni.
4. A [2] tervezet egy átmeneti szabályozást is meghatároz a számhordozás folyamatára, amely terv szerint 2004. jan. 1-jéig marad érvényben. Jelen tanulmány az átmeneti szabályozás kérdéseivel nem foglalkozik.

1.4. A számhordozhatósági központi referencia adatbázis kiterjesztései

A számhordozási központi referencia adatbázis a hordozott számok adatait tartalmazza. Azonban ez az adatbázis más funkciók ellátására is kiterjeszthető, illetve a számgazdálkodással kapcsolatos egyéb (például hatósági nyilvántartási) feladatot ellátó adatbázissal összekapcsolható.

Ebben a fejezetben összefoglaljuk, hogy a számhordozhatósági központi referencia adatbázis milyen további, a hívószámokkal kapcsolatos szolgáltatás, nyilvántartás megvalósításában vehet részt.

Itt három fő funkciót vizsgálunk:

1. színes számok nyilvántartása
2. hívószám adatbázis
3. hívószám kijelölési adatbázis.

Jelen ismereteink szerint a HÍF az 1. funkció megvalósítását a KRA megindulásakor illetve ahhoz nagyon közeli időpontra tervezi, míg a 2.-3. funkció a HÍF rövid távú tervei között nem szerepel, de jelenleg kizárva sincs az sem, hogy megvalósításuk hosszabb távon szükségessé válik.

1.4.1. A nemföldrajzi ("színes") számok egyedi nyilvántartása

Az egyedi számkijelölés azt jelenti, hogy a számot használatra a felhasználónak jelölik ki, aki a színes számot kiszolgáló (IN) szolgáltatók közül tetszés szerint választhat. (A kijelölés adminisztratív eljárása a KRA szempontjából irreleváns.) Mivel a színes szám nem tartalmaz semmilyen, az őt kiszolgáló szolgáltatóra vonatkozó adatot, a számhoz az őt kiszolgáló szolgáltatót ugyanolyan irányítási információval kell hozzárendelni, mint a hordozott számok esetén. Egyedi számkijelölésnél **irányítási szempontból** minden színes szám hordozott számnak tekinthető, így kézenfekvőnek tűnik a számhordozhatósági központi referencia adatbázis e célra való felhasználása is. A színes számok esetében is elsődlegesen azt kell tárolni, hogy a számot mely szolgáltatóhoz kell irányítani, hasonlóan a hordozott számokhoz. Az egyéb, járulékosan tárolandó adatok is megegyeznek a hordozott számoknál tárolandókkal vagy könnyen megfeleltethetőek egymással.

Az irányítási szám azt teszi lehetővé, hogy a hívás a színes számot kiszolgáló szolgáltató hálózatába jusson, a hívásnak a felhasználó által megadott földrajzi számon, vagy más módon történő végződtetése a színes szám szolgáltató feladata, amely a számhordozástól független. Az irányítási információt a KRA-ba a színes számot kiszolgáló szolgáltató küldi be a szám első használatba vételekor, illetve esetleges szolgáltatóváltáskor, "hordozáskor" ez az átvevő IN szolgáltató feladata lesz. Az irányítási információ mellett, a hordozott számokkal megegyező módon, a nyilvántartáshoz szükséges adatokat is tárolja a KRA, ezért a színes számok jelenlegi blokkos nyilvántartása helyett a KRA veheti át a színes számok egyedi nyilvántartásának funkcióját is.

A színes számok adatainak tárolása történhet *explicit* módon, vagyis ha az adatbázisban ténylegesen az összes lehetséges színes szám megtalálható, de történhet *implicit* módon is, amikor az adatbázis csak a ténylegesen a szolgáltatóknak kiosztott színes számok adatait tartalmazza, a ki nem osztottakét nem. Míg az első esetben az adatbázisból közvetlenül megtudható bármely szám adata, a második esetben értelemszerűen az, hogy egy szám nincs kiosztva, onnan derül ki, hogy az adatbázisban nem található. E kényelmetlenségért cserébe viszont az adatbázis mérete jelentősen kisebb lehet.

A HÍF szakértőivel való konzultáció [4] alapján tudjuk, hogy a HÍF a számhordozhatósági központi referencia adatbázist ténylegesen fel szeretné használni a színes számok nyilvántartásának céljára is, tehát **a tanulmány későbbi részében - hacsak erre másként kifejezetten nem utalunk - a számhordozhatósági központi referencia adatbázis integráns részének tekintjük a színes számok adatainak az előző bekezdésben leírt *implicit* módon történő nyilvántartását is.**

1.4.2. Hívószámok hatósági nyilvántartása - Hívószám adatbázis

A hívószám adatbázisnak alatt egy olyan adatbázist értünk, amely az összes lehetséges hívószám adatait - **a számok hatósági nyilvántartása érdekében** - tartalmazza.

A hívószám adatbázisnak a számok adatait nemcsak blokkonként, számmezőnként, hanem egyedileg is képesnek kell lennie nyilvántartani. Egy ilyen képességű adatbázis kialakítása a HÍF számára **a számok egyenkénti kijelölhetőségének bevezetésekor válik szükségessé**, a hívószámok hatósági nyilvántartása céljából.

A tárolás itt is történhet explicit és implicit módon. Az explicit módon való tárolás háttértárigénye összességében nagyon jelentős lehet, számottevő előnyei nincsenek, így a gyakorlatban itt is az implicit tárolási móddal érdemes foglalkozni.

Ez az adatbázis csak a HÍF hatósági illetve nyilvántartási feladatait segíti, tehát a szolgáltatók számára elérhetetlen kell, hogy legyen. A hívószám adatbázisnak ugyanakkor a

számkijelölésen felül a számok hordozottsági állapotát is tartalmaznia kell - szintén hatósági nyilvántartási célból. Emiatt a hívószám adatbázis és a számhordozhatósági központi referencia adatbázis között kapcsolatnak célszerű lennie.

Ez a kapcsolat alapvetően a következő módokon valósítható meg:

1. a két adatbázis egymástól független, közöttük valamilyen interfészen, adott protokoll szerint zajlik a kommunikáció és az adatcsere
2. a két adatbázis eleve egyetlen fizikai egységet alkot.

A kedvezőbb - a hasonló követelmények, kapcsolódások, gazdaságossági szempontok miatt - a 2. megoldás lenne, de a számhordozhatósági központi referencia adatbázis létrehozásának sürgető kényszere kevés esélyt ad arra, hogy egyszerre valósuljon meg a hívószám adatbázis és a számhordozhatósági központi referencia adatbázis. Áthidaló megoldás lehet, ha csak az egyik valósul meg először, de olyan feltételek mellett, ami lehetővé teszi, hogy egy átmeneti periódus után mindkét adatbázis egyetlen rendszert alkotva létrejöjjön, ami optimális feltételeket teremt a logikai konzisztenciájuk fenntartásához.

Bár jelenlegi ismereteink alapján a HÍF rövid távon nem tervezi a földrajzi és a mobil számok egyenkénti kijelölésének bevezetését, de későbbi bevezetésének szükségessége nincs kizárva sem. Ezért véleményünk szerint a számhordozhatósági központi referencia adatbázis kialakításánál azokat a megoldásokat célszerű előnyben részesíteni, amelyek nem zárják ki annak a jövőbeli, a teljes földrajzi, nemföldrajzi és mobil számok egyenkénti adatainak tárolására szolgáló alkalmazását, e célra való bővíthetőségének vagy egy ilyen adatbázishoz való későbbi illeszthetőségének a lehetőségét.

Ezért a tanulmányunkban több helyen kitérünk arra, hogy egy hívószám adatbázis mennyiben támaszt más, illetve többlet követelményeket a számhordozhatósági központi referencia adatbázishoz képest, azért, hogy további szempontokat nyújtsunk annak eldönthetősége érdekében, hogy a számhordozhatósági központi referencia adatbázis megvalósítási ajánlataiban szereplő esetleges többletszolgáltatások, opciók stb. előnyösek, hátrányosak vagy irrelevánsak a számhordozhatósági központi referencia adatbázis és a hívószám adatbázis integrálhatóságának szempontjából.

1.4.3. Hívószámok kijelölésének és visszavételének szolgáltatók felé való jelzése - Hívószámkijelölési adatbázis

A hívószámok egyedi kijelölésének bevezetésével, illetve amikor új távközlési szolgáltatók jelennek meg vagy meglévők megszűnnek, fontos értesíteni a szolgáltatókat, hogy egy szám vagy számmező használatban van-e, és ha igen, melyik szolgáltató által. Ez a probléma különösen akkor lesz számottevő, ha jelentős mennyiségű egyedileg kiosztott szám lesz (ekkor a probléma természete hasonlatos lesz a színes számokkal kapcsolatosan leírtakkal), vagy *az egyedi számkijelöléstől függetlenül* akkor is, ha a számok lekötése és visszaadása például a szolgáltatók közötti kiélezett verseny miatt viszonylag gyakorivá válik.

Az előző pontban említett hívószám adatbázisban tárolt adatok csak a hatóság számára szabad/kell, hogy elérhetők legyenek, itt azonban arra van szükség, hogy azt az adatot, hogy egy szám ki van-e osztva és kinek, a szolgáltatóknak is el kell tudniuk érni. Ez az információ természetesen elérhető a hívószám adatbázisban, tehát a megfelelő adatokon képezett publikus másolat (vagy nézet) lehet a szolgáltatók informálásának alapja, megvalósítható független adatbázisként vagy a KRA részeként, mivel a megvalósítás elve hasonló lehet a

színes számok esetében alkalmazotthoz, a lényegi eltérést csak a méretbeli (tárolandó számok darabszáma közötti nagyságrendbeli) eltérés jelent.

A későbbiekben **hívószám kijelölési adatbázisnak** fogjuk hívni azt az adatbázist, vagy a hívószám adatbázisnak azt a másolatát (nézetét), amelyből a szolgáltatók lekérdezhetik, hogy egy adott hívószám ki van-e osztva és ha igen, mely szolgáltatónak.

A hívószám kijelölési adatbázis tehát arra szolgál, hogy amikor a távközlő hatóság hívószámokat oszt ki a szolgáltatók között, vagy ha a szolgáltatók korábban használt számokat visszaadnak, ezt a hatóság a hívószám adatbázis segítségével teszi közzé minden érintett számára. Így a hívószám kijelölési adatbázisban figyelemmel kísérhető, hogy mely számok és mely szolgáltatóknak vannak kiosztva. Természetesen, a számok felhasználásának ténye egyenként vagy nagyobb egységekben egyaránt bejegyezhető.

Mindenképpen megfontolandónak tartjuk - bár ez a HÍF jelenlegi tervei között ismereteink szerint nem szerepel -, hogy ha a színes számok hasonló jellegű adatainak tárolására és ezek szolgáltatók számára hozzáférhetővé tételére a számhordozhatósági központi referencia adatbázist használjuk, akkor annak kialakításakor legalábbis ne zárjuk ki annak a lehetőségét, hogy a későbbiekben a számhordozhatósági központi referencia adatbázis hívószám kijelölési célra is bővíthető, átalakítható legyen.

2. Kiindulási peremfeltételek

Ebben a fejezetben gyűjtöttük össze a rendelkezésünkre álló forrásokból és információkból mindazokat az alacsonyabb szintű funkciókat, korlátozásokat, feltételeket, amelyek szükségesek ahhoz, hogy a számhordozás funkciója logikailag megvalósítható és teljes legyen.

1. **Hordozott számok beírása és idősoros tárolása:** Ehhez az átvevő (!) szolgáltató köteles a KRA üzemeltetője részére a hordozott számokat és az azokhoz tartozó irányítási információkat megküldeni. [2] 8.§
2. **Hitelesítés:** A fogadott és küldött adatoknak minősített elektronikus aláírással hitelesítettnek kell lenniük, valamint a hitelesítést ellenőrizni kell. [5]
3. **Hordozható számok:** Az előfizető az átadó szolgáltatónál fennálló előfizetői szerződésében szereplő számokra vagy azok egy részére kérheti a számhordozást. [2] 6.§ Ennek a követelménynek az ellenőrzését a KRA nem tudja biztosítani, csak legfeljebb - bizonyos, később részletezendő feltételek mellett - azt tudja ellenőrizni, hogy a hordozni kívánt szám valóban az átadó szolgáltató tulajdonában/használatában van-e, illetve szükség esetén ahhoz tud segítséget nyújtani, hogy az átadó szolgáltató azt tudja ellenőrizni, hogy a KRA-ba bekerült, eddig általa kiszolgált számokra engedélyezte-e a hordozást.
4. **Adatlekérdezés biztosítása illetve adattartalom változás jelzése:** Az adatlekérdezés lehetősége legyen folyamatosan biztosított, továbbá a KRA alkalmazás - szerver-kliens modellben történő megvalósítás esetén - az adatbázis tartalmának változásakor meghatározott időben illetve feltételek teljesülése esetén a szolgáltatót értesítheti (üzenet formájában) az őt érintő változás bekövetkeztének tényéről, de a megváltozott adatokról nem. [5]
5. **Teljes adatlekérdezés biztosítása:** Ilyenkor a szolgáltató hozzájut az őt érintő teljes, pillanatnyilag érvényes számhordozási adathalmazhoz (azaz a lekérdezés időpontjában hordozott számok listájáról), de annak históriájához nem. [8] [10]
6. **Különbségi ("delta") adatlekérdezés biztosítása:** Ilyenkor a szolgáltató csak azokhoz az adatokhoz jut hozzá, hogy egy előző időpillanat óta a hordozott számok között milyen változás következett be (azaz mely, az előző időpillanatbeli lekérdezéskor nem hordozott számok váltak azóta hordozottakká, mely, az előző időpillanatbeli lekérdezéskor hordozott számok váltak azóta nem hordozottakká [az eredeti számblokk szolgáltatóhoz való visszahordozás illetve előfizetői szerződés megszűnése miatt], mely, az előző időpillanatbeli lekérdezéskor hordozott számok váltak azóta továbbhordozottakká. Ha a két időpont között egy szám hordozottsági állapota többször is változott, de a "kezdő" illetve "vég" időpontban az őt kiszolgáló szolgáltató azonos - például a számot az eltelt időszakban elhordozták, de utána visszahordozták - az a "delta" lekérdezéskor nem jelenik meg. Ha a két időpont között egy szám többször is hordozásra kerül, akkor a "delta" lekérdezéskor a "közbülső lépcső(k)" nem jelenik/jelennek meg, csak a végállapot.). Várhatóan a KRA tipikus használati módja ez lesz. [8] [10]
7. **Továbbhordozás biztosítása:** Az előfizető jogosult a hordozott számot más szolgáltatóhoz tovább hordozni, beleértve bármely előző szolgáltatót. Két hordozás közötti idő nem lehet rövidebb 30 napnál. [2] 6.§ Ugyan itt expliciten nem jelenik meg, de a "bármely előző szolgáltató körébe" az eredeti számblokk szolgáltató is beletartozik. Ha a szám ehhez a szolgáltatóhoz kerül vissza, akkor hordozottsága megszűnik, adata "kikerül" a KRA-ból, de "delta" lekérdezéskor ezt a tényt közölni kell.

8. **Az időablak méretének korlátozása:** a szám átadására kijelölt időablak nem lehet több 12 óránál. [2] 7§
9. **Kiválasztott időablak tárolása:** Az előfizetői igény bejelentését követő 8 munkanapon belül az átvevő szolgáltató tájékoztatja az előfizetőt a szám átadására felajánlott időpontokról és számátadási időablakokról, melyek közül az előfizető választhat. [2] 7.§ A választás eredménye az átvevő szolgáltatótól származó információ alapján belekerül a KRA-ba.
10. **Naplózás:** a KRA minden adattárolási, módosítási, törlési és olvasási műveletet nyilvántart. [2] 8.§
11. **Előfizetői szám használati jogának megváltozása:** amennyiben az előfizető szolgáltatót változtat, a hordozott előfizetői szám használati joga az átvevő szolgáltatóhoz kerül és az átadó szolgáltatónál megszűnik. Ld. [2] 11.§ Ez a funkció szoros kapcsolatot teremt a számhordozhatósági központi referencia adatbázis és a hívószám adatbázis között.
12. **A hordozás megszűnése előfizetés megszűnése miatt:** Amennyiben a hordozott számra vonatkozó előfizetői szerződés megszűnik, a szabaddá váló előfizetői szám használati joga visszakerül ahhoz a szolgáltatóhoz, amelynek a hordozott számot a hatóság eredetileg kijelölte. A hordozott számra vonatkozó előfizetői szerződés megszűnéséről a szolgáltató köteles a KRA-t értesíteni. [2] 11.§ Ha az adott számra vonatkozó előfizetői szerződés megszűnik, akkor a szám hordozottsága is megszűnik, adata “kikerül” a KRA-ból, de “delta” lekérdezéskor ezt a tényt közölni kell.
13. **A számhordozási história elérésének korlátozása:** csak meghatározott magasabb jogosultság birtokában lehessen a számhordozási históriához hozzáférni, ehhez a szolgáltatók ne férhessenek hozzá [4]
14. **Számhordozási segédadatok tárolása:** derüljön ki a számhordozásról történt megállapodás ideje is és a számhordozás tényleges megvalósításának ideje is a KRA-ból [4]
15. **Nagyon régi adatok archiválása:** felesleges az adatbázist terhelni a teljes számhordozási históriával, adott időnél régebbi adatok másodlagos tárra menthetők [4].
16. **Archív adatok közötti keresés:** Az üzemi adattartalom veszélyeztetése nélkül legyen lehetőség az archív adatok visszatöltésére, az adatokban történő keresésre. [5]
17. **Számhordozási folyamat támogatása:** A számhordozhatósági központi referencia adatbázisnak nem kell a számhordozási folyamat szolgáltatók közötti ügyintézését támogatnia, erre a szolgáltatóknak más csatornákat kell kialakítaniuk. [2] [5]
18. **Számlázás támogatása:** A KRA támogassa a hordozott számok után fizetendő díj illetve díjvisszatérítés hiteles meghatározását, HÍF a számlázó rendszerével való összekapcsolhatóságot. A KRA adatbázisból minden számlázás alkalmával (manuális indítással) fájl formátumban a következő adatokat kell átadni a HÍF számlázó SAP programja számára: Minden KRA rekordból 2 rekordnak kell keletkeznie az alábbi szerkezettel: Átadó szolgáltató kód, hívószám, a hordozás időtartama, tranzakciókód, Átvevő szolgáltató kód, hívószám, a hordozás időtartama, tranzakciókód. [5]
19. **Hordozott számok kötegelt kezelése számtartomány átadás esetén:** - Ha a számtartomány átkerül egy másik szolgáltató tulajdonába, akkor a KRA-nak képesnek kell lennie az ebbe a számtartományba eső hordozott számok problémáját "kötegelve" kezelni. Ez a következőket jelenti:
    - Az ebben a számtartományban szereplő hordozott számoknál a tulajdonos mezőt át kell írni az új blokkszolgáltatóra.

- Az ebben a számtartományban, az új blokkszolgáltatóhoz eddig érvényben levő hordozott számokat érvényteleníteni kell (hiszen ettől kezdve ezek már nem hordozott számok).
- A régi blokkszolgáltató által megadott továbbra is nála maradó, élő számokat (lista) hordozott számként fel kell venni a KRA-ba, mert innentől kezdve ezek hordozott számok lesznek (a tulajdonos az új blokkszolgáltató).

Ennek a funkciónak a speciális esetei a következõk:

- A) A blokkszolgáltató visszaadja a számtartományt a HÍF-nek (mert már nincs nála élõ szám), de a tartományban vannak hordozott számok. Ebben az esetben az új tulajdonos nem egy szolgáltató, hanem a HÍF lesz és nem lesz olyan szám a tartományban, ami eddig az "új szolgáltatóhoz" (HÍF) tartozott volna, illetve olyan szám sem lesz, ami a régi szolgáltatónál élõ marad (azaz a 2. és 3. lépéseket nem kell elvégezni).
- B) Egy adott számtartomány blokkszolgáltatója megszûnik. Ebben az esetben az A) pontban leírt eljárást a megszûnt szolgáltató valamennyi számtartományára el kell végezni.
- C) A fenti két eset folytán a HÍF tulajdonába került számtartomány újbóli kiadása. Ebben az esetben nem lesz olyan szám, ami a "régi szolgáltatónál" (HÍF) élõ marad (azaz a 3. lépést nem kell elvégezni).

Természetesen a fentieket a díjszámítás során is kezeleni kell. A fentiek törvényi/szabályozási háttere még nem tisztázott, azonban a KRA-t fel kell készíteni erre, különösen a B) speciális eset miatt. [5]

Mivel a HÍF tervei között szerepel a színes számok egyenkénti nyilvántartása a KRA segítségével, a következőkben összeállítottuk azokat a követelményeket, amelyek a színes számok KRA általi tárolásához véleményünk szerint nélkülözhetetlenek. Mivel ezen hívószámok szolgáltatókhoz történő egyedi hozzárendelésének részletesebb követelményei és folyamata még nem ismertek, erre vonatkozóan - ismereteink szerint - még nincsenek rendelettervezetek, belső szábályozási tervezetek stb, így ezzel a felsorolással - többek között - ezek jövőbeli kialakításához is támpontokat szeretnénk nyújtani.

1. **Színes számok beírása és idősoros tárolása:** Ezeket az adatokat a hatóság (HÍF) állítja elő és juttatja el a KRA-ba a szám kiosztásakor/visszavételekor. Az adatbázis a hívószámhoz hozzárendelten tárolja, hogy melyik szolgáltatóhoz tartozik jelenleg a hívószám használati joga.
2. **Hitelesítés:** A fogadott és küldött adatoknak minősített elektronikus aláírással hitelesítettnek kell lenniük, valamint a hitelesítést ellenőrizni kell.
3. **Naplózás:** a színes számokra vonatkozó minden adattárolási, módosítási, törlési és olvasási műveletet szintén nyilván kell tartani.
4. **Színes szám megszűnése:** Amennyiben a színes számra vonatkozó szerződés megszűnik, a szám szabaddá válik és ezt a tényt az adatbázisnak rögzítenie kell.
5. **A színes szám históriája elérésének korlátozása:** csak meghatározott magasabb szintű jogosultság birtokában lehessen a históriához hozzáférni.
6. **Segédadatok tárolása:** derüljön ki például a színes szám használatára vonatkozó megállapodás ideje is és a színes szám bekapcsolásának ideje is a KRA-ból.
7. **Teljes adatlekérdezés biztosítása:** Ilyenkor a szolgáltató hozzájut a teljes, pillanatnyilag használt színes szám adathalmazhoz (azaz a pillanatnyilag használatban lévő színes számok listájához), de annak históriájához nem.

