Végvári Zsolt

A LEHALLGATÁS ELLEN VÉDETT MOBILTELEFONÁLÁS ÖSSZEHASONLÍTÓ VIZSGÁLATA

Abstract

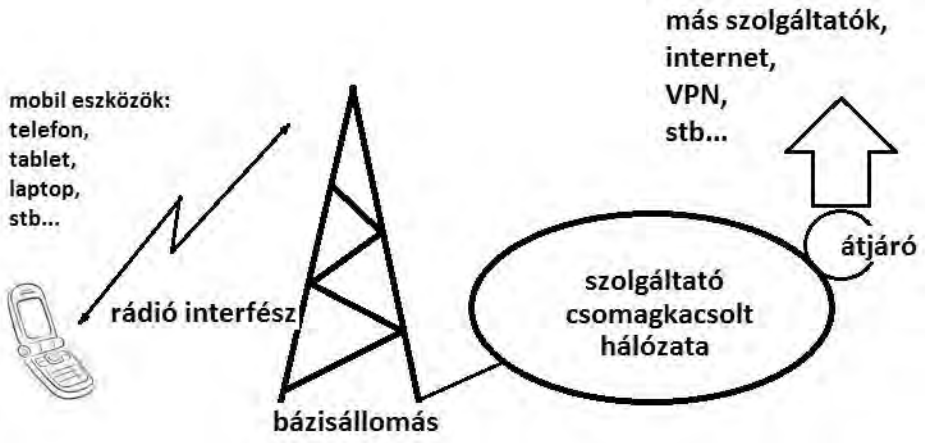
A tanulmány célja az elérhető lehallgatás ellen védett mobiltelefonos megoldások bemutatása és egymással történő összehasonlítása. Bemutatásra kerül a nemzetközi és hazai piac néhány kiemelkedő szereplője – különös tekintettel a NATO minősített adatok kezelésére alkalmas megoldásokra, a teljesség igénye nélkül. Az ismertetett megoldásokkal szemben előzetesen egyetlen kritérium került meghatározásra: legyenek képesek bármely szolgáltató hálózatán teljes körűen együttműködni a hagyományos (lehallgatás ellen nem védett, azaz nem titkosított) telefonokkal, de előnyös, ha rendelkeznek legalább „NATO RESTRICTED" (a továbbiakban: NR) minősítésű elektronikus adatkezelésre történő feljogosítással.

***Kulcsszavak**: mobiltelefon, védett kommunikáció, rejtjelezés, titkosítás.*

1. Technikai háttér

1.1. A cellás mobiltelefon-hálózatok biztonsága

Az elektronikus kommunikáció kezdete óta fontos kérdés az információbiztonság, amely napjainkban a mobilkommunikáció térnyerésével még inkább súlypontivá válik. Az 1. ábrán látható, a világszerte elérhető cellás kereskedelmi mobilkommunikációs (GSM)[1] szolgáltatóknál elérhető rendszerek felépítése, amely alapján könnyen definiálhatók azok a pontok, ahol az illetéktelenek hozzáférhetnek az információhoz.



1. ábra. A GSM rendszer vázlatos felépítése

[1] Global System for Mobile – „globális rendszer a mobilkommunikációért"

Jelen tanulmányban általában információról beszélünk (ahol nem, az ott jelzésre kerül), mivel a beszédkommunikáció digitalizálása már a mobilkészülékekben megtörténik, és ebben a formában kerül a szolgáltató hálózatába, ahol ugyanolyan csomagkapcsolt formában kerül továbbításra, mint a már eleve digitális forrásból származó bármilyen más információ (pl. cella vagy tarifa-információ). Általánosságban elmondható, hogy a GSM hálózatokon a beszédkommunikáció átvitele technológiájában nem, csak adminisztratív módon különbözik bármilyen más adatátviteltől.

Kézenfekvőnek látszik a mobilkészülék és a bázisállomások közötti rádióinterfész „lehallgatása", de már a legelső szabványos digitális GSM architektúra is olyan összetett eljárásokat alkalmaz – részben biztonsági, részben megbízhatósági okokból – , hogy az ehhez szükséges infrastruktúra rendkívül drága és komoly fizikai kiterjedéssel bír. Bizonyítottan léteznek olyan hamis mobil bázisállomások, amelyek néhány tíz, esetleg száz méteres hatókörben „túlharsogják" a szolgáltatók bázisállomásait, így a nem megfelelően beállított mobilkészülékek automatikusan rájuk kapcsolódnak. Az ilyen hamis cellák telepítésének nyilvánvaló nehézségei miatt ez a módszer más államok területén, vagy tömeges módon egyáltalán nem alkalmazható. Ennek köszönhetően az egyes államok területén az egyébként törvényesen működő titkosszolgálatok is általában arra kényszerülnek, hogy a jogszabályilag kötelezzék a szolgáltatókat, hogy azok adminisztratív központjaikban, ritkábban a bázisállomásokon tegyék lehetővé bizonyos adatforgalmak megfigyelését (tipikusan egy-egy mobilszámhoz tartozó hívások lehallgatását).

A szolgáltatók a saját gerinchálózatuk kiépítéséhez ugyanolyan csomagkapcsolt technológiákat alkalmaznak, mint az internet esetében, de ezek a hálózatok alapesetben az internettől szeparáltan működnek. A más szolgáltatókhoz, vagy éppen az internethez történő kapcsolódásra az átjárók szolgálnak. Az adatforgalom ezekből az irányokból is támadható, de ez olyan biztonsági kérdés, ami túlmutat jelen tanulmány keretein.

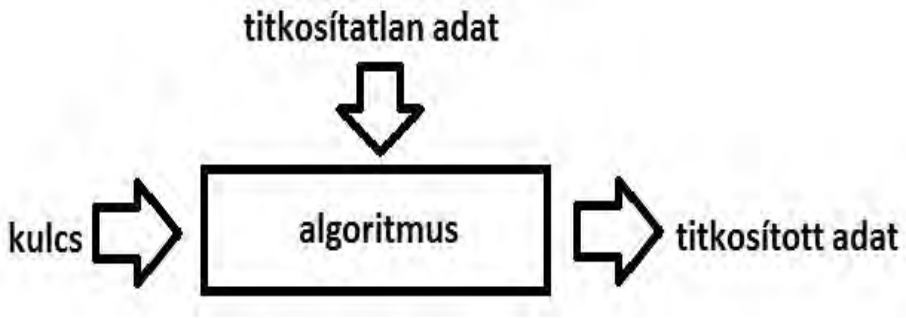
Az bizonyosan látszik, hogy a használt eszközön kívül a felhasználónak a rendszer semmilyen más elemére nincs ráhatása, így az egyetlen kielégítő módszer a beszélgetések (és egyéb telefonos adatforgalmak) védelmére, ha az információ már a szolgáltató rádió interfészére is titkosított formában kerül. A titkosított adat azután ugyanolyan módon továbbítódik a hálózaton, mint a nem titkosított, mivel a rendszer elemei nem tesznek különbséget a bitek között. Az egyetlen eltérés csupán annyi, hogy ha az adott bitsorozatot a rendszer bármely köztes elemén vagy akár egy felhasználói végberendezésben értelmezni kívánjuk, ahhoz fel kell oldanunk a titkosítást.

Hazánkban az adatok logikai védelmére szolgáló kódolás - dekódolást tartalmazó eljárásokra nincs egységes terminológia. A minősített adatok védelmére szolgáló eljárás a vonatkozó kormányrendelet szerint a „rejtjelzés", [1.]míg általánosságban említve – inkább a napi életben a „titkosítás" kifejezés az ismertebb. Szakmailag nem pontos, de gyakorlati szempontokat szem előtt tartó megoldásként a tanulmány következetesen a köznyelv által használt „titkosítás" kifejezést alkalmazza.

1.2. Kriptográfiai háttér

A titkosítás történhet hardveresen, illetve az erre alkalmas eszközökön (okostelefonok, táblagépek, PC-k) szoftveresen, sőt a kettő kombinációjával is. A titkosítás minősége, vagyis a feltörési kísérletekkel szembeni állóképessége alapesetben nem ettől, hanem az alkalmazott matematikai algoritmustól függ, mégis fontos eltérések tapasztalhatók a két módszer között. A hardveres titkosítás előnye, hogy a csak beszédkommunikációra alkalmas „buta" mobiltelefonokon is implementálható, így szoftveres oldalról nem is támadható. Ugyanakkor komoly hátránya, hogy a plusz hardver miatt drága, és általában csak azonos gyártó készülékei között működik. Az alkalmazott algoritmus frissítése, újabbra cserélése is nehézkes. Előnyök és hátrányok tekintetében a szoftveres megoldás a hardveres ellentéte. Olcsón kialakítható és könnyen frissíthető, tetszőleges szoftveres és hardveres környezetben is megvalósítható, de éppen a szoftveres környezet okán újabb támadási pontokat kínál.

A titkosítás alapsémája a 2. ábrán látható. Az alkalmazott algoritmus a titkosítatlan adat bitsorozatát egy másik – immár titkosított – sorozattá alakítja. A titkosító algoritmusok többnyire jól ismertek, ezért egy ún. egyedi kulcs (ez természetesen egy kulcs-bitsorozatot jelent) felhasználásával oldják meg, hogy az információt ne lehessen visszanyerni. Így még ha ismert is az alkalmazott eljárás matematikája, a konverzió során alkalmazott kulcs nélkül nem nyerhető vissza az eredeti bitsorozat. Mindebből látható, hogy a titkosítás minőségének szempontjából az alkalmazott eljárás összetettségén túl döntő szerepe van a kulcsnak is.

