Teréki Csaba

MOBIL HÍRKÖZLÉSI RENDSZEREK III.

A GSM VÉDELMI RENDSZERÉNEK FELÉPÍTÉSE ÉS MŰKÖDÉSE

A GSM felajánl olyan, a felépítésébe ágyazott jellemzőket, amelyek biztosítják a hívás integritását és bizalmasságát.

— a *hitelesítés* a hívás érvényességének ellenőrzésére szolgál; ezen kívül megakadályozza a más előfizetői néven bejelentkező felhasználó működését. Ez az előfizetői kártya bevezetésével érhető el (SIM[1]). A kártya csak a személyi azonosító szám (PIN[2]) használatával működik, amely kellő biztonságot nyújt a kártya ellopása esetén is. Lopott kártya használatának esetén a szolgáltató azonnal letilthatja a szolgáltatást;

— a *titkosítás* teljes bizalmasságot biztosít a hívásnak, hogy csak a hívásban résztvevő másik fél tudja azonosítani a hívót, míg beszélgetésük teljes mértékben titkosított;

— minden egyes mozgó állomás visel egy sorozatszámot (IMEI[3]), amely alapján bizonyos hálózatok ellenőrizhetik a lopott készülékeket. Ha lopott készülékről van szó, a hívást le lehet tiltani, vagy más intézkedést lehet életbe léptetni.

Az eljárások során a GSM különböző azonosítókat használ a folyamatok adminisztrálásához. Ebben a fejezetben használt azonosítók jelentését az alábbiakban ismertetjük:

Nemzetközi mobil-előfizetői azonosító

A nemzetközi mobil-előfizetői azonosító[4] egy GSM előfizetőt egyértelműen azonosít a teljes GSM hálózatban. A GSM ajánlása szerint az IMSI hossza max. 15 digit lehet. Minden hálózaton belüli jelzés, mely az előfizetővel kapcsolatos az IMSI alapján történik.

A nemzetközi mobil-előfizetői azonosító a SIM kártyán van tárolva, és a honos helyzet-regiszterben (HLR[5]) és a látogató helyzet-regiszterben (VLR[6]) talál-

[1] Subscriber Identity Module (SIM) — előfizető azonosító modul.
[2] Personal Identity Number (PIN) — személyi azonosító szám.
[3] International Mobile Equipment Identity (IMEI) — nemzetközi mobil-készülék azonosító.
[4] International Mobile Subscriber Identity (IMSI) — nemzetközi mobil-előfizetői azonosító.
[5] Home Location Register (HLR) — honos helyzet-regiszter.
[6] Visitor Location Register (VLR) — látogató helyzet-regiszter.

ható előfizetői információkhoz is a nemzetközi mobil-előfizetői azonosító azonosság alapján lehet hozzáférni.

$$IMSI = MCC + MNC + MSIN$$

ahol: MCC — mobil országkód[7], 3 digit;
MNC — mobilhálózat kód[8], 2 digit;
MSIN — mobil-előfizetői azonosító szám[9], max. 10 digit.

Ideiglenes mobil-előfizetői azonosság[10]

A hálózaton belüli ideiglenes előfizetői azonosságot biztosítja. Mivel az ideiglenes mobil-előfizetői azonosság csak helyileg fontos, a rendszer a mobil minden bejelentkezése alkalmával változtatja az ideiglenes mobil-előfizetői azonosságát, biztosítva ezzel egyfajta védelmet. Az azonosító szám hossza és felépítése a nyilvános földi mobil hálózat (PLMN[11]) üzemeltető által meghatározott, de hossza nem lehet nagyobb 4 oktettnél (32 bit).

Nemzetközi mobilállomás azonosító[12]

Ezt az azonosítót a mobilkészülék azonosítására alkalmazzák. Egy IMEI szám pontosan meghatároz egy mobil állomást, mint készüléket.

$$IMEI = TAC + FAC + SNR + sp$$

ahol:

TAC — típus-jóváhagyás kód[13], egy központi GSM testület által jóváhagyott kód, 6 digit;
FAC — készletkód[14], azonosítja a gyártót, 2 digit;
SNR — sorozatszám[15], pontosan azonosít minden készüléket minden típus-jóváhagyás kódon és készletkódon belül, 6 digit;
Sp — tartalék[16] későbbi használatra, 1 digit.

