HADMÉRNÖK

VI. Évfolyam 2. szám - 2011. június

Kuris Zoltán
Zoltan.Kuris@bm.gov.hu

A MOBILKOMMUNIKÁCIÓ DETERMINÁNSAI ÉS DILEMMÁI A NEMZETI MINŐSÍTETT ADATOK TOVÁBBÍTÁSÁVAL ÖSSZEFÜGGÉSBEN

Absztrakt

A nagy sávszélességű, nagymennyiségű és gyors adatelérésű megoldások és eszközök elterjedése, a publikus hálózatokon való kommunikáció ma már triviális. Ugyanakkor egy érdekes és feltáratlan terület a szenzitív, vagy nemzeti minősített adatok, a fenti elvek szerinti mobilkommunikációját megvalósító „teljes életciklusában hazai felügyeletű" szakszerűen és jogszerűen alkalmazható eszközök (rendszerek) rendszeresítési és rendszerengedélyeztetési folyamatának vizsgálata. A szerző publikációjában kifejti a témával kapcsolatos determinánsokat, elemzi a dilemmákat, összehasonlító elemzés módszerével bemutat néhány - általa alkalmasnak ítélt – technológiát és ajánlást, irányelveket fogalmaz meg a nemzeti akkreditációval összefüggésben.

The high-bandwidth, large and rapid date access solutions and the proliferation of public communication networks are now trivial. However, an interesting and unexplored area is the investigation of sensitive, or classified national information in accordance with these principles, mobile communication implementing "full life cycle of domestic supervision" properly and lawfully applied tools, and the system permission and the systematic process. The author explains the most relevant determinants in his publication, analyzing the dilemmas. He also shows some technologies and a recommendation determines guidelines in concern with national accreditation.

Kulcsszavak: *érzékeny adat, minősített adat, adatkapcsolati lefedettség, titkosítás, rejtjelzés, VOIP kommunikáció, TEMPEST ~ stacioner, encrypted phones, encryption keys, Low audio latency*

BEVEZETÉS

Az információbiztonsági szakemberek alapvető küldetése annak hangsúlyozása, hogy a biztonság minden korban alapvető szükséglete volt a társadalmaknak, az államoknak, az egyéneknek. Ebből következik az a felismerés is, hogy a fejlődésnek, a társadalom működésének és a túlélésnek egyik döntő feltétele hogy a környezetről, a másik társadalomról, a másik államról, a másik emberről folyamatosan valós idejű és autentikus, használható információkat szerezzünk annak érdekében, hogy optimalizált döntéseket hozzunk. Ne legyenek illúzióink azzal összefüggésben, hogy az államok - és a nem állami szervezetek - ma is ugyanúgy folytatnak hírszerzést (információszerzést), mint akár évszázadokkal korábban, azzal a különbséggel, hogy a technikai és a tudományos fejlettség, magasabb színvonalon áll, és ennek minden előnyét, eredményét azonnal felhasználják a saját céljaik elérése érdekében. Az is axióma, hogy a hírszerzés az állam elemi szükségletei közé tartozik. A régi mondást („Navigare necesse est! = Hajózni pedig kell!") a hírszerzés és az információbiztonság nyelvére lefordítva annyit jelent: „információt szerezni pedig kell! Az információbiztonsági szakemberek igaznak tartják ezt napjainkban is és a jövőt illetően is.

A vezetésnek (így a kritikus infrastruktúrákat üzemeltető vezetőknek is) egymástól elválaszthatatlan két funkciója a szükséges információk beszerzésére és elemzésére alapozott döntés. A hatékony, jól működő hírszerzés önmagában nem vezet hatékony, bölcs döntésekhez. , de az információk hiánya, a hamis vagy félrevezető információk biztosan csak rossz döntéseket eredményeznek. Ugyanakkor, ha a vezető döntéskényszerben van, akkor a kevés, nem hiteles, nem időszerű információkra utaltan is dönteni kell. Ebből ered a hírszerzői körökben evidenciaként kezelt mondás, hogy „sohasem tudhatsz eleget".

A fentiekben kifejtett fenyegetésekkel szembeni hatékony védelmi intézkedések az defenzív hírszerzési tevékenység hatókörébe tartozó feladatok, amely alapvetően befolyásolják a kritikus infrastruktúra szektorainak – és ezen keresztül az állam működését is. A defenzív hírszerzés fontosságát és szükségességét részletesebben már diplomamunkában és előző publikációimban is kifejtettem. A defenzív terület hatékony működésének okán szükséges biztosítani a kritikus infrastruktúra szektorait irányító vezetők részére a szenzitív és/vagy minősített adatokat tartalmazó információ továbbítására alkalmas mobilkommunikációs eszközök alkalmazását, ugyanis ez egy hatékony eszköze az offenzív hírszerzés elleni védekezésnek. Figyelemre méltó szempont az is, hogy a védett mobil kommunikációs eszközök hiányában a vezetés operativitása és hatékonysága kérdőjeleződik meg. Ennek fontosságát a mai felgyorsult információs társadalmi fejlődéssel összefüggésben nem lehet elégszer hangsúlyozni.

A kutatási témámhoz kapcsolódóan, előző publikációimban már kifejtettem, – és feltehetően igazoltam is – hogy az információs társadalmak létfontosságú (kritikus) infrastruktúráinak hatékony és optimális működését meghatározzák a kritikus információs infrastruktúrák. Irányadó tudományos kutatási eredmények igazolták, hogy a kritikus információs infrastruktúrák működésében bekövetkezett zavarok kihatnak más szektorokra és kritikus infrastruktúra elemekre, illetve ezen keresztül a társadalom működésére is. Különösen igaz ez a fejlett információs társadalmak esetén, amelyek éppen az információs társadalmi fejlődésük kapcsán sebezhetővé válnak. Irányadó információbiztonsági szakemberek szerint egy adott információs társadalmi fejlettségi szinten lévő társadalom, az információs hadviselés dimenzióiban indított összehangolt támadással „visszavethető" az információs társadalmi fejlettségi szint alacsonyabb fokára. Előző publikációimban kutattam a komplex információbiztonság rendszerét, alrendszereit és elemeit is, annak okán, hogy - irányadó szakemberekkel egyetértve – fontosnak tartom a kritikus információs infrastruktúra területén alkalmazott védelmi intézkedések komplexitását.

A fenyegetésekkel szembeállított, megfelelően alkalmazott komplex védelmi intézkedések a kritikus szint alá csökkentik a maradvány kockázatot és megfelelően egyenszilárdá teszik a kritikus információs infrastruktúra rendszereit. Kutatási témámon belül meglehetősen markánsan jelenik meg a szenzitív, és minősített adatok védelmével összefüggő kutatási terület. Előző írásomban részletesen kifejtettem a minősített adat védelméről szóló 2009. évi CLV. törvény (a továbbiakban: Mavtv.) [1] jótékony hatását a kutatási területemre. A Mavtv. kiadását követően megjelent kormányrendeleteket [2],[3],[4] is elemeztem, és kimutattam a NATO biztonsági szabályzatával [5] és az EU biztonsági szabályzatával [6] összefüggő koherenciát. Megállapítottam, hogy a minősített adatok védelmével összefüggő - nemzetközi törvényekben és szabályzatokban megfogalmazott irányelvek megfelelően átvezetésre kerültek a nemzeti jogszabályokba. Ez megteremtette annak lehetőségét, hogy a nemzeti minősített adatok kezelésére alkalmas elektronikus rendszereket lehessen akkreditálni és alkalmazni.