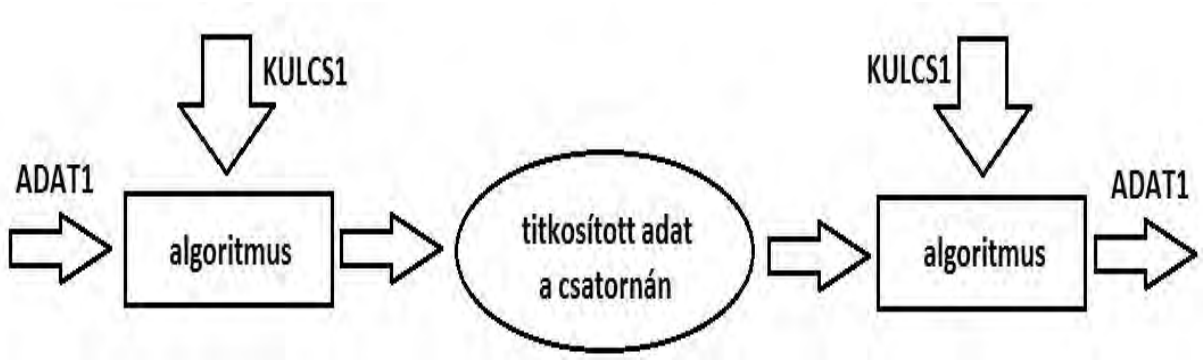


2. ábra. A titkosítás alapsémája

Léteznek elvileg megfejthetetlen (feltörhetetlen) titkosítási eljárások is, amelyek visszafejtése matematikailag is lehetetlen – de a vele járó nehézségek miatt ilyeneket a gyakorlatban csak nagyon ritkán használnak. Léteznek ún. gyakorlatilag megfejthetetlen eljárások, amikor a visszafejtés matematikailag lehetséges, de a hozzá szükséges idő a jelenlegi szuperszámítógépekkel is minimum évezredekbe telne. Azonos eljárás mellett természetesen a nagyobb kulcs-méret (pl. 64, 128, 256 bit) rendre nagyobb biztonságot jelent és a kulcs méretének növelésével nem lineárisan,

hanem exponenciálisan nő a feltöréshez szükséges idő. A 64 bites AES[2] titkosítás esetén a világ leggyorsabb szuperszámítógépének (amely jelenleg a másodpercenként 54 ezermilliárd műveletet elvégzésére képes kínai Tianhe-2) mindössze 5 percre lenne szüksége a visszafejtéshez, míg ha a kulcs nagyságát megduplázzuk 128 bitre, akkor ez az idő máris 1000 milliárd évre nő, ami meghaladja az univerzumunk várható élettartamát (!).

A kulcs alkalmazásának szempontjából további két nagy csoportja van a titkosító algoritmusoknak. Az ún. szimmetrikus kulcsú algoritmusok esetében csak egy kulcs létezik, vagyis ténylegesen ugyanaz a bitkombináció kell az adatok visszafejtéséhez, mint amit a titkosításnál is használtak. Az eljárás előnye az egyszerűség, ugyanakkor kockázatot jelent a kulcs kezelése (a kulcsot a kommunikáció előtt megbízható úton el kell juttatni a címzetthez). A gyakorlatban is alkalmazott ismertebb megvalósításai a DES, 3DES[3], AES és az IDEA[4] (PGP)[5].



3. ábra. A szimmetrikus kulcsú titkosítás

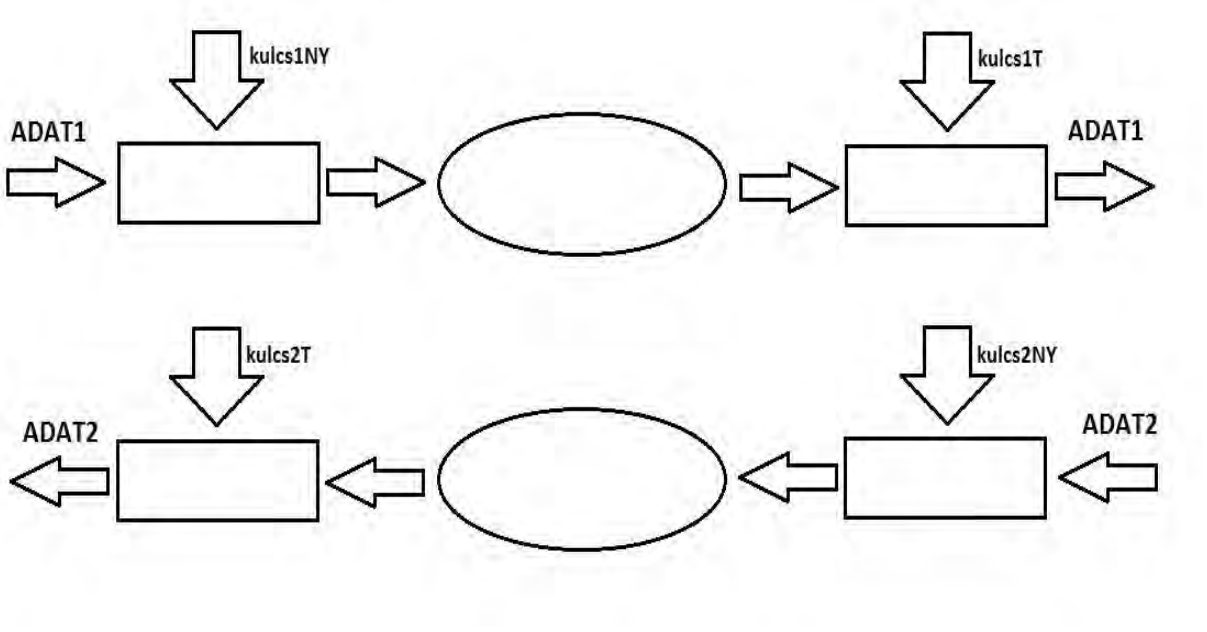
[2] Advanced Encryption Standard – a legelterjedtebb szimmetrikus kulcsú titkosító algoritmus. Két belga kriptográfus ötlete alapján végül az amerikai NIST (Nemzeti Standardizáló és Technológiai Intézet) adta ki a leírását 2001-ben, a korábban általánosan használt DES leváltása céljából. Mindeddig csak egyetlen vitatott sikeres törési kísérletet publikáltak vele kapcsolatban. Jelenleg teljesen elfogadott standard eljárás, és nincs benne NSA-kiskapu sem.

[3] Data Encryption Standard – a legelső szimmetrikus kulcsú titkosító algoritmusok egyike, amit még a 70-es évek elején az IBM-nél fejlesztettek ki. Fejlettebb változata a 3DES. A kidolgozását állítólag már a legkorábbi szakasztól az NSA felügyelte. A 90-es években feltörték, így ma már sehol nem alkalmazzák.

[4] International Data Encryption Algorythm – szimmetrikus kulcsú titkosító algoritmus, amit három kriptográfus mutatott be még 1991-ben. Mivel 2012-ig jogdíjas volt a használata nem terjedt el igazán, bár a biztonságát az AES-el egyenértékűnek tekintik. Jelentősége abban rejlik, hogy része a PGP 2.0-nak.

[5] Pretty Goog Privacy – ez egy több eljárást is magába foglaló komplett titkosító program, amelyet elsősorban szöveges információk védelmére használnak. Több verziót is megélt, és ma is széles körben használják, mert egy átlagos elektronikus leveleket küldő és fogadó felhasználó számára sem jelent nagy kihívást az alkalmazása.

Ezt a fajta sebezhetőséget küszöbölik ki az aszimmetrikus kulcsú algoritmusok. Itt két kulcs létezik, az ún. nyilvános kulcs és a titkos kulcs. A nyilvános kulcsot bárkinek oda lehet adni (így akár nyílt csatornán is lehet továbbítani), ennek birtokában olyan titkosított információ állítható elő, ami viszont csakis a titkos kulcs birtokában fejthető vissza (melyet természetesen bizalmasan kell tárolni, kezelni). A nyilvános kulcs a titkos kulcsból kerül előállításra, az alkalmazott matematikai eljárás (hash[6]) mégis biztosítja, hogy a nyilvános kulccsal a visszafejtés nem lehetséges, illetve annak birtokában (legalábbis gyakorlatilag) a titkos kulcs sem reprodukálható. Az eljárás egyetlen szépséghibája, hogy a két különböző kulcs (duplex[7] adatforgalom esetén a két kulcspár) előállítása rendkívül erőforrás igényes, így gyengébb hardveres környezetben a valós idejű titkosítás nem is lehetséges vele. Legismertebb implementációja az RSA[8].



4. ábra. Aszimmetrikus kulcsú titkosítás

[6] Hasítófüggvény. Olyan matematikai eljárás, ami bármilyen hosszúságú bitsorozatot adott hosszra képez le.

[7] Minden adatátvitelnél létezik egy forrás (adó) és egy címzett (vevő). Ha ez a szereposztás fix, akkor szimplex átvitelről beszélünk. Ha ugyanazon a csatornán mindkét fél lehet adó is és vevő is, de amíg az egyik ad, a másik csak vételre képes, akkor ún. félduplex átvitelről beszélünk. Mára általános a duplex vagy full duplex átvitel, ahol mindkét fél egyszerre adhat és vehet.

[8] Ron **R**ivest, Adi **S**hamir és Leonard **A**dleman által publikált eljárás az aszimmetrikus kulcsú titkosításokban használt publikus kulcsok hitelesítésére. A még 1977-ből származó módszer két rendkívül nagy prímszámra épül, ezért megvalósításakor kritikus a jó minőségű véletlenszám-generátor megléte. Számos titkosító rendszer gyengeségét éppen az adja, hogy bár az alkalmazott eljárások papíron tökéletesek, de csak egy nem teljes értékű véletlenszám-generátort implementálnak beléjük, ami máris jelentős támadási felületet kínál a hozzáértőknek.

