Kiber Pajzs

2025.02.19,
HTE előadás

Készítette: Fodor Attila

Yettel.

Témák

- Kibertámadási technikák
- Spoofing (Caller ID és SMS)
- Szakpolitikai dokumentum, szabályozás
- Érintett távközlési szolgáltatók
- Caller ID spoofing (CLI hamisítás):
  - CLI módosítási helyek
  - STIR/SHAKEN
  - Szakpolitikai dokumentumban rögzített megállapodások
  - Tervezett architektúra, operátorok közötti együttműködés
  - Mobil előfizető státuszának meghatározása
  - Átirányított hívások kezelése
  - Híváskezelési folyamatábra
  - CLI tiltás hatása a nem EU-s hívásfogadásra
- SMS spoofing:
  - SMS küldési lehetőségek mobil hálózatokon
  - SMS Home Routing
  - Leggyakoribb visszaélések SMS küldés esetében
  - SMS tartalom szűrés műszaki szemmel
- Nemzetközi példák

Kibertámadási technikák

A kibertámadás olyan rosszindulatú tevékenység, amelynek célja a hálózatok, eszközök, rendszerek vagy az azokon tárolt és továbbított adatok megsértése, manipulálása, megsemmisítése, illetéktelen hozzáférése, vagy a felhasználók megtévesztése és a megszerzett adatok rosszindulatú célokra való felhasználása.

Social Engineering (Társadalmi manipuláció)

- Phising (Adathalászat)
- Vishing, Smishing
- Tailgating (Hátulról belépés)
- Pretexting
- Baiting

Malware (Kártékony szoftverek)

- Zsarolóvírus
- Trójai program
- Kémprogram
- Reklámprogram
- Féregvírus

Network Attacks (Hálózati támadások)

- Man-in-the-Middle (MitM) támadás
- DNS Spoofing (DNS-mérgezés)
- Session Hijacking
- Packet Sniffing (Csomagelemzés)
- Port Scanning (Portszkennelés)

Denial of Service

- DoS (Denial of Service)
- DDoS (Distributed Denial of Service)
- SYN Flood
- HTTP Flood
- Amplification Attacks (Erősített támadások)

Spoofing

- **Caller ID spoofing**
- **SMS spoofing**
- E-mail Spoofing
- IP Spoofing, MAC Spoofing

Sérülékenységi támadások

- Zero-Day Exploit
- SQL Injection (SQL-befecskendezés)
- Cross-Site Scripting (XSS)
- Buffer Overflow (Puffer túlcsordulás)

IoT és OT támadások

- Botnetek
- SCADA és ICS támadások
- Firmware Exploit

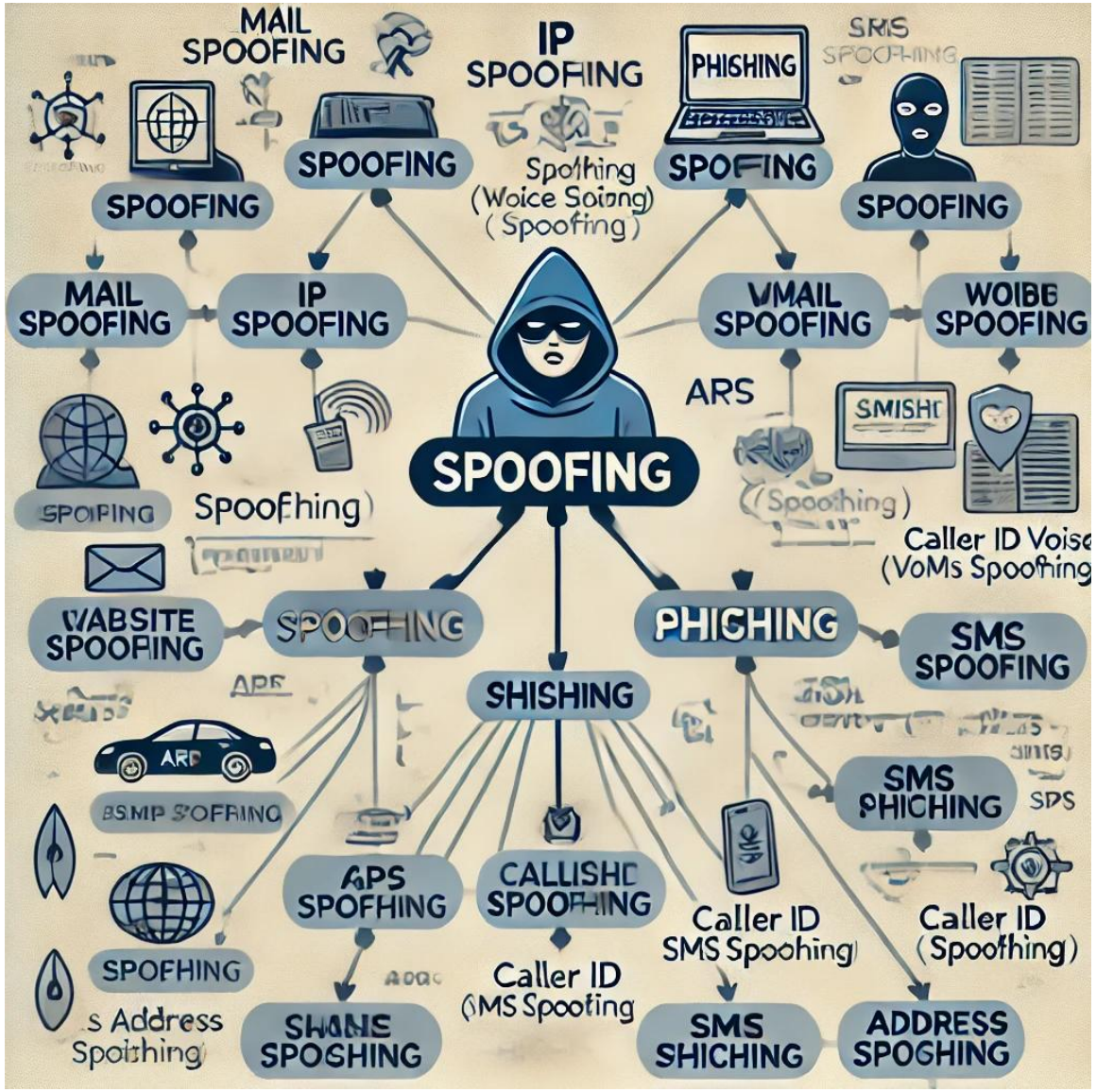
Adatlopás és identitáslopás

- Credential Stuffing
- Brute Force (Nyers erő támadás)
- Keylogging
- Rogue Access Point (Rogue AP)

Spoofing

A spoofing egy olyan támadási módszer, amelyben a támadó egy másik személy, szervezet vagy eszköz nevében lép fel, hogy megtévesztése az áldozatát és bizalmas adatokat szerezzen vagy hozzáférést nyerjen valamilyen rendszerhez. A spoofing célja az áldozat megtévesztése, hogy úgy vélekedjen, hogy egy megbízható forrástól származó üzenetet, hívást vagy kérést kap.