8. **Különbségi (“delta”) adathozzáférés biztosítása:** Ilyenkor a szolgáltató csak azokhoz az adatokhoz jut hozzá, hogy egy előző időpillanat óta a színes számok között milyen változás következett be (azaz mely, az előző időpillanatbeli lekérdezéskor nem használt színes számok váltak azóta használtakká, mely, az előző időpillanatbeli lekérdezéskor használt színes számok váltak azóta nem használtakká, mely, az előző időpillanatbeli lekérdezéskor egy szolgáltató által használt színes számok kerültek át más szolgáltatókhoz. Ha a két időpont között egy szám használtsági állapota többször is változott, de a “kezdő” illetve “vég” időpontban az őt kiszolgáló szolgáltató azonos vagy a szám az egyik időpillanatban sincs használva - az a “delta” lekérdezéskor nem jelenik meg. Ha a két időpont között egy színes szám többször is “hordozásra” kerül, akkor a “delta” lekérdezéskor a “közbülső szolgáltató(k)” nem jelenik/jelennek meg, csak a végállapot.)
9. **Nagyon régi adatok archiválása:** adott időnél régebbi adatok másodlagos tárra menthetők.
10. **Archív adatok közötti keresés:** Az üzemi adattartalom veszélyeztetése nélkül legyen lehetőség az archív adatok visszatöltésére, az adatokban történő keresésre. [5]
11. **Színes számok “hordozási folyamatának” támogatása:** A számhordozhatósági központi referencia adatbázisnak nem kell támogatnia a színes számok használati joga szolgáltatók közötti átadásának (a színes szám “hordozásának”) szolgáltatók közötti ügyintézését, erre a szolgáltatóknak más csatornákat kell kialakítaniuk.
12. **Számlázás támogatása:** A KRA támogassa a színes számok után fizetendő díj hiteles meghatározását, HÍF a számlázó rendszerével való összekapcsolhatóságot. Itt opcionálisan arra is legyen mód, hogy a KRA a különböző típusú színes számok használati “egységárát” is tárolni tudja. [5]
13. **Színes számok kötegelt kezelése számtartomány átadás esetén:** - Ha a számtartomány átkerül egy másik szolgáltató tulajdonába, akkor a KRA-nak képesnek kell lennie az ebbe a számtartományba eső színes számok problémáját "kötegelve" kezelni.

3. Funkcionális követelmények

Az előző fejezetbeli megállapításokat összefoglalva és azokat továbbgondolva, ebben a fejezetben összegyűjtjük azokat a legmagasabb szintű funkciókat, amiket a legszűkebben értelmezett (tehát **csak a hordozott számokat és a kiosztott színes számokat tartalmazó**) számhordozhatósági központi referencia adatbázisnak teljesítenie kell:

1. A hordozott számok / kiosztott színes számok adatainak tárolása minden szolgáltató számára elérhető formában (nyilvános adatok)
    - az adatbázis nyilvános részét minden szolgáltató olvashassa
    - a hordozott számokat az átvevő szolgáltatók az adatbázisnak megadhassák
    - az adatbázis nyilvános részét a KRA üzemeltetője is módosíthassa
    - az adatbázisba való íráskor a jogosultságot szigorúan ellenőrizni kell
    - az adatbázisból való olvasás jogosultságát is ellenőrizni kell
    - az adatbázis olvasásakor biztosítani kell a teljes nyilvános adattartalom letöltését és a "delta" lekérdezést is (várhatóan az egy/(néhány) napos "delta" lekérdezés lesz a tipikus olvasási forma)
    - legyen meg az a lehetőség, hogy a KRA - meghatározott időnként - például naponta maximum egyszer - üzenetben értesíthesse a szolgáltatókat, ha az adatbázis nyilvános részében változás állt be. Ez az üzenet ugyanakkor csak a változás tényét jelezze, de magukat a megváltozott adatokat ne tartalmazza. (Azokhoz célszrűen egy, az üzenet vételét követő, megfelelő "delta" lekérdezéssel lehet hozzájutni.)
2. A hordozott számok / kiosztott színes számok adataihoz egyéb, a szolgáltatók számára még csak nem is olvasható adatokat lehessen társítani (nemnyilvános adatok)
    - a nem nyilvános adatok írása csak a KRA üzemeltetője által történhessen
    - a nem nyilvános adatokat más, például jogszabályban erre feljogosított felhasználók olvashassák. A jogosultságot ellenőrizni kell.
    - A fentiek megvalósításához minimálisan háromféle adatbázis hozzáférési jogosultságot kell megvalósítani.
3. Számlázás támogatása
4. Hordozott számok kötegelt kezelésének támogatása számtartomány átadás esetén
5. Minden, az adatbázisban végzett műveletet naplózni kell
    - a napló ne csak a szűken vett adatbázisműveleteket tartalmazza, hanem a KRA, mint rendszer műveleteinek naplózása is szükséges (például rendszerindítás, -leállás, sikeres/sikertelen bejelentkezés stb.)
    - a napló tartalma ne legyen módosítható
    - a napló olvasására a szolgáltatók nem jogosultak, csak a KRA üzemeltetője és az egyéb, erre feljogosított felhasználók
    - adott időnél régebbi adatok háttértárra való mentését lehetővé kell tenni (archiválás)
    - az üzemi adattartalom veszélyeztetése nélkül legyen lehetőség az archív adatok visszatöltésére, az adatokban történő keresésre

A fenti funkciók megvalósítása megfelelő biztonsággal kell történjen. A biztonsági szint szempontjainak meghatározásához a következő tényekből lehet kiindulnunk.

1. Mivel a KRA-nak hiteles számlázáshoz segítséget kell nyújtania, ezért az adatbázisba való írás jogosultságát a legszigorúbban ellenőrizni kell
2. Mivel az adatbázis nem tartalmaz minősített adatokat, sőt, nyilvános részének adatai több szolgáltatónál tipikusan nem különösen védett helyen is hozzáférhetők, az adatbázis jogosulatlan olvasása a jogosulatlan írásnál sokkal kisebb kockázatot jelent.
3. Az adatbázisban tárolt adatok pótlása adatvesztés, -sérülés esetén különösen nehéz, ha egyáltalán lehetséges (a nyilvános adatok elvileg a szolgáltatóktól reprodukálhatók, de a nemnyilvános adatok nem), ezért az adattartalom biztonságos helyen való duplikálása kifejezetten célszerű.
4. Rendelkezésre állás tekintetében nincs különleges követelmény. Az adatbázis elérhetetlensége esetén ugyanis "csak" annyi történik, hogy az alatt az idő alatt nem lehet új hordozást bejelenteni, illetve már bejelentett hordozás adatait letölteni. Mivel a hordozások napi száma - még "pesszimista" becslés esetén is - általában legfeljebb százas nagyságrendű lesz, ezért egy esetleges egy-néhány napos elérhetetlenség nem látszik kritikusnak. Ez a kockázat tovább csökkenthető, ha a hordozás lebonyolításának (későbbiekben kidolgozandó) szabályai bizonyos tartalékidőt is tartalmaznak.
5. Az üzemi adatbázis megsemmisülése esetén is - véleményünk szerint a 4. pontban részletezettek analógiájára - elég annak a feltételeit megteremteni, hogy a duplikátumból néhány nap - hét időtartam alatt újra felépíthető legyen a rendszer.

4. Technikai követelmények

A számhordozhatósági központi referencia adatbázis gyakorlati kialakítása során figyelembe kell venni a jelenlegi technikai adottságokat is. Ezek közül csupán azt fogjuk feltételezni, hogy a szolgáltatók valamely bérelt vagy kapcsolt vonalon megvalósított adatkapcsolatot képesek kialakítani a KRA-val és ennek érdekében az ő oldalukon alkalmas programo(ka)t telepítenek. Mivel az is előfordulhat, hogy egy kezdeti időszakban még ezek az egyszerű feltételek sem állnak fenn, átmeneti megoldásként a (kis mennyiségű) adatoknak papíros alapú mozgatása, és az adatoknak a KRA működtetőjének operátora általi bevitele is elképzelhető.

4.1. Adatstruktúrák, adatbázis méretek

Először azt kell eldönteni, hogy milyen adatok szerepeljenek az adatbázisban. A korábbi fejezetek alapján kétféle lehetőség merül fel:

- a nemzeti referencia adatbázis kizárólag csak a - várhatóan néhány ezres nagyságrendű - hordozott számok, illetve a kiosztott színes számok adatait tartalmazza, vagy
- a teljes földrajzi, nemföldrajzi és mobil számtartomány adatait is.

A HÍF szakértőivel való konzultáció alapján [4] jelenleg elsősorban arra van igény, hogy a központi referencia adatbázis csak a valóban hordozott számokat, illetve az ún. színes számok adatait tartalmazza.

Azonban ebből kiindulva is feltétlenül figyelembe kell még venni, hogy

- bizonyos funkciók megvalósításához (például ellenőrzési lehetőség kialakítása szolgáltatói adatkapcsolat esetén - lásd részletesen később) a kiosztott számok nyilvántartására akkor is szükség van, ha a központi referencia adatbázist csak a számhordozás nyilvántartására akarjuk használni,
- másrészt, legkésőbb az egyedi számkijelölés lehetőségének a bevezetésénél szükség lesz egy olyan adatbázis kialakítására is, amely a teljes számtartományt egyedi számonként is nyilvántartani képes (hívószám adatbázis),
- harmadrészt, szintén elsősorban az egyedi számkijelölés bevezetésekor, (de ettől függetlenül is) szükség lehet egy olyan adatbázis funkcióra, amelyből a szolgáltatók megtudhatják, hogy egy adott hívószám ki van-e osztva, és ha igen, mely szolgáltatónak (hívószám kijelölési adatbázis)
- negyedrészt, mivel e két utóbbi adatbázis fizikai megvalósítása, követelményrendszere nem áll túlságosan távol a számhordozhatósági központi referencia adatbázisétól (sőt a hívószám adatbázis funkcionalitása teljesen analóg a színes számok adatbázisáéval),

ezért ebben a fejezetben két esetet vizsgálunk meg részletesen.

A 4.1.1 fejezetben javaslatot teszünk az adatbázisban tárolandó adatokra illetve becslést adunk az adatbázis ilyen adatstruktúra használata mellett kiadódó méretére abban az esetben, ha az adatbázis csak a hordozott számok valamint a kiosztott színes számok adatait tartalmazza. Ezek az információk lesznek relevánsak a KRA indításakor.

A 4.1.2 fejezetben azonban javaslatot teszünk az adatbázisban tárolandó adatokra illetve becslést adunk az adatbázis ilyen adatstruktúra használata mellett kiadódó méretére abban az esetben is, ha az adatbázis nem csak a hordozott számok valamint a kiosztott színes

számok adatait tartalmazza, hanem hívószám és hívószám kijelölési adatbázisként is funkcionál. **Ez utóbbi két funkció megvalósítása a HÍF jelenlegi tervei között nem szerepel**, de a számítások támpontot adnak arra vonatkozóan, hogy a későbbi esetleges bővítés milyen plusz erőforrásokat igényelhet.

Mielőtt a javaslatainkat megtennénk, illetve a számításokat elvégeznénk, két, későbbiekben használt fogalmat definiálunk.

A számhordozhatósági központi referencia adatbázis adattartalma, annak megfelelően, hogy az adatbázis használatára jogosult szolgáltatók hozzáférhetnek-e vagy sem, alapvetően két részre osztható: nyilvános és nemnyilvános részre. A továbbiakban az adatbázis *nyilvános részének* fogjuk hívni azokat az adatokat, amelyekhez az adatbázis használatára jogosult szolgáltatók hozzáférhetnek, míg *nemnyilvános résznek* azokat az adatokat, amelyekhez a fenti szolgáltatók nem férhetnek hozzá.

4.1.1. Számhordozhatósági központi referencia adatbázis adatstruktúrája

Ebben a fejezetben javaslatot teszünk az adatbázisban tárolandó adatokra abban az esetben, ha az adatbázis csak a hordozott számok valamint a kiosztott színes számok adatait tartalmazza. Ezek az információk lesznek relevánsak a KRA indításakor.

Az adatbázis (*számhordozhatósági referencia adatbázis*) nyilvános része minimálisan a következő adatokat kell, hogy tartalmazza annak érdekében, hogy a 3. fejezetben rögzített funkcionalitás egyáltalán megvalósítható legyen:

- átadott / átvett hívószám, illetve kiosztott színes szám (földrajzi számok esetében: körzetszám+előfizetői szám, mobil illetve nemföldrajzi számok esetében: szolgáltatás-kijelölő szám + előfizetői szám)
- hívószámot átvevő / átadó, illetve a kiosztott színes számot használó szolgáltató azonosítója (célszerűen a négyjegyű irányítási szám[1])
- hordozás / színes szám kiosztás kezdő dátuma és időpontja (Ez utóbbival az átadási időablak kezdetét kívánjuk meghatározni, annak egy adott - későbbi szabályozásban meghatározandó - hosszt (például 4 óra) feltételezve. Jelenleg nem kidolgozott, hogy mi történjék akkor, ha a számhordozás mégsem valósul meg az itt a többi szolgáltató számára előre jelzett időablakban.)
- hordozás / színes szám használat érvényesség vége dátuma és időpontja (ennek a tárolása esetleg elhagyható a nyilvános részből, hiszen ez a mező sokszor üres marad. Két fő ok miatt javasoljuk, hogy ez a mező mégis szerepeljen: 1. a színes számok esetén viszonylag sokszor előfordulhat, hogy valaki egy számot csak korlátozott időre (például 1 év, vagy valamilyen esemény ideje stb.) vesz meg, és ez a tény előre jelezhető; 2. Ha egy hordozott számot "visszahordoznak" a szám eredeti

[1]Mivel az "irányítási szám" fogalom többféleképp használatos, mi a tanulmányunkban irányítási szám alatt a következõt értjük:

Az irányítási szám 4-jegyû, struktúrája: SK+BK, ahol

SK 2-jegyû szolgáltató kód, az átvevõ szolgáltató kódja

BK 2-jegyû berendezés kód, mely csak az átvevõ szolgáltató hálózatán belüli irányításhoz használatos belsõ kód (a többi szolgáltató számára nincs jelentése) vagy 0.

tulajdonos szolgáltatójához, akkor ez a mező használható annak jelzésére, hogy a szám hordozottsági állapota mikortól szűnik/szűnt meg).
- célszerűnek tartjuk a hívószám eredeti tulajdonosának (számblokk szolgáltatójának) a tárolását is (ez a mező jelzi, hogy a hordozás esetleges megszűntekor kinek kell a számot visszaadni, illetve ennek a mezőnek a megléte szükséges a hívószám kijelölési adatbázis célra történő bővíthetőség szempontjából. Ez a mező a színes számok esetében üres marad.)
- tartalék (megfontolandónak tartjuk helyet biztosítani a hívószám kiadása illetve visszavétele időpontjának tárolására, ez a hívószám kijelölési funkció esetleges későbbi megvalósításakor kell majd.)

Az adatbázis nemnyilvános részének a következő fontosabb információkat kell tárolnia:

- a számhordozás bejelentésének időpontja. (Ez esetlegesen a nyilvános rész eleme is lehet, ha a számhordozás menetének részletes szabályozása után ez szükségessé válik.);
- esetlegesen a hordozás bejelentésének ügyiratszáma (papíros alapú adatbevitel esetére) vagy tranzakció-azonosítása ;
- egyéb információ (Tartalék későbbi funkcióbővítésre, a számhordozás menetének részletes szabályozása során esetlegesen felmerülő további azonosítók tárolására stb.).

Az egyéb információ mező tartalmazhatja például a szám használatának “egységárát”. Ez elsősorban a színes számok esetében lehet fontos. De mivel várhatóan a színes számokért fizetendő díj a színes számok alakjától függ, nem annak konkrét értékétől (azaz például ugyan a csupa egyforma jegyből álló (“aaaaaa” alakú) szám díja más lehet a két számjegy felváltva történő ismétlődést tartalmazó (“ababab”) alakú számétól, de az “111111” szám díja várhatóan ugyanaz lesz, mint a “222222”-é. Ha ez a feltételezés igaz, akkor nem javasolt az egységárnak a KRA-ban tárolása, hiszen az más formában jóval kisebb helyen tárolható, de ha a feltételezés nem lesz igaz, akkor célszerű ezt az információt itt tárolni.)

4.1.1.1. A számhordozhatósági referencia adatbázis mérete

Ebben a fejezetben becslést adunk az adatbázis 4.1.1 pontban javasolt adatstruktúra használata mellett kiadódó méretére abban az esetben, ha az adatbázis csak a hordozott számok valamint a kiosztott színes számok adatait tartalmazza. Ezek az információk lesznek relevánsak a KRA indításakor.

Első kérdésként egy becslést adunk arra vonatkozóan, hogy ilyenkor az adatbázis hány bejegyzést fog tartalmazni és összességében várhatóan mekkora méretű lesz.

A nemzetközi tapasztalatok alapján a hordozott számok várható száma évente nagy valószínűséggel maximum a néhány tízezres nagyságrendű tartományba esik. Ugyanakkor annak a hatása jelenleg még meg sem becsülhető, hogy Magyarországon, ha a vezetékes piacon is beindul a de facto verseny (azaz legalább még egy, országos, domináns jellegű szolgáltató színrelép) ez milyen hatással lesz a számhordozásra. Hasonló a helyzet a mobil szolgáltatók közötti hordozhatóság engedélyezésével kapcsolatban.

A színes számok nyilvántartásához a fentebb leírtak alapján csak a ténylegesen kiosztott, “élő” színes számok adatait használjuk, azaz **az implicit tárolást javasoljuk**. A HÍF-től kapott adatok alapján jelenleg a használt színes számok száma jóval a százezres nagyságrend alatt van, és az sem prognosztizálható, hogy az ezek iránti igény belátható időn belül jelentősen megnő.

A fenti két bekezdés alapján azt a becslést tehetjük, hogy a központi referencia adatbázisnak várhatóan néhány százezer szám adatait kell tudnia tárolni. Ennek a számnak a jelentős meghaladására reálisan nem kell számítani azon az időintervallumon belül, ameddig a KRA-t megvalósító hardver infrastruktúra nem amortizálódik (~5 év).

A következőkben becsüljük meg, hogy egy szám adatai mekkora helyet igényelnek minimálisan.

Nyilvános rész:

- átadott / átvett hívószám, illetve kiosztott színes szám (mobil számok esetén 9, míg földrajzi és nemföldrajzi számok esetén jelenleg 8, a későbbiekben várhatóan 9 számjegy)
- hívószámot átvevő / átadó illetve a kiosztott színes számot használó szolgáltató azonosítója (ha erre a célra az irányítási számot használjuk, akkor 4 számjegy)
- átadás / kiosztás kezdő dátuma és időpontja (a dátum év/hó/nap alakban történő tárolása 8 számjegyet igényel; az időponté óra/perc formában történő tárolásnál további 4 számjegy)
- érvényesség vége dátuma és időpontja (Az előző ponttal egyezően 8+4 jegy)
- a hívószám eredeti tulajdonos szolgáltatójának azonosítója (ha erre a célra szintén az irányítási számot használjuk, akkor 4 számjegy)
- tartalék (dátum esetén 2*8, dátum és időpont tárolása esetén 2*12 számjegy)

Nemnyilvános rész:

- a hordozás bejelentésének időpontja (8+4 számjegy)
- esetlegesen a hordozás bejelentésének ügyiratszáma (kb. 10-15 bájt)
- egyéb információ (néhány tíz bájt)

Az egy hordozott számhoz illetve kiosztott színes számhoz tartozó rekord nyilvános részének mérete 41 bájt körül lesz (a javasolt tartalékkal együtt 57 vagy 65 bájt), ehhez jön még a nemnyilvános rész szintén körülbelül ekkora mérete. A kettő együtt várhatóan maximum 100 bájt vagy annál kevesebb lehet. Így az adatbázis mérete (100 000 hordozott + 100 000 kiosztott színes számmal és 100 bájtos rekordmérettel számolva) 20 Mbájtra adódik. Ez véleményünk szerint - különösen az induláskor - felső korlátnak tekinthető, de a mobil számhordozás bevezetése illetve a vezetékes piacon kialakuló de facto verseny hatása megbecsülhetetlen, pesszimális esetben akár milliós nagyságrendre is fel kell készülni. Az adatbázis bruttó mérete a megvalósítástól függően az előzőleg számítottnál néhányszor nagyobb lesz, de 2-3-szoros szorzótényezőnél nagyobbal a gyakorlatban nem kell számolni.

Megállapítható tehát, hogy a hordozott számokat és a kiosztott színes számokat tartalmazó adatbázis mérete reálisan a 10 Mbájt, de még (a nem várható, de "worst case"-ként elképzelhető) milliós számhordozás esetén is csak a 100 Mbájt nagyságrendjébe fog esni. A becslés pontossága alapvetően a megvalósuló számhordozások és a ténylegesen használt színes számok összes számától függ. Ebbe a becslésbe az is belefér, ha biztonsági okokból az adatbázist meg kell kettőzni.

4.1.2. Hívószám adatbázis adatstruktúrája

Második esetként nézzük meg azt, amikor az adatbázis nemcsak a hordozott, hanem az összes hívószám adatait tartalmazza (*hívószám + hívószám kijelölési adatbázis funkciók*).

Ez utóbbi két funkció megvalósítása a HÍF jelenlegi tervei között nem szerepel, de a számítások támpontot adnak arra vonatkozóan, hogy a későbbi esetleges bővítés milyen plusz erőforrásokat igényelhet.

Ez esetben az adatbázis nyilvános része megegyezne az előző pontban tárgyalttal, hiszen ez az adatbázis szolgál egyúttal számhordozási referencia adatbázisként is.

Ugyanakkor a nyilvános résznek itt tartalmaznia kell a következő mezőket:

- a szám kiosztásának ideje
- a kiosztás érvényességének tartama vagy végdátuma

(ezek a mezők tartalékok voltak az előző esetben).

A nemnyilvános rész kiegészülne a következő adatokkal:

- a kiosztás ügyiratának száma
- egyéb (hatósági) információ

Ez összességében számonként körülbelül 50 további bájt tárolását igényli.

4.1.2.1. A hívószám adatbázis mérete

A hívószám adatbázisban a fentebb leírtak szerint csak a ténylegesen kiosztott számokat tároljuk, azaz az implicit tárolást célszerű megvalósítani. Ez azt jelenti, hogy a lehetséges mintegy 800 millió darab 9-jegyű szám helyett felülről becsülve, 10 millió kiosztott földrajzi és ugyanennyi kiosztott mobil számmal, valamint ezekhez képest elhanyagolható mennyiségű, összességében 100 000-es nagyságrendű nemföldrajzi számmal számolhatunk. A rekordméretet 150 bájtnak becsülve az adatbázis nettó mérete 3 Gigabájt körülire adódik. Ha ehhez hozzászámítjuk a megvalósítástól függő 2-3-szoros szorzótényezőt, akkor is 10 Gbájt alatti méretet kapunk, amely mindössze két nagyságrenddel nagyobb a csak a hordozott számok tárolására szolgáló adatbázis várható méreténél.

4.2. Interfészek és protokollok

Ebben a fejezetben áttekintjük, hogy milyen, bármilyen cég által használható, szabványos felületek jöhetnek szóba az adatbázishoz való hozzáférésnél.

Az interfészek alapvetően lehetnek egyirányú vagy kétirányú kommunikációra alkalmasak. Ezen kívül fontos jellemzőjük a rajtuk keresztül megvalósuló kommunikációhoz használható protokoll fajtája. A KRA esetén különböző funkciók megvalósításához akár különböző interfészek is alkalmazhatók, illetve azonos interfész mellett különböző protokollok. Jelen esetben feltétlenül csak olyan megoldások jöhetnek szóba, amely hiteles információk közvetítésére is alkalmasak (ld. a biztonságról szóló fejezetet).