1.3. A telefonkészülékek

A titkosítás módját és minőségét nagyban meghatározza maga a telefonkészülék is, ezért érdemes áttekinteni ezek főbb típusait. Mivel a táblagépek lényegében csupán nagyméretű, funkciójukban specializált okostelefonok (amelyekkel többnyire nem is lehet telefonálni), nem foglalkozunk velük külön.

1.3.1. Hagyományos telefonok

A hagyományos („buta") telefonokon általában a telefonáláson kívül csak néhány alkalmazás (óra, naptár, számológép, esetleg rádió, vagy zenelejátszó) érhető el, és nem kínálnak fejlettebb funkciókat. Azok, akiknek csak a telefonálás, esetleg SMS-küldés a fontos, gyakran használnak ilyen készüléket, de a gyártók már nem erre a területre koncentrálnak. A jelenleg kapható, ebbe a kategóriába készülékeket a gyártók annyira alapmodellként kezelik, hogy sok esetben már az okostelefonok elterjedését megelőző hagyományos készülékeken is elérhető technikákat (memóriakártya, fényképezőgép, médialejátszó) sem építik bele ezekbe.

Ezek a telefonok jellemzően valamilyen gyártó- vagy készülék-specifikus 8 bites operációs rendszert futtatnak, az innovatívabb készülékek esetleg Symbian-t. Ez utóbbi operációs rendszer már lehetőséget kínál néhány fejlettebb funkció megvalósítására (pl. érintőképernyő) is, de az okostelefonok térnyerése nyomán mára gyakorlatilag teljesen kifulladt ez a fejlesztési irány. Összességében ez a készülékkategória nem alkalmas szoftverek utólagos telepítésére, legfeljebb java-s alkalmazásokéra, illetve a bennük alkalmazott hardverelemek sem elégségesek az egyébként komoly erőforrás-igényű titkosítás megvalósítására, ilyen készülékek esetén tehát csak a hardveres megoldás jöhet szóba, a készülékházba integrált vagy utólagosan csatlakoztatható titkosító modul formájában.

1.3.2. Okostelefonok

Az ún. okostelefonok legfontosabb jellemzője, hogy olyan hardverekkel rendelkeznek, melyek olykor a néhány évvel korábbi asztali számítógépeket is felülmúlják. A 32 bites, GHz-es tartományban dolgozó processzorok, a több GB memória, a Wi-Fi, 3G és bluetooth kapcsolat lehetősége illetve a nagyméretű grafikus érintőképernyő lehetővé teszik olyan fejlett operációs rendszerek futtatását, amikhez utólagosan szoftverek írhatók, telepíthetők. Az operációs rendszerek mentén erős gazdasági szövetségek jöttek létre, ezek között jellemzően nincs átjárás és a szoftvereik sem kompatibilisek (bár a független szoftvergyártók több operációs rendszerre is megírhatják a programjaikat). Az operációs rendszereket és a hozzájuk tartozó szoftverek illetve szolgáltatások (pl. felhő) összességét ökoszisztémának nevezzük. Az erős hardverek és a fejlett operációs rendszerek okán a titkosítás akár teljes egészében szoftveres úton is megvalósítható. A hardveres titkosítás ezeken a készülékeken is megvalósítható lenne, de a fentebb sorolt paramétereik miatt lényegesen olcsóbb a szoftveres fejlesztés, így tisztán hardveres megoldással a gyakorlatban nem is lehet találkozni.

IOS

Az okostelefont, mint készülékkategóriát – több erőtlen próbálkozás után – lényegében az Apple cég hozta létre 2007-ben. Már a legelső iPhone is az ún. IOS operációs rendszert futtatta, ami jelenleg már a 7.x fő verziószámnál tart, illetve épp a tanulmány írásának idején válik elérhetővé a 64 bites (8.x) változat. Mivel mind a készülékgyártást, mind a szoftverek elérhetőségét az Apple tartja kézben, rendkívül zárt rendszerről van szó. A készülékek viszonylagos drágasága, és a sajátos felhasználói szokások miatt elsősorban Észak-Amerikában erős a pozíciója. Rendkívül gazdag ökoszisztéma tartozik hozzá, amely a zártság okán elég biztonságosnak tekinthető, az informatikai kártevőknek és bűnözőknek kevésbé kitett.

Android

A Linux alapokra épülő Android operációs rendszert 2008-ban mutatta be a keresőjéről ismertté vált Google cég és azonnal ingyenessé tette az iparág valamennyi szereplője számára. Emiatt a készülékgyártók sokasága épít hozzá telefonokat és az egészen olcsó árkategóriában is elérhetővé teszik az okostelefon élményét. Nem csoda, hogy Észak-Amerikán kívül messze ez a legelterjedtebb mobil operációs rendszer (az utolsó felmérések szerint már Észak-Amerikában is megelőzte az IOS-t). Rendkívül gazdagon burjánzó, de meglehetősen nyílt ökoszisztéma tartozik hozzá, amely így a kiberbűnözők elsődleges célpontjává teszi. Jelenleg a 4.4.x verziónál tart és szintén fejlesztik a 64 bites változatát Android L néven.

Windows Phone és Windows Phone 8

A Microsoft több hasonló elől után 2009-ben adta ki (a Windows CE alapjaira építve) a Windows mobiltelefonos változatát, amely több, most nem tárgyalt ok miatt végül sosem terjedt el. Mivel sem a Windows korábbi PC-s változataival, sem az újabb Windows 8-al nem kompatibilis, a 7.x-es utolsó verzióval, a Windows 8 megjelenésekor gyakorlatilag kihalt.

Hosszú vajúdás után 2012-ben adta ki a Microsoft a Windows 8 mobil eszközökre is használható változatát. Az IOS-hez és az Androidhoz képest késői start miatt a hozzá tartozó ökoszisztéma jelenleg még jóval szegényebb, mint a konkurensek esetében. Részben ennek is tudható be az egyelőre viszonylag alacsony piaci részesedés, de a Microsoft személyében óriási tőke és tapasztalat áll mögötte, ami nemrégiben kiegészült a Nokia mobiltelefonokat gyártó részlegével is. Jelen tanulmány szempontjából az teszi különösen érdekessé, hogy a közigazgatásban vagy akár a honvédelemben kevésbé fontos a sok elérhető alkalmazás (legkevésbé a játékok), viszont nagy jelentőséggel bír a professzionális terméktámogatás, és a PC-s múlt okán a Windows a konkurenseknél jóval fejlettebb MDM[9]-et és csoportadminisztrációt (flottakezelés, munkacsoportok) kínál már jelenleg is.

[9] Mobile Device Management – Mobil Eszköz Menedzsment. Egy napjainkban jelentkező probléma, ami leképezi a számítástechnika múltját. Az első PC-k gyakorlatilag „szóló" munkaállomások voltak, majd miután egy-egy intézményen belül hálózatba kötötték őket, felmerült egyfajta „házirend" kialakításának szükségessége. Ma már az emberek jelentős részének van valamilyen okos" mobileszköze, amik intézményi (munkahelyi) használatát egyre inkább szükséges adminisztrálni és korlátozni.

Blackberry

Kezdetektől külön utakon járt a Blackberry, amely csak a saját készülékeihez fejlesztett külön operációs rendszert. Mind hardveresen, mind szoftveresen folyamatosan a legújabb technológiákat alkalmazták ezekben a készülékekben, és mivel a Blackberry szándékosan az üzleti szegmensbe pozícionálta magát, a készülékek árcédulája is piacvezető volt sokáig. A Blackberry egészen az utolsó változatok megjelenéséig ragaszkodott az „okos" funkciók mellett érdekesen, sőt anakronisztikusan ható mechanikus QWERTY billentyűzethez. A cég végül 2013-ban csődbe jutott és bár még mindig forgalmazzák a készülékeit, jelenleg is bizonytalan a további sorsa. Amennyiben a Blackberry márkaként fenn is marad, a legújabb modelleken már valószínűleg Android, esetleg Windows fog futni. Jelen tanulmányban azért fontos mégis említést tenni róla, mert az üzleti vonalat képviselve, még a kihalás szélén is komolyabb biztonsági megoldásokat vonultat fel a konkurenseinél.

Létezik még néhány további operációs rendszer az okostelefonok piacán (Samsung – **Tizen**, Huawei, ZTE, Alcatel – **Firefox OS,** Amazon – **Fire OS**), de ezek igen szerény elterjedtségűek, titkosító alkalmazások még nem érhetőek el hozzájuk.

2. Kereskedelemben kínált, NATO tanúsítással rendelkező minősített adatkezelésre feljogosított, lehallgatás ellen védett mobiltelefon-megoldások

A továbbiakban a minimum NATO RESTRICTED (a továbbiakban: NR) minősítésű elektronikus adatok kezelésére feljogosított kereskedelmi termékeket tekintjük át a NATO hivatalos beszállítói honlapja alapján[10]. Az egyes eszközökre vonatkozó tanúsítást a NATO Katonai Tanácsa (Military Committee) hagyja jóvá, de nem publikus, hogy milyen kritériumok alapján. A titkosítási eljárások, illetve eszközök vonatkozásában általánosságban egy ún. garantált állóképességet szokás meghatározni, ami azt az időt jelenti, amennyi ideig, egy reális számítási kapacitást feltételezve, bizonyosan nem lehet azt feltörni. Ezek a sarokszámok nem ismeretesek, de valószínűsíthetően NATO SECRET és TOP SECRET minősítés esetén gyakorlati fejthetetlenséget feltételezhetünk, míg az alacsonyabb szinteken (NR – korlátozott terjesztésű, ill. „NATO CONFIDENTAL" – bizalmas) szinteken ez egy már belátható időintervallum lehet. Azt fontos megjegyezni, hogy önmagában már egy 128 bites AES algoritmus is gyakorlati fejthetetlenséget jelent, de ha pl. a kommunikációs csatorna felépítésekor alkalmazott eljárások során „elfogható" a kulcs, akkor akár néhány óra vagy akár perc is elég lehet a teljes kommunikáció visszafejtéséhez. Annyi valószínűsíthető, hogy a NATO nem fogadja el a tisztán szoftveres megoldásokat, mivel valamennyi NATO-minősített okostelefonos termék – bár ez kriptográfiai szempontból nem indokolt – tartalmaz egy hardveres kiegészítőt is (micro SD-kártya[11]).