- **Caller ID spoofing:** kifejezés kifejezetten a telefonhívásokkal kapcsolatos hamisítást jelöli, amikor a támadó a hívásazonosítót (Caller ID) manipulálja, hogy egy másik telefonszámnak tűnjön, mint amiről valójában a hívás érkezik.
- **SMS spoofing:** Ha az SMS feladót manipulálják, azt SMS spoofing-nak vagy egyszerűen SMS hamisításnak nevezik. Ebben az esetben a támadó hamis feladói számot állít be az SMS-ben, hogy úgy tűnjön, mintha egy másik, megbízható forrástól érkezett volna az üzenet, például egy banktól vagy egy hivatalos intézménytől.



Szakpolitikai dokumentum, szabályozás

A szolgáltatói fellépés célja

A szolgáltatói fellépés célja az elektronikus hírközlési szolgáltatók által alkalmazandó műszaki és egyéb intézkedések bevezetésével **a magyarországi hírközlő hálózatokban a hazai hívószám (A-szám) hamisításával elkövetett csalások jelentős visszaszorítása, ezzel a hazai hívószámokba vetett előfizetői bizalom helyreállítása.** Ennek érdekében az elektronikus hírközlési szolgáltatóknak ki kell építeniük és meghatározott keretek között együttműködve üzemeltetniük kell egy olyan rendszert, amely minél nagyobb százalékban képes nemzetközi irányból bejövő hanghívás esetében a hamisított A-számmal érkező hívások felépítését megakadályozni.

Jogi háttér

„12. § Az Eht. „Vegyes rendelkezések” alcíme a következő 163/R. §-sal egészül ki: „163/R. § E törvénynek az online csalások elleni további hatékony fellépés érdekében szükséges és egyéb törvények módosításáról szóló 2024. évi LXIV. törvénnyel megállapított 91/B. §-át a **nemzeti számozási tervben meghatározott földrajzi és a rövid számokat hívóazonosítóként használó hívások tekintetében 2025. október 15-től, a mobilszámokat hívóazonosítóként használó hívások tekintetében 2026. június 1-jétől kell alkalmazni.”**

Szakpolitikai dokumentum

Javaslat a magyarországi hívószámok hamisításával elkövetett csalások ellen szükséges elektronikus hírközlési szolgáltatói fellépésről.

- Első fázis: Caller ID spoofing – Hívószám hamisítás
- Második fázis: SMS spoofing – SMS feladó hamisítás (hivatalosan még nem indult el)

Érintett távközlési szolgáltatók

Forgalom típusa szerint	Hálózati típus szerint	Forgalom szintje szerint	Forgalom iránya szerint
Hanghívás szolgáltatók	**Mobil szolgáltatók**	**Végfelhasználói szolgáltatók**	Belföldi kimenő
Üzenetküldési szolgáltatók	**Vezetékes szolgáltatók**	**Nagykereskedelmi szolgáltatók**	Nemzetközi kimenő
Internetszolgáltatók	**VoIP és felhőalapú szolgáltatók**	**Gerinchálózati és tranzitszolgáltatók**	Belföldi bejövő
TV és média szolgáltatók	**Tranzit szolgáltatók**	Hálózatinfrastruktúra-szolgáltatók	**Nemzetközi bejövő**
Adatátviteli szolgáltatók	Műholdas szolgáltatók	Speciális és kormányzati hálózatok	

- **Érintett szolgáltató:** Az a nyilvánosan elérhető telefonszolgáltatást nyújtó szolgáltató, aki *nemzetközi irányból bejövő hívás*t közvetlenül végződtet vagy tranzitál Magyarországon.
- **Bekérdező szolgáltató:** Az érintett szolgáltató, aki megkérdezi az A-szám honos szolgáltatóját, hogy blokkolja vagy tovább engedje-e a hívást.
- **Honos szolgáltató:** Az a mobil rádiótelefon szolgáltatást nyújtó elektronikus hírközlési szolgáltató, akit megkérdez a bekérdező szolgáltató, hogy blokkolja vagy tovább engedje-e a hívást.

A magyarországi jogszabályok szerint a távközlési szolgáltatók olyan vállalkozások, amelyek elektronikus hírközlési szolgáltatásokat nyújtanak a felhasználók számára. Ezek a szolgáltatások magukban foglalják a vezetékes és mobiltelefon-szolgáltatásokat, az internet-hozzáférést, valamint a televíziós műsorszórást.
Elektronikus hírközlési szolgáltatás: olyan, általában díjazás ellenében, elektronikus hírközlő hálózatok révén nyújtott szolgáltatás, amely az elektronikus hírközlő hálózatok és elektronikus hírközlési szolgáltatások segítségével történő tartalomszolgáltatás, illetve az ilyen tartalom felett szerkesztői ellenőrzést biztosító szolgáltatások kivételével magában foglalja a következő szolgáltatástípusokat: internet-hozzáférési szolgáltatás; a személyközi hírközlési szolgáltatás és az olyan szolgáltatásokat, amelyek teljes egészükben vagy nagyrészt jelátvitelből állnak, mint például a gépek közötti szolgáltatások biztosítására és műsorterjesztésre használt átviteli szolgáltatások.