A fizikai megvalósítás szintjén az interfész lehet

- papír alapú, vagy
- elektronikus, elvileg mindkettő megfelelhet az alapvető kritériumoknak.

Az elektronikus interfészek közül két alapvetően különböző jöhet szóba (hiszen alapvetően minden felhasználónak egy adatbázissal kell kommunikálnia):

- fájl alapú

- valamely szabványos adatbázis interfész alapú (például ODBC).

A fájl alapú esetén az adatokat először egy ismert struktúrájú és kódolású fájlba írjuk és a fájlokat mozgatjuk a központi adatbázis és a szolgáltatók adatbázisa között. A szolgáltató oldalán a fájl tartalmát természetesen újfent meg kell feleltetni az adatbázis tartalmának. Ekkor tehát két adatbázis ⇔ fájl transzformációt kell az adatokon végrehajtani.

Amennyiben egységesen valamely szabványosnak tekinthető adatbázis interfészt használunk, akkor közvetlenül összekapcsolhatunk egymással az adatbáziskezelő rendszereket. Ilyenkor természetesen számos adat-transzformációt meg lehet takarítani, és nagyon könnyű annak a biztosítása, hogy az adatbázisból csak a valóban szükséges adatokat kérdezzük le (tehát például a teljes, illetve csak a változás adatok lekérdezése nem jelenthet gondot). Azonban ekkor sem célszerű az üzemi adatbázis táblák közvetlen összekapcsolása. Célszerűen munka- (buffer)táblákat hozunk létre mindkét oldalon az adatok fogadására. Ezzel robosztusabbá tehetjük a rendszert számos véletlen hibával vagy szándékos károkozási kísérlettel szemben, megkönnyíthetjük az események kontrollálását és reprodukálását. Ekkor tehát fájlok helyett átmeneti táblák fogják a kapcsolatot megteremteni a két oldal között.

A kétféle módszer közül bármelyik választható anélkül, hogy ez a versenysemlegességet veszélyeztetné.

Mindkét felületnek a használata természetesen valamely számítógép-hálózati protokollstack felett valósul meg, amely a TCP/IP választása esetén adja a legáltalánosabban használt hozzáférést.

4.3. KRA funkciók

4.3.1. Adatok feltöltése

Az adatok le,- illetve feltöltése az üzemi hívásirányítási adatbázisok és a KRA között elvileg "push" vagy "pull" technológiával egyaránt megvalósulhat. Push esetén a kezdeményező a küldő oldal, pull esetén pedig a fogadó oldal. A kettő közötti választást alapvetően az dönti el, hogy melyik oldalon történik olyan esemény, amely a folyamatot triggerelheti, illetve a biztonsági megfontolások melyiket engedik meg egyáltalán megvalósítani (lásd a Biztonság fejezetben).

A push technológia - amennyiben alkalmazása más (például biztonsági) szempontból megengedett - hatékony lehetőséget kínál a változások elterjesztésére. Egyszerűen lehet ugyanis olyan automatizmusokat kialakítani, amelyek bármelyik adatstruktúrát érintő változások esetén automatikusan küldenek adatokat a szolgáltatók felé (data broadcast). Ez nemcsak kényelmesebb a szolgáltatóknak, hanem csökkenti a központi valamint szolgáltatói adatbázisok között ideiglenesen óhatatlanul fennálló inkonzisztenciát is.

Úgy tűnik, hogy a referencia adatok napi frissessége kielégítő jelenleg a szolgáltatók számára. Ezért volt az a kiindulási feltételezés [8], hogy az adatok feltöltése a KRA-ba napközben, míg az adatok letöltése éjszaka történik. Ugyanakkor erre a feltételezésre technikai oldalról valójában nincsen szükség a mai adatbáziskezelő rendszerek alkalmazása mellett, hiszen ezek - többek között - éppen úgy vannak kialakítva, hogy az adatbázis tartalmát módosító folyamatok nagyfokú konkurenciája esetén is nagy hatékonyságot és biztos konzisztenciát valósíthassanak meg.

Első pontként vizsgáljuk meg az adatok feltöltésének a kérdését.

Korábban - [8] a hordozott számok feltöltésére az volt a koncepció, hogy a szolgáltatók on-line módon tölthetik fel az adatokat az adatbázisba az új illetve a megszűnő vagy meghiúsuló hordozásokról. A HÍF szakértőitől kapott információk alapján [4] - legalábbis induláskor - a feltöltés kizárólag off-line módon történik a következő formában: a szolgáltatóknak a hordozásokat a HÍF felé kell bejelenteniük valamely hiteles csatornán keresztül (ami akár papír alapú is lehet), és a változásokat az adatbázis üzemeltetője tölti majd be ellenőrzés után. A hosszú távú megoldás azonban mindenképpen az adatok szolgáltatók általi on-line feltöltésének engedélyezése is. Ehhez azonban célszerűen meg kell teremteni a feltöltendő adatok ellenőrzésének valamilyen szintű lehetőségét is. Ez az ellenőrzés kettős feladatot igényel.

- Egyrészt ellenőrizni kell tudni, hogy az adatbetöltési kérelem adatbetöltésre jogosult felhasználótól érkezik-e. Ezt a kérdéskört és a lehetséges megoldásokat a Biztonság fejezetben részletesen elemezzük.

Másrészt azt kell ellenőrizni, hogy a betöltendő adat helyes-e (nincs-e például elgépelve). Itt fontos felhívni arra a figyelmet, hogy **amennyiben az átvevő szolgáltató tölti fel a KRA-t [2], akkor nincs mód annak az ellenőrzésére a KRA-ban a jelenlegi feltételek mellett, hogy van-e joga az adott szolgáltatónak az adott számra a hordozást bejegyezni!** További tanulmányozást igényel a kérdés részletesebb vizsgálata a visszaélések és/vagy tévedések kizárása/csökkentése érdekében. Két olyan javaslatunk lehet a megoldás irányában, amit a KRA *támogatni* tud. Az első az lehet, hogy a hordozás szabályozásakor kötelezzük a szolgáltatókat arra, hogy a KRA-ból letöltött hordozott számok közül ellenőrizzék azokat, amelyek tőlük elhordozottak, a másik, hogy ha egy számhordozást bejelentenek, akkor az ne kerüljön be azonnal az adatbázisba, hanem az adatbázis egy megfelelő interfészen/módon üzenetet küldjön a számhordozási bejelentésben szereplő átadó szolgáltatónak ellenőrzési felkéréssel, és csak ha a megjelölt átadó szolgáltató ezt nyugtázza, akkor kerülhessen a változás ténylegesen bejegyzésre. A KRA automatikusan legfeljebb csak annyit tud ellenőrizni, hogy a hordozandó szám ténylegesen az átadónak bejelentett szolgáltató használatában van-e, de ezt is csak akkor, ha a KRA tartalmazza azt az információt is, hogy melyik szám melyik szolgáltató számára van kiosztva (azaz ha egyben hívószám vagy hívószám kijelölési adatbázisként is funkcionál), vagy legalábbis automatikusan le tudja kérdezni a szükséges adatokat a hívószám adatbázisból.

4.3.2. Adatok lekérdezése

A számhordozási központi referencia adatbázis hívásirányítási funkciókat nem lát el, így a szolgáltatók számára elegendő, ha csak viszonylag ritkán fordulnak az adatbázishoz. A szolgáltatók számára kizárólag az adatbázis nyilvános részének letöltése engedélyezett, a nemnyilvános adatokhoz nem férhetnek hozzá.

A nemnyilvános adatok lekérdezése csak külön jogosultság megléte esetén, a hatóság számára lehetséges. Ezek a lekérdezések várhatóan egyrészt alkalmiak és kevés adatot érintenek, másrészt lehetnek rendszeresek is, bizonyos ellenőrzések elvégzésére vagy statisztikák készítése céljából.

A továbbiak csak a nyilvános adatok letöltésére vonatkoznak.

Alapvetően kétféle lehetséges lekérdezési eshetőség merül fel.

1. Az első eset a teljes nyilvános adattartalom lekérdezése. Ez induláskor szükséges, a későbbiekben azonban csak nagyon ritkán, tipikusan szolgáltatói adatbázis sérüléskor vagy adatkonzisztencia ellenőrzésekor történik, és összességében az adatbázisban tárolt hordozott számok illetve kiosztott színes számok tényleges mennyiségétől függően néhány száz kbájttól - akár többtucat Mbájt nagyságrendig terjedhet.
2. A második eset a szolgáltató által történt előző lekérdezés vagy adott időpont óta történt változások lekérdezése ("delta" lekérdezés). Ez tipikusan naponta egyszer történik szolgáltatónként, várhatóan alkalmanként tipikusan legfeljebb néhány kbájt adat letöltését igényli. A "delta" lekérdezés eredményeképpen a kérdezőnek csak azoknak a számoknak adatait kell megkapnia, amelyek kiszolgáló szolgáltatója a lekérdezéskor megadott kezdő időpontban más volt, mint a lekérdezés időpontjában. (Azaz, ha a lekérdezésben szereplő kezdőidőpont és a lekérdezés időpontja között több változás is történt a szám kiszolgáló szolgáltatójában, de ez a változás-sorozat végeredményben azt okozza, hogy az kezdőidőpontbeli "eredeti" állapot "helyreáll" (például egy számot elhordoztak majd visszahordoztak), akkor ezt a "delta" lekérdezés során nem kell jelezni, illetve ha a kérdezett idő alatt például több hordozás is történt az adott számra, akkor csak a végállapot jelenjen meg "delta" lekérdezés során (vö. a szolgáltatók nem férhetnek hozzá az adatbázis históriájához, de erre irányítási szempontból nincs is szükségük.) Itt kell megjegyeznünk, hogy a "delta" lekérdezés során azoknak a számoknak az adatait viszont értelemszerűen át kell adni a lekérdező szolgáltatóknak, amelyeknél:
   - hordozott szám esetén: a hordozás ténye megszűnt, azaz a szám "kikerül" az adatbázisból (ez akkor fordulhat elő, ha a számot visszahordozták az eredeti szolgáltatónak vagy a hordozott szám előfizető általi használata megszűnt és emiatt kerül vissza a szám eredeti tulajdonosához) vagy ha egy már bejelentett és az adatbázisba felvett hordozás (például műszaki okok miatt) meghiúsul.
   - színes szám esetén: a szám használata megszűnik.

Célszerűnek látszik a "delta" lekérdezésnél megadható kezdőidőpontot korlátozni. Például, mivel [2] szerint két hordozás közötti idő nem lehet rövidebb 30 napnál, ezért, ha a maximálisan megadható kezdőidőpont 30 napnál nem nagyobb, akkor a többszörös hordozási vátozások problémája nem merül fel. Ez ugyanakkor a szolgáltatók számára sem jelent lényeges korlátozást, hiszen a "delta" lekérdezés tipikusan naponta történik [8], az egy napnál régebbi kezdőidőpont megadásának szükségessége akkor merülhet fel, ha a szolgáltató oldalán keletkezett egy napnál hosszabb olyan hiba, ami miatt a KRA-t nem tudta elérni. De mivel várhatóan a hordozás részletes szabályozása során úgyis lesz egy olyan időkorlát, amin belül a hordozásnak megfelelő irányítást egy szolgáltatónak biztosítania kell, tehát ennél a korlátnál hosszabb "delta" lekérdezés normális körülmények között nem fog felmerülni.

Felmerült annak az igénye is, hogy a szolgáltatóknak ne kelljen naponta lekérdezniük az adatbázist (illetve választhassák ezt a szolgáltatást opcionálisan), hanem az adatbázis értesítse a szolgáltatókat, ha változás történik (de csak például naponta legfeljebb egyszer). Az adatbázis kezelők ezt a szolgáltatást meg tudják valósítani, azonban ennek biztonsági kockázatai lehetnek. Célszerű kompromisszumként a kényelem és a biztonság között elfogadható, ha az adatbázis a változás tényéről értesíteni képes a szolgáltatót, de ez az értesítés magukat a változott adatokat nem tartalmazza, hanem azokhoz egy, az értesítés vételét követő megfelelő "delta" lekérdezéssel lehet hozzájutni.

4.3.3. Biztonság

E fejezetben térünk ki azokra a kérdésekre, hogy a nemzeti referencia adatbázis adattartalmának védelme milyen megoldásokat kíván.

A megfelelő szintű biztonság megteremtése összetett feladat. Ugyanis az IT technológia mai fejlettsége mellett a probléma akár lényegesen bonyolultabb rendszer és érzékenyebb adatok esetén is megoldható, így a pontos követelmények kiderítésének és definiálásának a jelentősége "csak" az, hogy mennyibe fog kerülni a rendszer létrehozása és üzemeltetése. Ha ezeket pontosan megfogalmazzuk, akkor lehetőség van arra, hogy a teljes rendszer és környezete számára olyan biztonsági stratégiát rögzítsünk, amelynek minden eleme konform az elvárásokkal.

A megoldástervezetnek ki kell térnie az IT biztonság klasszikus területeire, mint

- bizalmasság (confidentiality),
- sértetlenség (integrity),
- nyomonkövethetőség (accountability)
- letagadhatatlanság (non-repudiation)
- rendelkezésreállás (availability).

A továbbiakban mi is ezeknek a címszavaknak a mentén határozzuk meg a legfontosabb követelményeket. Fontos azt is rögzíteni, hogy a biztonság megteremtésének magában kell foglalnia a rendszerhez tartozó infrastrukturális elemeken kívül a KRA környezetét is, valamint azokat az eljárási szabályokat ("biztonságpolitika") is, amelyek nélkül a legbiztonságosabb rendszer is tökéletesen védtelenné válik. A **BS 7799** csoportosítása mindazokat a területeket átfogja, amelyek a vállalati biztonság területeinek lehet tekinteni és amelyek az eredő biztonságot befolyásolhatják:

- Biztonsági politika
- Biztonsági szervezet
- Eszközök és információ biztonsági osztályozása, szabályozása
- Személyzeti területhez kapcsolódó biztonság
- Fizikai és környezeti biztonság
- Kommunikáció és üzemeltetés
- Hozzáférés-szabályozás
- Rendszerfejlesztés és követés
- Üzlet-folytonosság
- Megfelelés az előírásoknak

4.3.3.1. Veszélyforrások

A harcászati technikákról írt könyvek mindegyikében szerepel az alábbi egyszerű tanács: Ismerd meg ellenfeled! Nem érdemes nekiállni az adatbiztonsági intézkedések kidolgozásának és végrehajtásának sem, míg nem tudjuk, mi fenyeget, mit miért teszünk.

A veszélyforrások egy gazdasági szervezet esetében emberi, technikai és természeti eredetűek lehetnek. Az emberi és technikai veszélyforrások a vállalat, illetve a vállalati információ-rendszer és az értékrendszer erőforrásaira vezethetők vissza, míg a természeti veszélyforrások a mindig jelen lévő környezetből adódhatnak. Látni kell azt is, hogy a veszélyforrások nem állandók, tehát egyszeri felméréssel nem lehet tartós eredményt elérni. Ez az oka annak, hogy a veszélyforrások feltárása nem egyszeri, hanem folyamatos feladat. Az alábbi ábra bemutatja a veszélyforrások típusait, néhány veszélyforrást, és azok okaira is utal.

A veszélyforrás típusa	A veszélyforrás például	A veszélyforrás oka
Környezeti	Árvíz, földrengés, villámcsapás	Természet
	tûz	Gyenge tûzvédelem
Fizikai	Jogosulatlan fizikai hozzáférés	Gyenge fizikai hozzáférés-védelem
	Eszközök rendelkezésre állása sérül	Eszközök megbízhatósága gyenge
Logikai	Jogosulatlan logikai elérés	Gyenge logikai hozzáférés-védelem
	Alkalmazói rendszer hibája	Gyenge minõség-ellenõrzés
	Logikai rendelkezésre állása sérül	Gyenge vírusvédelem
Humán	Jó szándékú károkozás, tudatos károkozás	Hibás humán politika, megfelelõ oktatás/tájékoztatás hiánya

A veszélyforrások adott esetben támadás formájában realizálódhatnak. Megkülönböztetünk aktív és passzív támadásokat.

- Az aktív támadás behatol a rendszerbe, célja a bizalmasság és/vagy a sértetlenség és/vagy a rendelkezésre állás ellen irányul.
- A passzív támadás nem hatol be a rendszerbe, hanem annak a környezetre gyakorolt hatását használja ki információ-szerzésre, a bizalmasság sérelmére.

Természeti veszélyforrások

Hazánkban növekvõ veszélyforrást jelentenek az árvizek. Az 1998-as és 1999-es magyarországi (elsõsorban alföldi és észak-magyarországi) árvizei váratlanul és feltartóztathatatlanul támadták meg több megye vállalatainak épületeit. Az árvizeket követõ belvizek szintén komoly veszélyeket és sajnos károkat is okoztak.

A földrengések az elmúlt évtizedekben nem okoztak jelentõs veszteségeket hazánkban. Azonban jó tudni, hogy a 19. század derekától napjainkig terjedõ idõszak rengéseinek gyakorisága alapján országunk területén évente négy-öt 2.5-3.0 magnitúdójú, az epicentrum környékén már jól érezhetõ, de károkat még nem okozó földrengésre kell számítani, míg 5.5-6.0 magnitúdójú földrengésre negyven-ötven évente egyszer kerül sor. A történelmi feljegyzések alapján a következõ évekre várható egy ilyen erõsebb földrengés.

A villámcsapások már a közvélemény szemében is jóval nagyobb valószínûséggel bírnak. Egy-egy villámcsapás következtében nemcsak tûz keletkezhet, de az elektromos és ezáltal a számítógépes rendszerekben is súlyos pusztítást okozhat.

Fizikai veszélyforrások

A fizikai veszélyforrások közül elsõként a jogosulatlan hozzáférésre összpontosítunk. A vállalat a jogosulatlanul belépõk, azaz a behatolók részérõl komoly fenyegetettségnek van kitéve. A behatolás célja értékek, információk, berendezések, eszközök megszerzése, azaz lopása lehet. Fizikai támadásnak minõsül például az informatikai eszköz gyártásánál konténer (elterjedtebb nevén trójai faló) beépítése. Emellett nem szabad kizárni a célok közül a berendezések, eszközök módosítását, tönkretételét sem. A jogosulatlan hozzáférés körébe tartozik a saját munkatársak részérõl az eszközök jogosulatlan használata, azaz szolgáltatások jogosulatlan igénybevétele is.

Az eszközök meghibásodási lehetõsége szintén veszélyforrást képez. Egyrészt a vállalat automatizált berendezései, mint például az épületautomatika és irodatechnika, másrészt az informatikai berendezések, mint a számítógépek, adatátviteli berendezések és adathordozók megbízhatósága is sérülhet. Ennek oka lehet például a zárt biztonsági területre (számítógép-központba) bevitt vezetékes távbeszelõ-hálózat nem szakszerû beszerelése vagy mobiltelefonok használata, elektromos kisülések, statikus elektromosság, mechanikai sérülések, rágcsálók és ízeltlábúak kártevései.

A fizikai veszélyforrások harmadik csoportját a vállalat épületeinek elhelyezése és az épületen belül az ún. érzékeny tevékenységek elhelyezése jelenti. Támadásra adhat lehetõséget például az utca felé nézõ ablak, vagy szomszéd épülettel közös fal. Kritikus lehet az épület elhelyezése a megközelíthetõség (rendõrök, tûzoltók) szempontjából is.

Végül meg kell említeni a vállalati objektumok épületautomatikájának mûködési zavarairól. Ide tartoznak többek között a felvonók, az energia-ellátó rendszerek, a légkondicionáló berendezések, illetve az irányító, védelmi rendszer.

Logikai veszélyforrások

A logikai veszélyforrást jelentõ kockázatok (akár véletlen, akár tudatos, rossz- vagy jóindulatú tevékenység következményeként) a következõ csoportokba foglalhatóak össze:

1. információk felfedése, majd felhasználása,
2. információk vagy programok jogosulatlan módosítása,
3. információk vagy programok rombolása,
4. a rendszer működésének megzavarása vagy megakadályozása.

Ennek megfelelően az adatbiztonságot háromféleképpen tudják megsérteni a támadások:

1. a *bizalmasság sérelmére* jogtalan hozzáféréssel,
2. a *sértetlenség sérelmére* jogtalan megváltoztatással, vagy hamis információk rendszerbe való juttatásával,
3. a *rendelkezésre állás és rendeltetésszerű működés sérelmére* az adatok rombolásával, jogosult részéről történő hozzáférés megakadályozásával.

A logikai veszélyforrásokra a legjellemzőbb, hogy ténylegesen bekövetkező hatásaiknak csak egy része kerül felfedezésre.

A logikai veszélyforrások sokszínűségének demonstrálásaként következzen egy (nem teljes) lista ezekről a veszélyekről:

- illetéktelen hozzáférés bizalmas információhoz (például hálózatok lehallgatásával),
- másik felhasználó megszemélyesítése a felelősség áthárítása vagy jogosultságának felhasználása céljából (hamis információ rendszerbe juttatása, hiteles információk megváltoztatása, hamis személyazonosság felhasználása illetéktelen hozzáféréshez, csalárd módon ügylet hitelesítése),
- ténylegesen megkapott vagy elküldött információ letagadása, vagy időpontjának megváltoztatása,
- más felhasználó jogosultságának illetékesség nélküli megváltoztatása,
- annak felderítése, hogy ki milyen információkhoz jut hozzá, fogalmi analízis készítése,
- program működésének megváltoztatása,

- vírus, féreg, trójai faló, csapóajtó, logikai bomba rendszerbe juttatása,
- karbantartási és fejlesztési tevékenységek során elkövetett biztonsági és egyéb hibák.

Humán veszélyforrások

A saját alkalmazottakon kívül jelen lehetnek külső személyek is (például szervizcégek munkatársai). E ténnyel számol a külföldi szakirodalom, és a hazai tapasztalatok is erre mutatnak, hogy komoly fenyegetést jelentenek. Az utóbbi évek bankrablásainak nagy részében volt belső szereplő is. A külső szerviz munkatársai beépíthetnek olyan hardver vagy szoftver elemeket, amelyek támadó eszközök lehetnek, vagy információkat szerezhetnek meg. A hazai gyakorlat szerint, mivel a gazdasági szervezetek vagy nem ismerik megfelelően saját információ-rendszerüket, vagy takarékoskodnak, a karbantartást, a rendszerkövetést külső szervezetekre bízzák.

Mindezekből következik, hogy az adatokat humán szempontból is védeni kell. Az információ-védelem, adatvédelem fogalmát említve általában mindenki arra gondol, hogy az adatokat, információkat valamiféle fizikai védelemmel, engedélyezések kiosztásával, technikai megoldásokkal meg lehet védeni, és ritkábban merül fel az a lehetőség, hogy sokszor a különböző munkakörökben lévő alkalmazottak juttatnak ki a vállalat számára fontos, sőt titkos információkat. Ezen csoportból a fő veszély a személyzet, a dolgozók által ismert érzékeny információk kijutása a nyilvános szférába. A nemzetközi statisztikák azt mutatják, hogy egy szervezet adatainak bizalmasságát, hitelességét és sértetlenségét az esetek többségében a szervezet munkatársai sértik meg, saját vagy külső motiváció hatására, illetve saját hibájukból.

Az emberi hibák lehetnek jó szándékkal vagy tudatosan elkövetett hibák.