[10] http://www.ia.nato.int/niapc

[11] Secure Digital – napjaink legelterjedtebb memóriakártya típusa, mobilkészülékekbe szánt változata a „micro".

2.1. Az ismert megoldások általános ismertetése

2.1.1. Aselsan 2110 SMP és 2110 MECT

A török hadiipari cég számos fejlesztésben érdekelt. A 2110-es sorozatú telefonjaik egyszerű, második generációs mobilkészülékek (a 900, 1800 és 1900 MHz-es GSM frekvenciák használatára képesek), kiegészítve egy közepesen erős (128 bites) hardveres AES titkosító egységgel. A szükséges kulcsok hardveres kulcskártyával vagy jelszóból generálva adhatók meg. A 2110 SMP készülékek NR, míg a 2110 MECT típusjelű készülékek „NATO SECRET" minősítésű adatokat kezelhetnek.. A MECT készülékek „RESTRICTED" módban együttműködnek az SMP jelű készülékekkel, de a technológia korábban említett sajátosságai miatt az Aselsan telefonjai semmilyen más készülékkel nem kompatibilisek (legalábbis titkosított üzemben bizonyosan nem). USB[12]-s forrásból bármilyen bitfolyamot képesek legfeljebb 9,6kbit/s sebességgel továbbítani, illetve a készülékek alkalmasak a szolgáltatótól független, titkosított SMS-ek küldésére és fogadására is, mindezt a titkosított beszédcsatorna felhasználásával.

A készülékek előnye, hogy bárki által, gyakorlatilag speciális ismeret nélkül is nagy biztonsággal használhatóak, ugyanakkor technológia szempontjából egy 10 évvel ezelőtti szintet képviselnek (harmadik generációs változatról nem található információ).

2.1.2. Blackberry BES10[13]

A szebb napokat megélt kanadai mobiltelefonos cég egy időben az üzleti telefonok etalonjának számított. A legutolsó Blackberry készülék-generációhoz (Z10 és Q10) rendelt üzleti szolgáltatás-halmaznak (BES) része a szoftveres titkosítás lehetősége is. A készülékek kis túlzással minden technológiát felvonultatnak, amit egy korszerű harmadik generációs telefon tudhat. Ennek fényében nem meglepő, hogy szinte minden létező szimmetrikus és aszimmetrikus algoritmus implementálható rájuk (pl. AES-ből akár az unikumnak számító 512 bites is). Bár a kanadai mérnökök kimondottan üzleti megoldásnak fejlesztették a BES-t, az 2013 őszén megkapta a NR adatok kezelésére jogosító minősítést is.

[12] Universal Serial Bus – Univerzális Soros Busz. Napjaink digitális eszközein leggyakrabban megtalálható adatkommunikációs csatlakozófelület. Mobil eszközökön a általában micro-USB csatlakozó található.
[13] Business Enterprise Solution – Innovatív Üzleti Megoldások.

A készülékeken tárolt adatok titkosítási lehetőségei példásak, de sajnos a BES titkosított kommunikáció tekintetében inkább tekinthető platformnak, mintsem konkrét terméknek, ugyanis a használatához elő kell fizetni egy megfelelő szolgáltatónál. Magyarországon ilyenről nincs tudomás, sőt még maga a BES sem érhető el magyar nyelven. A saját operációs rendszert használó Blackberry készülékek részesedése a mobilpiacon az IOS és az Android előretörése miatt mára marginálissá vált, ezért Kanadában elkészítették a BES-t erre a két operációs rendszerre is, de ezek elterjedtsége gyakorlatilag nulla maradt.

A Blackberry-féle megoldás innovatív technikák tömegét mutatja be, de ezek gyakorlati felhasználása az anyacéget sújtó nehézségek miatt jelenleg szinte egyáltalán nem lehetséges. Magyarországon különösképpen nem, mivel jelenleg még hivatalos Blackberry márkaképviselet sincs az országban és a mobilkészülékek is csak a szolgáltatók kínálatában érhetők el. Nem szól a Blackberry készülékek mellett az sem, hogy a saját operációs rendszere okán, a telefonok tudásának kihasználásához nemcsak egyszerű felhasználói ismeret, hanem Blackberry platformon szerzett tapasztalat is szükséges.

2.1.3. Cellcrypt Mobile Baseline

A brit Cellcrypt a mobil hangtitkosítási piac egyik legkomolyabb szereplője. A NATO információs oldalán NR adatok kezelésére jogosító minősítéssel szerepel a Cellcrypt Mobile Baseline, amely azonban nem a cég kínálatának zászlóshajója, hanem egy kizárólag Blackberry-re elérhető megoldás, amelyet jelenleg még viszonylag nagy számban alkalmaznak az Egyesült Királyság kormányzati kommunikációjában. A cég egyéb hasonló termékei az üzleti piacnak jelentős részét lefedik, de NATO minősítéssel jelenleg nem rendelkeznek. A Mobile Baseline-ról nem sok információ érhető el, de annyi bizonyos, hogy az alkalmazott technológiák nagyjából megfelelnek az „iparági szabványnak”.

2.1.4. Compumatica GSM

Az egyébként is mobil biztonsággal foglalkozó német Compumatica is elkészítette saját szoftverét, amely külön dedikált SD-kártyával működik. A Cellcrypt-hez hasonlóan a cég széles termékpalettájából csak a Blackberry platformra épülő szoftver kapta meg az NR minősítést. Mivel semmilyen konkrét információ nem érhető el róla, a minősítés ellenére valószínűleg sosem forgalmazták.

2.1.5. Sectra Panthon

A svéd Sectra cég elsősorban hardveres titkosító-berendezéseiről ismert, de okostelefonokra elkészítették a meglehetősen erős, 256 bites AES-re épülő szoftverüket is. A szoftver csak speciális dedikált SD-kártyáról futtatható, amelyre egy hardveres ECC[14]-t és egy AES co-processzort[15] is implementáltak. Ez a megoldás jelenleg adatkommunikáció titkosítására nem alkalmas, csak beszéd és SMS titkosítására

[14] Elliptic Curve Cryptography – elliptikus görbék alkalmazása a titkosítás során. Bizonyos eljárásokban lényegesen kisebb bitszám mellett is azonos biztonságot nyújtanak, mint a hagyományos módok. Ennek következtében rövidülnek a feldolgozandó bitsorozatok, és érezhetően nő a titkosítás sebessége is.

[15] Segédprocesszor.

képes. A szükséges kulcsokat is titkosítva tárolja, és felhasználóbarátnak tűnő grafikus felületen (angol nyelven) néhány kiegészítő szolgáltatást is kínál, mint emelt szintű felhasználó-azonosítást, titkosított telefonkönyvet. Az Android operációs rendszert futtató telefonokra szánt terméket jelenleg Panthon 3 néven forgalmazzák, ahol a 3-as ebben az esetben nem verziószám, ugyanis Panthon 2 néven létezik a szoftver Windows Phone-os változata is. Ez utóbbi elvben képes az androidos készülékekkel való titkosított kommunikációra, de a jelenleg feljövőben levő Windows 8-ra még nem készítették el, a korábbi Windows verziókat futtató telefonok pedig már nem elérhetőek, így ez a lehetőség gyakorlati jelentőséggel nem bír. A NR minősítésű szoftvernek magyarországi forgalmazója nincs.

A Panthon gyári oldala egyszerű használatot ígér bármilyen androidos telefonra, de bővebb specifikáció nem elérhető, mint ahogy nincsenek referenciák sem.

2.1.6. Sectra Tiger XS

A Tiger XS nem egy GSM specifikus megoldás. Az akár „NATO SECRET” minősítésű berendezés hagyományos telefonvonalak titkosításán túl GSM, UMTS[16], hagyományos IP[17], ISDN[18], Iridium és Inmarsat[19] kapcsolatok titkosítására is alkalmas. Az EU gyorsreagálású erők többnemzetiségű Északi Harccsoportjában és a holland közigazgatásban alkalmazzák, de nem GSM hálózatra telepítve. Méretéből, felépítéséből is látszik, hogy a GSM alkalmazás ez esetben inkább csak elvi lehetőség, mintsem napi gyakorlat. Komoly titkosító-eszköz lévén nem átlagos telefon-felhasználóknak készült, a működtetése speciális felkészítést igényel, és a (nem hivatalos forgalmazótól származó) darabonkénti 2500 dolláros ár is elgondolkodtató lehet.

2.1.7. Tecnobit TMS DEF

A számos védelmi projektben részt vevő spanyol cég is rendelkezik NR minősítésű mobilkommunikációs megoldással, amelyről csak annyit tudni, hogy okostelefonokra fejlesztették ki. Az elérhető platformok, a működési algoritmus tekintetében sincs róla nyilvános információ, a cég még angol nyelvű honlapot sem üzemeltet, így feltehetőleg ez is egy „halott” termék.

---

[16] Universal Mobile Telecommunications System – a harmadik generációs GSM hálózatokon elérhető adatátviteli mód, amellyel akár 42Mbit/s-os átviteli sebesség is elérhető.

[17] Internet Protocol – az internetre kötött eszközök által használt átviteli szabályok összessége. Napjainkban az interneten kívül zárt hálózatokban (intranet) is széleskörűen alkalmazzák.

[18] Integrated Services for Digital Network – a legelső általánosan használt digitális adatátviteli módok egyike. A 80-as, 90-es évek telefóniájában forradalminak számított az akkori analóg megoldásokhoz képest, de mára már alig használják.