[7] Mobile Country Code (MCC) — mobil országkód.
[8] Mobile Network Code (MNC) — mobilhálózat kód.
[9] Mobile Subscriber Identification Number (MSIN) — mobil-előfizetői azonosító szám.
[10] Temporary Mobile Subscriber identity (TMSI) — ideiglenes mobil-előfizetői azonosság.
[11] Public Land Mobile Network (PLMN) — nyilvános földi mobilhálózat.
[12] International Mobile station Equipment Identity — nemzetközi mobilállomás azonosító.
[13] Type Approval Code (TAC) — típus-jóváhagyás kód.
[14] Final Assembly Code (FAC) — készletkód.
[15] Serial Number (SNR) — sorozatszám.
[16] spare (sp) — tartalék.

Lokációs körzetazonosító szám[17]

A lokációs körzetazonosító szám a mobil-előfizetők helyzetének azonosítására használják a GSM-en belül. Minden előfizetőt lényegében a lokációs körzetazonosító szám alapján lehet megtalálni a rendszerben.

$$LAI = MCC + MNC + LAC$$

ahol:

MCC — mobil országkód, azonosítja az országot ugyanazzal a 3 digittel, mint a nemzetközi mobil-előfizetői azonosítóban;

MNC — mobilhálózat kódja, azonosítja a GSM nyilvános földi mobil hálózatot az adott országban, és ugyanaz az értéke, mint az mobilhálózat kódnak a nemzetközi mobil-előfizetői azonosítóban, 2 digit;

LAC — lokációs körzet kódja[18] azonosít egy-egy körzetet[19] a GSM nyilvános földi mobil hálózatán belül. Maximális hossza 16 bit, így egy GSM nyilvános földi mobil hálózaton belül összesen 65 536 különböző körzet azonosítható.

Figyelembe véve a rendszer részeit, a következő eljárásokat alkalmazzák biztonsági szempontból:

— a hálózathoz vezető út → autentikáció;
— a rádiós rész → titkosítás;
— a mobilkészülék → készülékazonosítás;
— a nemzetközi mobil-előfizetői azonosító → ideiglenes azonosság.

A rejtjelezésben résztvevő főbb funkcionális elemek:

— mobilállomás[20];
— bázisállomás[21], amely egy speciális digitális adó-vevő a mobilállomás és a mobil szolgálati kapcsolóközpont[22] között;
— a mobil szolgálati kapcsolóközpont legfontosabb részei a hitelesítő központ[23], a honos helyzet-regiszter és a látogató helyzet-regiszter.

[17] Location Area Identity (LAI) — lokációs körzetazonosító szám.
[18] Location Area Code (LAC) — lokációs körzet kódja.
[19] Location Area (LA) — lokációs körzet.
[20] Mobile Station (MS) — mobilállomás.
[21] Base Station (BTS) — bázisállomás.
[22] Mobile Services Switching Centre (MSC) — Mobil szolgálati kapcsolóközpont.
[23] Authentication Centre (AUC) — hitelesítő központ.

Hitelesítő eljárás

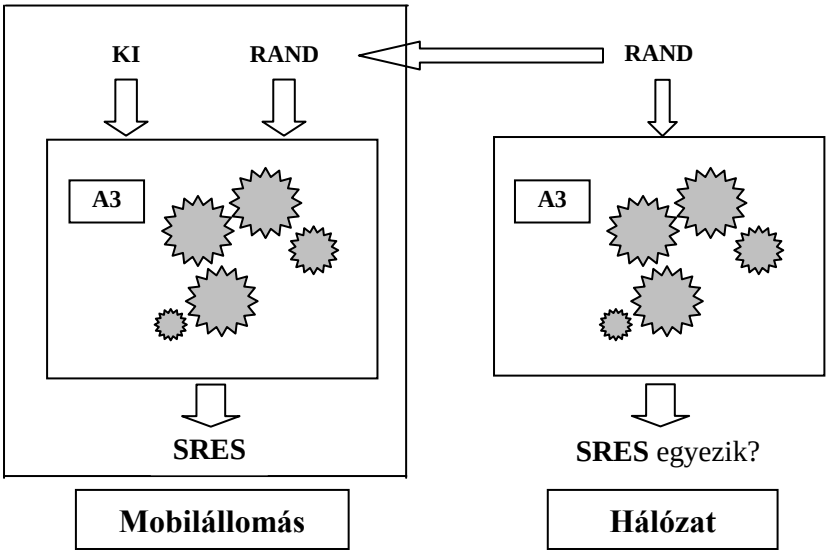
Az *autentikáció definíciója*: az előfizetői azonosság hitelességvizsgálata, amely az előfizetői azonosságot (IMSI) érvényesíti. Az előfizetői azonosság az azonosítási eljáráson belül kerül átadásra a mobilállomás által és csak egyszer igényelt.