A jó szándékú károkozás a munkaképesség, illetve a munkakészséggel kapcsolatos problémákra vezethető vissza. A munkaképességen a munkatárs szellemi és fizikai erőnlétén kívül az adott munkakörhöz szükséges szakképzettséget és a belső oktatással megszerzett tudást értjük.

Tudatos károkozást a főnök vagy a vállalattal kialakult konfliktus gerjesztette indulatok válthatnak ki (például fegyelmi eljárás, elbocsátás). Súlyos probléma lehet továbbá a káros szenvedélyekkel rendelkező dolgozó (például kábítószer, szerencsejátékok, túlzott költekezés), akinél igen nagy esély van a pénzszerzési kényszerből elkövetett károkozásnak. A bűnözés célja leggyakrabban a vagyonszerzés, a vállalatoknál található értékek megszerzése, ezek között kiemelkedő helyet foglal el a pénz és a titkok megszerzésére irányuló tevékenység. Idetartozik tehát a rablás, csalás, zsarolás, lopás, megvesztegetés, valamint a túszszedés és a terrorizmus is.

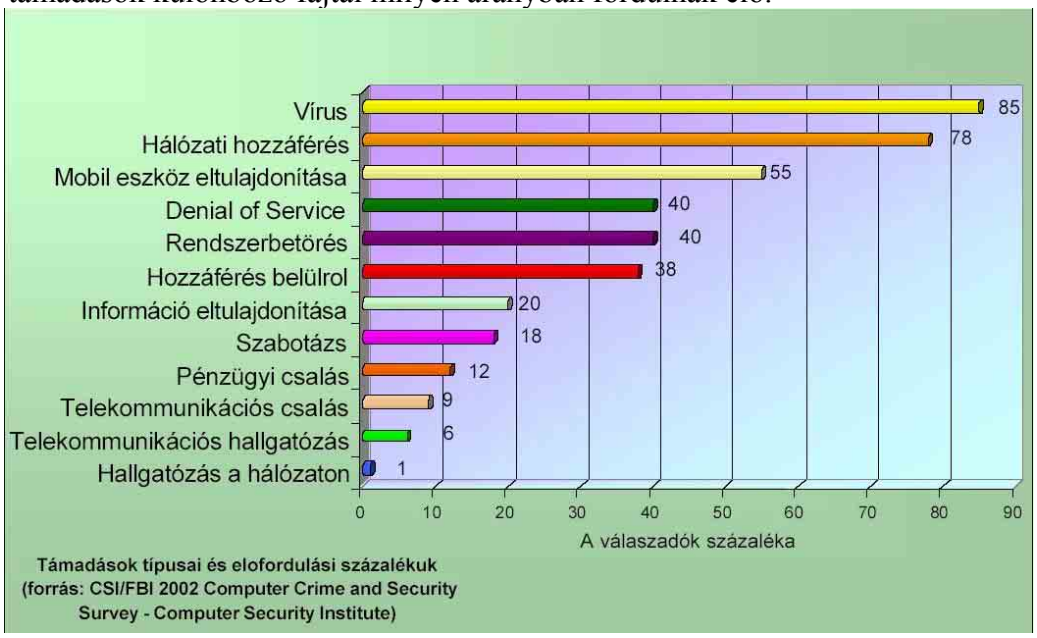
Végezetül megemlítjük, hogy az angol nyelvű szakirodalom 7-E néven említi az informatikai biztonságot fenyegető legfontosabb tényezőket. Ezek az alábbiak:

1. Ego (személyiség),
2. Eavesdropping (lehallgatás),
3. Enemity (ellenségeskedés),
4. Espionage (kémkedés),
5. Embezzlement (sikkasztás),
6. Extortion (zsarolás),
7. Error (hiba).

Ezekbõl is jól látható, hogy a legnagyobb problémát az emberi tényezõ okozza, hiszen a hét tényezõbõl egy sem függetleníthetõ az emberi tevékenységtõl. A számítógépek

természetesen nem követnek el bûnöket. Azokat az emberek követik el, akik bûnös célra használják a gépeket. Így tehát az informatikai biztonság hatékonyságát elsõsorban az emberi oldalra történõ odafigyelés növelheti.

A következõ ábra azt mutatja be, hogy tapasztalat szerint egy információs rendszer elleni támadások különbözõ fajtái milyen arányban fordulnak elõ.



4.3.3.2. Gyakorlati megoldások

Ennek a fejezetnek az a célja, hogy áttekintést adjon a legfontosabb, ill. legelterjedtebb, IT biztonság megvalósítását célzó ***technikai*** *megoldásokról. Semmiképpen nem volt cél a teljességre törekvés (nem is lehetséges, a területen tapasztalható viharos fejlõdés/változások mellett), sokkal inkább annak a bemutatása, hogy milyen lehetõségekkel érdemes számolni a KRA biztonságának tervezése és megvalósítása során. Az egyes megoldások/módszerek bemutatása után egy külön szakasz tartalmaz gondolatokat a KRA környezetében - véleményünk szerint - leginkább szóba jöhetõ megoldásokról.*

Az elektronikus adatok jellemzõje, hogy gyorsan, olcsón, egyszerûen, minõségromlás és nyom nélkül megváltoztathatóak vagy sokszorosíthatóak, amennyiben ez ellen külön nem védekezünk. Ideális esetben a bizalmasság, sértetlenség, nyomonkövethetõség és letagadhatatlanság biztosítására három alapvetõ adatvédelmi forma alkalmazható: a fizikai, az ügyviteli és az algoritmikus védelem.

A számítógépes biztonsággal foglalkozó írásokban többször találkozhatunk számos “ha ez történne, akkor azt így elõzzük meg” gondolatmenettel. Fel kell készülni a lehetséges hibákra, zavaró tényezõkre, hiszen Murphy törvényei ezen a területen különösképpen jól mûködnek: “Ha valami elromolhat, az el is romlik”. Azonban számos veszély fenyegeti a rendszereket az aktív támadás oldaláról is. Ezek ellen – bár jó megoldás – nem elég egy paranoiás rendszergazda.

A megfelelő adatbiztonság megvalósításának feltétele az elkötelezett vezetés. A vezetés felel a rábízott értékekért, ő képes eldönteni az adatvesztés okozta károk mértékét és ennek

megfelelően az adatbiztonságra fordítandó erőforrások nagyságát. A vezetőség feladatai közé tartozik tehát, hogy megteremtse a személyi, tárgyi, szervezeti és pénzügyi feltételeket, szabályozza a védelemért és az informatikai rendszerek használatával kapcsolatos felelősséget. Ha ezt nem teszi meg, minden informatikai biztonsághoz kapcsolódó probléma esetén őt terheli a felelősség.

Fizikai védelem

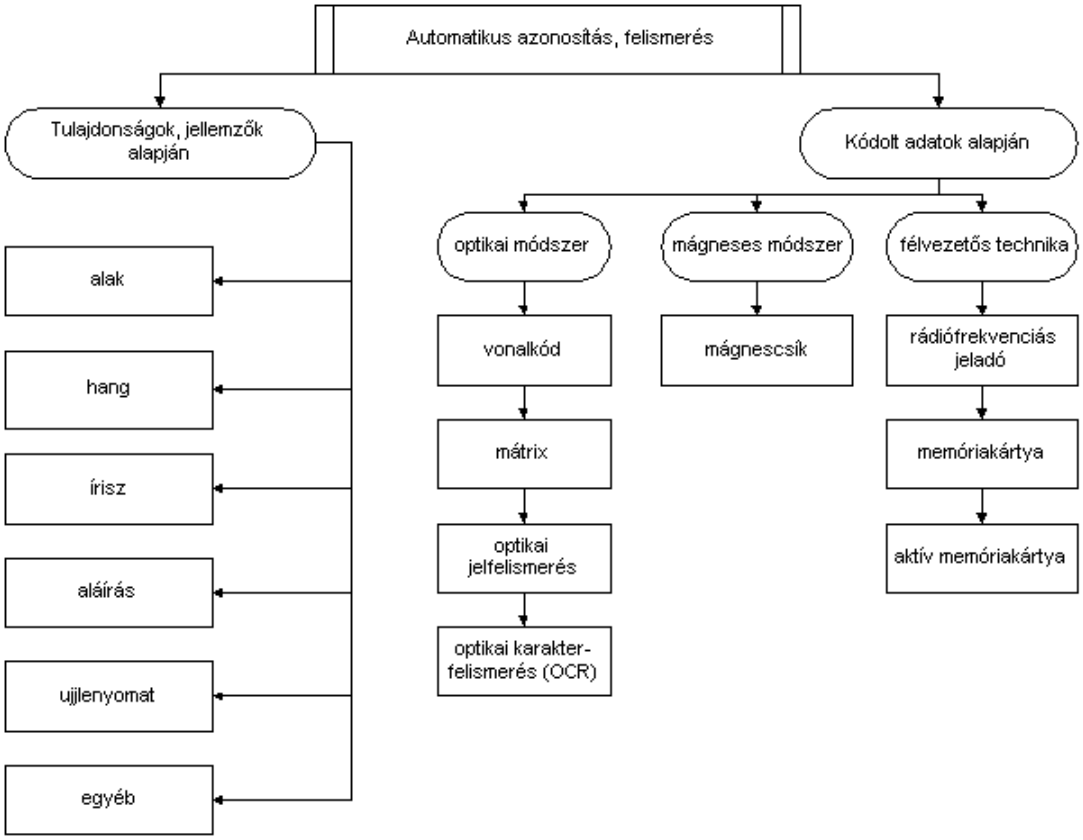
Egy informatikai rendszer fizikai védelmét a hardver és szoftver elemek (számítógépek, hálózati elemek, nyomtatók, adathordozók, dokumentumok és dokumentációk), valamint ezek közvetlen környezetének fizikai hatásoktól való védelmét jelenti.

Az *eltulajdonítás* ellen többnyire az elemek mechanikus rögzítésével szoktak védekezni, melyet külön áramforrással és rázkódásérzékelővel ellátott riasztó egészíthet ki. Ahhoz, hogy a számítógépek csak meghatározott körülmények között működhessenek, szükséges, hogy csak az arra felhatalmazottak férhessenek hozzá. Ezt többnyire *hardverkulcsos és jelszavas* védelemmel szokták megoldani, melyekhez egy vagy több személy férhet hozzá.

A hálózati elemek, számítógépek és perifériáik működés *közben elektromágneses hullámokat* sugároznak, amelyek speciális (és költséges) eszközökkel érzékelhetők és dekódolhatók, s így értékes információk birtokába juttathatják a rossz szándékú felhasználókat. Ráadásul a rendszer legális felhasználói mindebből semmit sem vesznek észre. Az elektromágneses sugárzás visszatartására legkönnyebben az elektromos berendezések leárnyékolásával lehet védekezni.

Az *áramkimaradás* okozta károk hasonló nagyságrendűek lehetnek, mint a legrosszabb szándékú támadásé. A probléma kezelésére szünetmentes áramforrásokat, szoktak használni, melyek automatikusan érzékelik a hálózati áramellátás megszakadását, s azonnal akkumulátoros üzembe kapcsolnak át. Ez általában mintegy félórás zavartalan üzemet tesz lehetővé, mely elegendő arra, hogy a rendszer használói befejezhessék a folyamatban lévő munkákat, s felkészülhessenek a leállásra.

Az informatikai rendszerek biztonságos működésének az is feltétele, hogy a rendszer hardverelemeinek helyet adó helyiségekbe csak az arra jogosultak léphessenek be. Ennek feltétele a felhasználók pontos azonosítása, s a jogosultsággal nem rendelkezők kitiltása az adott helyiségekből. A szigorúan védett helyiségek beléptető rendszerei az automatikus azonosítási módszerek közül leggyakrabban az aktív memóriakártyás, vagy mágneses kártyás módszert alkalmazzák. De ebbe a kategóriába tartoznak a biológiai jellemzőket számítástechnikával megtámogatva felismerő és összehasonlító biometrikus azonosítás eszközei: az írisz vagy retina és a kézenfekvő ujjlenyomat azonosítás. Előbbi módszerek kellemetlenek és drágák, utóbbi pedig bár olcsó olvasóval is megvalósítható ép, sérülésmentes és tiszta kezeket igényel, de pulzusérzékelő változatai egyértelműen az élő, teljes tulajdonost azonosítják. Más, kevésbé használható biometriai jellemzőkkel is folynak kísérletek, ilyen közepesen biztonságos eljárás a kéz vagy az arc geometriájának, a hangnak, az aláírásnak vagy a gépelési dinamikának a vizsgálata. Az alábbi ábra rendszerbe foglalja a különféle típusú azonosítási lehetőségeket.



[Ködmön József: Kriptográfia]

Ügyviteli védelem

A biztonság egyik alapvetõ eleme az ember. Amely rendszerben az emberek képzetlenek, hanyagok, nem ügyelnek a biztonságra, az a rendszer sosem lesz jó, hiába hozzuk létre a legprofibb adatbiztonsági megoldást. Amely rendszerben mindenki megbízható, képzett, mindent mindig gondosan megvizsgál, meggondol, ügyel saját és más értékeire, abban a rendszerben akár a biztonságot legkevésbé szavatoló elemek nélkül sem fog visszaélés bekövetkezni.

A biztonságnak nagyon fontos összetevõje tehát az ember. Mit sem ér pl. a legjobb rendszer, ha a készült naplófájlokat nem nézi át egy intelligens, a biztonsághoz értõ szakértõ. Ez a szakértõ lehet a számítógép is, de egyes esetekben mindenképpen szükséges az ember. Ha a technikai biztonság megteremtéséhez van pénz, akkor a megteremtett rendszert üzemeltetni is kell tudni.

A biztonságért felelõs szakértõk képzése általában sokkal kevésbé jelent nagy gondot, mint a felhasználók képzése. Az átlagos felhasználó minden gond nélkül elárulja saját jelszavát fõnökének, ha az megkérdezi, pedig erre nem biztos, hogy joga van. Hasonlóképpen hajlamosak a felhasználók elárulni jelszavukat egy ál-rendszergazdának, aki telefonban kéri meg a dolgozót, hogy árulja el jelszavát, mert ellenõrizni kell valamit. A felhasználók jelentõs része primitív jelszót használ, évenként sem cseréli, ráadásul monitora tetejére írva tartja.

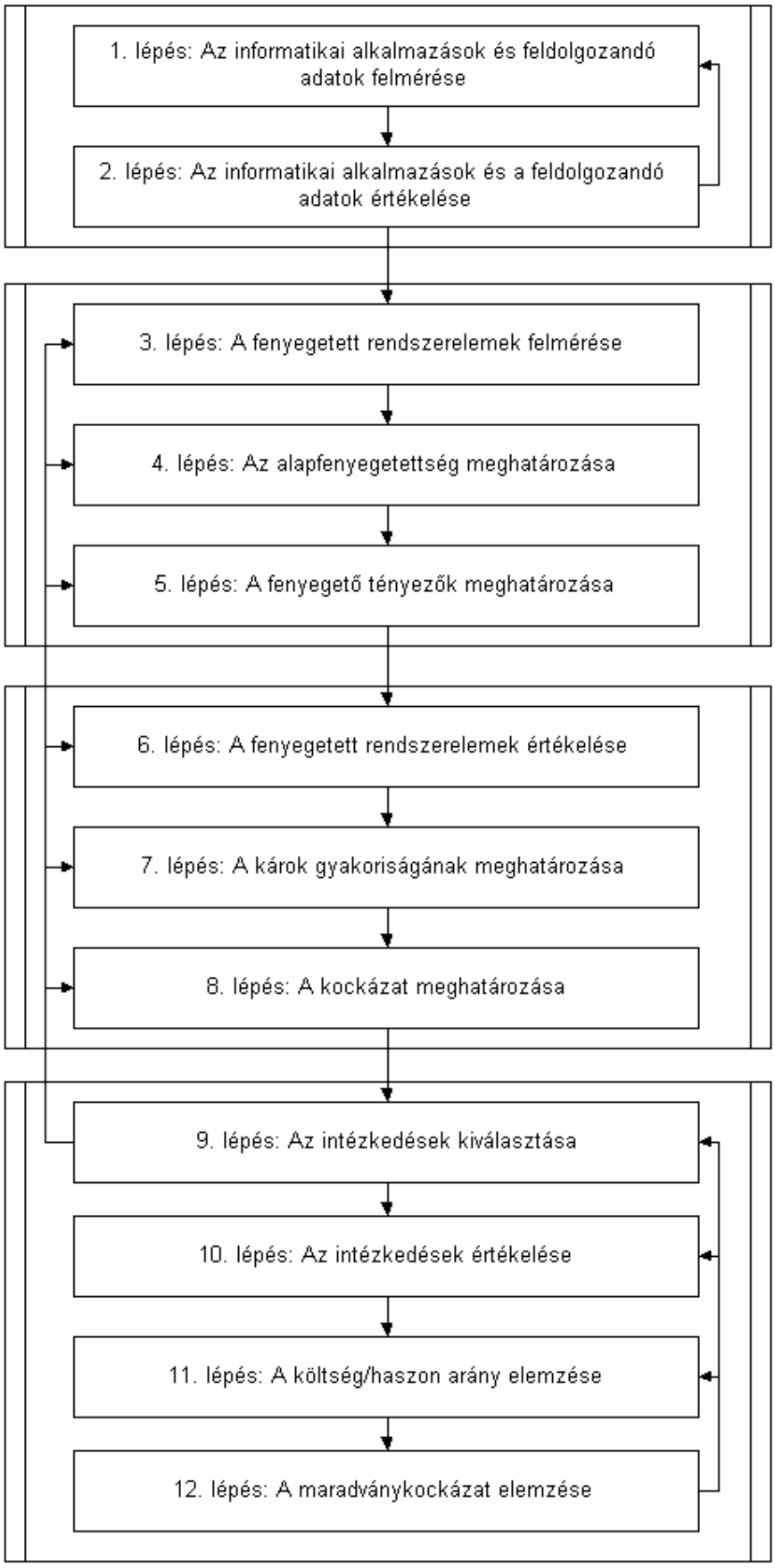
Ezeket a hibákat csak a képzéssel és számonkéréssel lehet megoldani. Nyilvánvalóan irreális biztonsági politikát nem lehet semmilyen eszközzel megvalósítani: Ha 50 karakterbõl álló jelszót kell használni a rendszerben, fele részben számokból, és naponta kell cserélni, akkor ott senki nem fogja tudni használni a rendszert.

A biztonságpolitika és az emberi erõforrás tehát szorosan összefügg egymással.

Ügyviteli védelmen az informatikai rendszert üzemeltetõ szervezet ügymenetébe épített védelmi intézkedések, biztonsági szabályok, tevékenységi formák összességét értjük, melyeket egy Informatikai Biztonsági Szabályzat ír le. Míg a fizikai védelem a rendszerbe való belépési pontokat jelöli ki, addig az ügyviteli védelem a belépési pontok használatának elfogadható, elvárt formáit határozza meg. Az ügyviteli védelem összekapcsolja a fizikai védelem területét az algoritmusos védelemével, s így teszi teljessé az informatikai védelmet.

Az ügyviteli biztonsági rendszer kidolgozásakor nem lehet automatikusan a hagyományos, papír alapú ügyvitel biztonsági intézkedéseit alkalmazni, mivel a hagyományos ügyvitel egy statikus, lassan változó rendszer, míg az informatikai rendszerekre a dinamikus fejlõdés jellemzõ. Biztonságos használatuk csak a változásokat megfelelõ ütemben követõ, szintén dinamikusan változó helyi szabályok megalkotásával lehetséges.

A biztonságpolitika kidolgozásakor több módszert is lehet alkalmazni, mint például a BS 7799-et vagy az Informatikai Tárcaközi Bizottság 12. számú ajánlását. A következõ összefoglaló ábra fõbb pontjaival mutatja be egy koncepció kidolgozásának lehetséges lépéseit:



Forrás: Ködmön József, Kriptográfia

Egy informatikai biztonsági koncepció kialakítása e szerint négy fõ szakaszra bontható, melyek a:

1. védelmi igény feltárása,
2. fenyegetettség-elemzés
3. kockázatelemzés
4. kockázat-menedzselés.

A védelmi igény feltárásakor történik meg azon informatikai rendszerek, alkalmazások kiválasztása, melyek a szervezet mûködése szempontjából érdemesek a védelemre.

A fenyegetettség-elemzés során rá kell mutatni mindazon veszélyforrásokra, melyek a kiválasztott alkalmazásokat fenyegethetik, bennük kárt okozhatnak. A vizsgálatnak minél széleskörûbbnek kell lennie, s itt kell feltárni az informatikai rendszer gyenge pontjait is.

A kockázatelemzés azt célozza, hogy meghatározzuk, az egyes fenyegetõ tényezõk milyen és mekkora károkat okozhatnak, illetve azok milyen gyakorisággal következhetnek be.

Az utolsó lépésben, a kockázat-menedzselésben ki kell választani a fenyegetõ tényezõk elleni intézkedéseket, s értékelni azok hatását. A lehetséges megoldások közül ki kell választani a költség-haszon arány szempontjából is megfelelõ védelmi intézkedéseket, illetve meg kell határozni milyen maradvány kockázatokkal kell a szervezetnek szembenézni.

Algoritmusos védelem

Mielõtt a klasszikus algoritmikus védelem kategóriájába tartozó eljárásokat számba vennénk, érdemes valamivel tágabb kontextusban is megvizsgálni egy számítógéphálózat különbözõ szintjeinek a védelmét. A konkrét, elvileg szóba jöhetõ technikai megoldások száma nagy. A választás során arra kell elsõsorban ügyelni, hogy az alkalmazott megoldások a védett információk értékével arányban álljanak. Ugyan a harc fõ színtere az alkalmazási réteg, de minden hálózati protokoll rétegben lehet védekezni a várható visszaélések, támadások ellen. A leggyakoribb támadásokat és az ellenük tett óvintézkedéseket a következõ táblázat tartalmazza:

	Támadás formái	**Védekezési módok**
1. Fizikai réteg	vezeték megcsapolása	gázzal feltöltött csõ riaszt
2. Adatkapcsolati réteg	két végpont közt haladó csomagok elfogása	a routerek között áramló adatcsomagok kódolása
3. Hálózati réteg	pl. vírusok küldése	tûzfalakkal
4. Szállítási réteg	illetéktelen hozzáférés	teljes kapcsolat titkosítása az alkalmazási folyamatok közötti szállításkor
5. Alkalmazási réteg	üzenet megváltoztatása, vagy a küldõ letagadása	hitelesség, letagadhatatlanság szoftveres biztosítása garantált, egyszeri, visszajátszhatóság nélküli célbajutás

Az algoritmusos védelmi szint azon eljárásokból, protokollokból áll, melyek a rendszer szolgáltatásaival egyidejûleg, velük szorosan együttmûködve látják el a védelmi feladatokat. Algoritmusos védelem helyett pedig gyakran használják a logikai védelem fogalmat is. Habár ennek a területnek külön tudománya alakult ki, nem szabad arról elfelejtkezni, hogy az

algoritmusos védelem csak a fizikai és ügyviteli védelemmel együtt képes elérni a kívánt védelmi funkciókat.

Az algoritmikus védelem részének tekinthetõ kriptográfiai védelem szükség esetén képes megfelelni a bizalmasság, sértetlenség, nyomonkövethetõség és letagadhatatlanság elvárásai által megfogalmazott követelményeknek. Léteznek olyan titkosítási eljárások, amelyek gazdaságosan titkosítanak, ami azt jelenti, hogy csak az üzenet értékéhez képest sokkal drágább ráfordítás mellett törhetõk fel.