[19] A két legismertebb műholdas telefonszolgáltatás. A GSM-től eltérően nem földi telepítésű bázisállomások biztosítják a készülékek közötti kapcsolatot, hanem műholdak. Olyan területeken is használhatók, ahol nincsenek GSM szolgáltatók, de ennek megfelelően igen drágák mind a készülékek, mind a tarifák.

2.1.8. SecuSmart SecuVoice

A német cég még 2011-ben készítette el a NATO minősítést nyert SecuVoice és az érdekes módon különálló SecuSMS alkalmazást. Az alap kriptográfiai elvárásoknak megfelelő szoftvert kizárólag SD-kártyákon telepítve árulták, és sajátossága volt, hogy nem tisztán VoIP[20]-ra épült, működése során felhasználta a GSM beszédcsatornát is. E termék további sorsáról nincs információ, a cég az elmúlt hónapokig gyakorlatilag tetszhalott volt. A Németországot is érintő amerikai lehallgatás-botrány kapcsán aztán váratlanul feltámadt a vállalkozás. Jelenlegi kereskedelmi termékei már nem a SecuVoice-ból származtathatók, hanem önálló, új fejlesztések, ám a gyártó nem ezekről, hanem a német kancellár-asszony (és kollégái) részére nagy hirtelen elkészített, a neten csak „Merkelphone”-ként emlegetett telefonokról lett ismert. Ezek kereskedelmi forgalomban természetesen nem kaphatók és a technikai részleteik sem publikusak…

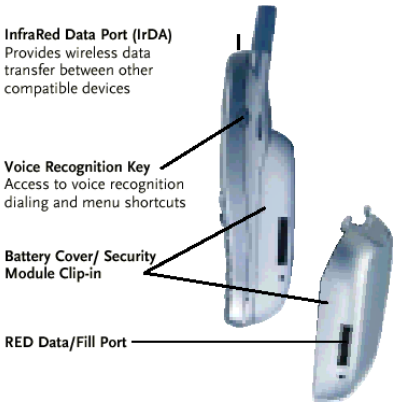
2.1.9. Silentel 5.2

A minősített megoldások közül az egyik legsokoldalúbb és legkiforrottabb a szlovák Ardaco cégé. A vállalkozás közel 20 éve kimondottan lehallgatásvédett hálózati kommunikációs megoldások kialakításával foglalkozik. A Silentel jelenlegi 5.2-es verziója NR, illetve „NATO CONFIDENTAL” minősítéssel is rendelkezik, és a hozzá tartozó kliensszoftvert minden jelentősebb okostelefon-platformra (IOS, Android, Windows Phone 8 és Blackberry), sőt még PC-re is elkészítették, amelyek természetesen képesek egymással titkosított módon kommunikálni. Ezt mindenképp érdemes hangsúlyozni, mert ez a fajta multiplatformosság, illetve ezen a szinten a „CONFIDENTAL” minősítéső adatok kezelésére való jogosultság is egyedülálló. A titkosítás természetesen az SMS-ekre is vonatkozik, sőt a titkosított bitfolyamok küldésével és fogadásával egyfajta lehallgatás ellen védett konferencia-chat is kialakítható.

A cég ugyanezen termékét kínálja üzleti megoldásként is, és az általános gyakorlattal ellentétben listaárakat is közöl. A csak beszédtitkosítást végző applikáció havi 30 €-tól (évi 300 €) érhető el. Az SMS-ek titkosítását végző modul további havi 20 € (évi 200 €), az SMS plusz titkosított file-átvitel 30 € (évi 300 €), a titkosított chat-konferencia pedig újabb 30 (300) €-ba kerül készülékenként.

[20] Voice over IP – hang átvitele digitalizálva, csomagkapcsolt formában, az Internet technológiáját felhasználva. A legkorszerűbb titkosított mobiltelefonok és telefonos alkalmazások kivétel nélkül erre épülnek.

2.1.10. General Dynamics Sectéra secure GSM



Az amerikai cég terméke abban az értelemben kimagaslik a mezőnyből, hogy egyedülálló módon NATO „TOP SECRET" adatok kezelésére alkalmas minősítést kínál. A technikai részletek taglalása nélkül is megfelelő reklám a készülék tényleges képességeinek, hogy az interneten számos kép található, amelyeken Barack Obama amerikai elnök a kezében egy ilyen eszközt szorongat. Mindezek ellenére a termékvonal gyakorlatilag halottnak tekinthető, mivel egy hardveres modulról van szó, ami csakis és kizárólag a Motorola Timeport típusú, második generációs telefon akkumulátora helyére felcsatolható. Az említett készülék gyártása valamint forgalmazása kb. 10 éve megszűnt.

2.2. Az elérhető minősített megoldások számbavétele

A fenti megoldások közül a valós alkalmazás szempontjából hazánkban csupán néhány jöhet szóba. Az Aselsan és a General Dynamics hardveres eszközeinek használata az elavult technika, és elsősorban a készülékek elérhetősége, szervizháttere (illetve annak hiánya) miatt gyakorlatilag kizárható. A működtetés nehézségei, és nem utolsósorban a magas ár miatt sem célszerű a Sectra Tiger XS alkalmazása. Elvben lehetséges, de nem javasolt a csak Blackberry készülékekre elérhető szoftveres alkalmazások valamelyikének bevezetése, mivel a gyártó céget sújtó nehézségek miatt ezeknek a termékeknek a várható tényleges életciklusa csekély, semmiképp sincsen arányban a várható ráfordításokkal. Végezetül eltekinthetünk a gyakorlatban már nem forgalmazott egyéb szoftveres termékektől is, így a tényleges kínálat mindössze két lehetőségre szűkül. A jelen pillanatban is kereskedelemben elérhető megoldások közül csak a Sectra Panthon nevű, illetve a Silentel 5.2-es verziójú alkalmazása felelnek meg a korábban említett NR kritériumoknak.

2.3. Az elérhető alkalmazások technikai hátterének elemzése

Amennyiben a NATO elektronikus adatok kezelésére jogosító minősítés kizárólagos szempont lenne, akkor csak a fenti két termék jöhetne szóba, de ha eltekintünk ettől, akkor megállapítható, hogy a piac sokkal több szereplős, csak a legtöbb termékre a gyártók (vélhetően üzletpolitikai okok miatt) sosem kértek és kaptak NATO minősítést. Bár az egyes ökoszisztémákhoz tartozó alkalmazásboltokban többnyire nem elérhetők, de valójában se szeri, se száma a lehallgatás ellen védett telefonálást kínáló szoftveres megoldásoknak, és ezek közül sokról feltételezhető, hogy jóval hatékonyabb is, mint a fent említett kettő. E két termék csupán az elérhető szoftvertenger két átlagos darabja, amelyekre a gyártók ki tudja miért, de megszerezték a NATO minősítését. Általános felépítésükben és működésükben valamennyi ilyen típusú alkalmazás (természetesen ideértve a Sectra és a Silentel megoldásait is) megfelel egyfajta iparági szabványnak tekinthető trendnek és csak részleteikben különböznek, bár mint tudjuk, a lényeg sokszor itt található.

Egyik szoftveres szolgáltatás sem használja alapesetben a hagyományos GSM beszédátviteli csatornát, működésük a VoIP technológián alapul, így állandó internetes kapcsolatot igényelnek (meg nem erősített információk szerint a Panthel rendszere internetkapcsolat hiányában a hangminőség jelentős romlása mellett képes „visszaváltani" 2G-re). Ebből következően ezek a szoftverek nem kizárólag GSM-specifikus megoldások, az okostelefonos platformokon kívül létezik vagy elvben létezhetne hagyományos PC-s megvalósításuk is, sőt ad abszurdum, igény esetén akár okostelevíziós vagy játékkonzolos alapokon is megvalósíthatók lennének. Valamennyi szolgáltatáshoz tartozik (legalább) egy szerver, amely alaphelyzetben nyilvántartja a felhasználókat és azok elérhetőségét, illetve segít a kapcsolat kialakításában. Miután a kapcsolat létrejött, a szerver – néhány adminisztrációs részlettől (pl. percdíjas megoldásoknál díjszámlálás) eltekintve – kiszáll a kommunikációból, és azt a továbbiakban a felhasználók P2P[21] módon folytatják. Ez nem csupán a szerverek és hálózat leterheltségét csökkenti, de mivel a titkosított adatfolyam már nem folyik át egy központi egységen, nagyban növeli a biztonságot is.

Lényeges kérdés, hogy mivel ezek a szolgáltatások minden esetben előfizetésesek, az árak nagyságrendileg havi 10.000 Ft/készülék-ről indulnak és nem ritka a százezres nagyságrendű havidíj sem. A szervert is mindig a szolgáltató biztosítja, ezek kihelyezésétől vagy eladásától többnyire elzárkóznak. Néhány cég hajlik arra, hogy az alkalmazott szerver-oldali megoldást is értékesítse, így miután valaki megfizette a vélhetően nem csekély árat, a saját munkatársai részére elvileg már tetszőleges számban és ingyen biztosíthatja a szolgáltatást. Mivel ilyenkor a szerver „saját" adminisztratív területen található, a rendszer biztonsága nagyban javul, a biztonsági incidensek kezelése a szolgáltatótól függetlenül is megoldható. Talán hátrány, talán előny, hogy ilyenkor az azonos technológiát használó, de nem másik flottához tartozó (másik szervert vásárló cégek illetve egyéni előfizetők) telefonok sem érhetők el külön átjáró nélkül.