A hitelesítés *szándéka*, hogy megvédje a hálózatot a jogosulatlan használattal szemben. Védelmet nyújt a GSM nyilvános földi mobil hálózat előfizetőinek is azáltal, hogy kiszűri a jogosult felhasználók esetleges megszemélyesítési kísérleteit.

Hitelesítést alkalmaz a GSM minden bejelentkezéskor, minden hívás kezdeményezésekor és fogadásakor, helyzet korszerűsítésekor és kiegészítő szolgáltatások indítása, megállítása, felvétele vagy törlése előtt.

A hitelesítő központ (AUC[24]) és a hitelesítés általánosságban hivatott védeni a GSM rendszert a jogosulatlan felhasználóktól. A hitelesítő központ létrehozza az hitelesítéshez és a titkosításhoz használt számhármast *(triplet*-et). Egy triplet egy *véletlen számból (RAND)*, egy *titkosítási kulcsból (Kc)* és egy hitelesítési *válaszból (SRES)* áll.

A hitelesítő központ kiszámítja a SRES értékét az A3 algoritmust felhasználva, melynek bemenő paraméterei az *előfizető különleges 128 bites kulcsa (KI)* és egy szintén 128 bit hosszúságú *véletlen szám*. Ugyanezen bemenő paraméterek kerülnek felhasználásra az A8 algoritmusban is, melynek eredménye a *titkosítási kulcs*. A véletlen számot a hitelesítő központ állítja elő, a KI pedig az előfizető felvételekor kerül a hitelesítő központ adatbankjába.

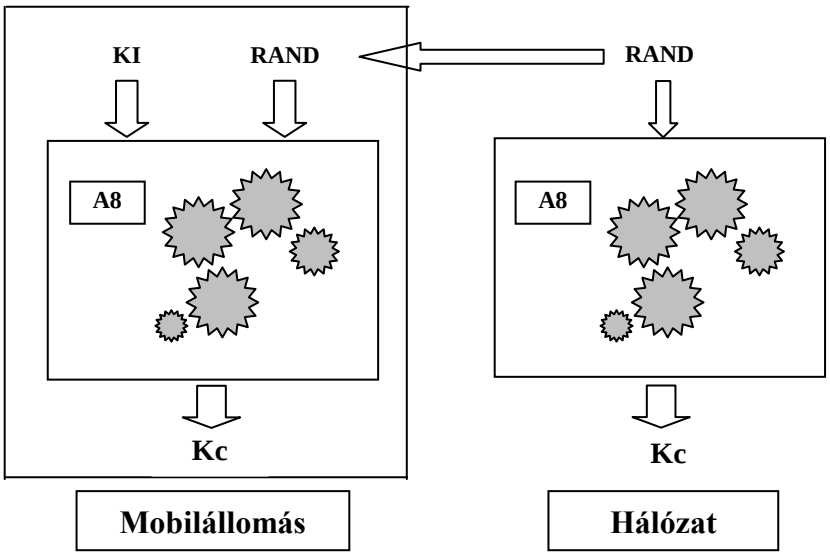


1. ábra. A SRES előállítása

[24] Authentication Centre (AUC) — hitelesítő központ.

Az ily módon előállított triplet-et a hitelesítő központ elküldi a HLR-nek későbbi felhasználásra. Tíz triplet-et tárolnak egyszerre az előfizető nemzetközi mobil-előfizetői azonosítójával és az ideiglenes mobil-előfizetői azonosítójával együtt, tehát első nekifutásra a hitelesítő központ tízszer hajtja végre ezt a folyamatot. A látogató helyzetregiszter használja a triplet-eket, amint szükséges a hitelesítési eljárás indítása.