Minden kriptográfiai eljárás 4 alapvetõ részbõl áll:

- · *Szöveg:* az eredeti, emberi olvasásra alkalmas szöveg.
- · *Rejtjeles szöveg (ciphertext)*: az eredeti szöveg átkódolt, nem olvasható változata.
- · *Titkosítási algoritmus*: matematikai formula amellyel a titkosítás/visszafejtés végbemegy.
- · *Kulcs:* a titkos kód, amivel a titkosítás/visszafejtés megvalósítható

A védelem megfelelõ szintjét a kódolási eljárás határozza meg. A kódolás alapja maga az alkalmazott algoritmus és az algoritmushoz használt titkosítási kulcs. Általában szabványosított algoritmusokat érdeme használni. Az információ ki- és becsomagolása csak a helyes titkosítási kulcs alkalmazásával lehetséges. A titkosításra használt eljárás meghatározza, hogy a visszafejtéshez ugyanaz a kulcs szükséges-e vagy annak egy fejtõpárja használandó. Elõbbi jellemzõ az egyik alapvetõ titkosítási fajtára, a konvencionális kódolásra, utóbbi pedig a másik módszerre, a nyilvános kulcsú kriptográfiára.

Szimmetrikus titkosítás vagy privát kulcsos titkosítás

A szimmetrikus kulcsú titkosítás különféle helyettesítéses eljárásokon alapul és az egyszerû helyettesítésen kívül, többek között, lehet periodikus permutáció, kulcsfolyamos vagy véletlen átkulcsolásos módszerû. A szimmetrikus vagy más néven konvencionális, vagy rejtett-kulcsú titkosítóknál a titkosító kulcs kiszámítható a megoldó kulcsból, és ez fordítva is igaz. A legtöbb szimmetrikus algoritmusnál a titkosító kulcs megegyezik a megoldó kulccsal.

A szimmetrikus algoritmusok két kategóriába sorolhatók: *folyam kódolók (stream ciphers)* és *blokk kódolók (block ciphers)*. A folyam kódolók egyszerre csak a nyílt szöveg egy bitjén (vagy egy bájtján) dolgoznak, a blokk kódolók pedig bitek egy csoportján dolgoznak. A modern számítógépes algoritmusok blokkmérete általában 64 bit, ami elég nagy ahhoz, hogy kizárja az analízist, de elég kicsi, hogy dolgozni lehessen vele.

A titkosítást alapvetõen bitenként vagy blokkonként hajtják végre és e módszereket gyakran kombinálják is.

A legszélesebb körben 1977. óta alkalmazott eljárás (volt) az 56 bites amerikai titkosítási szabvány DES (Data Encryption Standard). A kizáró vagy mûvelettel operáló blokk kódoló eljárás feltörhetõségét ugyan már bizonyították, de többször alkalmazva (tripla-DES) elég nagy biztonságot ad. Egy fokkal jobb az azonos módszereken alapuló IDEA (International Data Encryption Algorithm), ami már emberi idõ alatt a végigpróbálós faltörõ (brutal force) módszerrel még nemzetközi hálózati együttmûködéssel és feladatmegosztással sem törhetõ fel.

Néhány példa szimmetrikus algoritmusokra: DES, RC4, RC5, RC2, IDEA, LUCIFER, SKIPJACK, BLOWFISH, SAFER, CAST, GOST, FEAL, MMB, REDOC, LOKI, CRAB, MADRYGA, 3-WAY, SEAL, WAKE, CA-1.1, A5, KHUFU és KHAFRE. A legújabb

standard, ami fokozatosan kiváltja a DES/3DES-t, az az AES (Advances Encryption Standard).

Korunk legkedveltebb módszerei ezzel szemben a következõ, nyilvános kulcsú titkosítás algoritmusai között találhatóak.

Nyilvános kulcsú titkosítás / aszimmetrikus titkosítás

Egy kulcspár adja a nyilvános kulcsú titkosítás alapját. Minden egyes felhasználóhoz tartozik egy nyilvános és titkos kulcsból álló kulcspár. Az aszimmetrikus titkosítások megoldják a kulcskiosztás problémáját azáltal, hogy két különbözõ matematikailag összefüggõ, de egymásból elõ nem állítható kulcsot használnak: egyet a titkosításra, egy másikat a dekódolásra. Matematikai alapját tekintve a nyilvános kulcsú módszerek három kategóriába sorolhatók: nagy számok faktorizálásán alapuló, diszkrét logaritmust számoló, a hátizsák tartalmát összsúly alapján meghatározó algoritmusok.

Ilyen a számelmélet tételein alapuló **RSA** (Rivest – Shamir - Adleman) algoritmus. A nyilvános kulcsgyártás alapja az óriás egész számok prímtényezõkre bontásának nehézsége és két véletlenszerûen kiválasztott száz-kétszáz-jegyû prímmel végzett bonyolult, de automatizált matematikai mûveletekkel valósul meg. A nyilvános kulcs ismeretében gyakorlatilag nem lehet visszafejteni a hozzá tartozó magánkulcsot. A két kulcs közötti matematikai összefüggés miatt, ha az egyiket titkosításra használjuk, az eredményt mindig a kulcspár másik tagjával lehet dekódolni.

A magánkulcsot tulajdonosának titokban kell tartania, megfelelõ intézkedésekkel védenie kell az illetéktelen felhasználás, eltulajdonítás ellen. A privát kulcs nem csupán a számítógépen vagy lemezen, hanem önálló dátum-áramkörrel rendelkezõ csipkártyán is tárolható. A nyilvános kulcs bárki által hozzáférhetõ, sõt kívánatos, hogy minél szélesebb körben megismerhetõ legyen (pl. a hitelesítés-szolgáltatónál vagy címtár szolgáltatónál), mert a címzett nyilvános kulcsával kell titkosítani a neki szóló üzeneteket.

A nyilvános kulcshoz kapcsolt adatok alapján azonosítható a kulcs tulajdonosa, amit a **hitelesítõ központok** kérésre meg is tesznek. A hitelesítõ központok osztják ki a tanúsitványokat és akár a kulcspárokat is (bár ezt általában a kérelmezõ generálja). A legismertebb hitelesítõ az amerikai VeriSign.

Érdemes megjegyezni, hogy a hitelesítõ központok között is létezik egyfajta hierarchia. A sorban végül a gyökér hitelesítõ központ (Root CA) áll.

A titkosítás hatékonysága

A titkosítás hatékonyságának mérése nem triviális feladat. A titkosítási eljárás biztonságának egyik legfontosabb mérõszáma az alkalmazott kulcs hosszúsága. Ezzel kapcsolatos néhány megfontolás következik az alábbiakban *szimmetrikus kulcsú* titkosítás esetére.

Elméletileg minden titkosított üzenet visszafejthetõ, de megfelelõ hosszúságú kulcs esetén ez a visszafejtési idõ évmilliárdokban mérhetõ. Ma már minimálisan 40 bites kódolásúak a használatban lévõ kulcsok. Az egy bittel hosszabb kulcs kétszer annyi kulcsvariációt eredményez, a 8 bittel hosszabb pedig 2^8 azaz 256-szorosára növeli a variációs lehetõségeket. A 40 bites kulcsok használata esetén 2^{40}- azaz több, mint 1000 milliárd az összes lehetõség. A mai otthoni számítógépek teljesítménye: 1 másodperc alatt 1000 kulcs kipróbálása. 100 ilyen számítógép esetén naponta több mint 8 milliárd kulcsot lehet kipróbálni. Így legalább 3 hónapra van szükség, hogy az összes kulcsot kipróbáljuk. Azonban

így csak a 3 hónappal ezelõtt kódolt üzenet kerülhetne napvilágra, mivel mindig újabb és újabb kulcsokat generál a titkosítási rendszer. A nagyobb biztonságra törekvõ szervezetek már ma is128 bites kódolású kulcsokat alkalmaznak, melyek összes variációs lehetõsége 2^{128}. Gyakorlatilag nincs az a számítógépes kapacitás, amivel ennyi kulcsot ki lehetne próbálni.

A támadhatóság függvényében a kriptográfiai eljárások három kategóriába sorolhatók:

- *elméletileg biztonságos*: ha feltörésének a valószínûsége független a számítástechnikai erõforrásoktól és az idõtõl, amelyet egy támadó képes arra fordítani.
- *gyakorlatilag biztonságos*: ha a feltöréshez egy támadónak véges mennyiségû számítást kell végezni, de ez irreálisan nagy.
- *nem biztonságos*: ha megfejthetõ.

Elméletileg biztonságos titkosító létezik, de gyakorlati alkalmazásuk szinte lehetetlen. Sokkal nagyobb jelentõséggel bírnak a gyakorlati biztonságot nyújtó algoritmusok, a kriptográfia leginkább ezekkel foglalkozik.

A szimmetrikus és nyilvános kulcsú algoritmusok összehasonlítása

A szimmetrikus rejtjelezõk elõnyei

- A szimmetrikus rejtjelezõknek nagy az adatsebessége. Némely hardver implementáció több száz megabájtot is fel tudnak dolgozni másodpercenként, míg a szoftveres implementációk sebessége a néhány megabájt/másodperc tartományban van.
- A kulcsok viszonylag rövidek.
- A szimmetrikus rejtjelezõk felhasználhatók építõelemekként különbözõ kriptográfiai szerkezetek kialakításában, mint például álvéletlen szám generátorokhoz, hash függvényekhez.
- A szimmetrikus titkosításnak nagy múltja van, bár a legjelentõsebb tudás a számítógép felfedezése óta gyülemlett fel.

A szimmetrikus rejtjelezõk hátrányai

- Egy nagy hálózatban sok kulcsot kell kezelni (annyit, ahány résztvevõ van). Következésképpen a hatékony kulcs kezelés egy megbízható harmadik személy segítségével kell, hogy történjen, aki ismeri mindenkinek a kulcsát.
- A tapasztalatok azt mutatják, hogy egy két-résztvevõs kommunikációban a kulcsot gyakran kell cserélni.
- A szimmetrikus rejtjelezést használó digitális aláírás konstrukciók egy megbízható harmadik személy közremûködését igénylik.
- A biztonságosság elvi követelményeinek a szimmetrikus titkosítással rejtjelezett dokumentumok csak bizonyos megszorításokkal felelnek meg:

- Authentikáció: mivel a kulcsot minimum kettõ fél ismeri, nem állapítható meg bizonyosan, hogy a két fél közül melyik küldött el egy kérdéses üzenetet.
- Titkosság, bizalmasság: alapvetõen eleget tesz a bizalmasság követelményének
- Adatintegritás: Mivel az adatokat csak a megfelelõ kulccsal lehet megváltoztatni, eleget tesz adatsértetlenség elvének.

- Letagadhatatlanság: mivel minimum két fél ismeri a titkos kulcsot, a szimmetrikus kulcsú algoritmussal végzett kódolás önmagában használva nem tesz eleget a letagadhatatlanság elvének.

A nyilvános kulcsú rejtjelezõk elõnyei

- Titkosságot tudnak nyújtani anélkül, hogy a titkos üzenetküldést megelõzõen a kommunikáló felek bármiféle titkos kulcsot cseréltek volna egymással.
- A kulcsok adminisztrálása egy hálózatban egy megbízható harmadik személy jelenlétét igényli, de a privát kulcsokat nem ismeri ez a szereplõ és az sem szükséges, hogy mindig rendelkezésre álljon.
- A használattól függõen a privát és a nyilvános kulcs pár változatlan maradhat meglehetõsen hosszú ideig (akár évekig is).
- A bizalmasságon kívül a sértetlenség és a letagadhatatlanság elvárásainak is meg tud felelni.

A nyilvános kulcsú rejtjelezõk hátrányai

- A nyilvános kulcsú titkosítók feldolgozási sebessége jó néhány nagyságrenddel kisebb, mint a szimmetrikus titkosítóké.
- A kulcsok mérete nagy.
- A nyilvános kulcsú kriptográfiának nincs akkora múltja, mint a szimmetrikus titkosításnak, mert csak az 1970-es évek közepe felé fedezték fel.

Összességében a konvencionális és a nyilvános kulcsú titkosításnak számos egymást kiegészítõ elõnye van, amit a jelenlegi kriptográfiai rendszerek fel is használnak. A nyilvános kulcsú kriptográfiát általában digitális aláírásokhoz és kulcs megosztásra használják, a szimmetrikus kriptográfiát pedig rejtjelezésre.

Digitális aláírás

A **digitális aláírás** manapság gyakran a nyilvános kulcsú titkosítás fordítottja. Aláíráskor nem a címzett nyilvános kulcsát használom, hanem a saját magánkulcsommal hagyok nyomot az iraton. Népszerûségének oka egyszerû: ez a széles körben ismert és elsõsorban Amerikában alkalmazott, nyilvános kulcsú módszer a hitelességen túl a sértetlenséget és a letagadhatatlanságot is biztosítja. A titkosítással kombinálva, az aláíró azonosságát igazoló hitelesítõ központok autorizációjának igénybe vétele mellett garantálhatja a ma elérhetõ maximális, a gyakorlatban bõségesen elégséges biztonságot.

Alapértelmezésben a nyílt szöveg nincs titkosítva, csak egy digitális jelsorozattal, az “aláírással” látják el, de ezt titkosítás is követheti, például RSA-módszernél a fogadó nyilvános kulcsával. Aláíráskor elõször a tetszõleges hosszúságú szövegbõl (pl. MD5 algoritmussal) fix hosszúságú, ellenõrzõ összeg-szerû bitsorozatot, **digitális lenyomatot** állítanak elõ, amely egyértelmûen jellemzõ az adott dokumentumra. Gyakorlatilag lehetetlen két különbözõ olyan dokumentumot alkotni, amelyek azonos digitális lenyomatokat eredményeznek (egyértelmûség) és a lenyomatból az eredeti szöveg sem állítható vissza, mert információveszteség történik (egyirányúság).

Az irat digitális lenyomatát az aláírója saját magánkulcsával kódolja, ezáltal írja alá a dokumentumot. Ezt a kódolt jelsort, a digitális aláírást, esetleg a nyilvános kulccsal együtt,

csatolja a szöveghez, majd így továbbítja vagy tárolja. Digitális aláírása a partnerei felé és a késõbbiekben igazolja az irat hitelességét és integritását vagy változatlanságát. Az aláírás hiteles idejét, dátumát **idõbélyegzõ** hozzáfûzésével rögzíthetjük, amit a titkos kulcsával kódolva küld el.

Az **ellenõrzés** automatikusan folyik több párhuzamos tevékenységgel. A fogadó újra elkészíti a dokumentum digitális lenyomatát, a megkapott digitális aláírást dekódolja a küldõ nyilvános kulcsával, majd összehasonlítja a két lenyomat jelsorozatát. Ha megegyeznek, biztos lehet benne, hogy az irat tartalma az aláírás óta nem változott és a dekódoló kulcs titkos párjával történt az aláírás. ettõl még a küldõ azonossága nem lenne bizonyított, hiszen nincs igazolva, kihez tartozik a használt kulcspár. Ezt az ûrt **hitelesítés szolgáltatók** töltik be, akik tanúsítják az aláíró személyét, azonosító adatait és az adott kulcs érvényességét. Az általuk kiadott tanúsítvány hitelességét az azt aláíró hitelesítés-szolgáltató aláírásának a közismert nyilvános kulcsával történõ ellenõrzése igazolja. A nyilvános kulcsok és a hozzájuk tartozó aláírók adatai mindenki által könnyen hozzáférhetõ adatbázisban is tárolandók, hogy a módszer széles körben, könnyen használható legyen.

A privát kulcs titokban tartása a tulajdonos felelõssége, tõle kell számon kérni ha a titkos (de személyére nem jellemzõ, tõle elválasztható) kulcsa nyilvánosságra kerül, s ezáltal elektronikus aláírása is érvényét veszti.

PGP

A leírt elveket és elektronikus aláírást a gyakorlatban alkalmazza az Interneten ingyenesen is elérhetõ PGP (Pretty Good Privacy) programcsomag. Kulcstovábbításra az RSA, üzenettitkosításra az IDEA algoritmust valamint a digitális aláíráskor generált lenyomat elkészítésére az MD5-öt használja.

Jelszavak

Szinte minden többfelhasználós rendszer jelszót kér bejelentkezéskor, illetve kapcsolatfelvételkor. A jelszó használata számos más esetben is szokásos: képernyõvédõ, setup beállítások, rendszerindítás, partíciók, könyvtárak, fájlok, adatbázisok elérésénél, programok indításánál.

Gyakran többszintû jelszavas védelmet alkalmaznak, azaz egymás után több jelszókérést kell kielégíteni a kívánt erõforrás alkalmazhatóságának eléréséhez. A jelszavas védelem más módszerekkel kombinálható (például smart kártya, ujjlenyomat), ez az ún. többfaktoros védelem, a három faktorból ("valamit tudsz, valamid van, valami vagy") legalább kettõn alapuló autentikációt nevezik erõsnek a szakirodalomban. A jelszavas védelem olcsó, könnyen kivitelezhetõ, egyszerû, jól bevált és széles körben elterjedt módszer, viszont számos gyengeséggel bír.

A jelszóval gyakorolt védelem leggyengébb láncszemei:

- Felhasználók hanyagsága, tájékozatlansága;
- nem megfelelõ jelszavak használata;
- nem biztonságos jelszó-tárolás és továbbítás;
- a felhasználó nem ismeri a fájl-megosztás biztosításának módjait, s csak a jelszó átadásával tudja más részére átadni a hozzáférést;
- program által generált, megjegyezhetetlen jelszavak alkalmazása;
- a rendszer egyes esetekben visszaírja a jelszavat a monitorra;
- õrizetlenül hagyott terminálok megfelelõ time-out nélkül.

A többször használatos (jobb esetben idõközönként lecserélendõ) jelszavak helyett terjedõben vannak az egyszer használatos jelszavak. Az egyszer használatos jelszó lényege,

hogy a jelszó a bejelentkezéskor képzõdik, és csak az adott esetben használható. Ez a folyamat a következõ:

1. Az elsõ bejelentkezéskor a többször használatos jelszó-rendszerrel azonos folyamat megy végbe.
2. A rendszer egy véletlen számot generál, és elküldi a bejelentkezõhöz.
3. A bejelentkezõ a rendelkezésére álló algoritmussal a véletlen számból jelszót készít, és azt visszaküldi.
4. A rendszer (ismerve a számot és a bejelentkezõhöz tartozó algoritmust) elõállítja a jelszót és összehasonlítja a bejelentkezõtõl kapottal.
5. Ha a két jelszó megegyezik a rendszer engedélyezi a belépést.

Azonban ha nincs mód ilyen egyszer használatos jelszavak alkalmazására, akkor érdemes a következõket figyelembe venni:

- A jelszót csak a jogosult ismerje.
- A behatolási kísérleteket naplózni kell, és például három bejelentkezés után célszerû a kísérletezést blokkolni.
- Amennyiben a terminálon meghatározott idõn belül nincs aktivitás, meg kell szüntetni a kapcsolatot (time-out).
- A jelszavakat különbözõ idõközönként cserélni kell, elõzõleg használt jelszó újabb alkalmazása tilos.
- A jelszavakat rejtjelezve kell tárolni, korlátozott hozzáférési jogosultsággal.
- A jelszó legyen:
    - nehezen kitalálható
    - szótárban nem szereplõ,
    - könnyen begépelhetõ,
    - megjegyezhetõ (például: TkMe2$t.L=”Take me to St. Louis”),
    - tartalmazzon betûket, számokat és írásjel-karaktereket.

World-Wide Web

A World-Wide Web megjelenésével az Internet átalakult, akadémiai hálózatból általános világhálózattá vált, melyen üzleti tranzakciók folynak, üzleti információk áramlanak. A Web üzleti alkalmazása töretlenül hódít, ezen akarnak vásárolni, kereskedni, pénzátutalást teljesíteni, bizalmas üzleti információkat lehívni.

Az egyre terjedõ használat egy szélesebb problémakört vet fel. Nézzük a leglényegesebb megoldandó biztonsági kérdéseket:

- felhasználó (kliens) azonosítás;
- szerver azonosítás;
- biztonságos út titkos információk számára (jelszavak, hitelkártya-információk, stb.);
- információk hitelességének ellenõrzése és hitelesítés;
- kulcs menedzsment;
- lehallgatás elleni védelem;
- kompatibilitás (például a különbözõ védelmi és titkosítási módokat alkalmazó rendszerek között);
- kliensek védelme;
- szerverek támadás elleni védelme;
- szerverek szándékos és akaratlan túlterhelése elleni védelem;
- garantált szolgáltatás elérhetõsége, megfelelõ sávszélesség, ismert korlátú válaszidõk.

Ezek a sokszor egymást is átfedõ problémákra egyértelmû megoldás nem mindig adható, hiszen a World-Wide Web technikája ehhez túl gyorsan fejlõdik.

A titkosság és hitelesítés kérdéseire napjaink megoldásai közül talán a TLS (Transport Layer Security), illetve egy másik szabványjavaslat, Netscape Co. Secure Socket Layer (SSL) szabvány tervezet és implementációi a legtöbbet ígérõek.

Dial-up kapcsolat

Napjainkban a dial-up kapcsolat mind az Internet használatában, mind a távmunkában jelentõs szerephez jutott. A felhasználók általában egy kereskedelmi szolgáltató keresztül érik el az Internetet, vagy munkahelyükre csatlakoznak modemen (esetleg terminál adapteren) keresztül.

Klasszikus biztonsági megoldásként alkalmazták a dial-back-et, azaz a felhasználó visszahívását. Ekkor a felhasználó bejelentkezik majd bont a kapcsolat és a hívott gép visszahívja (esetleg egy másik vonalon) a felhasználót. Ezzel a felhasználó telefonszámának azonosítása megoldódott. Megjegyzendõ, hogy az ISDN sokkal több biztonsági szolgáltatást nyújt, mint az analóg vonal.

Bár kapcsolt telefonvonali hívásnál is lehet alkalmazni titkosított vagy egyszer használatos jelszavakat, vagy a vonal forgalmának titkosítását, de ez gyakran nem valósul meg. Ilyenkor a dial-up jelszavaink titkosítatlanul haladnak az Internet szolgáltatóhoz vagy az egyéb online szolgáltatókhoz. Ilyen esetben érdemes tájékozódni, hogy milyen biztonsági politikát követ a szolgáltató, s milyen megoldások vehetõk igénybe. Egyes szolgáltatók nyílt biztonsági politikát követnek, mások titkolódznak. Utóbbi esetben semmi okunk a bizalomra.

A Remote Authentication Dial-In User Service (RADIUS) egy kliens-szerver protokoll és program, amely lehetõvé teszi távoli, adott esetben dial-in kapcsolattal elérhetõ szerverek számára, hogy kommunikáljanak egy központi szerverrel annak érdekében, hogy autentikálják a dial-in felhasználókat és hozzáférést biztosítsanak számukra egy adott rendszerhez vagy szolgáltatáshoz. A RADIUS biztosítja a vállalat számára a felhasználói profilok kezelését egy központi adatbázisban, melyet valamennyi remote szerver közösen használ. A központ léte azt is jelenti, hogy könnyebb a számlázás és a hozzáférés nyomonkövetése. A RADIUS a Livingstone (ma a Lucent része) alkotása, amelyet számos hálózati termékeket gyártó cég használ és így mára de facto standarddá vált.