Caller ID spoofing

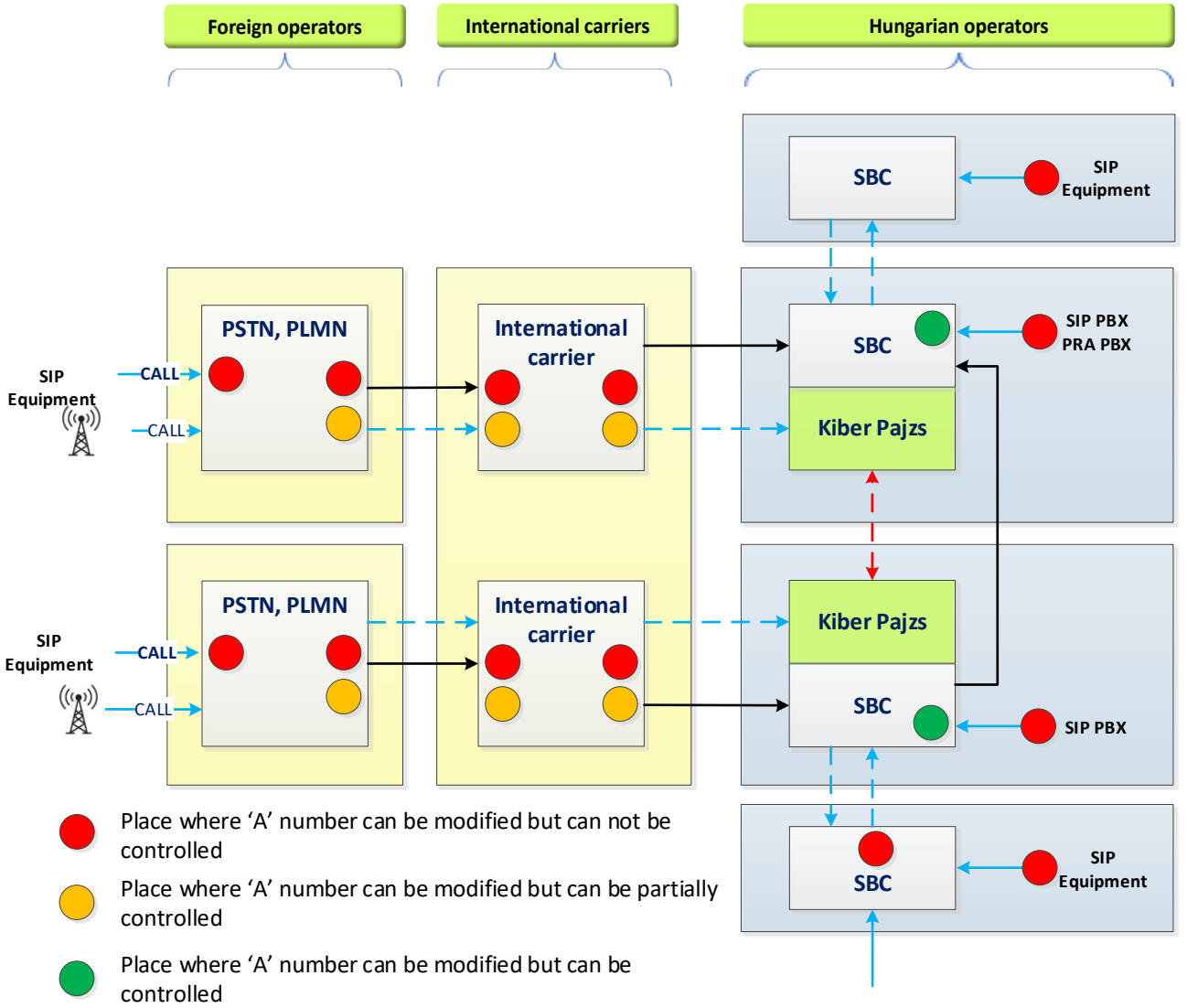
CLI módosítási helyek

A nemzetközi távközlési hálózatokban a spoofing több ponton is előfordulhat, mivel az adatok és a hívások több szolgáltatón, protokollon és technológián keresztül haladnak. A támadók különböző pontokat kihasználva manipulálhatják a forgalmat, hogy megtévesszék a végfelhasználókat vagy rendszereket.

- Hívásindításnál: Hamisított hívások gyakran VoIP szolgáltatókon keresztül indulnak, ahol könnyen beállítható hamis hívószám.
- Nemzetközi távközlési hálózatban: Egyes kevésbé szabályozott országokban működő tranzit szolgáltatók szándékosan módosíthatják a hívószámokat, hogy a hívásokat olcsóbb díjszabási kategóriába sorolják.

Belföldi távközlési hálózatokban is több pontos fordulhat elő hívószám módosítás:

- VoIP szolgáltatók és PBX rendszerek
- Belföldi tranzit szolgáltatók



STIR/SHAKEN Protokoll – Védelem a Caller ID Spoofing ellen

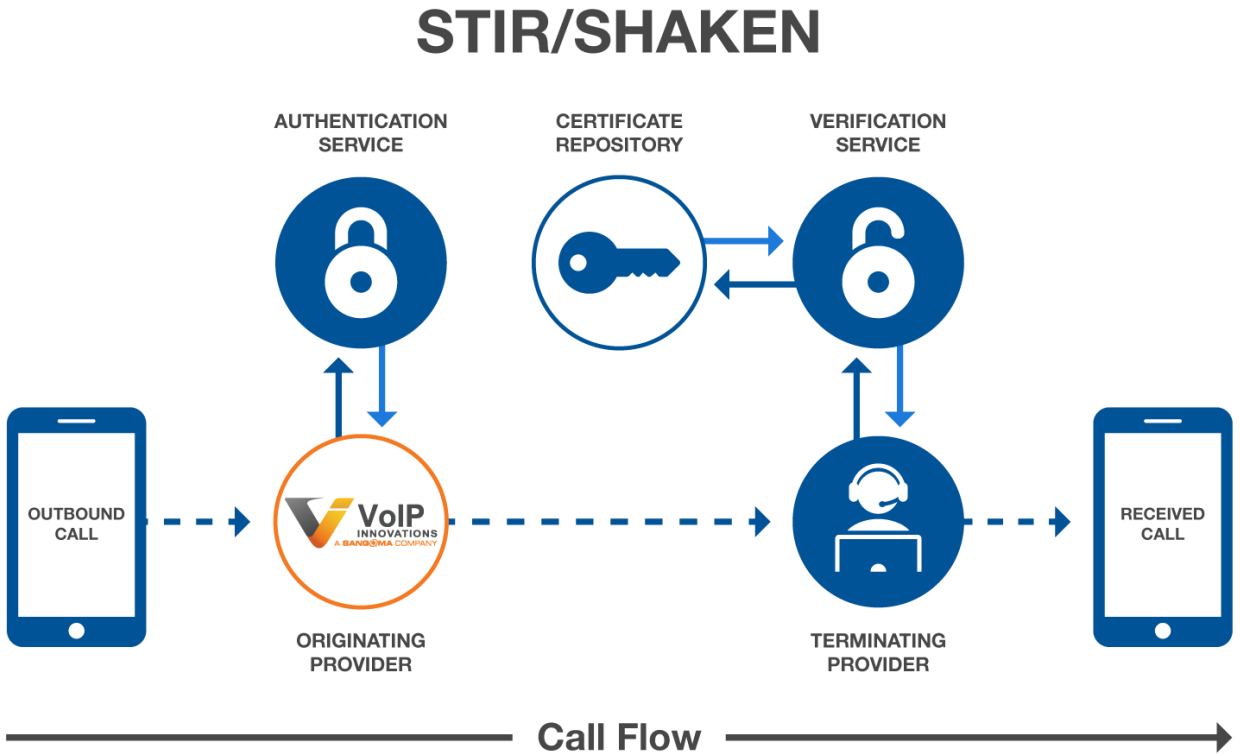
A STIR/SHAKEN egy szabványosított technológiai megoldás, amelyet a telefonhálózatokban alkalmaznak a Caller ID spoofing elleni védekezés érdekében.

Mit jelent a STIR/SHAKEN?

A STIR és a SHAKEN két különböző, de egymást kiegészítő rendszer:

- STIR (Secure Telephone Identity Revisited): Egy protokoll, amely a telefonhívások eredetiségét igazolja kriptográfiai aláírással.
- SHAKEN (Signature-based Handling of Asserted Information Using toKENs): Egy gyakorlati keretrendszer, amely az STIR protokollt alkalmazza a valós telefonhálózatokban.

Együtt alkalmazva a STIR/SHAKEN lehetővé teszi a távközlési szolgáltatók számára, hogy ellenőrizzék, egy bejövő hívás valóban attól a számtól származik-e, amelyet a kijelzőn látunk.