Az előfizető bejelentkezésekor a következő rendelkezésre álló előfizetői triplet-et a hitelesítő központ elküldi a HLR-ből a VLR-be. A RAND értékét ezután megkapja a mobilállomás. A VLR egy hitelesítési *kérést* küld a mobilállomás felé. Ezen üzenet paraméterei: a 128 bites *véletlen szám* (RAND) és a 3 bites *titkosítási kulcs sorozatszáma* (CKSN[25]). Amikor a mobilállomás veszi a hitelesítési kérést, eltárolja a titkosítási kulcs sorszámát, amelyet később visszaküld, pl. egy kiszolgáláskéréskor. Azután kiszámítja a hitelesítési *paramétert* (SRES-t) az A3 algoritmussal, a SIM-en tárolt *előfizetői kulcs* (KI) és a kapott véletlen szám alapján. A SRES visszajut az MSC/VLR-be az hitelesítési *válaszban*. Az MSC összehasonlítja a hitelesítő központ által előállított SRES-t a mobilállomás által küldöttel. Ha egyeznek, akkor a mobilállomás megfelelt a hitelesítési eljárásnak.



2. ábra. A titkosítási kulcs előállítása

Ha a hitelesítés nem sikerül, az nem mást jelent, mint hogy a mobilból származó SRES nem egyezik az MSC/VLR-ben tárolt értékkel. A hálózat különbséget tesz két, a mobilállomás azonosítására használt út között:

— TMSI volt használva;
— IMSI volt használva.

[25] Ciphering Key Sequence Number (CKSN) — titkosítási kulcs sorozatszám.

Ha TMSI volt, a hálózat elindíthatja az azonosító eljárást, amelyben a mobilállomásnak fel kell küldenie a rendszerbe az IMSI-jét. Ezután, ha a mobiltól kapott IMSI eltér attól, amelyet a hálózat tárol, a hitelesítés újra indul helyes paraméterekkel. Ha a kapott IMSI egyezik a tároltak egyikével, az MSC a továbbiakban leírtak szerint halad.

Ha IMSI volt használva, vagy a hálózat úgy dönt, hogy nincs szükség azonosítási eljárásra, akkor az MSC egy hitelesítés-*visszautasítás* üzenetet küld a mobilkészüléknek. A továbbiakban minden kapcsolat megszakad. A mobil készülék — véve a hitelesítés-visszautasítás üzenetet — törli SIM-jéről az ideiglenes mobil-előfizetői azonosítót, a lokációs körzetazonosító számot, a titkosítási kulcsot, a titkosítási kulcs sorszámát és a továbbiakban csak segélyhívásokat tesz lehetővé.

Ez egy nagyon komoly eset, mivel a SIM kártya letiltását jelenti. Hogy ezt megakadályozza a bit- vagy szoftverhiba miatt történtektől, a CME 201 rendszer rendelkezik egy cserélhető paraméterrel a sikertelen hitelesítés irányítására. Ha ez a paraméter be van állítva, akkor az MSC nem fog küldeni hitelesítés-visszautasítást, helyette azonban visszautasítja a mobil belépését a rendszerbe, a következő négy üzenetet küldve a kiváltó okoktól függően:

— az IMSI ismeretlen a VLR-ben (mobil által kezdeményezett hívás);
— nincs üzenet, csak szétkapcsolás (mobil által befejezett hívás);
— a PLMN nincs engedélyezve (helyzet korszerűstés)
— az IMSI ismeretlen a VLR-ben (kiegészítő szolgáltatásokat vezérlő műveletek)

A mechanizmus biztonsága a *KI*-n alapszik, így ez a legvédettebb. A rendszer különféle megfontolásoknak tesz eleget. A SRES előállítása nagyon könnyű és gyors, viszont maga a SRES és a RAND annyira komplex, amennyire csak lehetséges, nehogy vissza lehessen kapni a KI-t. A KI bármi lehet, így maximális az operátor flexibilitása. Az A3 titkos és egységes, ezzel lehetővé teszi a nemzetközi bolyongást.