Tűzfalak

Az Internethez való kapcsolódás veszélyeket is rejt magában, az Internet-en keresztül lehetõség válik arra, hogy ellenséges emberek, vagy csoportok illegálisan „behatoljanak” informatikai rendszerekbe, és ezen keresztül bizalmas információkhoz jussanak, ilyen jellegû információt hamisítsanak vagy semmisítsenek meg.

Ezért az Internethez való kapcsolatot körültekintõen kell kezelni.

Az intézményeknek szükségük van olyan biztonsági rendszerre (ún. **tûzfal rendszerre**), amely:

- nem engedi meg a jogosulatlan hozzáférést a belsõ erõforrásokhoz és információkhoz,
- könnyû átjárhatóságot nyújt a jogosult felhasználóknak az Internet felé,
- könnyen illeszthetõ a már meglevõ belsõ IP hálózathoz,
- egyszerûen kezelhetõ,
- opcionálisan lehetõséget ad a rendszerbe való jogosult belépésre az Internet felõl,
- felfedi a betörési kísérleteket, és a betörési kísérlet részleteit is.

A **tûzfal** egy olyan hálózati eszköz, illetve hálózati eszközök sokasága, amely szoftveres és hardveres módon elszigeteli a belsõ hálózatot a nyilvános hálózattól.

A legismertebb tûzfal rendszerek az alábbiak:

Ellenõrzõ útválasztó (screening router)

Ennél a megoldásnál az Internet kapcsolat egy ellenõrzõ útválasztón keresztül valósul meg. Ebben a megoldásban a routerben egy listában van rögzítve, hogy mely IP egységek és milyen IP szolgáltatások mehetnek és jöhetnek az Internetre és onnan. A listát nem lehet valamilyen algoritmussal generálni, kézzel kell karbantartani, és ahogy nõ az intézmény, úgy nõ a lista. Az információ áramlás engedélyezése csak az információ áramlás két végpontjától függ és nem az információ minõségétõl illetve a tranzakció jellegétõl. Ezen felül ha valahogy mégis valamilyen módon valakinek sikerül betörnie az intézet információs rendszerébe, utólag nincs meg a megfelelõ információ, hogy hogyan történt a dolog, és információ hiányában nem lehet a biztonsági elõírásokat, szoftver, hardver rendszereket úgy megváltoztatni, hogy a késõbbiekben ne történhessen meg ilyen betörés.

Ez a megoldás olyan, mintha a bank ajtajában álló õrök csak azt engednék be, akinek a neve szerepel egy kis füzetben, még akkor is ha az illetõ fején fekete harisnya és kezében pisztoly van. Ezenkívül ebben a bankban nincsenek kamerák és az õrök is mindent elfelejtenek.

Két Ethernet-es gateway (bastion gateway)

Ez a megoldás annyival jobb, mint az elõzõ, hogy itt a routert egy kapu funkciójú számítógép helyettesíti, így sokkal könnyebb karbantartani az egyes listákat (erre megvannak a megfelelõ szoftverek), kisebb a valószínûsége, hogy a lista karbantartó személyzet hibázik. Ezenkívül az egyes csomagok naplózhatóak is. Hátrány, hogy az egyes belsõ IP utakat nyilvánossá kell tenni a külvilág számára.

A hasonlat nem különbözik sokban az elõzõ megoldásétól. Itt is a füzetet nézik az õrök, és nem azt, hogy valakinek a kezében pisztoly van-e vagy betétkönyv. Most sincsenek kamerák felszerelve, de legalább az õrök emlékeznek, és képesek valamilyen személyleírást adni.

Ellenõrzött alháló (screened subnet)

Itt a belsõ hálózat ketté van választva egy belsõ zárt, és egy ellenõrzõ hálózatra. Az ellenõrzõ hálózaton az IP csomagok megállnak és ellenõrzésre kerülnek és a kapu gépen keresztül jutnak a belsõ hálózatra. Ebben az esetben a belsõ hálózat mûködése már el van rejtve, az egyes csomagok nem jutnak el a végállomáshoz ellenõrizetlenül és nem lehetséges kívülrõl direkt IP kapcsolatot létesíteni egy belsõ IP címmel. Az architektúrális különbség ez és az elõzõ megoldás között csak a kapu gép szoftverében, és az azt karbantartó személyzet felkészültségében van. A hasonlatbeli bank már nagyon hasonló egy igazi bankhoz. A kapuban õr áll, kamerák is fel vannak szerelve. Ami még mindig nem tökéletes, az az, hogy ha valaki átjutott ezen a zsilipen, az rögtön a páncélterembe jut a pénzeszsákokhoz.

Az igazi megoldás a **KAPUÕR (screen host gateway)**

A belsõ, szokás szerint kék, biztonságos hálózatot a külsõ, veszélyes, piros hálózattal egy kapu gép kapcsolja össze, de nem ez a gép végzi a teljes ellenõrzést. Ez a gép csak egy egyszerû zsilip szerepet tölt be. A külsõ piros hálózaton van a kapuõr (gatekeeper) gép, amely

ellenõrzi az egyes csomagokat - pontosabban azok fejlécét - és megállítja vagy továbbítja õket (csomagszûrés, packet filtering). A kapu gépnek csak két nagyon egyszerû szabályt kell betartania:

- · a kapuõr bármilyen csomagot beküldhet a belsõ, kék hálózatra, és a kapuõrhöz a belsõ kék hálózatról bárki kiküldhet csomagot,
- · semmilyen más címzésû csomagot nem szabad továbbengednie.

Így egy kívülrõl jövõ ping kapcsolatfelvétel elakad a kapu gépen, feljegyzésre kerül és vészjelzést ad, mint jogosulatlan kapcsolatfelvétellel való próbálkozás.

Ezzel az architektúrával a belsõ hálózat szerkezete egyáltalán nem látható kívülrõl (demilitarized zone), így ha valaki be akar törni, akkor elõször fel kell derítenie a belsõ hálózati struktúrát. Már ez a próbálkozás is sok vészjelzést generálhat. Ezután, vagy ezenközben fel kell törnie a kapuõr védelmét, ez is generál vészjelzéseket, majd ezután meg kell küzdenie a belsõ hálózati védelmekkel.

A külsõ kapuõr feltörése sokkal nehezebb, mint egy más gépé, hiszen rendkívüli módon rezisztenssé van téve az ilyen támadások ellen, többek között azzal, hogy nincsenek rajta felhasználói accountok, és minden karbantartás alkalmával, amikor a gép védelme csökken az Internet kapcsolat fizikailag ki van kapcsolva.

A felhasználók nem jutnak ki direkt módon az internet-re, hanem csak a kapuõr gépen keresztül. Ez nem jelent kényelmetlenséget, mert ezt a felhasználók nem érzékelik. Például a külsõ gépekhez való telnet kapcsolatnál a közönséges telnet program nem a külvilággal, hanem a kapuõr gépen futó telnet proxy programmal kommunikál. A telnet proxy szerver program veszi fel a kapcsolatot a külvilággal és továbbítja a felhasználó és a távoli gép között az adatforgalmat. Ezzel lehetõség nyílik a kommunkiáció figyelésére, naplózására, és ha szükséges a beavatkozásra.

Virtuális magánhálózatok

Ha egy munkatárs távolról (pl. saját otthonából) el kívánja érni a cége szerverét (pl. azért, hogy elolvassa leveleit), akkor közvetlenül a vállalati szerverrel kénytelen kapcsolatot létesíteni, amely igen költséges lehet, ha a nemzetközi telefontarifákra gondolunk. Drágaságával szemben kétségtelen elõnye, hogy a sávszélesség állandó és az üzenetet nem lehet lehallgatni.

VPN (Virtual Private Network – Virtuális Magán Hálózat) ennek Internet-es megvalósítása, amely során olyan zártközösségû hálózatot hoznak létre az Internet-en belül, amelyet illetéktelenek nem használhatnak. Hatékony, biztonságos, olcsó megoldás; a sávszélességet viszont nehéz garantálni.

A biztonság megteremtéséhez un alagút technológiát (tunneling) használnak. Ennek lényege, hogy a cég belsõ hálózatán (LAN) használt adatokat elõször a céges szerver titkosítja, majd a titkosított üzenetet IP csomagokká alakítja és így küldi el a felhasználónak.

Az alagút technológiával lehetõség nyílik továbbá multiprotokoll technológia alkalmazására is. Ekkor a titkosított IP csomagok egyben a cég belsõ hálózatán (LAN) használt protokoll (pl IPX) csomagjai amely lehetõvé teszi, hogy a felhasználó számára a kapcsolat úgy jelenjen meg mintha közvetlenül a cég belsõ hálózatához csatlakozott volna.

VPN-t számos eszköz segítségével létre lehet hozni. A jövõben leginkább talán az IPSEC fog elterjedni. Windows rendszer alatt a Microsoft PPtP megoldása is igen elterjedt, azonban ebben például már számos komoly biztonsági hiányosságot találtak.

SecurID

Az RSA cég SecurID tokenje segítségével felhasználók azonosítása végezhetõ el két faktor alapján. Ebbõl az egyik egy jelszó (amit tudnak), a másik pedig amit birtokolnak, ez a SecurID token. Így erõs autentikáció valósítható meg.

Mivel a SecureID kulcsgenerátor 60 másodpercenként új kódot állít elõ, így a megoldás védett a visszajátszás típusú támadások ellen is (ami pl. az egyszerûbb tokenes megoldásokat vagy biometrikus autentikációs megoldásokat sebezhetõvé teszi).

SecurID támogatást mára számos népszerû termékbe építettek bele, mint az Axent, Check Point, Cisco, CyberGuard, NetScreen, Nokia, WatchGuard és több mint 130 más gyártó termékeibe.

PKI

A nyilvános kulcsú (PKI - Public Key Infrastructure) a nyílt távközlési hálózatokon (pl. Internet) napjainkban alkalmazott elektronikus biztonsági rendszer. Alapja az aszimmetrikus kulcsú titkosítás, melynek segítségével elektronikus aláírási funkciót valósít meg.
Az összetartozó kulcsok egyikével kódolt elektronikus adatsort csak a másik, hozzá tartozó kulccsal lehet dekódolni. A felhasználó kizárólagos birtokában lévõ, ún. magánkulcs az elektronikus aláírás létrehozására (kódolás) használható. Az ehhez tartozó nyilvános kulcs az elektronikus aláírás ellenõrzésére (dekódolás) szolgál.
A nyilvános kulcsot egy hitelesítõ szervezet által hitelesített és a nyilvánosságra hozott tanúsítvány tartalmazza, ezáltal a nyilvános kulcshoz tartozó magánkulcs birtokosának, vagyis az üzenet küldõjének azonosítása a tanúsítvány alapján egyértelmûen lehetséges.

A PKI segítségével egyaránt megvalósítható a bizalmasság, nyomonkövethetõség, az üzenet sértetlenségének és letagadhatatlanságának a biztosítása.

A PKI az alábbi komponensekbõl áll:

- Certificate Authority (CA, hitelesítõ szervezet), ami kiadja és hitelesíti a digitális tanúsítványokat. A tanúsítvány tartalmazza a nyilvános kulcsot vagy információt róla.
- Registration Authority (RA, regisztrációs szervezet), amely a hitelesítõ szervezet számára ellenõrzõ szerepet tölt be, mielõtt a digitális tanúsítványt kiadják a kérelmezõnek.
- Egy vagy több könyvtár, ahol a tanúsítványokat és a hozzájuk tartozó nyilvános kulcsot tárolják és könnyen hozzáférhetõvé teszik.
- Tanúsítvány menedzsment rendszer.

SSL

Az SSL egyrészt az egyik legegyszerûbb PKI-implementáció. Az SSL egy teljes értékû nyilvános kulcsú hitelesítést és titkosítást megoldó adatcsatorna, mely a sebesség növelése érdekében a tényleges adatforgalmat privát kulcsú titkosítással oldja meg, melyhez a privát kulcsot nyilvános kulcsú titkosítás segítségével (többnyire RSA) keresztül cserélik ki a kliensek.

Az SSL másrészt egy általános célú, nyitott, szabadon felhasználható, viszonylag alacsony szintû protokoll. Az SSL elsõsorban a szállítási rétegben helyezkedik el, valahol az alkalmazási réteg és a TCP között. Szigorúan egyik réteghez sem köthetõ egyedül, és ez több nehézséget is okoz.

Az SSL protokollt arra tervezték, hogy biztosítsa TCP/IP kapcsolatok felett a hiteles azonosítást, a bizalmasságot és a sértetlenséget.

Az SSL protokoll minden új kommunikációs kapcsolat felvételekor kiválaszt egy kódolási algoritmust és egy eseti kulcsot, és egyúttal autentikálja a szervert mielõtt az alkalmazás-protokoll elküldi vagy fogadja az elsõ adatbájtot. Minden adat kódolva kerül elküldésre a kétoldali biztonság érdekében.

Az SSL kapcsolatfelvételi kézfogás során a nyilvános kulcs(ok) egy X.509 formátumú bizonyítvány részeként kerülnek átvitelre. Egy X.509 bizonyítványt arra használnak, hogy ellenõrizzék, hogy a nyilvános kulcs valóban a bizonyítványt felmutató személyé-e. A bizonyítványt alá kell írnia egy Hitelesítõ Szervezetnek (Certification Authority), akiben a bizonyítványt ellenõrzõ fél megbízik. Az International Telecommunications Union (ITU) az X.509 ajánlásában definiálja a bizonyítványok standard formátumát. A bizonyítvány szerepe, hogy egy entitás nevét hozzárendelje egy nyilvános kulcshoz. A Hitelesítõ Szervezet vagy CA (Certificate Authority) egy olyan megbízható hatóság, amely az entitás nevét és nyilvános kulcsát egy bizonyítványban igazolja.

A kliens illetve a szerver az SSL kézfogás során elküldik egymásnak a „bizonyítvány láncukat”, amely tartalmazza a saját bizonyítványukat és az aláírók bizonyítványait. A protokoll szerint nem szükséges, hogy az alkalmazások az összes bizonyítványt ellenõrizzék, elég ha addig vizsgálják azokat, amíg egy általuk megbízhatónak tartotthoz érnek.

A kapcsolatfelvétel után a hatékonyság növelése érdekében a két oldal szimmetrikus kulcsú titkosításra vált át.

Az SSL alapú kommunikáció során tehát megvalósítható a magas szintû bizalmasság. A nyomonkövethetõség abban az értelemben teljesül, hogy reprodukálható, hogy ki és mikor lépett kapcsolatba a kliens és a szerver, de az nem, hogy eközben milyen mûveletek történtek, milyen adatok cserélõdtek ki. Hasonlóan valósul meg a letagadhatatlanság is: az bizonyítható, hogy mikor és kik léptek egymással kapcsolatba, de az nem, hogy eközben mivel foglalkoztak.

Az SSL-re épült megoldások tekinthetõek a virtuális magánhálózatok egy típusának is. Az SSL néhány feladatra igen jól használható, azonban nem általános VPN-es alkalmazásra lett tervezve.

HTTPS

A HTTPS (Hypertext Transfer Protocol a Secure Socket Layer felett) egy web protokoll, melyet a Netscape fejlesztett ki és épített bele a web böngészõjébe, hogy titkosítsa a felhasználók web oldal kéréseit és az erre küldött válaszokat. A HTTPS valójában az SSL, mint alacsonyabb szintû réteg használatát jelent a hagyományos HTTP protokoll által. A HTTPS a 443-as portot használja az alacsonyabb réteggel való kommunikációhoz a HTTP hagyományos 80-as portja helyett.

Az SSL-hez hasonlóan a HTTPS is X.509 digitális tanúsítványt használhat autentikálási célra.

A HTTPS nem keverendõ össze az S-HTTP-vel, amely a HTTP-nek egy biztonsági szempontból javított változata. Az S-HTTP-t az EIT fejlesztette ki és javasolta szabványként, de eddig nem igazán terjedt el.

Kerberos

A Kerberost a MIT Athena Projekt keretében fejlesztették ki a Needham-Schroeder protokollra alapozva. A Kerberos egy elosztott hitelesítési és kulcskiosztási szolgáltatás, ami lehetõvé teszi a rendszer egy szereplõje (a továbbiakban kliens) számára, hogy bebizonyítsa személyazonosságát az azt ellenõrzõ félnek (a továbbiakban szervernek) anélkül, hogy a

hálózaton keresztül küldött adatokat egy támadó, vagy esetleg a szerver fel tudná használni a kliens megszemélyesítésére.

A leegyszerûsített rendszerben három szereplõt különböztethetünk meg: a Klienst, a Szervert, és a Kerberos Hitelesítési Rendszert (Kerberos Authentication System), röviden Hitelesítõt.

A Hitelesítõ egy adatbázisban nyilvántartja a rendszer szereplõit és azok titkos kulcsait (vagy másnéven szerver kulcsait). Mivel csak a Hitelesítõ ismeri az egyes szereplõk kulcsait, ezért képes olyan üzeneteket generálni, amelyek meggyõzik a rendszer egyik szereplõjét a másik személyazonosságáról. Emellett a Hitelesítõ kapcsolati kulcsokat is generál, amelyek két fél közötti kommunikáció során a rejtjelezésre valók, és a kapcsolat végén megsemmisülnek.

A protokoll a rejtjelezéshez a DES algoritmust használja, a Kerberos Version 5 a CBC[2] módot alkalmazza.

Adatbáziskezelők által közvetlenül támogatott megoldások

Bizonyos adatbáziskezelõk beépített szolgáltatásként kínálják, hogy az adatbázisszerver és az adatbáziskliens között a kapcsolat biztonságosan (is) megvalósítható legyen.

Az Oracle Advanced Security (OAS) lehetõvé teszi kliensek egyértelmû azonosítását (akár jelszavakkal, SecureID-vel, tokenekkel, X.509 tanúsítványokkal vagy külsõ autentikációs szerverekkel), a kapcsolat titkosítását egy sor algoritmussal (mint 3DES, RC4_40, RC4_56, RC4_128, RC4_256, DES, DES_40).

4.3.3.3. Magyar jogi szabályozás

Jogi értelemben az információvédelmi tevékenység – figyelemmel az adat- és titokvédelem hazai és nemzetközi normáira, a magyar jogszabályi környezetre – védelmi követelményeket és lehetõségeket jelent biztonsági feladataink megtervezéséhez, elvégzéséhez. Csak olyan védelmi-biztonsági elõírások, mechanizmusok alkalmazása indokolható, amelyek a rendelkezésre álló lehetõségek (emberi erõforrások, tárgyi, technikai, anyagi feltételek) mellett végrehajthatók.

Az információk végül is vagyoni értéket jelentenek, ez az érték viszont tulajdonjog tárgyát is képezheti. A tulajdonjog tartalmilag a birtoklás, a használat, és a rendelkezés jogát jelenti. E jogokat pedig emberek, természetes személyek gyakorolhatják még akkor is, ha történetesen a tulajdonos nem természetes, hanem jogi személynek minõsül.

Úgy is mondhatjuk, hogy az információvédelem a vagyonvédelem egyik sajátos jogterületének is minõsíthetõ, és mint ilyen, nem maradhat érintetlen a jogszabályok által sem. Emiatt kimondható, hogy az információvédelem jogi szabályozásának céljai a következõk:

1. az információ, mint vagyoni érték megõrzése;
2. az ismerettel rendelkezõ körön kívüli jogosulatlan elõnyhöz jutás megakadályozása, elrettentés;
3. az ismerettel rendelkezõ körbõl vagy a körön kívülrõl eredõ titoksértés elkövetésének megállapíthatósága;

[2] Blokk kódolóknál CBC (Cipher Block Chaining) üzemmódban minden egyes blokk rejtjelezése függ az azt megelõzõ összes blokktól, ezáltal az üzenet nehezebben támadható.

4. az esetleges titoksértõ személyek leleplezése és cselekményének szankcionálása polgári jogi, ezen belül munkajogi és büntetõjogi eszközökkel.

Magyar törvények, rendeletek

A biztonsággal kapcsolatos feladatok irányításához olyan hatékony eszközökre van szükség, amelyek pontosan leírják, meghatározzák, kikényszeríthetõvé és ellenõrizhetõvé teszik a tennivalókat, jogokat és kötelességeket. Az irányítás, szabályozás leghatékonyabb eszközeinek a szabályzatokat, intézkedéseket tekinthetjük.

Míg vállalati szinten ezek az intézkedések általában vezérigazgatói, vagy más vezetõ, esetleg testület által kiadott utasításban testesülnek meg, állami szinten számos formában léteznek biztonsági vonatkozású szabályozók. Például:

- § Alkotmány,
- § Államigazgatási törvény,
- § Miniszteri rendeletek,
- § Polgári Törvénykönyv,
- § Munka Törvénykönyve,
- § Büntetõjogi Törvénykönyv,
- § Tûzvédelmi Törvény,
- § Vagyonvédelmi Törvény,
- § ágazati törvények, rendeletek, szabályzatok (például Pénzintézeti Törvény),
- § egyéb rendeletek, szabályzatok,
- § magyar szabványok.

A jogilag védett információk körében kiemelt figyelmet érdemelnek az üzleti titkok. Ezek jogi védelme nélkül elképzelhetetlen a gazdasági élet folyamatainak vagyonbiztonsága, az információk védelméhez kapcsolódó vagyoni jogok gyakorlása. Üzleti titok megsértésének szankcionálásáról gondoskodik az 1990. évi LXXXVI. és az 1991. évi LXIX. törvény.

A számos szabályozás közül például a tisztességtelen piaci magatartás és versenykorlátozás tilalmáról szóló 1996. évi LVII. tv. 4. §-a szerint tilos üzleti titkot tisztességtelen módon megszerezni vagy felhasználni, valamint jogosulatlanul mással közölni vagy nyilvánosságra hozni. Üzleti titok tisztességtelen módon való megszerzésének minõsül az is, ha az üzleti titkot a jogosult hozzájárulása nélkül, vele – titok megszerzése idején vagy azt megelõzõen – bizalmi viszonyban vagy üzleti kapcsolatban álló személy közremûködésével szerezték meg.

Természetesen a Btk. is büntetni rendeli az üzleti titok megsértését: “Aki üzleti titkot haszonszerzés végett, vagy másnak vagyoni hátrányt okozva jogosulatlanul megszerez, felhasznál vagy nyilvánosságra hoz, büntetendõ.”

Az elektronikus aláírásról szóló törvény

Az elektronikus aláírásról szóló törvény az elektronikus aláírások három típusát különbözteti meg. Ezek az "egyszerû" elektronikus aláírás, a fokozott biztonságú elektronikus aláírás és a minõsített elektronikus aláírás.

- "**Egyszerû" elektronikus aláírás**: ide tartozik mindenfajta, akár a technológiai biztonságot nélkülözõ eljárás (pl. ha az aláíró egy elektronikus szöveg végére odaírja a nevét vagy más azonosítóját). A törvény kimondja, hogy az aláírás elfogadását megtagadni nem lehet kizárólag amiatt, hogy elektronikus formában létezik.
- **Fokozott biztonságú elektronikus aláírás**: olyan elektronikus aláírás, amely az aláíróra és az aláírandó dokumentumra egyaránt jellemzõ elektronikus adatsor. Ha

jogszabály írásban foglalást ír elõ, a fokozott biztonságú elektronikus aláírással aláírt elektronikus irat e követelménynek eleget tesz.