DETERMINÁNSOK, DILEMMÁK ÉS HIPOTÉZISEK

A fentiekben leírt szabályozók determinálták a rendszerek fejlesztésének rendszeresítési és rendszerengedélyezési eljárásainak szabályait. Ezeket a szabályokat a „stacioner" rendszerek esetén jól lehet alkalmazni, különösen abban az esetben, ha a minősített adatot kezelő elektronikus rendszer fogalmát a klasszikus értelemben vett informatikai rendszer irányából közelítjük meg. Ebben az esetben ugyanis a minősített adatok előállításáról gyűjtéséről, tárolásáról és továbbításáról van szó. Az ilyen rendszer teljes életciklusában előforduló tevékenység és az azzal összefüggésben alkalmazott személyi, adminisztratív, fizikai és elektronikus védelmi intézkedések halmaza – nemzetközi jogszabályokkal koherensen - többé kevésbé jól meghatározhatóak. Ugyanakkor, ha az „absztrakt" részben megfogalmazott „mobilproblematikát" vizsgáljuk, az információbiztonsági szakemberekben felmerülhet néhány megválaszolatlan (vagy félig megválaszolt) kérdés. A védett mobilkommunikáció értelmezési tartományában kutatva olyan érdekfeszítő témák elemzésére nyílik lehetőség, mint például a szóbeli közlés információtartalmának és az információtartalom minősített adatokkal összefüggő kapcsolatrendszerének vizsgálata. Ezzel összefüggésben a modellezésnél figyelemmel kell lenni arra, hogy az így értelmezett szenzitív, esetenként minősített adattartalommal is rendelkező információ mobilkommunikációs védett átviteli úton, - a kor színvonalának megfelelő infokommunikációs eszközök igénybevételével – történő átvitelére a felhasználói igények egyre markánsabban fogalmazódnak meg. Ezt az igény nem is olyan nehéz igazolni, hiszen az információs társadalom kritikus infrastruktúráinak biztonságos üzemeltetésének alapvető feltétele az operativitás, ennek pedig egyik előfeltétele az azonnali (védett mobilkommunikációs) eszközök) alkalmazása. Ezt felismerve a nemzetközi kutatási eredményeket és a nemzetközi sajtóban megjelent híreket, a közelmúltban a külföldi kritikus infrastruktúrák szektoraiban tapasztalható – a saját nemzeti hatóságaik által engedélyezett – a védett mobilkommunikációs eszközök megjelenése, elsősorban a védelmi és kormányzati szektoron belül [18]-[20].

Kiindulva tehát abból, hogy vannak determinált védelmi intézkedések, célszerű (mert az információs társadalmi fejlődés szakaszában a felhasználói igények kikényszerítik) kutatásokat végezni a nemzeti minősített adatok mobil kommunikációját biztosító lehetőségek és eszközök jogszerű és szakszerű alkalmazhatóságának területén. Publikációmban bemutatom a területet szabályozó jogszabályi környezetet, a jelenleg tapasztalható dilemmákat, kutatom a jelenlegi jogszabályi környezetben rejlő lehetőségeket, a szakszerű és jogszerű alkalmazás érdekében új – a jogszabályi környezetbe való beillesztésre alkalmas – irányelveket, javaslatokat fogalmazok meg. Összehasonlító elemzés módszerével bemutatok néhány „általam alkalmasnak talált" technológiát. Ezen túl leíró jellegű folyamatként

bemutatom a minősített információ továbbítására alkalmas mobil kommunikációs rendszer rendszeresítési és rendszerengedélyeztetési eljárásának főbb állomásait és dilemmáit.

AZ ÁLTALÁNOS SZABÁLYOZÁSI KÖRNYEZET LEHETŐSÉGEI ÉS KORLÁTAI

Mielőtt a védett mobil kommunikáció hazai lehetőségeinek elemzésére sor kerülne, szükségszerű néhány alapvető fogalom és a fogalmak közötti kapcsolatrendszer összehasonlító elemzését elvégezni. Ezzel összefüggésben, alapvetően szükséges helyesen értelmezni – illetve különbséget tenni – a közérdekű adat [17] 2.§ (4), a közérdekből nyilvános adat [17] 2.§ (5), nem nyilvános adat [17]19/A. § , a minősítéssel védhető közérdek [1] 5.§, az üzleti titok [16] 81.§ (2), és a minősített adat [1] 3. § (1) a) fogalmakat és azok tartalmát. Ugyanis az alkalmazható eljárásokat nagyban befolyásoló tényezőkről van szó. Tapasztalati tény, hogy a fogalmak helytelen értelmezéséből fakadóan –gyakran az információbiztonsági szakemberek is – téves következtetésekre juthatunk.

Ha a kritikus információs infrastruktúra elemek (szervezetek) irányából közelítjük meg a problémát, megállapíthatjuk, hogy az „adatbiztonság” érvényesítésével összefüggésben elmondhatjuk, hogy az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezeti intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek [17].

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, illetőleg a távközlési vagy informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik [17]. A védett mobil kommunikációs eszközöket illetően szögezzük le, hogy a továbbiakban a”védett mobil kommunikációs eszközök” fogalma alatt olyan eszközöket és alkalmazásokat értünk, amelyek olyan magas biztonsági szintű hardveres és szoftveres titkosítási algoritmusokat alkalmaznak, amelyek lehetővé teszik a hang és adat alapú információk adatátviteli úton történő magas titkosítási szintű nagy egyenszilárdságú továbbítását, kihasználva a publikus mobilkommunikációs hálózat adta lehetőségeket.

Figyelemmel arra, hogy adatkezelő természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet is lehet, az adatvédelem alanyát illetően igen széleskörű értelmezési tartomány határozható meg. Ugyanakkor az alkalmazott védelmi intézkedések kialakítását illetően egészen a minősítéssel védhető közérdek eléréséig nem találkozunk kötelező érvényű és megfelelően szankcionált szabályozókkal. Ebből az következik, hogy a nem nyilvános és üzleti titkoz képező adatok tekintetében nincsenek kötelező érvényűen meghatározva a személyi, fizikai, adminisztratív és elektronikai védelmi intézkedések, illetve a büntetőjogi szankciók sem jelennek meg egyértelműen. Ebből az következik, hogy ezeken az adatterületeken a védett mobilkommunikációs eszközök alkalmazását és alkalmazási szabályait az adatkezelő határozza meg, de ez az adatkezelőt illetően a közérdekű nem nyilvános és az üzleti titkot képező adat tekintetében nem kötelező érvényű. Ezzel összefüggésben született meg a Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszere (MIBIK). Természetesen az információbiztonsági irányítási rendszer szabvány szintű szabályozásának [9], [10] alkalmazása megfelelő ismereteket és alapokat ad a szervezetek részére, de jegyezzük meg, hogy az irányítási rendszer alkalmazása a szervezetek részére nem kötelező.