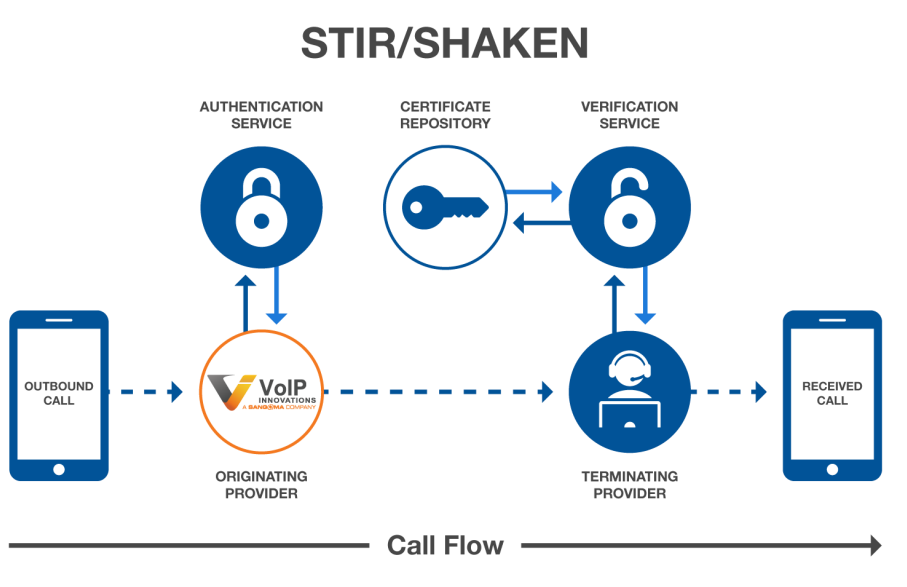


STIR/SHAKEN Protokoll – Védelem a Caller ID Spoofing ellen

Az alapfeltevés az, hogy a kiinduló operátor mindig tud valamit a híváskezdeményezésről: hívószám, CLI beillesztés, belépési pont, stb. A SHAKEN biztonságos mechanizmust biztosít a hívást kezdeményező operátor számára, hogy megbízható adatokat, információkat tudjon közölni a hívást végződtető operátorral. Más szóval, a **SHAKEN garantálja, hogy amit a kezdeményező operátor tud, az biztonságos és megbízható. Ennek érdekében a kezdeményező operátor digitális aláírást hoz létre és azt beilleszti a jelzésüzenetbe, amely a hívást végződtetőhöz kerül. A hívást végződtető operátor ellenőrzi a digitális aláírást és ha eltérést tapasztal, akkor jelzi a változást. Ezenkívül van egy speciális szám is a hívásüzenetben, amely egyedileg azonosítja a híváskezdeményezést és minden híváshoz generálódik.** Ennek célja a hívások visszakövethetősége probléma esetén.

A STIR/SHAKEN nem blokkolja közvetlenül a hamisított CLI-kkel történő hívásokat. A SHAKEN ellenőrzésének eredménye közvetlenül megjeleníthető, az alapján be lehet irányítani a jelzésüzenetet egy „hívásblokkoló alkalmazásba", amely lényegében jónak, megkérdőjelezhetőnek vagy valószínűleg csalónak azonosítja a hívásokat. A hívásblokkoló alkalmazás ezután képes a hívott fél nevében működni, hogy megakadályozza a nem kívánt hívások átjutását. Ha a hívott fél nem használ hívásblokkoló alkalmazást, akkor a hívott végfelhasználó hívásonként dönthet a hívás fogadásról. Mivel a SHAKEN az IETF által kifejlesztett STIR protokollon alapul, ezért **tanúsítványkezelő rendszerekre van szüksége, amit operátori szinten kell implementálni.**

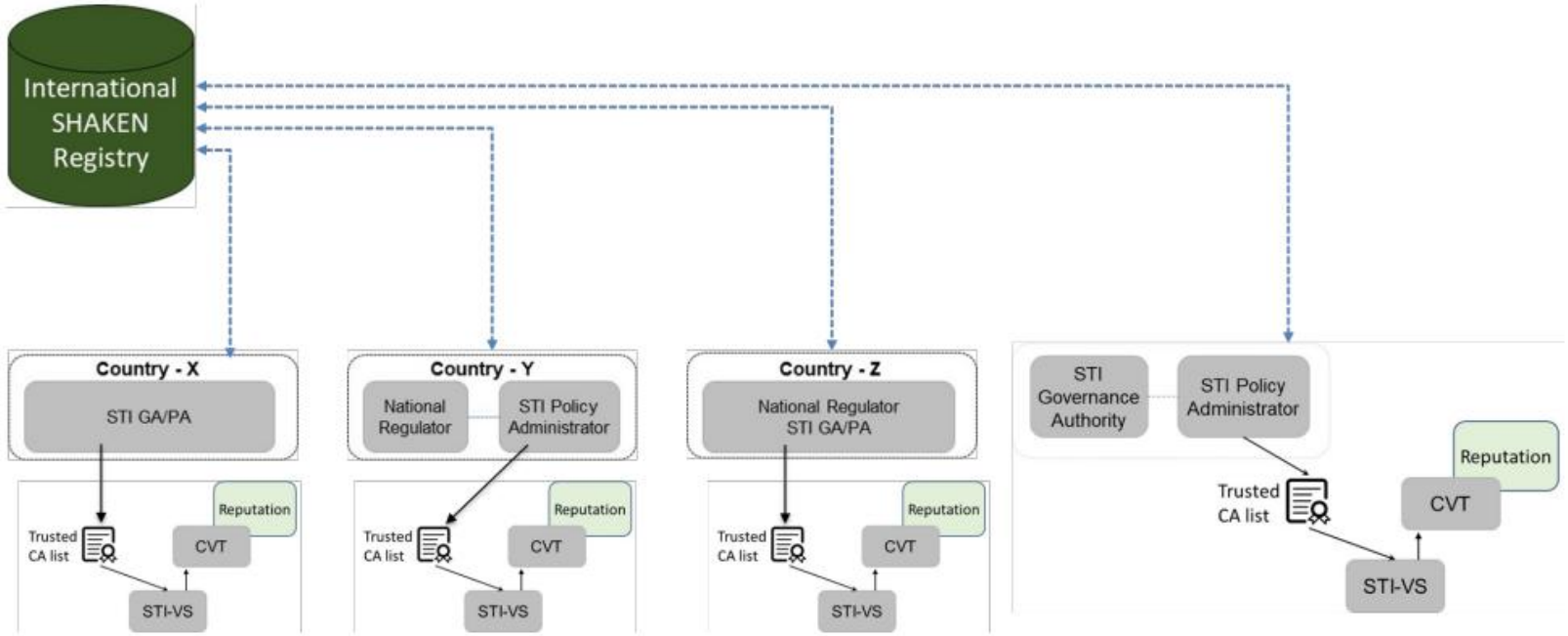
Ahol a hívás SIP alapú hálózaton lévő felhasználók között zajlik, ott a hitelesítési és ellenőrzési szolgáltatások megkövetelik a Secure Phone Identity – Authentication Service (STI-AS) meglétét a kezdeményező szolgáltatónál és a Secure Phone Identity - Verification Service meglétét a (STI-VS) a végződtető szolgáltatónál. Ha a hívás SS7-es hálózatból indul ki, akkor a hívás nem a végpontok közötti SIP-n alapul. Mivel több tranzit szolgáltató is lehet a kezdeményező és végződő szolgáltat között, ezért a hitelesítést az első belépési ponton kell aláírni.