Az adatcsomagok titkosítása szinte minden esetben az AES algoritmus 256 bites verziójával történik. Ez az algoritmus nyílt forráskódú, bárki által használható, és jelenleg nincs ismert sérülékenysége. Az erőforrásokkal is takarékosan bánik, ami szintén előnyös a mobilalkalmazások esetében. Elvben már 128 bit is biztosítja a gyakorlati fejthetetlenséget, ilyet vagy 168, esetleg 192 bites megoldást mégis ritkán találni. A magasabb számú, pl. 512 bites kialakítás a gyakorlatban nem nyújt nagyobb biztonságot, de nagyobb az erőforrásigénye, így ilyen is csak elvétve fordul elő. Néhány éve igen népszerűek voltak a twofish és blowfish[22] algoritmusok is, de az utóbbi időben kiderült néhány olyan gyengeségük, ami nyomán a felhasználásuk mostanra gyakorlatilag megszűnt.

[21] Peer-to-Peer – „peer"-ek, azaz egyenlő partnerek közötti kapcsolat. A tradicionális hálózati modell szerint egy szerver szabályozza a kapcsolatot, és a kliensek ettől kérhetnek szolgáltatásokat. A P2P esetében viszont a szolgáltatást a résztvevő partnerek szabályozzák egymás között.

[22] Bruce Shneier által 1997-ben kifejlesztett szimmetrikus kulcsú titkosító algoritmus. Az AES alternatívájaként tekintettek rá, és egy ideig óriási jövőt jósoltak neki. Több továbbfejlesztése (Twofish, Threefish) is elkészült, de a 2000-es évektől kezdve több támadhatóságára is fény derült, így mára nem elfogadott a használata

A titkosító szoftvereknél általános megoldás, hogy a kulcscseréhez a Diffie-Hellman[23] algoritmust használják, amelyet jobb esetben 2048 bites RSA-val hitelesítenek. A nem hitelesített vagy csak RSA-kulcscserés megoldások komoly kockázatot jelentenek, így alkalmazásuk nem elfogadott. Sok tájékoztató anyag hatalmas nóvumként hangsúlyozza az ECC alkalmazását a Diffie-Hellman algoritmusban, de ez a tény a biztonságot nem növeli. Az ECC jelentősége mindössze abban keresendő, hogy a görbék matematikája kb. fele-harmada bitszám is ugyanolyan biztonságot nyújt, mint a „hagyományos" megoldás. Ez a tény pedig az egyébként igen erőforrásigényes Diffie-Hellman algoritmus működését felgyorsítja.

3. Alternatívák

Jelen tanulmánynak nem volt célkitűzése a NATO által nem minősített alternatívák keresése, de mivel az NR kritériumoknak megfelelő megoldások száma gyakorlatilag kettő, és ezeknél számos elismerten biztonságosabb alkalmazás is elérhető NATO minősítés nélküli kereskedelmi termékként, ez utóbbiak bemutatása is indokolt.

Miután szinte az összes szolgáltatás a fentebb ismertetett technológiákra épül, fontos hangsúlyozni, hogy egyfajta alapszintű biztonságot mindegyikük nyújt. Az alkalmazott protokollok alapján a kommunikáció ténye könnyen felfedhető, a szolgáltatók hálózatán közlekedő adatcsomagokat elfogó személy, vagy gép mégsem tudja értelmezni azt. Lényeges kérdés, hogy a fenti, lényegében azonos elemekből eltérő architektúrák állíthatók össze, amelyek elsősorban a kulcsok kezelésében térnek el egymástól. Ezek alapján a konkrét rendszerek sokszor a biztonság egészen más dimenzióit valósítják meg, bár támadható pontja szinte mindegyiküknek van.

Példaként említhető az egyik NR minősített alkalmazás, a Silentel 5.2. A NATO minősítése a laikusok számára magas biztonságot sejtet, azonban kriptográfiai szakmai körökben nem tartozik az igazán elismert megoldások közé, mivel a kulcsokat a kliens eszköz nyílt formában tárolja. Ez azt jelenti, hogy a korábban elfogott a titkosított adatcsomagok birtokában (ez önmagában nem túl bonyolult informatikai művelet), az esetlegesen ellopott készüléken tárolt adatok alapján a teljes kommunikáció könnyen visszafejthető.

3.1. Az ismert alternatívák bemutatása

3.1.1. Silent Circle és Blackphone

Az amerikai cég jelenleg a piac legerősebb szereplője a világon és látványos marketingje nyomán számos előfizetőre tett szert. Kliens alkalmazása IOS és Android platformra is elérhető, amelyek kezelése felhasználóbarát, és sok kényelmi szolgáltatást is kínál. A szolgáltatás percdíjas, a legolcsóbb és csak beszédtitkosítást kínáló 100 perces csomag 13 dolláros havi díjért érhető el. A legtöbb kritika azért éri, mert a Silent Circle nem informatikai, nem szoftveres cég (a többi gyártó általában ilyen),

[23] Withfield Diffie és Martin Hellman matematikusok által 1975-ben publikált aszimmetrikus kulcsú titkosítási eljárás. Az ötlet első ránézésre elég képtelennek tűnt, hiszen ha valaki az egyik irányban ismer egy eljárást, akkor elvben a másik irányban is meg tudja azt adni, de itt egy általunk nem részletezett magas szintű matematikai eljárás ezt mégis kizárja. Minden manapság alkalmazott aszimmetrikus kulcsú eljárás erre épül.

hanem egy távközlési szolgáltató. Ez azt jelenti, hogy a korábban említett „lehallgatási pont” törvényileg, gyárilag be van építve a rendszerbe. Bár a reklámjaiban P2P szolgáltatásként hirdetik a terméket, az adatcsomagok a gyakorlatban mégis áthaladnak egy központi szerveren, ami szintén bizalmatlanságra adhat okot a felhasználók részéről.

Legújabb termékük a nagy hírverést kapott Blackphone. Ez tulajdonképpen egy, a spanyol GeeksPhone vállalat által gyártott közepes tudású és minőségű androidos készülék, aminek az operációs rendszerét jelentősen átalakították, és eltávolították a biztonsági kockázatot jelentő elemeket – így az ökoszisztéma lelkét jelentő Play Market-et is – továbbá gyárilag integrálták a Silent Circle alkalmazásait. A készülék kb. 630 dollárért vásárolható meg, ami meghaladja az android-paletta csúcskészülékeinek árát, de ebben benne van egy év előfizetés is, ami aztán a továbbiakban évi 120 dollárért újítható meg.

3.1.2. Bull

A fent említett Blackphone IT körökben a tanulmány írásakor nagyon felkapott téma, pedig nyilvánvalóan nem új a koncepciója. A francia Bull cég lényegesen kevesebb hírverés mellett már közel egy éve forgalmazza Hoox m2 típusjelű telefonját, ami paramétereiben (butított Android) nagyon hasonló a konkurenséhez, csak arra a francia fejlesztő saját megoldásait integrálták. A viszonylagos ismeretlenség oka az amerikainál szűkebb reklámköltségvetés mellett a némileg soknak tűnő 2.000 €-s listaár is lehet.

A készülék egy alsó-középkategóriás androidos darab, amit az operációs rendszer átalakításán kívül egy SD-kártyával is megerősítettek. Kriptográfiai szempontból a várható paramétereket hozza a rendszer, úgymint AES-256 médiatitkosítás és RSA-2048-al hitelesített Diffie-Hellman kulcscsere. Támogatja az MDM-et és védett a MITM[24] támadások ellen is, de kevés egyéb részlet ismert (emiatt nem is szerepel majd az összehasonlító táblázatban). Ellátták, egy a cég által biometrikus azonosítóként reklámozott ujjlenyomat olvasóval is, de ennek működése valószínűleg megbízhatatlan (a legújabb iPhone-okon kívül jelenleg az androidos mezőnyben csupán a Samsung Galaxy S5 rendelkezik hardveres ujjnyom-azonosítóval, és még ez is gyakorta téved, az erre a célra jóval kevésbé alkalmas képernyős megoldások-

[24] Man In The Middle – azaz „ember középen”. Egy napjainkban népszerű adatszerzésre irányuló kiber támadási mód, amikor a támadó oly módon épül be egy két fél között zajló kommunikációba, hogy mindkét fél azt hiszi, ő közvetlenül a partnerével kommunikál, pedig az információ átfolyik a középen levő eszközön (személyen) is.

tól – mint amilyen a Hoox m2-é is, – így még ennyit sem szabad várni). Elképzelhető, hogy mivel ez egy integrált megoldás, vagyis a hardvert és a szoftvert is optimalizálták egymáshoz, a titkosított telefonálás nem használ külön szoftver-interfészt, mint a sima alkalmazások, hanem az megegyezik a hagyományos GSM hívások megjelenítésével, és így az átlagostól egyszerűbb használhatóságot nyújt.

Létezik a cégnek Hoox m1 néven egy a korábban említett Aselsan telefonokhoz hasonló régimódi készüléke is, amit ugyan már nem gyártanak, de még forgalmaznak. Bár ez is „csak" egy hagyományos telefon, de komolyabb titkosítást implementáltak rá, mint a török konkurensnél, és maga a készülék is modernebb. Rendelkezik színes kijelzővel, kamerával és média-lejátszóval is, bár a harmadik generációs készülékek nyújtotta előnyökről, mint az e-mail és a file-átvitel itt is le kell mondanunk.

A Bull készülékeknek a legtöbb konkurenstől eltérően van magyarországi viszonteladója. A Hoox m2 telefon rendelkezik ANSSI minősítéssel, illetve a viszonteladó szerint folyamatban van a NATO általi minősítése is, de ezt megerősíteni nem tudjuk, mivel a folyamatban levő ügyekről a NATO honlapján nem találhatóak információk.