A védett mobilkommunikációs eszköz használata (rendszeresítése) a fent említett adatterületeken nincs hatósági engedélyezési eljáráshoz kötve és az alkalmazásukkal

összefüggésben nincs szabályozva az alkalmazandó személyi adminisztratív, fizikai és elektronikai védelmi intézkedések köre. Ez az anomália a nem nyilvános adatok és az üzleti titkok továbbítására alkalmas rendszerek használata esetén kétséget kizáróan (a szabályozás hiányából eredő) problémákat jelenthet, ugyanakkor az információs társadalmi fejlődés jelen szakaszában a kritikus információs infrastruktúrákat üzemeltető természetes és jogi személyek, illetve jogi személyiséggel nem rendelkező szervezetek részére ezen a szinten lehetővé teszik, (megengedik) a kor színvonalának megfelelő elektronikai rendszerek (ezen belül a mobilkommunikációs rendszerek) alkalmazását.

A MINŐSÍTÉSSEL VÉDHETŐ KÖZÉRDEK HATÓKÖRÉBE TARTOZÓ SZABÁLYOZÁSI KÖRNYEZET BEMUTATÁSA

Az előzőekben kifejtett adatkörökkel összefüggésben megállapíthatjuk tehát, hogy a védett mobil kommunikációs eszközök, eljárások alkalmazhatósága nem esik jelentős korlátozás alá, gyakorlatilag az adatkezelő belső szabályokban meghatározott védelmi intézkedések alkalmazása mellett igénybe veheti a védett mobilkommunikációs eszközök nyújtotta szolgáltatásokat.

Feltételezve azt, hogy a kedves olvasó már ismeretekkel rendelkezik ezen a szakterületen és a minősítéssel védhető közérdek hatókörébe tartozó szabályozási környezetet vizsgáljuk, azt tapasztaljuk, hogy a minősített adat védelméről szóló 2009. évi CLV törvény[1] és annak végrehajtási rendeletei[2], [3], 8] részletesen és szinte teljes körű szabályozást jelentenek a védelmi intézkedések teljes vertikumában. Megállapítható az is, hogy a nemzetközi törvényekkel meglévő koherencia jól érzékelhető akkor, ha részletesen tanulmányozzuk és összehasonlítjuk a NATO biztonsági szabályzatát, az EU Tanács biztonsági szabályzatát a fent említett Mavtv-el és végrehajtási rendeleteivel. Ez kétség kívül pozitív eredmény, de egyben statikussá teszi a hazai szabályozási környezetet, annak ellenére, hogy szakmai körökben vannak törekvések a hazai szabályozás módosításával összefüggésben. Irányadó szakmai körök véleményével azonosulva kisebb, módosítások (a védett mobil kommunikáció területén is) alkalmasak lennének optimális elektronikus rendszerek szakszerű és jogszerű bevezetésének elősegítésére. A jelenlegi hazai szabályozás kisebb anomáliáit jól példázza egy védett mobil kommunikációs rendszer bevezetésének modellezése, amelyre az alábbiakban gondolatkísérletet teszek.

Nemzeti minősített adat (információ) továbbítására alkalmas védett mobil kommunikációs rendszer hazai jogszabályi környezetbe illeszkedő bevezetésének lehetőségei (gondolatkísérlet)

Ha a külföldi minősített adatok továbbítására alkalmas védett mobilkommunikációs eszközök nemzetközi tapasztalatait elemezzük, arra a következtetésre jutunk, hogy számos eszköz és rendszer áll rendelkezésre a kritikus információs infrastruktúrát üzemeltető felhasználók igényeinek kielégítésére. Ezt a későbbiekben igazolom néhány NATO és EU tanúsítvánnyal is rendelkező „encrypted phone” bemutatásával(GoldLock 3G, SecuVOICE, SecuGATE, Silentel SecureCall, TigerXS,). De a hazai piacon is találhatóak hasonló fejlesztési irányok, (NETIPHONE) amelyek ígéretes nemzeti megoldásokat jelenthetnek.

Gondolatkísérletünk első fázisa az, hogy a nemzeti minősített adatok (szóbeli információk) továbbításával összefüggésben tisztázzuk azt, hogy mikor is beszélhetünk minősített adatról és milyen feltételek teljesülése esetén beszélünk nemzeti minősített adatról.

A mavtv. [1] 3.§ (1) bekezdés a) pontja szerint „ nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat amelyről – a megjelenési formájától függetlenül – a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn

belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza;"

A fenti szakaszban megfogalmazottakkal összefüggésben – azon túl, hogy a „formai követelményeknek megfelelően tartalmazó olyan adat" szóhasználat zavaróan hat (és talán nem is helyes). Elgondolkodtató az, hogy ha a fenti szakasz értelmében a formai követelményeknek megfelelő és minősítési eljáráson keresztül esett adat minősül minősített adatnak, akkor a – nem tárgyiasult formában – egy adott „Bizalmas!" minősítési szint fölötti adathoz kapcsolódóan szóban elhangzott (de nyilvánvalóan a formai követelményeknek nem megfelelő és minősítési eljáráson keresztül nem esett), mobilkommunikációs, vagy stacioner eszközön, illetve rendszeren továbbított szóbeli információ milyen elbírálás alá esik. Ugyanis, különösen a „Bizalmas!" minősítési szint fölött szigorú feltételeknek megfelelően magas szintű személyi, adminisztratív, fizikai és elektronikai védelmi intézkedéseket kell kötelező érvényűen alkalmazni, és ha ez a terület szabályozatlan a minősített adatok védelmével összefüggő (jól felépített) komplex védelmi rendszer egyenszilárdsága csökkenhet.

Egyetértve és elfogadva a nemzetközi törvényekből is eredő (magas szintű egyenszilárdságot biztosító) hazai szabályozással is koherens követelményrendszert, a felhasználói igényeknek megfelelő védett mobilkommunikációs rendszerek szakszerű és jogszerű üzemeltethetősége érdekében is szükségesnek mondható a „nem tárgyiasult formában" szóban elhangzó és elektronikus rendszereken továbbított minősített adatok megjelenítése a hazai szabályozásban.

Gondolatkísérletünk következő fázisa az, hogy a hazai (nemzeti) minősített adatok továbbítására alkalmas elektronikus rendszerek használatbavétele és használata során nem kerülhetjük meg azt az Mavtv. végrehajtási rendeletében [8] 42.§ (3)-(5) bekezdésében megfogalmazottakat, miszerint:

„(3) A rejtjeltevékenységet folytató szerv rejtjeltevékenysége során csak olyan rejtjelző eszközt alkalmazhat, amelyre vonatkozóan az NBF rendszerengedélyt adott ki.

(4) Nemzeti minősített adat rejtjelzésére csak olyan rejtjelző eszköz alkalmazható, amelynek fejlesztője, illetve gyártója rendelkezik a minősített adat kezeléséhez szükséges, jogszabályban meghatározott személyi és tárgyi feltételekkel, és amely szerv esetében az NBF a rejtjelző eszközre vonatkozóan – a létrehozására vonatkozó döntéstől a tervezést,

a fejlesztést, a beszerzést, a telepítést, az üzemeltetést, a továbbfejlesztést és a módosítást is érintően, a rendszer egyes elemeinek vagy egészének a kivonásáig és megsemmisítéséig – megbízhatóan meggyőződött arról, hogy nem áll fenn a bizalmasság elve sérülésének veszélye.