STIR/SHAKEN hátránya

STIR/SHAKEN hátránya magyarországi bevezetés esetén:

- Központosított megoldás és eredetileg országon belüli megoldásra tervezték (sok piaci szereplős és nagyobb országok alkalmazzák)
- Országok közötti együttműködéshez kétoldalú szerződések kellenek, illetve szükség van egy nemzetközi SHAKEN nyilvántartásra
- Nemzetközi megvalósítás esetében kérdés ki hajlandó csatlakozni a rendszerhez és mikor (fő kérdés a nem EU-s országok csatlakozása)
- Költséges és időigényes megvalósítani
- Speciális szabályozást igényel a tanúsítvány kezelés miatt
- Jelenleg nem oldja meg a nemzetközi irányból bejövő hívások esetében a CLI hamisítás detektálását



Szakpolitikai dokumentumban rögzített megállapodások [1]

A szakpolitikai dokumentum készítése során az NMHH és a mobil szolgáltatók a következőkben állapodtak meg:

- Nincs központosított megoldás ami valós időben tartaná nyilván egy mobil előfizető tartózkodási helyét.
- Nincs PROXY megoldás ami biztosítana egy központosított irányítási módszert a mobil hívó helyének meghatározásához.
- Nincs jelzésüzenet alapú megoldás, nem kell jelzésüzenetben továbbítani a nemzetközi hívást tranzitálónak, hogy egy hívás nemzetközi irányból érkezett vagy belföldi hívásról van szó -> nemzetközi irányból érkező hívást fogadónak a felelőssége az ellenőrzés lefolytatása
- Nincs szükség valós idejű kapcsolódásra az NMHH azonosítónyilvántartási adatbázishoz, hogy valós időben legyen látható mely mobil számtartományokat jelölte ki az NMHH.
- A megoldásnak csak az azonosítógazdálkodási rendeltben meghatározott hívószámokat kell tudni ellenőrizni, azaz nemzetközi számmal beérkező hívásokkal nem kell foglalkozni.
- **A hívóazonosítóval való visszaélést megelőző vizsgálatot annak az érintett szolgáltatónak kell elvégeznie, aki a hívást a nemzetközi hálózatból fogadja.**
- **Nemzetközi irányból bejövő hívást csak az az elektronikus hírközlési szolgáltató kezelhet, aki képes – saját maga vagy megbízott társszolgáltatója útján – elvégezni a nemzetköz irányból bejövő hívások hívóazonosítóval való visszaélést megelőző vizsgálatát, és indokolt esetben képes a vizsgálaton fennakadt hívások blokkolására.**
- Amennyiben az Érinett szolgáltató nem látja el megfelelően saját maga vagy megbízott társszolgáltatója útján a hívóazonosítóval való visszaélést megelőző vizsgálatot, akkor a nem megfelelő működést észlelő szolgáltató bejelentést tehet az NMHH-nél a problémáról. Az NMHH felügyeleti hatáskörében megvizsgálja a bejelentést és jogsértés megállapítása esetén az Eht. szerinti jogkövetkezményeket alkalmazza. Indokolt esetben már az eljárás folyamat alatt is ideiglenes biztosítási intézkedést hozhat, amelyben megtilthatja a nem megfelelően eljáró szolgáltatónak, hogy nemzetközi irányból bejövő hívást fogadjon.

Szakpolitikai dokumentumban rögzített megállapodások [2]

- **Az A-szám honos szolgáltató hálózatába való bekérdezésre csak a nem saját szolgáltatói körbe tartozó mobil A-szám (esetleg B-szám) esetén van szükség.**
- **Az elvárt válasz (GO-NOGO) megadása a bekérdező szolgáltatónak a bekérdezésre a honos szolgáltató felelőssége. A bekérdező szolgáltató NOGO válasz esetén blokkol, vagy hiányzó válasz (meghatározott időn belül nem érkezik válasz) esetén főszabály szerint a hívást tovább engedi, de a hiba naplózásra kerül.**
- **Nemzetközi irányból bejövő hívások esetében a hívó szám csak akkor lehet magyarországi mobil szám ha a magyar mobil előfizető roamingol.**
- **A belföldi mobil szolgáltatók hálózatába történő bekérdezéshez MAP protokoll és ATI parancs kerül alkalmazásra.**
- Bekérdezés esetén mindig a Bekérdező szolgáltató felelőssége meghatározni, hogy melyik szolgáltatóhoz tartozik a száma (honos szolgáltató: donor vagy átvevő) és a MAP ATI üzenetet csak oda küldheti.
- Nemzetközi irányból bejövő hívások végződtetéséhez és/vagy tranzitálásához SIP-et kell alkalmazni.
- A csalások visszaszorítása érdekében blokkolt hívások esetén a hívóazonosítóval való visszaélét megelőző vizsgálatban és a blokkolásában résztvevő szolgáltatóknak a blokkolás tényét és adatait naplófájlban kell meghatározott adatartalommal és módon rögzíteni.
- Olyan szabályozás szükséges ami egységesen érvényes minden magyarországi szolgáltatóra akik hírközlési szolgáltatást nyújtanak és nemzetközi irányból bejövő hívásokat vagy végződtetnek vagy tranzitálnak.

Szakpolitikai dokumentumban rögzített megállapodások [3]

Nemzetközi irányból bejövő hívások esetében a következő hívószámok esetében a hívást blokkolni kell:

- Nemzeti számozási tervben nem rendszeresített
  - rövid szám
  - földrajzi szám
  - díjmentes szolgáltatás száma (SHS = 80)
  - emelt díjas szolgáltatás száma (SHS = 90, 91)
  - teszt-körzet szám (KS = 55)
  - nomadikus telefonszolgáltatás száma (SHS = 21)
  - SHS = 39
  - üzleti hálózatok számai (SHS = 38)
  - gépek közötti szolgáltatás száma (SHS = 71)
  - nem roamingoló mobil számok (SHS=20, 30, 31, 50, 70)
  - magyarországi alközpontoknak kijelölt nemzeti számozási tervben szereplő mobil szám
- Formátumhibás számok (*A nemzeti számozási tervben rendszeresített számtípus felépítésének nem megfelelő szám*)
- Nemzeti számozási tervben nem rendszeresített körzetszámok vagy Szolgáltatás és Hálózatkijelölő számok:
  - SHS: 40, 41, 51, 60, 61, 81
  - KS: 43, 58, 64, 65, 67, 86, 97, 98

Kivételeként kezelendő hívások, amelyeket vizsgálat nélkül a szolgáltatóknak át kell engedniük:

- A fehér listán szereplő technikai hívószámot tartalmazó hívás (ahol a technikai hívószám hívott számként szerepel):
  - ezen a listán olyan hívószámok, hívószám tartományok szerepelhetnek, amelyek nem kapcsolódnak előfizetőhöz
  - minden olyan E.164 formátumú, kijelölt szám felkerül a listára, amit a szolgáltatók a hatóság tudomására hoznak,
  - a szolgáltatók felelőssége, hogy milyen számok felvételét kérik a listára.
- A hívóazonosítóval való visszaélést megelőző vizsgálat eredményeként továbbengedett, nemzeti számozási tervben szereplő kijelölt mobil A-számot tartalmazó hívás:
  - ahol az A-szám honos szolgáltatója legalább arról meggyőződött, hogy az A szám a vizsgálat idején nemzetközi roaming állapotú.
  - amennyiben a honos szolgáltató az A-szám roaming állapotán túl képes további vizsgálattal az A-számmal való visszaélés tényét megalapozottan alátámasztani, akkor a hívás továbbítását megtagadhatja.