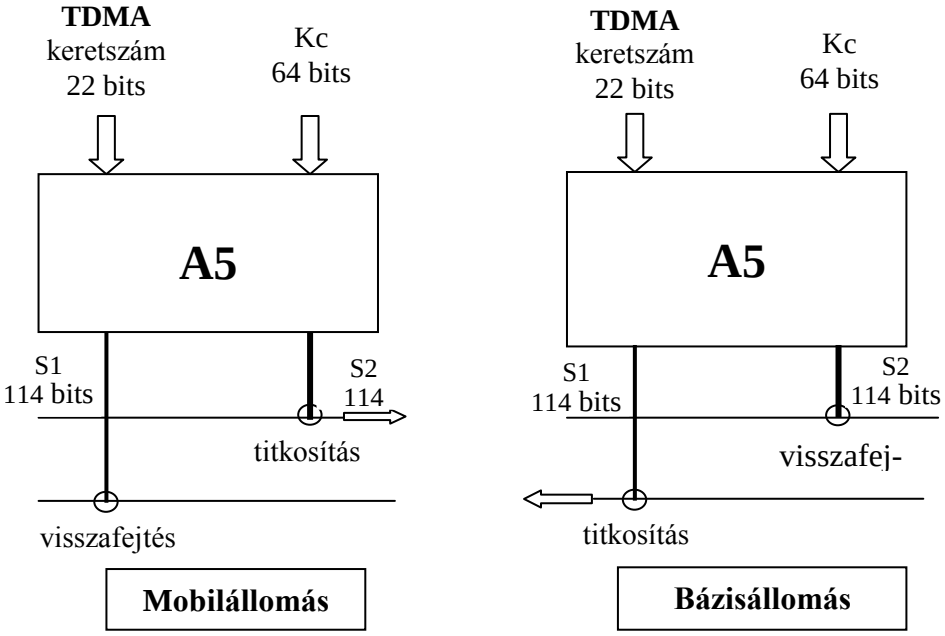
Titkosítás, biztonság a rádiós részben

A titkosság a fizikai rádiócsatornán azt jelenti, hogy a bázis adóvevő állomás[26] és a mobilállomás között lezajló információ és jelzés nem áll a jogosulatlan személyek rendelkezésére. Szándéka, hogy biztosítsa a felhasználói információ titkosítását. Minden beszélgetés és adat titkosított, és minden velük társuló jelzés-információ védett.

Ha a hitelesítés sikeresen lezajlott, a titkosítási eljárás elindulhat az MSC/VLR által, amely ekkor küldi a mobilállomás felé a titkosítási mód parancs[27] üzenetet. Ez egy Kc-ből álló üzenet, amelyet természetesen a bázis adóvevő állomás kap meg.

[26] Base Transceiver Station (BTS) — bázis adóvevő állomás.
[27] Ciphering Mode Command — titkosítási mód parancs.

A bázisállomás tárolja a titkosítási kulcsot és megmondja a mobilállomásnak, hogy indítsa a titkosítást. A bázis adóvevő állomás indítja a visszafejtést. A titkosítási mód parancsa a bázisállomásból a mobilállomásba nincs titkosítva. A mobilállomás az A8 algoritmust használva kiszámítja a titkosítási kulcsot a Ki-ből és a véletlen számból, amely a hitelesítés kérés üzenetben érkezett. Ez a titkosítási kulcs és az idő szerinti hozzáférés[28] (TDMA-keret) sorszáma mind a mobilállomás, mind pedig a bázisállomás részéről ismert. Ezt a két bemenő értéket használja az A5, előállítva egy titkosított keretsorszámot. Minden felhasználói bit XOR kapuk bemeneteire kerül, a titkosított sorszám egy bitjével előállítva a titkosított adatot. A vevőállomáson ugyanaz a titkosított sorszám kerül a titkosított adattal a XOR kapukra az adat visszafejtésekor.



3. ábra. A titkosítási folyamat

Egy biztonsági előnye van ennek a titkosítási metódusnak: a titkosítási kulcs minden hívás alkalmával cserélődik, és a rádiós átvitelben se nyíltan, se titkosítva nem szerepel.

Az A3 és A8 algoritmusok titkosak, és csak az egyetértési nyilatkozatot[29] aláírt tagoknak áll rendelkezésükre. Ráadásul az eredeti A5 algoritmus, amely csak

[28] Time Division Multiple Access (TDMA) — idő szerinti hozzáférés.

[29] Memorandum of Understanding (MoU) — egyetértési nyilatkozat, amelyet 1987 szeptemberében 13 ország írt alá, s amelynek értelmében elhatározás született az új összeurópai digitális rendszer bevezetésére.

az európai távközlési szabványosítási intézethez[30] tartozó országokban levő GSM-vezérlők rendelkezésére áll, általában nem hozzáférhető az Európai Közösség országain kívüli országokban. Kétféle A5 van:

— az A5/1, amely az ETSI tagoknak és Magyarországnak is;
— az A5/2, amely nem ETSI tagoknak.