(5) Nemzeti minősített adat rejtjelzésére külföldi eszköz csak akkor alkalmazható, amennyiben a (4) bekezdésben meghatározott rejtjelző eszköz nem áll rendelkezésre, vagy a katonai műszaki követelmények nem teszik lehetővé külön nemzeti és külföldi rejtjelző eszköz együttes alkalmazását katonai műveletekben."

A fentiekben megfogalmazott követelmények a szakértő olvasó számára többé -kevésbé egyértelmű szabályokat fogalmaz meg, melynek lényege (kissé leegyszerűsítve) az alábbiakban összefoglalásra is kerül. Ugyanakkor a rendelet értelmezését követően arra a következtetésre is juthatunk, hogy nemzeti minősített adat továbbítására külföldi eszközt is igénybe lehet venni [42 § (5)]. A kutató számára bizonytalanul megválaszolható „nyitott kérdés" marad az, hogy vajon ebben az esetben - amennyiben a (4) bekezdésben meghatározott eszköz nem áll rendelkezésre – milyen szabályokra kell figyelemmel lenni a külföldi rejtjelző eszköz nemzeti minősített adat továbbítására való használatbavételét illetően.

- Hazai nemzeti minősített adat továbbítására csak hazai rejtjelző eszköz használható (és külföldi rejtjelző eszköz csak akkor használható ha hazai eszköz nem áll rendelkezésre). Ebből az következik, hogy „általában" minősített adatot rejtjelző eszközzel kell továbbítani, ami rejtjelzésnek minősül és a rejtjeltevékenységgel összefüggő előírásokat kell alkalmazni.
- Rejtjelző eszközök rendszeresítési engedélyezését a Nemzeti Biztonsági Felügyelet (mint hatóság) végzi. Minősített adat továbbítására alkalmas rejtjelző eszközt az NBF engedélye nélkül nem lehet fejleszteni és használni.
- Rejtjelző eszközt fejleszteni csak Telephely Biztonsági Tanúsítvánnyal rendelkező, többségi magyar tulajdonban lévő gazdasági társaság végezhet [3].
- Az NBF-et a rejtjelző eszköz engedélyezésének teljes életciklusába be kell vonni. Ez azt jelenti, hogy a fejlesztés megkezdését megelőzően a fejlesztő kérelemmel fordul az NBF felé, az NBF rendelkezésére bocsájtja a fejlesztési célt megfogalmazó műszaki dokumentációt, majd ezt követően a szabályoknak megfelelően rendszeresítési engedély kérelemmel fordul az NBF felé aki közigazgatási eljárás keretében a fejlesztési ciklus befejezését követően rendszeresítési engedély ad ki. A fentieket még akkor is alkalmazni kell, ha esetlegesen külföldi eszköz használatbavételéről beszélünk.
- A rendszeresítési engedély csak a rejtjelző eszköz jogszerű használhatóságát teszi lehetővé Ennek birtokában a fejlesztő a hazai piacon forgalomba hozhatja a rejtjelző eszközt. Az üzemeltető szervezet ezen túl egy rendszerengedélyeztetési (akkreditációs) folyamat keretében (a megfelelő tartalommal) rendszerengedély kérelmet kell előterjeszteni az NBF részére, aki a kérelem elbírálását követően közigazgatási eljárás keretében hatósági rendszerengedély ad ki.

Összefoglalva: Adott minősítési szintnek megfelelő minősített adat továbbítására alkalmas nemzeti védett mobilkommunikációs eszköz fejlesztőjének (a nemzeti hatósággal szorosan együttműködve) rendszeresítési eljárás keretében rendszerengedélyt kell beszerezni az adott rejtjelző eszközre. Majd ezt követően a védett mobilkommunikációs rendszer üzemeltetője rendszerengedélyeztetési eljárás keretében rendszerengedélyt kér és kap a nemzeti hatóságtól (NBF). A fenti két közigazgatási eljárás lebonyolítását – annak eredményességét – lényegesen meghatározza az alkalmazni kívánt minősítési szint, ezért ennek megfontolása (a védelmi intézkedések költségeit is figyelembe véve) a projekt sikerét, vagy bukását alapvetően meghatározza. Ezért is fontos egy feltételezett célprojekt végrehajtása esetén az irányadó információvédelmi szakemberek által (nem elégszer hangsúlyozott) kockázatelemzés elkészítése és a projektszerű (ahol van projekt szponzor, megfelelő projektszervezet és ehhez rendelkezésre állnak a megfelelő emberi és anyagi erőforrások is) működési keretek közötti kockázatmenedzsment működtetése. Erre jó példát adnak (és természetesen megfelelő szakmai alapokat is jelentenek) a NATO és EU biztonsági szabályzatában megfogalmazódó irányelvek [4],[5] és például a NATO direktívákban részletesen meghatározott kockázatmenedzsment előírásai. Ezt a hazánkban nem gyakran (és nem szívesen alkalmazott) módszertan olyannyira fontos eleme a sikeres projekt végrehajtásának, hogy külön publikáció keretében kutatom és fejtem ki a témával kapcsolatos megállapításaimat.

A mobilkommunikációs eszközök bevezetésének és használatának dilemmái és azok feloldásának lehetőségei a minősített adatok védelmének tükrében.

Az előző fejezetben kifejtett alapállapotban a mobilkommunikációs rendszer fejlesztőjének és üzemeltetőjének, sok költségigényes feltételnek kell megfelelni. Különösen igaz ez abban az esetben, ha a minősítési szint eléri a „Bizalmas!" minősítési szintet, vagy azt meghaladja.

Ma a fejlesztők és az üzemeltetők legnagyobb dilemmája a „Költséghatékony” rendszer fejlesztése és üzemeltetése! Sok esetben a minősített adatot kezelő szervezetek vezetői túlzottan felülbecsülik az alkalmazott védelmi intézkedések anyagi terheit. Irányadó információbiztonsági szakemberek, a megfelelő ismeretek birtokában – ismerve a hazai szabályozás adta lehetőségeket – költséghatékony megoldásokat tudnak prezentálni a minősített adatot kezelő szervezet vezetőjének.

A fenti szempontrendszer alkalmazása mellett a védett mobil kommunikációs rendszer fejlesztésével és üzemeltetésével összefüggésben, szükség szerint az alábbiakra célszerű figyelemmel lenni.

Az előző fejezetben kifejtésre került, hogy minősített adatok továbbítására, általában rejtjelző eszközt kell alkalmazni. Ugyanakkor kiindulhatunk abból is, hogy a Mavtv. végrehajtási rendeletében [8] 2.§ (4)-(5) bekezdéseiben az alábbiak kerültek megfogalmazásra.

„(4) A felhasználó rendszer használata nem minősül rejtjeltevékenységnek, ha a minősített adatok kezelése vagy továbbítása olyan informatikai rendszeren történik, amelyben a rejtjelző eszköz, rejtjelző szoftver vagy rejtjelző eljárás is telepítésre került és a rendszer biztonsági beállítása nem teszi a felhasználó számára lehetővé a rejtjelzés biztonsági beállításainak módosítását vagy a minősített adatok rendszerben történő kezelése vagy továbbítása során

a rendszerben alkalmazott rejtjelzés kiiktatását.