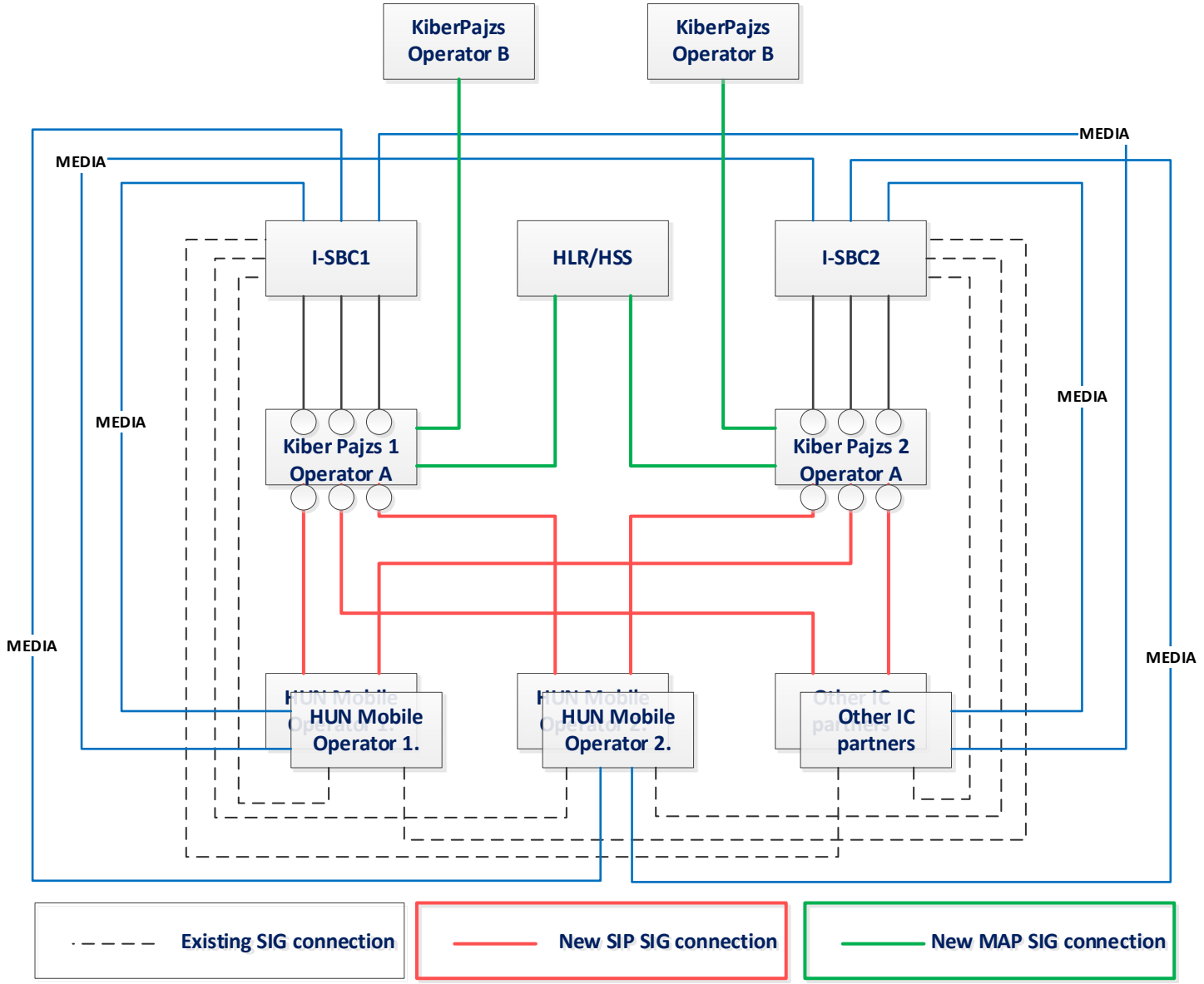
Kiber Pajzs lehetséges signalling architektúrája

Architektúra főbb jellemzői:

- GEO-redundáns
- Automatikus visszaállás hiba esetén a közvetlen SBC-SBC kapcsolatra (Bypass)
- Éves rendelkezésre állás: 99,8%
- MAP protokoll az operátorok között a bekérdezés támogatására
- Közvetlen HLR/HSS elérés a Kiber Pajzs Operator B-től tiltott

Architektúra hátránya:

- Az összes nemzetközi InterConnect kapcsolatot át kell terhelni a közvetlen kapcsolatról a Kiber Pajzs rendszer felé.



Mobil előfizető státuszának meghatározása

A szakpolitikai dokumentum szerint ez érintett szolgáltatónak legalább arról meg kell győződnie, hogy a mobil A-szám a vizsgálat időpontjában roamingolt-e. A kérdés, hogy ez elegendő? A válasz, hogy NEM.

Mit lehet tenni, hogy minél pontosabban meg lehessen határozni, hogy hamis-e az A-szám (A SZOGÁLTATÓKNÁL A LEHETŐSÉGEK ELTÉRHETNEK)?

- Meg lehet nézni, hogy a magyarországi mobil számra van-e érvényes kijelölési határozat az NMHH azonostógazdálkodási nyilvántartásában. Nem támogatott megoldás, mert költséges és a vizsgálat egyéb fázisában ez az információ kideríthető.
- Az A-szám szolgáltatója első lépésben a saját adatbázisában (HLR) megnézi, hogy az A-szám roamingol-e, azaz van-e külföldi VLR cím bejegyezve. Ha van akkor V-PLMN-től, a **honos hálózat lekérdezi az előfizető státuszát** (Unknown, Busy, Not Reachable, Assumed Idle).
  - Ha nincs válasz, akkor nem blokkolunk
  - Ha van válasz akkor a válasz tartalma alapján vagy blokkolunk (Unknown, Not Reachable, Assumed Idle), vagy továbbr engedjük a hívást (Busy)
- **Ahol csak lehet bekapcsoljuk a CAMEL Homingot (nem minden szolgáltatónál érhető el ez a funkció Magyarországon).** CH lényege: ha egy mobil előfizető roaming során hívást indít, akkor a hívott szám tartózkodási helyétől függetlenül a hívást egy technikai számmal hazahozzuk és itthon elemezzük. Ezért olyan hívást látunk ahol a hívó szám ugyan Yetteles mobil előfizető de a hívott szám egy CH Technikai szám, akkor a hívást nem kell blokkolni mert ilyen esetben nem lehet az A-számot hamisítani.
- **Ellenőrizzük, hogy van-e CAMEL Homing szerződés a V-PLMN-el**. Abban az esetben ha van szerződés, akkor a B-szám technikai szám lehet csak. Ha TN nélkül érkezik hívás a V-PLMN-től (akivel van roaming szerződésünk) akkor a hívást blokkolni kell.
- Ahol csak lehet **bevezetjük a VoLTE roamingot S8HR alapon**. Ez esetben a hívás nem érinti a Interconenct forgalmat.