- **Minõsített elektronikus aláírás**: olyan fokozott biztonságú elektronikus aláírás, amely biztonságos aláíró eszközzel készült és melynek hitelesítése céljából minõsített tanúsítványt bocsátottak ki. A minõsített elektronikus aláírással ellátott elektronikus dokumentum teljes bizonyító erejû magánokiratnak minõsül.

A fokozott biztonságú elektronikus aláírás ma Magyarországon gyakorlatilag PKI-n alapul, ezért:

- alkalmas az ellenõrzés során alkalmazott eljáráson és a hozzá tartozó tanúsítványon keresztül az aláíró személyének azonosítására;
- egyedülállóan az aláíróhoz köthetõ;
- olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll;
- lehetõvé teszi a dokumentum tartalmának az aláírás elhelyezését követõ bármely megváltozásának kimutathatóságát;
- biztosítja az aláírás megtörténtének letagadhatatlanságát.

Az aláírás létrehozó eszközök megfelelõségének tanúsítására erre specializálódott, a gyártótól független tanúsító szervezetek jogosultak. A kijelölt tanúsító szervezetekrõl és az általuk tanúsított aláírás-létrehozó eszközökrõl a Hírközlési Fõfelügyelet nyilvántartást vezet és teszi közzé. Ha egy tanúsított eszköz szerepel a Hírközlési Fõfelügyelet nyilvántartásában, akkor az ellenkezõ bizonyításáig feltételezni kell, hogy az aláírás-létrehozó eszköz biztonságos.

A HÍF elektronikus aláírással kapcsolatos nyilvántartásai

Fokozott biztonságú szolgáltatók: (A fokozott biztonságú szolgáltatás végzését a belföldi lakóhelyû vagy belföldön tartózkodási hellyel rendelkezõ természetes személy, illetve belföldi székhelyû (telephelyû) jogi személy vagy jogi személyiség nélküli szervezet 30 nappal a megkezdést megelõzõen köteles bejelenteni a Felügyeletnek. (Eat. 7§ (1) bekezdés))

- GIRO Elszámolásforgalmi Rt.
- Magyar Távközlési Részvénytársaság
- Microsec Számítástechnikai Fejlesztõ Kft.
- MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.
- NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft.

Minõsített szolgáltatók: (Minõsített hitelesítés-szolgáltató: az Eat 8. § (3) bekezdése szerint nyilvántartásba vett hitelesítés-szolgáltató. (Eat. 2§ 18) pont). A szolgáltatókra vonatkozó részletes követelményeket az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekrõl szóló 16/2001. (IX. 1.) MeHVM rendelet tartalmazza.)

Ilyen szolgáltató ma Magyarországon egy sincs.

Tanúsított elektronikus aláírás termékek: (Az aláírás-létrehozó eszköz: olyan hardver, illetve szoftver eszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza. Elektronikus aláírási termék: olyan szoftver vagy hardver, amely elektronikus aláírással kapcsolatos szolgáltatások nyújtásához,

így különösen elektronikus aláírások illetõleg idõbélyegzõ készítéséhez vagy ellenõrzéséhez használható.(Eat 2§ 3) és 11) pont))

Ilyen készülék jelenleg mindössze 4-fajta van Magyarországon:

- Eracom CSA 8000 Adapter
- IBM 4758-002 PCI
- Kopint-Dat MultiSigno Developer aláíró alkalmazás fejlesztõ készlet
- Kopint-Datorg Rt. MultiSigno Standard aláíró alkalmazás komponens.

4.3.3.4. A KRA biztonsága

Ez egy elemzõ jellegû fejezet, amely összegyûjti a legfontosabb, 2003. februárjában rendelkezésre álló információkat a KRA biztonságával összefüggõ kérdésekrõl

4.3.3.4.1. Bizalmasság

A bizalmasságot biztosító megfelelõ módszerek kiválasztásához elõször arra kell tudni választ adni, hogy mit okozhat a legrosszabb esetben, ha a KRA adatainak bizalmassága sérül.

Nyilvánvalóan nem azonosak a KRA különbözõ adatai ebbõl a szempontból. Elöljáróban szögezzük le azt, hogy a *számhordozási referencia adatbázis* nem fog tartalmazni olyan *hívószámokat*, amelyek nemzetbiztonsági szempontból kritikusak lehetnek. Ezt az teszi lehetõvé, hogy elvileg a referencia adatbázis nélkül is lehetséges a számhordozás megvalósítása, illetve akár azt is feltételezhetjük, hogy az ilyen kritikus számok hordozását nem akarjuk támogatni, vagy kiindulhatunk abból, hogy a szám önmagában nem árulja el azt, hogy az különösen védendõ.

Már korábban is megállapítottuk, hogy ettõl függetlenül is kétféle érzékenységû adatcsoport különíthetõ el: szolgáltatók számára nyilvános és a szolgáltatók számára nem nyilvános. A szolgáltatók számára nyilvános adatok még szélesebb körben való nyilvánossá válása leginkább személyes érdekek sérelmét eredményezheti, amennyiben valamely elõfizetõ egyébként nem kívánja nyilvánosságra hozni, hogy melyik szolgáltatótól melyikhez pártolt át. A szolgáltatók számára nem nyilvános adatok (a hordozás bejelentésének idõpontja, a hordozás bejelentésének ügyiratszáma és egyéb adatok) legfeljebb az "egyéb" adatok között tartalmazhat olyat, amelynek a szükségesnél szélesebb körben való ismertté válása érdemleges kárt okozhat. Azonban még az egyéb adatok között sem lesznek nemzetbiztonsági szempontból érzékeny adatok. Ezen információk alapján lehet megítélni, hogy mekkora kárt okozhat a KRA adatai bizalmasságának sérülése és így mekkora kockázatot jelentenek a lehetséges veszélyforrások (ld. Veszélyforrások c. fejezet).

4.3.3.4.2. Nyomonkövethetõség

A KRA adatainak a valódi értékét elsõsorban az határozza meg, hogy ennek alapján határozza meg a HÍF a szolgáltatók számára a hívószámok használata után fizetendõ díjat. Ha tehát a KRA-ba téves/hamis adatok kerülnek, az nemcsak az érintett hívószámok használhatóságát fogja befolyásolni, hanem közvetlenül forintosítható kárban, ill. haszonban jelentkezik a szolgáltatóknál. Emellett meg kell emlékeznünk az okozott erkölcsi kárról is.

A KRA-ba írás a jelenlegi szabályozás szerint mindenképpen a számot fogadó szolgáltató közlése alapján fog történni vagy papíros vagy elektronikus alapon. A KRA-hoz

így eljuttatott adatok ellenõrzésére a lehetõségek erõsen korlátozottak (mint láttuk, a hívószám adatbázissal való összekapcsolás jelent valamennyi segítséget ebben). Ennélfogva elsõsorban annak van jelentõsége, hogy pontosan kideríthetõ legyen, hogy bármely adat honnan, mikor és hogyan került be az adatbázisba. A nyomonkövethetõség kritériuma éppen fogalmazza meg.

A nyomonkövethetõség biztosításának alapvetõ eszköze a napló. A KRA-ban az elképzelések szerint minden adatot egyetlen adatbázisban fogunk tárolni. Ha a naplózás képes arra, hogy minden, az adatbázison végzett mûveletet rögzítsen, akkor reprodukálhatókká válnak az *adatbázison* véletlenül vagy szándékosan elkövetett módosítások, bizonyos illetéktelen hozzáférések. Minimálisan rögzíteni kell minden adatbázis tranzakció

- tulajdonosát,
- időpontját,
- az általa végrehajtott műveleteket.

Megfontolandó, hogy szükséges-e a tranzakciók által írt/olvasott adatokat is naplózni. A mai adatbáziskezelõk erre többnyire lehetõséget adnak és a naplózandó adatokat széles skálán be lehet állítani. Tudni kell ugyanakkor, hogy a rendszer erõforrásigényét mindez jelentõsen megnöveli.

Másrészrõl, a KRA nemcsak az adatbázisból áll, hanem a hozzá kapcsolódó alkalmazásokból is. Ezeknek az alkalmazásoknak is lehetnek olyan funkcióik, amelyek adatbázismûveletet (még) nem eredményeztek, mégis fontos lehet az adott mûvelet aktiválásának nyomonkövetése. Ilyen ok lehet pl. a különbözõ adatbetörési kísérletek vagy a szolgáltatás megbénítására tett kísérletek észlelésének az igénye. A nyomonkövethetõség érdekében tehát az adatbázismûveletek naplózását ki kell egészíteni az egyéb, a KRA más architekturális elemeinek (pl. tûzfal, esetleges web-szerver,…) mûködésével kapcsolatos mûveletek naplózásával is.

4.3.3.4.3. Sértetlenség

Ha már tudjuk azt, hogy a KRA-ba bizonyos adatokat ki (vagy mi) írt be, a következõ lépés annak a bizonyítása, hogy az adatbeírást kezdeményezõ valóban azt az adatot kívánta beírni, ami végül bekerült az adatbázisba. Ennek érdekében garantálni kell, hogy a szolgáltatóktól a KRA-ig eljuttatva az adatokat azok semmilyen torzulást ne szenvedhessenek el.

A KRA adatainak sérülése kettõs veszéllyel járhat:

1. egyrészt anyagi veszteséggel, mert számlázás alapjául szolgáló adatokat tartalmaz,
2. másrészt a távbeszélõ szolgáltatás zavaraival, mert téves vagy egyáltalán nem igényelt hívásátirányításokat okozhat.

A KRA sérülését elsõsorban az alábbi tényezõk okozhatják:

1. hibás adatbevitel a számhordozást bejelentõ szolgáltató oldalán, illetve a papíros alapú bejelentés következtében
2. adatátviteli vonalon fellépõ adathiba (csomagvesztés)
3. emberi hiba következtében hibás/hiányos adatok elektronikus küldése
4. illetéktelen adatmanipuláció

5. rendszerhiba az adatbáziskezelõben.

Ezek közül az 1. tûnik a legvalószínûbbnek, amely ellen egyúttal nagyon nehéz védekezni is (de azért lehet: four eyes principle).

A 2. ellen hatékony védelmet jelenthet egy alkalmas magas szintû rétegprotokoll, amely nyugtázási/újraküldési mechanizmusokkal biztosíthatja az elküldött üzenetek sértetlenségét.

A 3. hiba és kezelése az elsõhöz hasonlít.

A 4. ellen hatékonyan védekezhetünk, ha biztosítjuk azt a követelményt, hogy az adatbázisba csak olyan adatok kerüljenek be, amelyeket legalább "fokozott biztonságú" elektronikus aláírással (ld. az elektronikus aláírásról szóló törvényt) hitelesítettek [9].

Végül az 5. tényezõ ellen alkalmasan választott, bevált adatbáziskezelõ választása védhet, ezen kívül rendszeres biztonsági másolatok készítése, redo állományok redundáns adathordozón való tárolása, vagy akár a teljes szerver duplikálása.

4.3.3.4.4. Letagadhatatlanság

Ha a KRA-ba adatokat írtunk be (melyekre elértük, hogy se nem torzultak, se nem férhettek hozzá illetéktelenek), még azt is biztosítani kell, hogy az adatot bizonyíthatóan csak egyetlen személy vagy szervezet küldhesse. A gyakorlatban ez a letagadhatatlanság követelményének megvalósítását jelenti.

Amennyiben nem lenne egyértelmûen megállapítható, hogy egy adott bejegyzést az adatbázisba ki tett, annak a következményei:

- a telefonszámok (esetleg akár tömeges) rosszindulatú átirányítása esetén nem bizonyítható, hogy kit terhel az anyagi és erkölcsi felelõsség. Ez különösen egy szabotázs esetén beláthatatlan következményekkel járhat.
- a számok használata után fizetendõ díjak téves számlázása estén nem bizonyítható, hogy ki tévedett vagy okozott szándékosan kárt.

Egy üzenet letagadása elleni védekezésnek a standard módja, hogy egy olyan elektronikus aláírást helyeznek el az üzeneten, amely egyrészt biztosítja az üzenet sértetlenségét, másrészt egyértelmûen azonosítja a küldõjét is.

Mivel az üzenet és annak az adatbázisba írása között akár még torzulhat is, ennek elkerülésére a bejövõ üzenetnek a naplózása is szükséges, mégpedig az aláírással együtt. Így lehet késõbb a KRA tartalmát ellenõrizni, hogy a kérdéses bejegyzéseket valóban annak a szolgáltatónak a kezdeményezésére tették-e, akihez a KRA-ban tartozik.

4.3.3.4.5. Rendelkezésreállás

A számhordozhatósági központi referencia adatbázis rendelkezésreállása nem kritikus szintû. A szolgáltatók naponta max. néhányszor fordulnak a rendszerhez, ráadásul ennek akár sok órás - de akár egy-két napos - késlekedése sem feltétlenül eredményez észrevehetõ szolgáltatáskiesést vagy hibás számlázást, hiszen a számhordozás KRA-ba bejelentése napokkal meg kell elõzze a hordozás fizikai megvalósításának kezdetét.

A rendelkezésreállást alapvetõen veszélyeztetõ tényezõk:

1. szerverhiba

2. diszkhiba
3. adatátviteli vonalak sérülése
4. adathálózati hardver elemek meghibásodása
5. szoftverhiba (például vírus által okozott sérülés következtében)
6. katasztrófa.

Az 1. tényezõ ellen egy hidegtartalék szerver vagy egy 1-2 napos garantált javítást biztosító szupport megoldás elegendõ védelmet nyújt.

A 2. diszkhibák ellen valamilyen redundáns megoldással (RAID) és a diszkek rendszeres ellenõrzésével valamint/vagy backup rendszeres készítésével védekezhetünk.

A 3. elhárítása esetleg tetemes idõt igényelhet, ez ellen a védelmet alternatív összeköttetés megléte jelentheti.

A hálózati hardver elemek hidegtartalékban való megléte elegendõ védelmet nyújt 4. ellen.

A szoftverhibák ellen egyrészt a diszkhibák elleni védekezés egyes módszerei lehetnek hatásosak, másrészt folyamatosan frissített vírusvédelmi megoldások alkalmazása.

A katasztrófa által okozott kiesésen csak több 10 km-re lévõ tartalékrendszer segíthet, de nyilván az adatmentésekbõl kell távol is tárolni egy példányt

4.3.3.4.6. Archiválás

Az archiválás a KRA nem kritikus funkciója. Mindazok a módszerek, amelyek egy átlagos célú, kis-közepes méretû információs rendszer adatainak archiválására alkalmasak, itt is megfelelnek. Az adatmennyiség kifejezetten kicsinek mondható, az adatok dinamikája sem nagy, ráadásul a rendszer indulása után néhány évig az archiválásra semmi szükség sincsen, hiszen a rendszer erõforrásai- megfelelõ tervezés esetén - ezt egyáltalán nem teszik indokolttá.

4.3.3.5. Megoldási lehetõségek

Jelen fejezet nem kísérli meg, hogy a kizárólagosság igényével fogalmazzon meg elvárásokat a KRA fizikai megvalósításával kapcsolatban. Nem célja továbbá a tanulmánynak konkrét mûszaki tervek készítése vagy konkrét megoldási javaslat kidolgozása sem. A jelenleg ismert feltételek mellett a lehetséges alternatívák száma még mindig nagy. Ezek közül pl. gazdaságossági szempontok, korábbi üzemeltetési tapasztalatok, az elérhetõ biztonság foka, mint legfontosabb szempontok alapján lehet kiválasztani a legkedvezõbbet.

Alábbiakban csak a legfontosabb következtetéseket rögzítjük.

4.3.3.5.1. Adatbázis szerver

Célszerûen egy Unix alapú, kis teljesítményû szerver, elsõsorban a stabil és folyamatos üzemeltethetõség érdekében. A diszk alrendszere valamely RAID megoldás, akár tükrözés is lehet, hiszen az adatmennyiségek nem indokolnak bonyolultabb megoldásokat.

4.3.3.5.2. Adatbáziskezelõ

Nincs szükség a legmodernebb, legdrágább DBMS-re. A rendszer az üzemidejének nagy részében várakozni fog. A konkurencia foka várhatóan alacsony. A válaszidõk nem kritikusak és várhatóan nem is az adatbáziskezelõ fogja meghatározni, hanem az adatátviteli vonalak sávszélessége. Legalább háromféle jogosultsági szintet kell tudni kezelnie és képesnek kell lennie lehetõleg folyamatos üzemben is mûködnie. Az adatbázismûveletek naplózhatósága fontos követelmény és itt elõny, ha nemcsak a mûveletek kódja és a kezdeményezõjük kerül bele a naplóba, hanem maguk az adatok is.

4.3.3.5.3. Kommunikációs hálózat

A KRA közvetlen környezete egy LAN, amelyen keresztül az üzemeltetési feladatok elvégezhetõk és az adatbázisnak az ad-hoc lekérdezése, a kezdeti idõben pedig a papíros alapú adatbevitel megoldható. A szolgáltatókkal célszerûen menedzselt bérelt vonalakon keresztül érdemes a kapcsolatot tartani, hiszen ezek védettebbek a kapcsolt vonalaknál, továbbá meghibásodását a szolgáltató figyeli és automatikusan gondoskodik a fizikai kapcsolat helyreállításáról. A szolgáltatók és a KRA közötti kommunikáció sávszélességigénye alacsony, normál üzemben (hordozott számok feltöltése, KRA változások letöltése) kifejezetten kevés adat forgalma várható, egy 64 kbit/sec sebességû kapcsolat megfelelõ. A nagyobb sávszélességet csak a teljes letöltések idejének csökkentése tenné indokolttá. Ugyanakkor ezek csak váratlan és így vélhetõen igen ritka esetekben fordulnak elõ, amikor akár az adatok mágneslemezen történõ közvetlen szolgáltatókhoz való eljuttatása is szóba jöhet. Nem feltétlenül érdemes tehát ez utóbbi esetekre méretezni a sávszélességigényt.

Alternatívaként felmerülhet természetesen akár egy Internet alapú, akár a nyilvános kapcsolt hálózaton keresztül történõ adattovábbítás is. A biztonságtechnika jelenlegi szintje mellett elvi akadálya nincsen ilyen megoldások kialakításának sem, ugyanakkor az alkalmazandó biztonságtechnikai megoldások drágábbak lesznek ezekben az esetekben. Részletesebb tervezés és áranalízis alapján lehet a kérdést eldönteni.

4.3.3.5.4. Biztonsági komponensek

Az alkalmazható megoldások nagyban függenek a szolgáltatók és a KRA között kialakított kommunikációs csatorna jellegétõl. Elsõ közelítésben induljunk ki privát bérelt vonali összeköttetésekbõl. Ekkor a KRA külsõ támadások általi fenyegetettsége várhatóan az átlagosnál lényegesen kisebb lesz, hiszen mûködése elsõsorban néhány hazai távközlési céget és a HÍF-et érinti és véletlenül aligha válik hackerek célpontjává. A "támadás" ilyenkor - legalábbis közvetetten - a szolgáltatók vagy a színes számokat kiszolgáló tartalomszolgáltatók részérõl várható elsõsorban, hiszen másnak nemigen van kimutatható érdeke a KRA mûködésének megzavarására.

[4] szerint a fogadott (és küldött) adatok legyenek minõsített elektronikus aláírással hitelesítettek. A minõsített elektronikus aláíráshoz azonban minõsített hitelesítés szolgáltatóra lenne szükség, amilyen ma Magyarországon még nincs. A minõsített elektronikus aláírás biztosítása tehát jelenleg (2003. február) még nehézségekbe ütközik. Másrészt nem is biztos, hogy valóban szükséges ez a szigorú követelmény. A bankok között pl. régóta mûködik az elektronikus átutalások rendszere e nélkül is, tehát önmagában az a tény, hogy a KRA adatait számlázásra is felhasználja a HÍF, még nem indokolja a minõsített elektronikus aláírás

használatát. Másrészt a KRA tartalmát valamennyi szolgáltató folyamatosan láthatja, így elvileg észlelheti az összes, õt esetleg hátrányosan érintõ rossz bejegyzést. Ettõl kezdve véleményünk szerint a biztonságra engedmények tehetõk.

Egy egyszerû, de mégis kellõen hatékony megoldás lehet egy VPN kialakítása SecureID tokenekkel, kombinálva szimmetrikus kulcsú titkosítással. Ebben az esetben erõs autentikáció megvalósítható, biztosítva annak letagadhatatlanságát, hogy ki és mikor lépett kapcsolatba a KRA-val. A kommunikáció tartalmának elmentése megvalósítja annak reprodukálhatóságát, hogy mit küldött a szolgáltató. Egy 3DES vagy hasonló erõsségû titkosítást használó, adatcserét biztosító kliensprogrammal viszonylag egyszerûen eleget tehetünk a bizalmasság és a sértetlenség követelményének is. Ilyenkor tehát a szolgáltatók között alapvetõen állománycserét tudunk megvalósítani.

Egy elegáns alternatíva lehetõsége merül fel pl. Oracle adatbáziskezelõ alkalmazása esetén. Az Oracle 8i (és magasabb) verziói java alapú kliensek és az Oracle Advanced Security szolgáltatás segítségével szintén lehetõvé teszik a kliens oldali felhasználó erõs autentikálását, valamint itt is megvalósítható a kommunikáció titkosítása pl. a 3DES algoritmussal. Ezzel a megoldással közvetlenül a KRA adattábláival tudnak a szolgáltatók kapcsolatba lépni (természetesen csak annak egy erre a célra szolgáló bufferével/másolatával), így a szolgáltatók valóban akkor és azt kérdezhetnek le az õket illetõ adatokból, amit csak akarnak. Elegánsan megoldható a szolgáltató által küldött adatok naplózása is, ha az adatbeviteli táblába egyszer beírt adatokat nincs joguk késõbb törölni.

Amennyiben a szolgáltatók és a KRA között pl. az Internetet használjuk kommunikációs közegként, akkor természetesen tûzfal megoldásra is szükség van, ez esetben viszont gondoskodni kell a támogatott kommunikációhoz tartozó csomagoknak a tûzfalon való átjuttatásáról is.

4.3.3.5.5. Rendelkezésreállás

Mint már kifejtettük, a KRA rendelkezésre állása nem kritikus. A szerver kellõen robosztussá tehetõ duplikált diszkekkel és a gép 1-2 napon belüli javítását biztosító support szerzõdéssel. A kommunikáció rendelkezésreállása tartalék útvonalakkal biztosítható. Menedzselt bérelt vonal estén ezt a feladatot átháríthatjuk a vonalat biztosító szolgáltatóra. Katasztrófa esetére (és más okból is) érdemes lehet a KRA szerverét duplikálni néhányszor 10 km-re az elsõdleges szervertõl. Ennek viszont csak akkor van igazán értelme, ha a szolgáltatók katasztrófahelyzetben a tartalék szerverrel is kapcsolatba tudnak lépni, ami nem magától értetõdõ, amennyiben az elsõdleges szerverhez bérelt vonalakon csatlakoznak.