(5) Nemzeti „Korlátozott terjesztésű!” minősítési szintű adatot – ha az elektronikus rendszer magasabb minősítési szintű adat kezelésére vonatkozó rendszerengedéllyel nem rendelkezik és a megvalósítási lehetőségek adottak – rejtjelzéssel védett virtuális magánhálózat útján kell továbbítani. „

A fenti információkat értelmezve a védett mobilkommunikációs rendszer fejlesztőjének és üzemeltetőjének van lehetősége megfontolni a (4) bekezdésben megfogalmazottaknak megfelelő rendszer kifejlesztését és üzemeltetését. Ebben az esetben lehetőség ként merül fel az a megoldás, hogy csak a VPN rendszer szerverparkjának biztonsági területén kell megteremteni a minősítési szintnek megfelelő fizikai és elektronikai biztonsági környezetet, és a végponti eszközök (mobiltelefonok) esetében nem kell kialakítani a fenti biztonsági környezetet. Ez különösen figyelemreméltó gondolatmenet akkor, ha tudjuk, hogy ugyanezen rendelet 28.§ (3) bekezdése szerint „A katonai, nemzetbiztonsági és bűnügyi műveletekben a személyi biztonsági tanúsítvánnyal rendelkező személy folyamatos személyes felügyelete alatt álló rendszer, valamint annak eleme a biztonsági vezető által meghatározott biztonsági intézkedések betartása mellett biztonsági területen kívül is használható.

Ebben az esetben a fenti rendelet kisebb módosításával - a 28.§ (3) bekezdés megfontolt kiterjesztésével - lehetséges megalapozni a minősített adatok beszéd és SMS alapú továbbítására alkalmas mobilkommunikációs rendszer jogszerű alkalmazásának lehetőségét, olyan kritikus infrastruktúrát, vagy kritikus információs infrastruktúrát üzemeltető szervezeteknél, ahol ez igazán indokolt. Amint azt a későbbiekben példákkal is igazolom, a fenti modellnek megfelelő alkalmazások, mind a nemzetközi, mind a hazai piacon elérhetőek.

A fenti feltételek teljesülése esetén lehetőség nyílhat hazai fejlesztők által fejlesztett rendszer rendszerengedélyeztetésére úgy, hogy csak a központi egység esetében kell a minősítési szintnek megfelelő rendszeresítési eljárást lefolytatni és a megfelelő rendszerengedélyt az NBF-től kérelmezni, melyet a hatóság közigazgatási eljárás keretében ad ki. Ha összehasonlító elemzésnek vetjük alá az EU-s és NATO-s szabályozásokat [4], [5] megállapítható hogy a hazai szabályozással ellentétben a „Korlátozott Terjesztésű!„ minősítési szintű minősített adat kezelését nem kötik adminisztratív zónához, csupán annyit írnak elő, hogy meg kell akadályozni az adathoz való illetéktelen hozzáférést (NATO információbiztonsági direktíva). Az EU, NATO szabályozás adminisztratív zónáról azt mondja ki, „hogy az a biztonsági terület körül alakíthatók ki és ott legfeljebb KT minősített

adat kezelhető". Ehhez a rendezőelvhez való igazodás tapasztalható az EU és NATO tagországok esetében amikor a védett mobilkommunikációs nemzeti eszközeiket tanúsítja a saját nemzeti hatóságuk. Ha tehát a nemzetközi szabályokkal összhangban a hazai védett mobilkommunikációs eszközök rendszeresítésének és használatbavételének során ehhez a rendező elvhez módjában állna igazodni a hazai fejlesztőnek, (illetve az üzemeltetőnek) nemzeti „korlátozott Terjesztésű!" minősítési szintig nem lenne akadálya a védett mobilkommunikációs eszközök használatbavételének.

NÉHÁNY KÜLFÖLDI ÉS HAZAI FEJLESZTÉSŰ MOBILKOMMUNIKÁCIÓS RENDSZER BEMUTATÁSA.

Hazai és külföldi fejlesztő és gyártó cégek a mobil hálózatokban folytatott szenzitív információkat tartalmazó kommunikáció védelmére alkalmas számos technológiai megoldást ajánlanak. Az általuk alkalmazott műszaki megoldások közül elsősorban az IP alapú technológiák biztosítanak hosszú távú megoldást.

Annak igazolására, hogy a közelmúltban a nemzetközi kritikus infrastruktúrák szektorain belül – az operatív irányítás támogatása érdekében –előtérbe került a védett mobilkommunikációs (infokommunikációs) eszközök alkalmazása, ennek okán az alábbiakban néhány jellemző technológiai megoldási lehetőség kerül bemutatásra. Ennek keretében célszerűen bemutatásra kerül, hazai fejlesztésű alkalmazott technológia is.

Gold Lock TM PBX Gateway

A fenti izraeli védelmi minisztérium által tanúsított technológia, katonai titkosítási szintű titkosítási algoritmussal biztosít háromrétegű (laptop, Nokia telefon, Android készülék) költséghatékony védelmi lehetőséget VOIP beszélgetésekre, szöveges üzenetek küldésére és fájlátvitelre. A technológia megfelelő védelmet nyújt a celluláris információk elfogása és illetéktelenek általi feldolgozása ellen. Ez által költséghatékony védelmet nyújt magán személyek, állami szervezetek, és katonai és rendvédelmi szervek vezetőinek illetéktelen személyek általi lehallgatását illetően.

1. ábra.

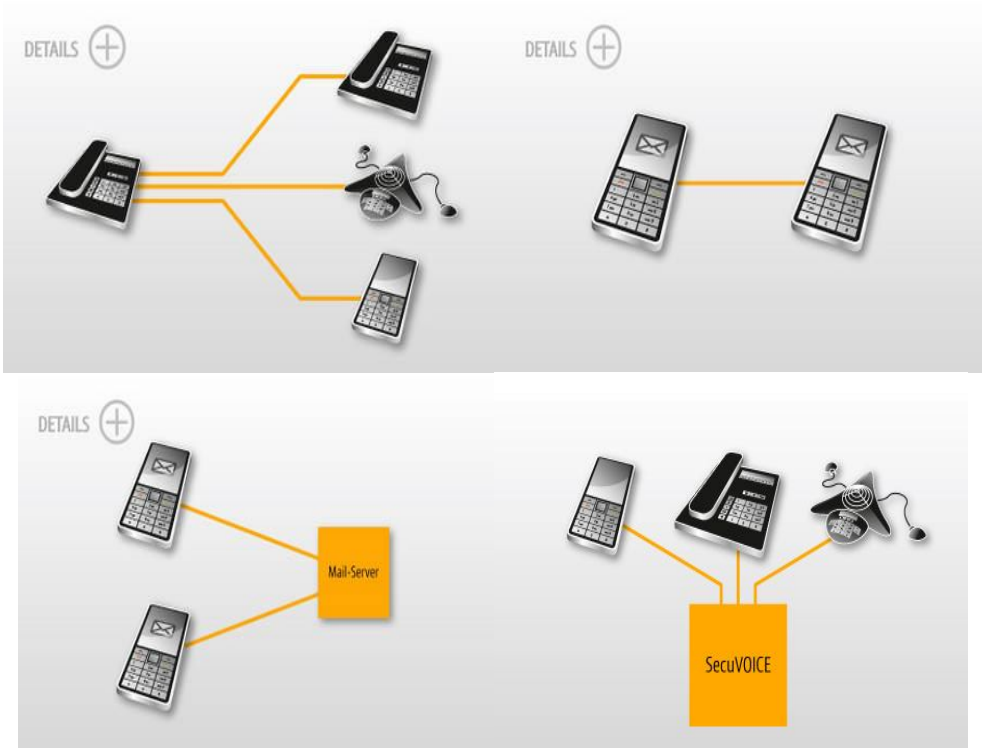
Jellemző tulajdonságok:

- A Gold Lock PBX Gateway-n keresztül egyszerűen kezelhetően végzi el a telefonos kapcsolat biztonságos meghosszabbítását.
- Egy audio jel erősíti meg a biztonságos kapcsolat létrehozását.
- Linux alapú stabil platform
- Jól skálázható, a biztonságos kommunikációt terjeszti ki a mobil eszközök felé.

- Kompatibilis a meglévő digitális alközpontokkal és kihasználja azok előnyeit.
- A rendszerhez egyaránt lehet csatlakoztatni analóg, digitális és IP készülékeket.
- A Gold Lock PBX Gateway kommunikál más Gold Lock PBX Gateway központi egységekkel.
- A Gold Lock PBX Gateway biztonságosan kummunikál 3G adatvonalon, más (Nokia, PC, BlackBery,iPhone) mobil eszközökkel.
- Biztonságos katonai szintű 256 bites (EAS) titkosítási algoritmus használata, megbízható hitelesítés.

Secuvoice [18] NATO KT (Német fejlesztő és gyártó)

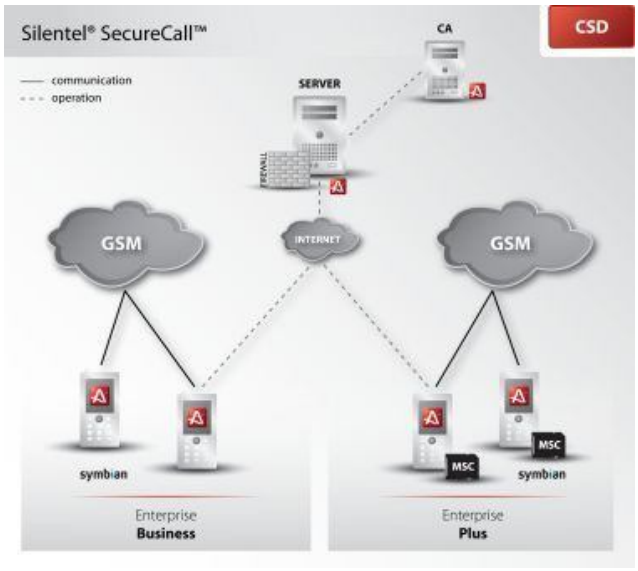
A rendszer jellemzően az egyedi Secusmart biztonsági kártyával biztosítja a hardveres titkosítás megvalósítását, annak minden előnyös tulajdonságát kihasználva. Ebből következően az egyedi azonosítás és a egységes kulcsmenedzsment is biztosított. A SecuSmart biztonsági kártya alkalmazása megfelelő egyenszilárdságú védelmet nyújt a mobil hang és adatátviteli funkciókban egyaránt. A rendszer NATO „Korlátozott Terjesztésű!" minősítési szintű minősített adatok továbbítására hatósági engedéllyel rendelkezik. A SecuSmart kártyát egyszerűen be kell helyezni egy kompatibilis mobiltelefonba. a kártya tartalmaz egy hamisíthatatlan kriptográfiai modult, amely titkosítja (128 bites EAS titkosítás) az adatátviteli útra kerülő (hang, SMS) adatokat. A kártya tartalmaz egy identitást, amelynek segítségével a „végponti eszköz" egyedi azonosítása (tanúsítvány alapú hitelesítése) megtörténik. Ez alapján kizárt a"Man int the Middle" támadás lehetősége. A fentiekből az következik, hogy titkosított kommunikációra azon készülékek képesek, akik rendelkeznek ezzel az identitással. Az alkalmazott hardveres megoldás jellemzően elliptikus kriptográfiai görbét biztosít. A rendszer alkalmas a rugalmas felhasználói igények (mobil-mobil; mobil-ISDN vezetékes; konferencia; SMS) kielégítésére.



2. ábra

Silentel SecureCall [19]

A Silentel SecureCall egy olyan megoldás, amely a dedikált kommunikációs résztvevők részére biztosít mobilkommunikációs lehetőséget. A rendszer architektúráját illetően alapvetően két változatban került forgalomba. Az „üzleti „és a „kormányzati változat között alapvető különbség, hogy az üzleti változat tisztán szoftveres titkosítást végez és a titkosító szoftver e mobiltelefon memóriájára van installálva, addig a kormányzati változat a titkosító szoftverből és egy Mobile Security micro SD (MSC) kriptográfiai chipből épül fel, amelyen egy belső titkosítási algoritmus fut (hardveres kulcsgenerátor és titkosító). A szlovák Nemzeti Biztonsági Felügyelet (Národný Bezpečnostný Úrad) által szlovák nemzeti „Bizalmas!" legmagasabb minősítési szintre tanúsított Silentel SecureCall Plus rendszert használják minősített adatok mobilkommunikációjának megvalósítására a szlovák kormányzati szervek. A „NATO Bizalmas!" szintre történő akkreditációja jelenleg folyamatban van.



3. ábra

A megoldás előnye, hogy könnyű és relatívan olcsó a bevezetése és üzemeltetése. A rendszer architektúrája lehetővé teszi kommunikációs végpontként Android, Symbian, Windows Mobile/Windows Phone, Windows platformú eszközök (smartphone, PDA, Tablet PC, számítógép) együttes alkalmazhatóságát. Lehetőséget teremt arra is, hogy mobil eszközökről titkosított adatátvitellel elérhetők legyenek központi adatbázisok szolgáltatásai (pl. térinformatikai rendszer). Silentel rendszer GSM hálózat áramkörkapcsolt adatátvitel (CSD) technológia alkalmazása helyett standard IP protokoll alapúan is kialakítható, ez esetben egy rendszerben alkalmazhatók WiFi-s, WiMax-os, műholdas, vezetékes végpontok, a különböző Silentel rendszerek összekapcsolhatók.

A fentiekben kifejtett kétségtelen előnyös tulajdonságok miatt rendkívül figyelemreméltó megoldásnak tekinthető a Silentel SecureCall kormányzati és katonai verziója is, amely mindenképpen további részletes tanulmányozást érdemelne és talán ezt követően költséghatékony, felhasználóbarát és megfelelően egyenszilárd megoldás bontakozhat ki a hazai információbiztonsági szakemberek számára.