Mikor nem lehet sikeres a hívó szám ellenőrzése (példa)?: Akkor ha a nemzetközi trönkönk olyan mobil A-számmal érkezik be a hívás Magyarországra amikor a hívó szám egy nem CAMEL-es országban roamingol és a V-PLMN nem válaszolja meg a honos hálózatnak, hogy mi az előfizető státusza (vagy szándékosan rossz státusz információt küld vissza).

Átirányított hívások kezelése

A legnagyobb kihívást az átirányított hívások kezelése jelenti, mivel vagy nagyon bonyolult vagy nem is lehetséges annak az ellenőrzése, hogy kell vagy nem kell blokkolni a hívást. Ezért a Szakpolitikai dokumentum szerint a **nemzetközi hálózatban átirányított hívásokat blokkolni kell.**

Hogyan játszható ki a hívószám ellenőrzés ha nem tiltjuk a hívásátirányítást? (példa)

Alap hívás eset: Magyarországi földrajzi számról (A-szám) felhívunk egy mobil előfizetőt (B-szám) aki éppen roamingol 2G rádióhálózat alatt. A B-szám csengetése megkezdődik, de a hívott nem veszi fel a telefont, viszont neki van Late Call Forwarding beállítása egy magyarországi mobil C-számra, aki Magyarországon tartózkodik. A hívás beérkezik az Érintett szlogáltatóhoz - az Interconnect összeköttetéseken - aki látja, hogy nemzetközi irányból jött be egy hívás magyarországi vezetékes A-számmal.

Trükközés: A csaló vásárol egy magyarországi SIM kártyát és feljelentkezteti külföldön (ő less a B-szám), majd beállít hívásátirányítást egy olyan C-számra akit kiszemelt magának, mint áldozat. Ezek után például egy SIP-es trönkön elindít egy hívást ahol az A-szám egy magyarországi bank száma.

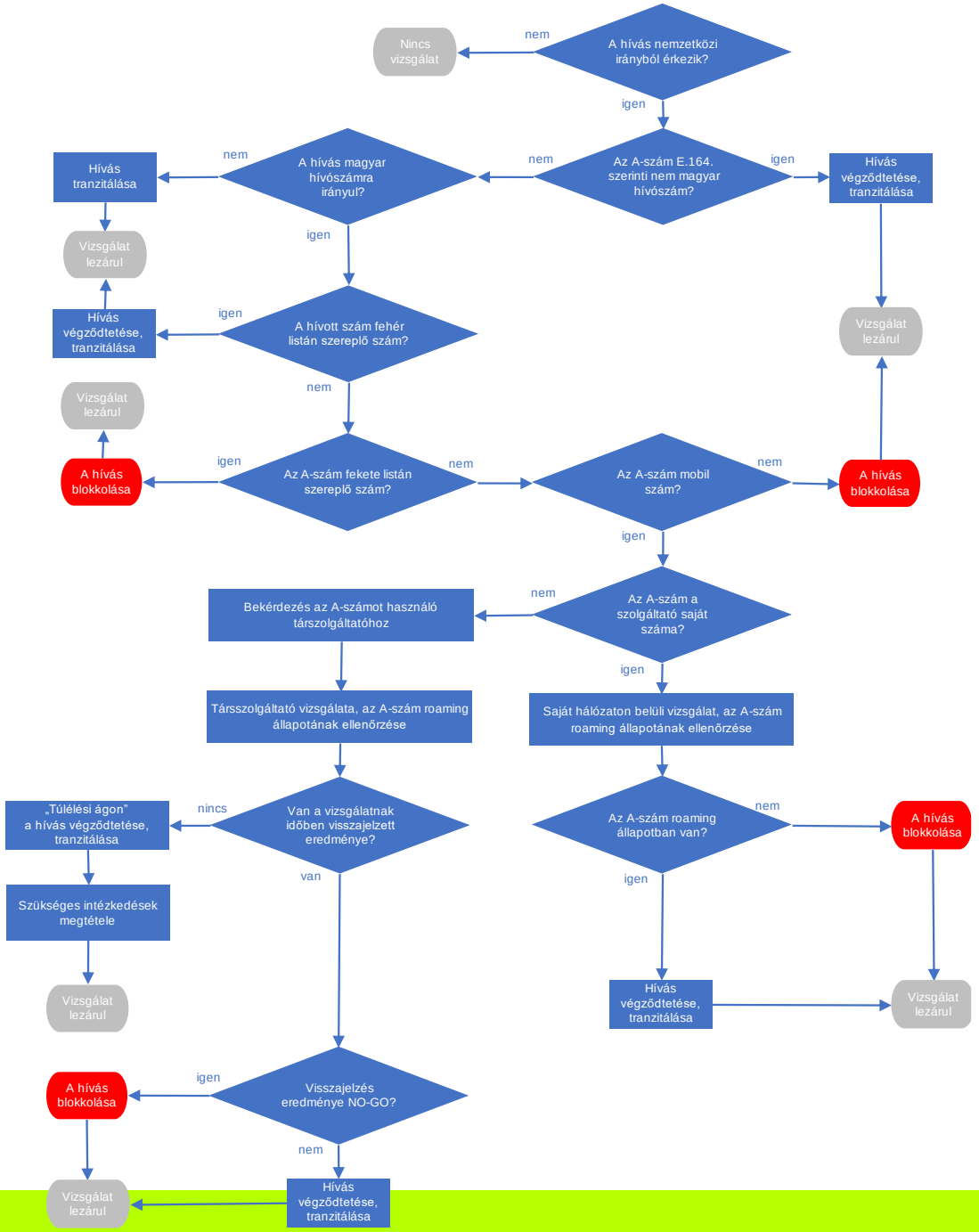
Mit tapasztal a hívott fél: A hívott fél készülékén megjelenik a hamis A-szám mint hívó szám

Probléma: A hívószám vizsgálat során csak bonyolult módszerrel lehetne ezt ellenőrizni, hogy hamis vagy nem hamis a hívószám (amellett, hogy a B-számot is ellenőrizni kell, be kellene kérdezni a vezetékes szolgatónál, hogy van-e aktív nemzetközi hívása a földrajzi számnak).

Okoz-e problémát az átirányított hívások blokkolása? IGEN okoz. Lesznek ügyfelek akiknél ez problémát fog okozni, amit ÁSZF-ben is kommunikálni kell majd. DE ahogy megyünk előre az időben a VoLTE (4G rádió alatti hívás) roaming szerződések száma egyre több lesz. Ez azért fontos, mert a VoLTE roaming hívást nem a V-PLMN kezeli le hanem a honos hálózat, ezért ott az átirányítások már működni fognak.