A Bull rendszerarchitektúrájának kötelező eleme egy security gateway[25], amely nélkül a készülékek egyáltalán nem használhatók. A hazai viszonteladó nem hivatalos érdeklődésünkre 8 db készülék + gateway + 1 év támogatás konfigurációban 37.000 €-s irányárat adott meg m2 készülékekkel és 30.000 €-t m1 készülékekkel. Ez kb. 115.000 illetve 95.000 Ft-os havidíjnak felel meg készülékenként, ami a konkurencia ismeretében enyhe túlzásnak tűnhet, de azt fontos hangsúlyozni, hogy itt szerver-kihelyezésről van szó, vagyis a rendszer központi egysége is a vásárló tulajdonába kerül és azt saját területén is elhelyezheti, ami a biztonság szempontjából nyilvánvalóan egy magasabb szintet valósít meg. Több készülék esetén az egy készülékre eső ár nyilvánvalóan még kevesebb lehet, hiszen a szerver valószínűleg több száz készülékből álló flottát is képes kiszolgálni további ráfordítás nélkül.

3.1.3. Cellcrypt

Szintén a szegmens legnagyobbjai közé tartozik a korábban már említett brit Cellcrypt. A nagyság okán sajnos a csupán néhány tucat előfizetéssel kecsegetető partnerekkel nem is foglalkoznak igazán, jobbára az olyan „nagyhalakat" célozzák meg termékeikkel, mint az angolszász közigazgatás és a multinacionális óriáscégek. A termék ennek megfelelően nem kimondottan olcsó, listaáron 5 évre 3.500 font/készülék, ami átszámolva évi kb. 300.000 forint. A rendkívüli drágaság nem jelent feltétlen kiemelkedő biztonságot, mivel az USA kormányának hivatalos beszállítójaként a gyári „kiskapu" a CellCrypt rendszerében is biztosított.

3.1.4. Gold-Lock

Nemzetközileg viszonylag széles körben elterjedt még ez az izraeli megoldás, ami tulajdonképpen egy katonai technológia (a kapcsolódó jogok birtokosa az Izraeli Védelmi Minisztérium) üzleti implementációja. Kriptográfiai szempontból kimondottan gyengének mondható a központilag generált kulcsok okán és sok kritika éri a hangminőséget is, ami érezhetően elmarad még a hagyományos GSM hívásokétól is.

[25] Biztonsági átjáró. Az infokommunikációban átjárónak nevezik azokat az eszközöket, amelyek különböző technológiájú (vagy az azonos technikai háttérrel rendelkező, de más által felügyelt) hálózatok között létesítenek kapcsolatot.

Szolgáltatásként a Gold-Lock 3G elnevezésű termék 120 dolláros havi, vagy 1.400 dolláros éves díjért vásárolható meg egy-egy készülékre. A Gold-Lock cégnek létezett egy az Aselsan 2110-hez és a Bull Hoox m1-eshez hasonlatos második generációs készüléke is Gold-Lock GSM néven, de ezt már nem forgalmazzák.

3.1.5. Zybex

A paletta egyik üdítő színfoltja a magyar illetékességű (Sóskúton bejegyzett) Zybex Információbiztonsági Kft. Secure Phone nevű alkalmazása. Csak Android 4.x platformon működik, de már havi 10.000 forinttól elérhető, így kisebb hazai vállalkozások által is megfizethető. Egyszerű használatot, és alacsony sávszélesség mellett is jó hangminőséget ígér, de túl sok kiegészítő szolgáltatása nincsen. Kritikaként még annyi említhető a szoftverrel kapcsolatban, hogy az általa használt és még a reklámanyagban is hangsúlyozott FIPS[26] 140-2 minősített algoritmusok kompromittálódtak leginkább az elmúlt időszak NSA-botrányában, így a rendszer biztonsága legalábbis megkérdőjelezhető.

3.1.5. Secfone

A lichensteini bejegyzésű cég egyes hírek szerint magyar tulajdonosi háttérrel rendelkezik. Az alkalmazásuk bármilyen IOS, Android vagy Blackberry készüléken használható – amennyiben az rendelkezik microSD kártya fogadóhellyel, mert a rendszer használatához elengedhetetlen az ún. „Crypto Card" használata. Ennek ára egyszeri 300 €, amihez havi 55 € előfizetési díj társul. Az alkalmazott titkosítási eljárások szakmai körökben egyáltalán nem elfogadottak. Az adatcsomagok Blowfish algoritmussal kerülnek kódolásra, a kulcscserére pedig egy egyszerű RSA szolgál.

3.1.6. CryptTalk

Az egész piac talán legígéretesebb tagja a svéd Arenim Technologies szoftvere. A név a skandináv tőkeinjekció hozadéka, de valójában a cég fejlesztői és értékesítési központja is Budapesten található. A cég és a termék is szinte minden szakmai díjat besöpört az utóbbi időben (ISACA Security Award 2013, Developer Heroes CE 2014, Eurocloud Partnership Award 2014, Technoshow 2014 – leginnovatívabb megoldás, 2014 legjobb magyar startup-ja), de a legnagyobb elismerés talán mégis a Silent Signal oklevele. Ebben a jeles hackercsapat elismeri, hogy kétheti igyekezettel sem tudta feltörni a CryptTalk védelmét.

A CryptTalk tulajdonképpen ugyanazokra a nyílt forráskódú algoritmusokra épül, mint valamennyi konkurense, de az architektúrát úgy tervezték, hogy a legrosszabb eshetőséget vették alapul, így többek között azt feltételezik, hogy a támadó nem „kívülről jön", hanem már házon (rendszeren) belül van. Az NSA-botrány kipattanása után a fejlesztők tudatosan eltávolítottak minden kompromittálódott elemet. Auditált információbiztonsági szakértők szerint a CryptTalk korábban elfogott adatfolyamából csak akkor van esély az eredeti kommunikáció reprodukálására, ha egyidejűleg törik fel a központi szervert, a kliens készüléket és szerzik meg a felhasználó PIN-kódját

[26] Federal Information Processing Standards – az USA kormánya által sztenderdizált informatikai eljárások.

is. Jelenleg valószínűleg ez a világon a legerősebb ismert biztonsági megoldás a mobiltelefonok piacán, a fejlesztő csapat pedig áll elébe minden „white box[27]" tesztelési kísérletnek is.

Egyelőre csak iPhone-okon használható a szolgáltatás (illetve iPad-eken és iBook-okon), és az ökoszisztéma ismert magas kockázata miatt androidos verzió fejlesztését nem is tervezik, de Windows Phone-ost – a piaci igény függvényében – igen. A szolgáltatás alapvetően itt is előfizetéses konstrukcióban érhető el, de a cég képviselői elmondták, hogy volt már példa szerver-kihelyezésre is. A rendszer moduláris felépítése miatt előnyös, hogy ilyen esetekben az alkalmazott algoritmusok is a megrendelő igényei szerint változtathatóak.

A honlapjuk szerint a havidíjak a vállalt „hűségidő"-től függően 60 és 110 € között alakulnak, amelyből sávosan (az előfizetések számától függően) ad további kedvezményeket a cég. A szerverkihelyezés árát (ha valóban volt ilyen) az Arenim Technologies üzleti titokként kezeli.

3.2. Összefoglalás

Összefoglalva elmondható, hogy a lehallgatás ellen védett mobiltelefonok piaca igen sok szereplővel bír. Amelyek között „amatőr" fejlesztőktől kezdve az óriásszolgáltatókig számos cég képviselteti magát. A felhasznált technológiák és eljárások többnyire ugyanazok, így egyfajta alapszintű biztonságot mindegyik kínál, de a rendszer teljes körű biztonságát tekintve már jelentős eltérések vannak az egyes megoldások között. A jelenleg is elérhető két NATO minősítésű adatok kezelésére alkalmas megoldás biztonsági szempontból csupán a piac derékhadát képviseli.

Ha valakinek a NATO minősítésének hiánya mindenképpen kizáró tényező, akkor a jelenleg ténylegesen elérhető megoldások száma kettőre korlátozódik, konkrétan a Sectra Panthon-ra és a Silentel 5.2-re. Ugyanakkor mindenképp javasolt a Bull Hoox m2 számbavétele is, mert valószínűleg néhány hónapon belül ez utóbbi is megkapja a minősítést. Mivel mindhárom megoldás közel azonos szintű biztonságot nyújt, a Bull hatalmas előnye lehet az integrált készülék, a magyarországi képviselet és az a tény, hogy nemcsak szolgáltatást kínálnak, hanem (fizikailag is) átadnak egy teljes rendszert, amely a továbbiakban házon belül adminisztrálható és rugalmasan skálázható.

Ha a NATO általi minősítés hiánya nem kizáró ok, és az elvárt biztonság szintje csupán minimális, akkor bármelyik a tanulmányban szereplő megoldás szóba jöhet, amelyek között pusztán az ár, esetleg a szolgáltatások gazdagsága dönthet. A „véletlen" vagy „amatőr" lehallgatástól még a technikailag legkevésbé kiforrott megoldások is tökéletes védelmet nyújtanak, de profi hackercsoportok vagy nemzetközi titkosszolgálatok ellen nyilvánvalóan nem sokat érnek.

Ha a NATO minősítésű adatok kezelésére alkalmas jogosítvány hiánya nem kizáró ok, de az elvárt biztonság szintje magas, akkor Magyarországon kézenfekvő meg-

[27] „Fehér doboz". Egy szoftvertesztelési eljárás. Teljes ellentéte a fekete doboznak (black box), amikor semmit nem tudunk egy vizsgált rendszerről. Itt a rendszer teljes leírása és minden forráskód átadásra kerül a hackerek részére. Amennyiben azok a program működésének teljes körű és részletekbe menő ismerete mellett sem képesek megszerezni az áhított információt, akkor valóban igen jónak lehet mondani a rendszer biztonságát.

oldás lehet a CryptTalk. Bár komoly kötöttséget jelent a felhasználók számára, hogy jelenleg csak IOS-en működik a szolgáltatás, azonban a termék e pillanatban az elérhető legmagasabb szintű biztonságot nyújtja – még az NSA számára is lehallgathatatlan. Itt fontos megjegyezni azt is, hogy az üzleti életen túl, a védelmi szférán kívül a magyar közigazgatásban számos helyen keletkezhetnek olyan szenzitív információk, amelyek védelme nemzeti érdek. A közigazgatás élén álló egyes személyek telefonbeszélgetései bizalmasságának megóvása létjogosultságot adhat – az egyébként zsúfolt piacon – a magyar üzleti hátterű, vagy magyar szellemi tulajdonon alapuló megoldásoknak.