Sectra [19] (Holland fejlesztő és gyártó NATO, EU Titkos)

4. ábra. Sectra TigerX készülék és asztali kiegészítő terminálja (Tiger XS Office)

A Tiger XS rendszerről a NATO katonai bizottsága tanúsítványt állított ki, amelyben igazolta, hogy a rendszer lehallgatás mentes biztonságos kommunikáció lefolytatására alkalmas „NATO Titkos!" Minősítési szintig. Ugyanezt a rendszert a közelmúltban az EU-ban is tanúsították"EU Titkos!" minősítési szintig. Ebből következik, hogy az eszköz jelen pillanatban kettős tanúsítással rendelkezik (NATA; EU), ezért egyedülálló helyzetben van az európai piacon. A fentiekből következik, hogy a szövetségi rendszeren és az Európai Unión belül lehetőség nyílt a minősített adatok mobilkommunikációjára „Titkos!" minősítési szintig. A rendszer alapvető jellemzője, hogy ugyanazon eszköz egyaránt lehetőséget biztosít a védett vezetékes és mobilkommunikáció megvalósítására. A NATO tagországok katonai vezetőinek és az EU 27 tagországának döntéshozóinak több mint fele rendelkezik a rendszer által biztosított minősített adatok mobilkommunikációs lehetőségével. A rendszer fő funkciója a beszédkommunikáció védelme, de lehetőséget biztosít védett SMS, Fax továbbítására és egyéb adatátviteli lehetőségegek is támogat.

A Sectra Tiger XS személyi titkosító eszközt (n. számú ábra) alkalmazásához felhasználójának bluetooth-szal kell csatlakoztatnia mobil készülékhez, vagy behelyeznie a vezetékes vonalra csatlakoztatott terminájába (Tiger XS Office), az azonosítás kártyával és kóddal történik, ezután a Tiger XS készülékről fogadható, vagy kezdeményezhető a hívás. A rendszer kiépítésétől függően alkalmazhat offline és online kulcsmenedzsmentet, míg előbbinél a kiosztott kulcsokat manuálisan kell telepíteni és időszakosan frissíteni a készüléken, addig online kulcsmenedzsment esetén ezek a hálózaton levő készülékeken automatikusan frissülnek.

5. ábra. Sectra Tiger biztonságos mobiltelefon

A Sectra új fejlesztése [23] a Tiger biztonságos mobiltelefon (n. sz. ábra), mely a Sectra Tiger XS technológiáján alapul. A készüléket úgy tervezték, hogy az mindenhol használható

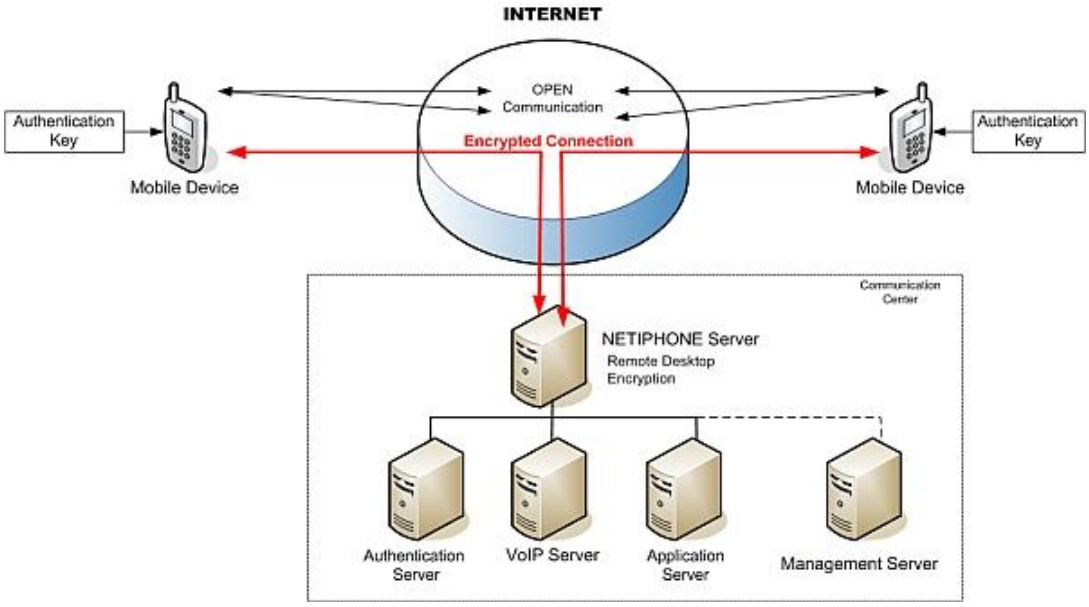
legyen, cellás és műholdas mobilhálózaton egyaránt alkalmazható (GSM, 3G, Iridium, Inmarsat, Thuraya). A készülék kompatibilis a Tiger XS készülékkel és a Tiger XS Office kiegészítő modullal. A svéd-holland fejlesztésű terméknek jelenleg folyamatban van a svéd és holland nemzeti „Titkos!" minősítési szintre történő engedélyezési eljárása, melyet követően EU és NATO „Titkos!" szintre kívánják tanúsítatni.

NETIPHONE [21]

Az állami szervezetek, és a gazdasági társaságok felhasználói részéről igény mutatkozik a belső, bizalmas információkat tartalmazó, publikus hálózatokat használó kommunikációs csatornák – legyen az hang, multimédiás vagy adatkommunikáció – titkosítására. A kommunikációs lehetőségeken túl cél a központi alkalmazások, illetve a levelezés elérése is Mindezt úgy kell megvalósítani, hogy a lehető legkevesebb információ hagyja el a biztonsági területet és az adatok ne kerüljenek tárolásra a külső, nem biztonsági területen elhelyezkedő felhasználói terminálokon. Amint azt a fentiekben láthattuk, az igényeket részben és egészében kielégítő software komponensek már léteznek a piacon. A NETIPHONE™ viszont, amely teljes egészében magyar fejlesztés, tartalmazza a fent említett összes szolgáltatást. Mindemellett felhasználóbarát, könnyen kezelhető és számtalan kényelmi funkcióval ellátott megoldás, amely a titkosított kommunikációt ugyanolyan egyszerűvé teszi, mint a hétköznapi mobiltelefon használatot.

A rendszer felépítése

A NETIPHONE™ alkalmazás a mobil készülékek és a központi NETIPHONE™ szerver között létrehozott titkosított adatcsatornán biztosít megbízható kommunikációt, a nyilvános mobil adathálózatot használva. A hangkommunikációt a központi oldalon található VoIP központ alkalmazás biztosítja a hálózathoz csatlakozó terminálok között. Ezen felül a rendszer lehetőséget nyújt elektronikus levelezésre, illetve központi szolgáltatások használatára is, mint például fájlok küldése és fogadása. Lehetőség van a titkosított csatornán keresztül folytatott kommunikáció központi megfigyelésére, illetve a használat és a működés, rendszer logok alapján történő felügyeletére.



6. ábra.