A titkosítási kulcs sorozatszám a következő módon használatos: az MSC/VLR-ből küldött hitelesítés-kérés a véletlen számból és a titkosítási kulcs sorozatszámból állt. A titkosítási kulcs sorozatszám a látogató helyzet regiszterben a titkosítási kulccsal együtt van eltárolva, amely a véletlen számból lett kiszámítva. Amikor a mobilállomás veszi az hitelesítés-kérést, kiszámítja a SRES-t valamint a titkosítási kulcsot, és a titkosítási kulcsot a titkosítási kulcs sorozatszámmal együtt a SIM-en tárolja.

A következőkben a mobilállomás be akar lépni a rendszerbe, ezért felküldi a titkosítási kulcs sorozatszámát egy kiszolgáláskérés üzenetben. Így a mobilszolgálati kapcsolóközpont tudja, melyik titkosítási kulcs van tárolva a mobilban, és nem kell elküldenie a véletlen számból álló hitelesítés-kérést. Helyette a mobilszolgálati kapcsolóközpont egyenesen a titkosítási eljárást indítja.

Egy titkosított üzenet leghatékonyabb feltörési metódusa az, amikor minden lehetséges kulcsot megkeresünk. Az 1. táblázat mutatja, hogy mennyi időt vesz igénybe egy üzenet visszafejtése adott kulcshossz esetén, ha egy olyan számítógépet használunk feltörésre, amely másodpercenként 1 millió titkosítást képes végrehajtani.

Feltörési idők változó kulcshossz esetén 1. táblázat

Kulcshossz bitekben:	32	40	56	64	128
Összes lehetséges kulcs teszteléséhez szükséges idő:	1,19 óra	12,7 nap	2,291 év	584,542 év	$10{,}8\times10^{24}$ év

128 bites kulcs esetében a szükséges idő extrém nagy; összehasonlítási alapul szolgál az Univerzum életkora, amelyről úgy tudják, $1{,}6\times10^{10}$ év. 128 bites kulcsot használó algoritmusra egy példa[31]. Egy üzenet adott időtartamon belüli visszafejlesztéséhez meghatározott számú feltörő gép szükséges a kulcshossztól függően (2. táblázat).

A szükséges gépek száma 2. táblázat

Kulcshossz bitekben	1 nap	1 hét	1 év
40	13	2	–
56	836,788	119,132	2,291
64	$2{,}14\times10^{8}$	$3{,}04\times10^{6}$	584,542
128	$3{,}9\times10^{27}$	$5{,}6\times10^{26}$	$10{,}8\times10^{24}$

[30] European Telecommunications Standardisation Institute (ETSI) — európai távközlési szabványosítási intézet.

[31] International Data Encryption Algorithm (IDEA) — nemzetközi adat algoritmus.

A mai számítógépek lehetővé teszik, hogy másodpercenként 1 millió kulcsot tudjunk tesztelni. Egy titkosító algoritmus erősségének meghatározásakor a védendő információ értékét is figyelembe kell venni. A GSM-ben használatos 128 bites titkosítási kulcs minden beszélgetés alkalmával cserélődik, ezért kellő biztonságot nyújt felhasználójának.

Készülékazonosítás

A készülék azonosítása a nemzetközi mobilkészülék azonosító adminisztrációjának használatával történik, amely lehetővé teszi a rendszer számára, hogy ellenőrizhesse a mobilkészülékek azonosságát (pl. feljelentkezéskor). A szándék a lopott vagy jogosulatlan készülékek kiszűrése a rendszerből. Azt, hogy kell-e készülék-azonosítás vagy sem a rendszer dönti el, a GSM javasolja minden hívás beállításakor.

A mobilkészülékek azonosító adatait a készülékazonosító regiszter[32] tárolja. A készülékazonosító regiszter egy funkcionális adatbázis, amely biztosítja a nyilvános földi mobil hálózat vezérlőnek a lehetőséget, hogy letilthassa a lopott mobilkészülékeket, vagy azt a mobilkészüléket, amely nem felel meg az üzemeltetési követelményeknek (nincs jóváhagyva vagy hibás). Minden egyes GSM mobilkészülék rendelkezik egy egyedülálló nemzetközi mobilkészülék azonosítóval, amelyet a készülék gyártója jelöl ki. A készülékazonosító regiszter a nemzetközi mobilkészülék azonosítót a mobilkészülékek osztályozására használja. Eszerint léteznek fehér-, szürke-, ill. feketelistás készülékek:

— *fehér lista* minden résztvevő GSM ország nemzetközi mobilkészülék azonosító számának listája. A lista csak a típusengedélyezési kód[33] 6 digitjét tartalmazza. Ez csökkenti a készülékazonosító regiszter adatbázis-tárolási követelményeit;
— *szürke lista* azok a jóváhagyott készülékek, amelyek nem működnek helyesen;
— *fekete lista* a lopott készülékek teljes nemzetközi mobilkészülék azonosítóját tartalmazza.