Hangsúlyozandó, hogy az egyébként is igen robbanásszerűen változó információtechnológián belül ebben a szegmensben különösen gyorsan átfordulhatnak a trendek, és csak kevés szereplő rendelkezik többé-kevésbé biztos piaci pozícióval. Ez utóbbiak pedig többnyire nem a szoftverfejlesztők, hanem a távközlési szolgáltatók, akiknek a státusza már önmagában is biztonsági kockázat. Mindezeknek megfelelően ez a tanulmány nem is vállalkozik arra, hogy jóslatokba bocsátkozzon a jövőben várható irányokról.

3.3. Összehasonlító táblázat

Az alábbi táblázatban az NR minősített és a gyakorlatban is elérhető két megoldás, valamint az ismertebb piaci alternatívák kerülnek összevetésre (a Bull Hoox kivételével). A legjobb paramétereket zöld színnel, a legrosszabbakat pirossal jelöljük.

Gyártmányok és megoldások összehasonlítása

1. számú táblázat

Fejlesztő cég:	Ardaco as.	Sectra AB.	CellCrypt Ltd.	Zybex Informá-cióbiztonsági Kft.	Arenim Techno-logies AB.	Gold Line Gro-up Ltd.	Silent Circle Ltd.	Navayo Interna-tional AG.
Ország:	Szlovákia	Svédország	USA (KF: UK)	Magyarország	Svédország (KF: Magyarország)	Izrael	Svájc (USA offshore)	Lichenstein (offshore)
Honlap:	www.silentel.com	www.sectra.com	www.cellcrypt.com	www.biztonsagostelefon.hu	www.CryptTalk.com	www.gold-lock.com	www.silentcircle.com	www.secfone.co.uk
Termék:	**Silentel 5.2**	**Phanton 3**	**CellCrypt Mo-bile**	**Zybex Secure Phone**	**CryptTalk**	**Gold Lock 3G**	**Silent Voice**	**Secfone**
Telecom part-ner:	nincs	nincs	nincs	nincs	nincs	nincs	van	nincs
Kommunikáci-ós csatorna:	VoIP	VoIP	VoIP	VoIP	VoIP	VoIP	VoIP, XMPP (SMS)	VoIP
Hitelesítés:	RSA-2048	RSA-2048	RSA-2048 és ECDSA	N/A	RSA-2048, OTP, SÍP digest	„16348 bit Authentication”	ZRTP	RSA-2048 (szerver), RSA-1024 (P2P)
Kulcscsere:	ECC Diffie-Hellman	ECC Diffie-Hellman	ECC Diffie-Hellman	N/A	ECC Diffie-Hellman + OTP (RSA)	ECC Diffie-Hellman	ECC Diffie-Hellman	MVCN
Média titkosí-tás:	AES-256	AES-256	AES-256 és RC4	„very strong”	AES-256 CTR módban	AES-256 + ECC-384	AES-256 CTR módban	448 bit Blowfish
SRTP[28] hitelesí-tés:	nincs	nincs	nincs	nincs	HMAC-SHA1	nincs	HMAC-SHA1	nincs

[28] Secure Real-time Transport Protocol – Biztonságos Valós idejű Átviteli Protokoll. Az RTP a beszédátvitelben is rendkívül fontos, valósidejű kommunikációt biztosító protokoll. Ezek vezérlése egy tipikus támadási pont a titkosított adatátvitelnél, amelynek kivédésre szolgál a titkosított változat, az SRTP.

Termék:	Silentel 5.2	Phanton 3	CellCrypt Mobile	Zybex Secure Phone	CryptTalk	Gold Lock 3G	Silent Voice	Secfone
Végpontok közötti kommunikáció:	szerveren is átmenő	szerveren is átmenő	tisztán P2P	tisztán P2P	tisztán P2P	szerveren is átmenő	szerveren is átmenő	tisztán P2P
Privát kulcs védelem:	nincs	N/A	N/A	N/A	Parented	N/A	csak eszközön	Smartcard
Integritásvédelem:	nincs	nincs	nincs	nincs	hitelesített voice/IM csomagok	nincs	hitelesített voice/IM csomagok	nincs
„Perfect Secrecy[29]" támogatás:	van	N/A	van	N/A	teljes, egyedi kulcsokkal	van	teljes, egyedi kulcsokkal	nincs
Ismétlődő támadások elleni védelem:	N/A	N/A	N/A	N/A	„chellenge-response" kulcscsere	N/A	„chellenge-response" kulcscsere	N/A
MITM elleni védelem:	van	N/A	van	van	RSA-2048	„16k authentication"	van	van
P2P SMS és adatátvitel:	van	nincs	van	nincs	van	N/A	nincs	N/A
Konferenciahívás:	csak szerveren	nincs	csak szerveren	nincs	P2P	nincs	csak szerveren	nincs
Jelenlét információ:	van	N/A	nincs	nincs	van	nincs	nincs	van

[29] Tökéletes titkosság. Azon törekvés jele, hogy a titkosítási megoldásokban elvi (azaz tökéletes) fejthetetlenséget eredményező eljárásokat is alkalmazzanak. Ezek legismertebbje az OTP (One Time Pad), ami egy olyan egyszer használatos kulcs, amelynek hossza megegyezik a titkosítandó objektuméval, ami most a példa okán legyen egy egyszerű szöveg. Ha valaki mindenféle szofisztikált feltörési módszert mellőzve a nyers erőt (brute force) alkalmazva az adott hosszúságú összes létező karakterláncot ráilleszti a titkosított szövegre, azt fogja tapasztalni, hogy megszámlálhatatlanul véges számú értelmes szöveg keletkezik, amelyek közül még mindig ki kellene választania az eredetit, ami nyilvánvaló lehetetlenség.

Termék:	Silentel 5.2	Phanton 3	CellCrypt Mobile	Zybex Secure Phone	CryptTalk	Gold Lock 3G	Silent Voice	Secfone
Videohívás:	nincs	nincs	nincs	nincs	nincs	nincs	van	nincs
Hangminőség:	GSM	GSM	GSM	GSM	HD	ismerten rossz	HD	GSM
P2P SMS és adatátvitel:	van	nincs	van	nincs	van	N/A	nincs	N/A
Konferenciahívás:	csak szerveren	nincs	csak szerveren	nincs	P2P	nincs	csak szerveren	nincs
Jelenlét információ:	van	N/A	nincs	nincs	van	nincs	nincs	van
Videohívás:	nincs	nincs	nincs	nincs	nincs	nincs	van	nincs
Hangminőség:	GSM	GSM	GSM	GSM	HD	ismerten rossz	HD	GSM
MDM támogatás:	nincs	nincs	nincs	nincs	van	nincs	limitált	nincs
Szerverkihelyezés:	van	N/A	limitált	nincs	van	van	nincs	van
Lopásvédelem:	van	nincs	van	van	van	nincs	van	nincs
Hardveres kiegészítő:	opcionális	SD-kártya	nincs	nincs	nincs	nincs	nincs	SD-kártya

Termék:	Silentel 5.2	Phanton 3	CellCrypt Mobile	Zybex Secure Phone	CryptTalk	Gold Lock 3G	Silent Voice	Secfone
Felhasználói menedzsment:	van	N/A	nincs	van	van	nincs	limitált	nincs
Támogatott platformok:	IOS, Android, Blackberry, Windows Phone és Desktop OS	Android	IOS, Android, Blackberry	Android	IOS (de áthelyezhető bármilyen platformra	IOS (Android, Blackberry limitált)	IOS, Android, Desktop OS	Android, Blackberry
Alternatív kripto-mód (igény szerint):	nincs	nincs	nincs	nincs	van	nincs	nincs	nincs
Audit:	NATO, NSASR	NATO, NLNCSA	FIPS 140-2	FIPS 140-2	Deloit, Silent Signal, stb. + white box lehetőség	Israeli Ministry of Defense	nincs	nincs
Legolcsóbb változat egy készülékes havidíja:*	18.600	N/A	52.000	12.400	20.100	21.700	49.600	17.000 + egyszeri díj
A legolcsóbb változatban elérhető szolgáltatások:	csak beszéd	beszéd, SMS	csak beszéd	beszéd, SMS	beszéd, SMS, file-átvitel, konferenciahívás	beszéd, SMS	csak beszéd	beszéd, SMS

* Az árak a tanulmány írásakor aktuális euró és dollár árfolyamon számított közelítő bruttó árak. A legtöbb cég a vásárolt mennyiség függvényében további jelentős kedvezményeket ad, míg bizonyos mennyiség felett az ár teljes egészében tárgyalás alapját képezi.

Felhasznált irodalom

[1.] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[2.] Agar, Jon, Constant Touch: A Global History of the Mobile Phone, 2004 ISBN 1-84046-541-7

[3.] Katz, James E. & Aakhus, Mark, eds. Perpetual Contact: Mobile Communication, Private Talk, Public Performance, 2002

[4.] www.biztonsagostelefon.hu

[5.] www.silentel.com

[6.] LG Secret Official Website

[7.] www.sectra.com

[8.] LG Secret KF750 - review, price, specification - Cell phone

[9.] www.cellcrypt.com

[10.] http://hu.samsungmobile.com/mobile/SamsungWAVE/spec

[11.] www.CryptTalk.com

[12.] www.gold-lock.com

[13.] www.silentcircle.com

[14.] http://www.ia.nato.int/niapc

A cikket lektorálta:

Dr. Kassai Károly ezredes

Ternyák István nyugállományú ezredes

Komáromi Zsolt alezredes