A rendszer szolgáltatásai:

- Központi alkalmazások távoli desktop-on keresztüli elérése
- Titkosított hangkommunikáció
- Automatikus SMS alapú híváskezdeményező értesítés, a rendszerhez pillanatnyilag nem csatlakozó hívott fél irányába
- Központilag tárolt Telefonkönyv
- Központilag tárolt Hívásnapló a nem fogadott, fogadott, indított hívásokról
- Rendszerüzenetek nem fogadott hívásról, illetve új e-mail beérkezéséről

Biztonság:

- Központilag tárolt érzékeny információk. A kliensen tárolt azonosító adatok védelme jelszóval
- AES 256 bites titkosítás használata
- Szeparált külső és belső hangkommunikáció – nyílt hálózat alkalmazásakor blokkolt titkosított hangkommunikáció funkciók
- A kulcs és beállítási információk jelszavas védelme a készülékben
- Központilag futtatott applikációk, a felhasznált adatok kizárólag központban történő tárolása

Menedzselhetőség, megfigyelhetőség:

- A rendszerkomponensek hibaeseményeinek naplózása
- A kommunikációs események naplózása
- A rendszerben folytatott kommunikációk rögzítése és tárolása, visszakereshetőségük biztosítása
- A rendszerkomponensek központi menedzselhetősége, konfigurálhatósága

A NETIPHONE rendszer előnye, hogy kliens oldalon nem igényel speciális eszközt, a titkosítást megvalósító kliensalkalmazása minden Symbian S60 platformú mobiltelefonra telepíthető. Használatához csomagkapcsolt adatátviteli (GRPS, EDGE, 3G/HSDPA) mobilszolgáltatás szükséges. A készüléket egy hónapig módomban állt tesztelni, tapasztalataim azt mutatják, hogy 3G adatkapcsolat esetén a készülék jól használható, ugyanakkor jelenleg ez még az ország területének nagyobbik részén ez még nem elérhető, 2G adatkapcsolat esetén a beszédhang gyakran volt szakadozott, késleltetett, a problémás helyeken a hagyományos GSM hívások minősége lényegesen jobb volt.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A Mav. végrehajtási rendeleteinek (90/2010. Korm. rendelet és a 161/2010. Korm. rendelet) KT minősített adat kezelését illető rendelkezései nincsenek teljesen összhangban az EU-s és NATO-s szabályozással, ugyanis az utóbbiak nem kötik adminisztratív zónához a KT minősített adatok kezelését. Ugyanakkor a hazai jogi szabályozás katonai, nemzetbiztonsági és bűnügyi műveletekben biztonsági területen kívül is a megfelelő szabályok mellett akár nemzeti SZT minősített adat kezelését is biztosítják, melyet viszont a NATO és EU szabályozás nem enged meg. (Megj: biztonsági terület jármű belsejében is kialakítható). Ahhoz hogy védett mobilkommunikációs rendszereken legalább nemzeti KT minősített

adatokat lehessen kezelni, szükséges hogy azt az EU-s és NATO-s szabályozással összhangban a hazai szabályozás is lehetővé tegye.

Széleskörű (hazai) kormányzati és államigazgatási felhasználásra a nemzeti KT minősítési szint megcélzása a célszerű, személyi, fizikai, adminisztratív, elektronikai biztonsági szempontból a biztonság és a felhasználhatóság, egyenszilárdság (személyek köre, felhasználás helyei, ár-érték) közt „optimális középút „megválasztása mellett.

A NETIPHONE mint hazai kezdeményezés ígéretesnek tűnik, de a megfelelő lefedettség biztosítása mellett a továbbfejlesztésére lenne szükség, melyhez a szlovák fejlesztésű SecureCall szolgáltatja a legjobb követendő mintákat. A legprofesszionálisabb megoldás kétségtelenül a SECTRA, ennek viszont hátránya az egyedi készülékek magas ára lehet.

Az ideális nemzeti védett mobilkommunikációs rendszer paraméterei:

- hazai fejlesztésű (jogszabályok, nemzetbiztonság)
- mobilhálózaton áramkörkapcsolt (GSM hívás) és csomagkapcsolt (GPRS, EDGE, 3G/HSDPA) adatátviteli módban is alkalmazható
- kereskedelmi forgalomban kapható mobilkészülékkel alkalmazható
- készülékei MicroSD formátumú hardveres titkosító kártyát alkalmaznak, GPS modult tartalmaznak
- PKI alapú authentikációt és titkosítást alkalmaz
- Végpont-végpont közti titkosított adatcsatornát alkalmaz
- Tanúsítványok online kezelését biztosítja (központi tanúsítvány szerverrel)
- központi adatbázisokkal alkalmazható (pl. katasztrófavédelmi, rendvédelmi)
- TETRA állomásokkal tud kommunikálni
- + műholdas mobilkészülékekkel is alkalmazható

Az EU-s és NATO viszonylatban a minősített adatok védett mobilkommunikációval történő kezelése, egyértelműen a SECTRA megoldása az egyetlen szóba jöhető lehetőség.

Felhasznált irodalom

[1] A minősített adat védelméről szóló 2009 évi CLV. törvény

[2] A Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010.(III.26.) Korm. rendelet. (58.§ (1),(2))

[3] A telephely biztonsági tanúsítvány kiadásának részletes szabályairól szóló 92/2010. (III. 31.) Korm. rendelet.

[4] C-M (2002) 49 A NATO Biztonsági szabályzata

[5] A Tanács 2001. március 19-i 2001/264/EK határozata a Tanács Biztonsági szabályzatának elfogadásáról.

[6] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV törvény.

[7] Az államtitkot, vagy szolgálati titkot, illetőleg alapvető biztonsági, nemzetbiztonsági érdekeket érintő vagy különleges biztonsági intézkedést igénylő beszerzések sajátos szabályairól szóló 143/2004. (IV.29.) Korm. rendelet.

[8] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Korm. rendelet. 49§-51§

[9] MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények; A mellék-let, A 8.1- A 8.3. p.

[10] MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve (ISO/IEC 27002), 8.1 – 8-3. p.

[11] Magyar Informatikai Biztonsági Ajánlások, Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), Informatikai Biztonsági Követelmények v 1.1. 2008, p. 76-87.

[12] ISO/IEC 20000-1 Information technology – Service management - Part 1: Specification; 3.3. p. és 6.6. p.

[13] Kassai Károly Az elektronikus adatkezelés során szükséges személyi biztonság kérdései.(Hadtudományi Szemle 3. évfolyam 3. szám 2010. 1. oldal)

[14] A Nemzeti Biztonsági Felügyelet elnökének (NBF bemutatása biztonsági vezetőknek.ppt 2010.11.12) előadása.

[15] 1996. évi CXII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (49.§, 55.§, 55.§6A, 116.§, 137.§/A, 189.§)

[16] Az 1959. évi IV. törvény a polgári törvénykönyvről (81.§ (2)-(3) bekezdései)

[17] A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény.

[18] http://www.secusmart.com/home.html (2011.05.10)

[19] http://www.ia.nato.int/niapc/category/mobile-communications_51 (2011.05.10)

[20] http://www.sectra.com/global/news/press_releases/security/2009-2010/pdf/Sectra%20Panthon.pdf (2011. 05.10.)

[21] http://www.neti.com/products/neti-phone (2011. 05.10.)

[22] http://www.ardaco.com/downloads/doc/SGDIS_leaflet.pdf (2011.05.20)

[23] http://www.sectra.nl/Data/Sites/1/Sectra%20Folders/Tiger%207401%20101101.pdf (2011.05.20.)