A készülékazonosító regiszter elérhető a hívásfelépítés[34] vagy a helyzet korszerűsítés alatt, ekkor a mobilállomás nemzetközi mobilkészülék azonosítója át van utalva a három listának. Először összeveti a fekete listával, és ha a nemzetközi mobilkészülék azonosító fekete listán van, a hívás le lesz tiltva. A lopott készüléket használó személy nemzetközi mobil-előfizetői azonosítója kimutatható, így megkönnyíti a további teendőket. Azután a szürke listával hasonlítja össze. Ha a nemzetközi mobilkészülék azonosító szürke listás, az operátor választhat: vagy megtagadja az elérést, vagy megengedi és feljegyzi az előfizető nemzetközi mo-

[32] Equipment Identity Register (EIR) — készülékazonosító regiszter.
[33] Type Approval Code (TAC) — típusengedélyezési kód.
[34] Call Setup — hívásfelépítés.

bil-előfizetői azonosítóját. Végső esetben a rendszer az üzemeltetési és fenntartási központon[35] keresztül jelenti le a nemzetközi mobilkészülék azonosítót és a nemzetközi mobil-előfizetői azonosítót. A nyilvános földi mobil hálózat operátor elindíthatja a proaktív korrekciós kezelési eljárásokat azáltal, hogy kapcsolatba lép a szürke listás készüléket használó előfizetővel. Ha a nemzetközi mobilkészülék azonosító nincs a fekete vagy a szürke listán, akkor összeveti a fehér listával, és engedélyezi a hívást.

A rejtett előfizetői azonosság

A rejtett előfizetői azonosság azt jelenti, hogy a nemzetközi mobil-előfizetői azonosító nem áll rendelkezésre, illetve el van zárva a jogosulatlan egyének és eljárások elől. Ez megvédi az előfizetők rejtett azonosságát, akik a GSM nyilvános földi mobil hálózati erőforrásokat használják. Megakadályozza, hogy rádiós jelzések megfigyelésével ki lehessen nyomozni egy mobil-előfizető tartózkodási helyét.

Az eljárás a következő: a mobilállomás minden pillanatban kérhet egy rendszerfolyamatot (pl. helyzet-korszerűsítés, híváskezdeményezés vagy kiszolgáláskérés). Az MSC/VLR kiutal a nemzetközi mobil-előfizetői azonosító helyett egy új ideiglenes mobil-előfizetői azonosítót és továbbítja a mobilállomásba azzal az utasítással, hogy ő is utalja ki a nemzetközi mobil-előfizetői azonosító helyett az ideiglenes mobil-előfizetői azonosítót. A mobilállomás a SIM-en tárolja az ideiglenes mobil-előfizetői azonosítót. Innentől kezdve az MSC/VLR és a mobilállomás közti jelzésátvitel csak az ideiglenes mobil-előfizetői azonosító használatával működik, így a valóságos előfizetői azonosság nincs újra átküldve a rádiós részen. Amint a nemzetközi mobil-előfizetői azonosító be van kérve a rádiós részen keresztül, a nemzetközi mobil-előfizetői azonosítót az ideiglenes mobil-előfizetői azonosítóra cserélik. A rendszer csak akkor hivatkozik a nemzetközi mobil-előfizetői azonosítóra, amikor elégtelen a helyzet korszerűsítés vagy amikor a mobilállomás számára nincs rendelkezésre álló ideiglenes mobil-előfizetői azonosító.

FELHASZNÁLT IRODALOM

[1] Géher Károly: Híradástechnika. Műszaki könyvkiadó, Budapest, 1993.
[2] Buzás Ottó: Telefon kultúra. Műszaki könyvkiadó, Budapest, 1995.

[35] Operation and Maintenance Centre (OMC) — üzemeltetési és fenntartási központ.