5. Erőforrásigény

A fentiek alapján már meg tudjuk becsülni, hogy az KRA működtetése során milyen műveleteket mekkora adatmennyiségeken és milyen gyakorisággal kell tudni végrehajtani. Nem elhanyagolható körülmény, hogy eközben minden adatbázisműveletet naplózni is kell. Mindez alapot ad ahhoz, hogy a KRA-t kiszolgáló adatbázis szerver teljesítőképességére becslést adjunk. A fentiek összefoglalása az alábbi táblázatokban látható.

A számhordozhatósági adatbázis jellemzői:

FUNKCIÓ	**BECSÜLT GYAKORISÁG**	**BECSÜLT ADAT-MENNYSÉG**
A szolgáltató által másnak átadott valamennyi szám feltöltése	Kezdeti adatfeltöltéskor, illetve abban a ritka estben, ha a központi referencia adatbázist reprodukálni kell (minden szolgáltató).	max. 100 kbájt nagyságrendben
A szolgáltató által a legutóbbi sikeres feltöltés óta átadott számok feltöltése (inkrementális töltés)	Ha változás van, de nem gyakrabban, mint például naponta annyiszor, ahány időablak definiált (minden szolgáltató).	legfeljebb kbájt nagyságrendben
Az adatbázis teljes nyilvános részének letöltése	Alkalmanként, ha például az adott szolgáltató adatbázisa megsérül, illetve esetlegesen rendszeresen, például hetente (az alkalmazott egyéb védelmek függvényében)	teljes mentés: max. néhány Mbájt
Hordozott számok adataiban beállt változás lekérdezése (“delta” lekérdezés)	rendszeresen, naponta (vagy legfeljebb naponta annyiszor, ahány időablak definiált)	várhatóan tipikusan kbájt nagyságrendben

Megállapítható, hogy ezeknek ez adatoknak a mennyisége és használatuk gyakorisága abba a nagyságrendbe esik, amit a ma elérhető kisebb teljesítményű PC-k is könnyedén tudnak kezelni.

A hívószám kijelölési adatbázisnak az alábbi főbb funkciókat kell ellátnia az előző táblázatban ismertetetteken felül:

FUNKCIÓ	**BECSÜLT GYAKORISÁG**	**BECSÜLT ADAT-MENNYSÉG**
A hatóság által meghatározott hívószám-szolgáltató összerendelés feltöltése	Egyszer, az adatbázis üzembeállítása során. Jelenleg blokkos az allokáció, tehát nem egyedileg kell szolgáltatót hozzárendelni a hívószámokhoz, de később lehet egyedi kiosztás is.	A hívószámok összes száma jelenleg 10 millió alatt van, ez mintegy 500 Mbájtnak felel meg
Hívószám allokáció a szolgáltatók között a még ki nem osztott hívószámokra	Eseti, nagyobb tételben várhatóan ritkán (évente legfeljebb néhányszor), egyenkénti kijelölésnél esetleg gyakrabban, (minden szolgáltató felé).	Igen nehezen becsülhető, de például új szolgáltató megjelenésének esetén néhány Mbájt is lehet
Hívószám újraallokáció a szolgáltatók között	Eseti, nagyobb tételben várhatóan ritkán (évente legfeljebb néhányszor), minden szolgáltató felé), egyenkénti kijelölésnél esetleg gyakrabban, (minden szolgáltató felé).	Igen nehezen becsülhető, de esetleg néhány Mbájt is lehet
Hívószámok lekérdezése	Erre csak irreguláris körülmények között van feltétlenül szükség, hiszen a szolgáltatók ismerik a nekik allokált számokat. Ezért egyedi megoldás is használható, tömörítés indokolt.	Igen nehezen becsülhető, de alkalomszerűen akár a teljes adatbázis is lehet (Gbájt)
Hívószám felszabadulásának jelzése	Eseti, nagyobb tételben várhatóan ritkán (évente legfeljebb néhányszor), minden szolgáltató felé), egyenkénti kijelölésnél esetleg gyakrabban, (minden szolgáltató felé)	Igen nehezen becsülhető, de esetleg néhány Mbájt is lehet
Kiosztott számok adataiban beállt változás lekérdezése (“delta” lekérdezés)	Eseti, nagyobb tételben várhatóan ritkán (évente legfeljebb néhányszor), minden szolgáltató felé), egyenkénti kijelölésnél esetleg gyakrabban, (minden szolgáltató felé)	Igen nehezen becsülhető, de esetleg néhány száz kbájt is lehet
Mentés/helyreállítás	rendszeresen, például hetente (az alkalmazott egyéb védelmek és backup stratégia függvényében)	Teljes mentés néhány Gbájt mennyiségű adatot jelent

Az előző fejezetben a hívószám adatbázis méretére és a fenti táblázatban a lehetséges adatforgalomra tett becslések alapján kijelenthetjük, hogy ezeket a követelményeket is teljesíteni lehet egy (jobb minőségű, nagy kapacitású), PC-s rendszerrel.

6. Konklúzió

Ebben a fejezetben összefoglaló áttekintést adunk a KRA-nak a tanulmányunkban érintett főbb tuajdoságairól, a vele szemben támasztott minimális követelményekről és ahol lehetséges, az általunk előnyösnek tartott megoldási módozatokról.

Ebben a fejezetben azt tételezzük fel, hogy a **KRA csak a valóban hordozott számok és a kiosztott színes számok adatait tartalmazza**.

A kiosztott színes számok tárolására az *implicit* formát javasoljuk.

1. A hordozott számok / kiosztott színes számok adatainak tárolása minden szolgáltató számára elérhető formában történjen (nyilvános adatok)
    - az adatbázis nyilvános részét minden szolgáltató olvashassa
    - a hordozott számokat az átvevő szolgáltatók az adatbázisnak megadhassák
    - az adatbázis nyilvános részét a KRA üzemeltetője is módosíthassa
    - az adatbázisba való íráskor a jogosultságot ellenőrizni kell, célszerűen legalább "fokozott biztonságú"elektronikus aláírás segítségével
    - az adatbázisból való olvasás jogosultságát is ellenőrizni kell
    - az adatbázis olvasásakor biztosítani kell a teljes nyilvános adattartalom letöltését és a "delta" lekérdezést is (várhatóan az egy/(néhány) napos "delta" lekérdezés lesz a tipikus olvasási forma)

    Teljes nyilvános adattartalom letöltése alatt a következőt értjük:
    Hordozott számok esetén: Ilyenkor a szolgáltató hozzájut a lekérdezés időpontjában hordozott számok listájához, de annak históriájához nem.
    Színes számok esetén: Ilyenkor a szolgáltató hozzájut a lekérdezés időpontjában használatban lévő színes számok listájához, de annak históriájához nem.

    Különbségi ("delta") adatlekérdezés alatt a következőt értjük:
    Ilyenkor a szolgáltató csak azokhoz az adatokhoz jut hozzá, hogy egy előző időpillanat óta a hordozott számok / színes számok között milyen változás következett be.
    Hordozott számok esetén:
    ⇒ mely, az előző időpillanatbeli[3] lekérdezéskor nem hordozott számok váltak azóta hordozottakká,
    ⇒ mely, az előző időpillanatbeli lekérdezéskor hordozott számok váltak azóta nem hordozottakká [az eredeti számblokk szolgáltatóhoz való visszahordozás illetve előfizetői szerződés megszűnése miatt],
    ⇒ mely, az előző időpillanatbeli lekérdezéskor hordozott számok váltak azóta továbbhordozottakká.
    ⇒ ha a két időpont között egy szám hordozottsági állapota többször is változott, de a "kezdő" illetve "vég" időpontban az őt kiszolgáló szolgáltató azonos - például a számot az eltelt időszakban

[3] "Elõzõ idõpillanatbeli lekérdezés" alatt a "delta" lekérdezésben megadandó lekérdezési kezdõidõpontot értjük.

elhordozták, de utána visszahordozták - az a "delta" lekérdezéskor nem jelenik meg.

⇒ ha a két időpont között egy szám többször is hordozásra kerül, akkor a "delta" lekérdezéskor a "közbülső lépcső(k)" nem jelenik/jelennek meg, csak a végállapot.

Színes számok esetén:

⇒ mely, az előző időpillanatbeli lekérdezéskor nem használt színes számok váltak azóta használtakká,

⇒ mely, az előző időpillanatbeli lekérdezéskor használt színes számok váltak azóta nem használtakká,

⇒ mely, az előző időpillanatbeli lekérdezéskor egy szolgáltató által használt színes számok kerültek át más szolgáltatókhoz (színes szám "hordozása").

⇒ ha a két időpont között egy szám használtsági állapota többször is változott, de a "kezdő" illetve "vég" időpontban az őt kiszolgáló szolgáltató azonos vagy a szám az egyik időpillanatban sincs használva - az a "delta" lekérdezéskor nem jelenik meg.

⇒ ha a két időpont között egy színes szám többször is "hordozásra" kerül, akkor a "delta" lekérdezéskor a "közbülső szolgáltató(k)" nem jelenik/jelennek meg, csak a végállapot.

Célszerűnek látjuk a "delta" lekérdezéssel átfogható időintervallumot korlátozni.

- legyen meg az a lehetőség, hogy a KRA - meghatározott időnként - például naponta maximum egyszer - üzenetben értesíthesse a szolgáltatókat, ha az adatbázis nyilvános részében változás állt be. Ez az üzenet ugyanakkor csak a változás tényét jelezze, de magukat a megváltozott adatokat ne tartalmazza. (Azokhoz célszrűen egy, az üzenet vételét követő, megfelelő "delta" lekérdezéssel lehet hozzájutni.)
- a nyilvános adattartalom minimálisan a következőket tartalmazza:
  - ⇒ átadott / átvett hívószám, illetve kiosztott színes szám (földrajzi számok esetében: körzetszám+előfizetői szám, mobil illetve nemföldrajzi számok esetében: szolgáltatás-kijelölő szám + előfizetői szám)
  - ⇒ hívószámot átvevő / átadó, illetve a kiosztott színes számot használó szolgáltató azonosítója (célszerűen a négyjegyű irányítási szám[4])
  - ⇒ hordozás / színes szám kiosztás kezdő dátuma és időpontja (Ez utóbbival az átadási időablak kezdetét kívánjuk meghatározni, annak egy adott - későbbi szabályozásban meghatározandó - hosszt feltételezve.
  - ⇒ hordozás / színes szám használat érvényesség vége dátuma és időpontja (ennek a tárolása esetleg elhagyható a nyilvános részből, hiszen ez a mező sokszor üres marad. Két fő ok miatt javasoljuk, hogy ez a mező mégis szerepeljen: 1. a színes számok esetén viszonylag sokszor előfordulhat, hogy valaki egy számot csak korlátozott időre (például 1 év, vagy valamilyen esemény ideje stb.) vesz meg, és ez a tény előre jelezhető; 2. Ha egy hordozott számot "visszahordoznak" a szám eredeti tulajdonos

[4] "Iirányítási szám" alatt a következõt értjük:

Az irányítási szám 4-jegyû, struktúrája: SK+BK, ahol

SK 2-jegyû szolgáltató kód, az átvevõ szolgáltató kódja

BK 2-jegyû berendezés kód, mely csak az átvevõ szolgáltató hálózatán belüli irányításhoz használatos belsõ kód (a többi szolgáltató számára nincs jelentése) vagy 0.

szolgáltatójához, akkor ez a mező használható annak jelzésére, hogy a szám hordozottsági állapota mikortól szűnik/szűnt meg).

⇒ célszerűnek tartjuk a hívószám eredeti tulajdonosának (számblokk szolgáltatójának) a tárolását is (ez a mező jelzi, hogy a hordozás esetleges megszűntekor kinek kell a számot visszaadni, illetve ennek a mezőnek a megléte szükséges a hívószám kijelölési adatbázis célra történő bővíthetőség szempontjából. Ez a mező a színes számok esetében üres marad.)

⇒ tartalék (megfontolandónak tartjuk helyet biztosítani a hívószám kiadása illetve visszavétele időpontjának tárolására, ez a hívószám kijelölési funkció esetleges későbbi megvalósításakor kell majd.)

1. A hordozott számok / kiosztott színes számok adataihoz egyéb, a szolgáltatók számára még csak nem is olvasható adatokat lehessen társítani (nemnyilvános adatok)
   - a nemnyilvános adatokat a KRA üzemeltetője olvashassa. A jogosultságot ellenőrizni kell.
   - a nemnyilvános adatok írása csak a KRA üzemeltetője által történhessen. A jogosultságot ellenőrizni kell.
   - a nemnyilvános adatokat más, például jogszabályban erre feljogosított felhasználók csak olvashassák. A jogosultságot ellenőrizni kell.
   - Az adatbázis nemnyilvános részének a következő fontosabb információkat kell tárolnia:
     ⇒ a számhordozás bejelentésének időpontja. (Ez esetlegesen a nyilvános rész eleme is lehet, ha a számhordozás menetének részletes szabályozása után ez szükségessé válik.);
     ⇒ esetlegesen a hordozás bejelentésének ügyiratszáma (papíros alapú adatbevitel esetére) vagy tranzakció-azonosítása ;
     ⇒ egyéb információ (tartalék későbbi funkcióbővítésre, a számhordozás menetének részletes szabályozása során esetlegesen felmerülő további azonosítók tárolására stb.).
   - Az egyéb információ mező tartalmazhatja például a szám használatának “egységárát”, de ez az információ más módon - például a számlázóprogramban - valószínűleg hatékonyabban lehet tárolható.

1. Számlázás támogatása: A KRA támogassa a hordozott számok után fizetendő díj illetve díjvisszatérítés hiteles meghatározását, HÍF a számlázó rendszerével való összekapcsolhatóságot. A KRA adatbázisból minden számlázás alkalmával (manuális indítással) fájl formátumban a következő adatokat kell átadni a HÍF számlázó SAP programja számára:

Minden KRA rekordból 2 rekordnak kell keletkeznie az alábbi szerkezettel:

- Átadó szolgáltató kód, hívószám, a hordozás időtartama, tranzakciókód,
- Átvevő szolgáltató kód, hívószám, a hordozás időtartama, tranzakciókód.

1. Hordozott számok kötegelt kezelésének támogatása számtartomány átadás esetén: Ha a számtartomány átkerül egy másik szolgáltató tulajdonába, akkor a KRA-nak képesnek kell lennie az ebbe a számtartományba eső hordozott számok problémáját "kötegelve" kezelni. Ez a következőket jelenti:
   - Az ebben a számtartományban szereplő hordozott számoknál a tulajdonos mezőt át kell írni az új blokkszolgáltatóra.

- Az ebben a számtartományban, az új blokkszolgáltatóhoz eddig érvényben levő hordozott számokat érvényteleníteni kell (hiszen ettől kezdve ezek már nem hordozott számok).
- A régi blokkszolgáltató által megadott továbbra is nála maradó, élő számokat (lista) hordozott számként fel kell venni a KRA-ba, mert innentől kezdve ezek hordozott számok lesznek (a tulajdonos az új blokkszolgáltató).

Ennek a funkciónak a speciális esetei a következõk:

- A) A blokkszolgáltató visszaadja a számtartományt a HÍF-nek (mert már nincs nála élõ szám), de a tartományban vannak hordozott számok. Ebben az esetben az új tulajdonos nem egy szolgáltató, hanem a HÍF lesz és nem lesz olyan szám a tartományban, ami eddig az "új szolgáltatóhoz" (HÍF) tartozott volna, illetve olyan szám sem lesz, ami a régi szolgáltatónál élõ marad (azaz a 2. és 3. lépéseket nem kell elvégezni).
- B) Egy adott számtartomány blokkszolgáltatója megszûnik. Ebben az esetben az A) pontban leírt eljárást a megszûnt szolgáltató valamennyi számtartományára el kell végezni.

C) A fenti két eset folytán a HÍF tulajdonába került számtartomány újbóli kiadása. Ebben az esetben nem lesz olyan szám, ami a "régi szolgáltatónál" (HÍF) élõ marad (azaz a 3. lépést nem kell elvégezni).

1. Minden, az adatbázisban végzett műveletet naplózni kell
   - Minimálisan rögzíteni kell minden adatbázis tranzakció
     - ⇒ tulajdonosát,
     - ⇒ időpontját,
     - ⇒ az általa végrehajtott műveleteket
     - ⇒ előny, ha a művelet által módosított adattartalom is bekerül a naplóba
   - a napló ne csak a szűken vett adatbázisműveletek adatait tartalmazza, hanem a KRA, mint rendszer műveleteinek naplózása is szükséges, különös tekintettel például a következőkre:
     - ⇒ rendszerindítás, -leállás,
     - ⇒ sikeres/sikertelen bejelentkezés
   - a napló tartalma ne legyen módosítható
   - a napló olvasására a szolgáltatók nem jogosultak, csak a KRA üzemeltetője és az egyéb, erre feljogosított felhasználók
   - adott időnél régebbi adatok háttértárra való mentését lehetővé kell tenni (archiválás)
   - az üzemi adattartalom veszélyeztetése nélkül legyen lehetőség az archív adatok visszatöltésére, az adatokban történő keresésre
2. A fentiek megvalósításához minimálisan háromféle adatbázis hozzáférési jogosultságot kell megvalósítani:
   - szolgáltatói: csak a nyilvános rész olvasása, a számhordozás bejelentésének lehetősége
   - üzemeltetői: minden adatelem olvasása (beleértve a naplót és az archív adatokat is), a napló és az archív adatok kivételével bármilyen adatmező írása
   - egyéb feljogosított használó: minden adatelem olvasása (beleértve a naplót és az archív adatokat is).
3. Adatbázis szerver: Célszerűen egy Unix alapú, kis teljesítményű szerver, elsősorban a stabil és folyamatos üzemeltethetőség érdekében. A diszk alrendszere valamely RAID

megoldás, akár tükrözés is lehet, hiszen az adatmennyiségek nem indokolnak bonyolultabb megoldásokat.

4. Adatbáziskezelő: átlagos teljesítményű rendszer is elegendő. A betöltendő funkcióban az üzemidő legnagyobb része várakozással fog telni, a műveletek konkurenciája alacsony lesz, a válaszidők nem kritikusak.
5. Kommunikációs hálózat:
   - üzemeltetői környezet: LAN (menedzselés, adatlekérdezés, papíros alapú adatbevitel)
   - szolgáltatók felé: menedzselt bérelt vonalak, 64 kbit/s csatorna elég, de internet/PSTN alapú hálózat is megfelelő lehet, ám ilyenkor komolyabb biztonságtechnikai megoldások szükségesek.
6. Biztonság:
   - *menedzselt bérelt vonal használata esetén*: Egy egyszerű, de mégis kellően hatékony megoldás lehet egy VPN kialakítása SecureID tokenekkel, kombinálva szimmetrikus kulcsú titkosítással. Ebben az esetben erős autentikáció megvalósítható, biztosítva annak letagadhatatlanságát, hogy ki és mikor lépett kapcsolatba a KRA-val. A kommunikáció tartalmának elmentése megvalósítja annak reprodukálhatóságát, hogy mit küldött a szolgáltató. Egy 3DES vagy hasonló erősségű titkosítást használó, adatcserét biztosító kliensprogrammal viszonylag egyszerűen eleget tehetünk a bizalmasság és a sértetlenség követelményének is. Ilyenkor tehát a szolgáltatók között alapvetően állománycserét tudunk megvalósítani.
   - *Internet használata esetén:* tűzfal megoldásra is szükség van, ez esetben viszont gondoskodni kell a támogatott kommunikációhoz tartozó csomagoknak a tűzfalon való átjuttatásáról is.
7. Rendelkezésreállás: A KRA rendelkezésre állása nem kritikus. A szerver kellõen robosztussá tehetõ duplikált diszkekkel és a gép 1-2 napon belüli javítását biztosító support szerzõdéssel. A kommunikáció rendelkezésreállása tartalék útvonalakkal biztosítható. Menedzselt bérelt vonal estén ezt a feladatot átháríthatjuk a vonalat biztosító szolgáltatóra. Katasztrófa esetére (és más okból is) érdemes lehet a KRA szerverét duplikálni biztonságos helyen néhányszor 10 km-re az elsõdleges szervertõl.

A jelenlegi és a jövőbeli igényeket egyaránt figyelembe véve úgy látjuk, hogy egy integrált, azaz a számhordozást és a hívószám nyilvántartást együttesen biztosító referencia adatbázis kialakítása lenne célszerű. Bár ez az idő rövidsége miatt nem valósítható meg, de azt javasoljuk, hogy a központi referencia adatbázis megvalósításakor azokat a megoldásokat célszerű előnyben részesíteni, amelyek nem zárják ki annak a jövőbeli, a teljes földrajzi, nemföldrajzi és mobil számok adatainak egyenkénti tárolására szolgáló alkalmazhatóságát, e célra való bővíthetőségének vagy egy ilyen rendszerhez kapcsolhatóságának a lehetőségét.

Forrásjegyzék

[1] 2001. évi XL törvény a hírközlésről, ("Hírközlési törvény", Hkt)

[2] Kormányrendelet tervezet a számhordozhatóság alkalmazásának szabályairól, Informatikai és Hírközlési Miniszter 001497/2002 sz. előterjesztés, Budapest, 2003. január

[3] A szolgáltatók egyeztetett javaslata a hazai számhordozhatóság megvalósításának egyes kérdéseiről (2002. júl. 26.)

[4] Személyes konzultáció a HÍF szakértőivel (Méhes András, Madarász Erika, Dömötörné dr. Ács Katalin) 2003. jan. 8.

[5] Személyes konzultáció a HÍF 2003. február 19.

[6] Hidvégi-Elekes-Dely: Földrajzi hívószámok szolgáltatók közötti hordozhatósága, PKI Közlemények 46. szám, 2002.

[7] Hírközlési Felügyelet szakmai napja a számhordozhatósági Országos Referencia Adatbázis megvalósítási lehetőségeiről, 2002. május 29.,

[8] Hírközlési és Informatikai Tudományos Egyesület munkacsoportja: A szolgáltató választás és a számhordozhatóság szolgáltatások megvalósításának műszaki elemzése, 2001. december

[9] Személyes konzultáció Nyuli Attilával, a HÍF Informatikai Fejlesztési Osztály vezetőjével, 2003. jan. 27.

[10] Adamis Gusztáv - Csopaki Gyula - Gajdos Sándor: Nemzeti számhordozhatósági referencia adatbázis - Megvalósíthatósági tanulmány a HÍF számára, Budapest, 2002. április

[11] 2001. évi XXXV. törvény az elektronikus aláírásról. http://www.hif.hu/menu4/m4_6/eatszvveg.pdf

[12] http://www.polysys.hu/java/certreq/info.htm

[13] http://www.hif.hu:7777/pls/portal30/ESIGN_PORTAL.menu.show Elektronikus aláírással kapcsolatos nyilvántartások a HÍF-nél

[14] A „Számhordozhatósági Központi Referencia Adatbázis” című BME tanulmányról, HÍF 2003. febr. 17.

[15] Biztonsági Rendszerek Szervezése

[16] http://informatika.bke.hu/

[17] Ködmön József: Kriptográfia

[18] Antal Kristóf: Vállalati adatbiztonság kialakítása, http://informatika.bke.hu/

[19] Informatikai Tárcaközi Bizottság: Informatikai rendszerek biztonsági követelményei : http://www.itb.hu/ajanlasok/a12/

[20] http://otn.oracle.com/products/oracle9i/datasheets/advanced_security/advanced.html