Híváskezelési folyamatábra

Szakpolitikai dokumentum mellékletében elérhető tervezet:



CLI tiltás hatása a nem EU-s hívásfogadásra

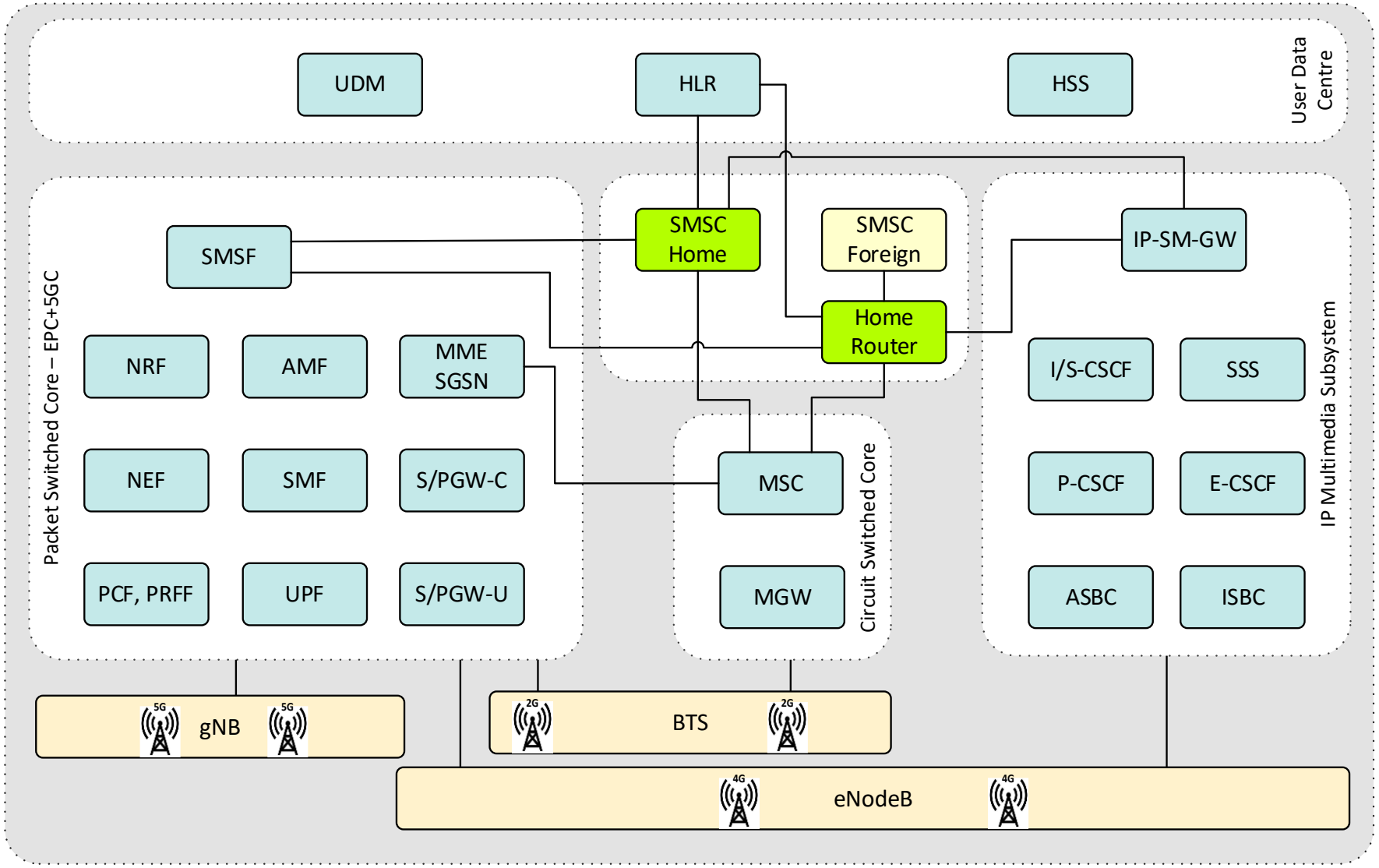
- **Az „A” szám megváltoztatás a végződtetési díjak csökkentése érdekében**
  Jelentős különbség van az EU-ban kezdeményezett és végződtetett hívások, valamint az EU-n kívül kezdeményezett és végződtetett hívások végződtetési díjaiban. Ezért a tranzitszolgáltatók sok esetben lecserélik az ‘A’ számot egy EU-számra, általában a célország számára
  Példa: Az eredeti hívószám ukrajnai vagy szerbiai szám. A kiinduló hálózat az EU-n kívüli végződtetési díjat fizeti annak a tranzit szolgáltatónak, aki az eredeti ‘A’ számot EU-számra cseréli (pl. +36 20 9876543), és magyarországi szolgáltatóknak jóval alacsonyabb végződtetési díjat fizet, mindamellett hogy téves hívószám jelenik meg a hívott készülékén.

- **A tervezett megoldás hatása a CLI módosításra**
  A Kiber Pajzs bevezetése után a tranzitszolgáltatók várhatóan más uniós számokat fognak használni a magyar helyett, amit a rendszer nem tud leellenőrizni. Abban az esetben, ha a magyar előfizető készülékén (hívott fél) nem magyar telefonszám jelenik meg, a hívó fél az esetek többségében nem fogja felvenni a hívást. Ebből fakadóan várhatóan csökkenni fog a bejövő, felépült hívások száma. Ez panaszokat válthat ki a hívóktól, ami hatással lehet a csalásra.

- **Tárgyalások az EU-n kívüli hívásokat végző IC-partnerekkel (pl. szerb, Svájc, Ukrajna)**
  Az IC partnert arra kell kényszeríteni, hogy közvetlenül ezen országok szolgáltatóival szerződjön ahelyett, hogy a hívó fél számát módosítani tudó közvetítő szolgáltatókat használna.

SMS spoofing

Egyszerűsített Mobile Core hálózat rövid bemutatása

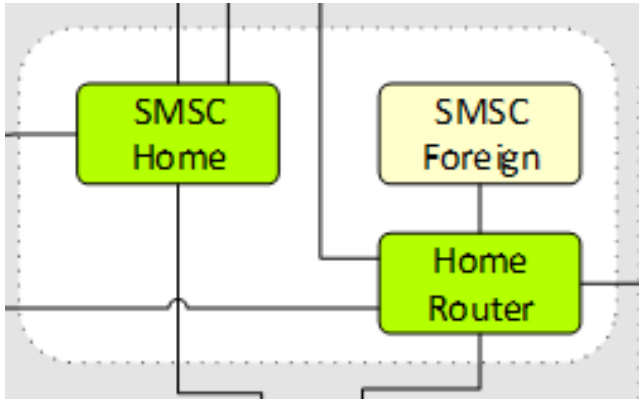


SMS Home Router – Miért is kell?

Mivel az SMSC nem ismeri az SMS-t fogadó előfizető tartózkodási helyét, ezért az SMSC ezt az információt HLR-től kéri el, amely tartalmazza a végződő előfizetőre vonatkozó információkat. Ez a MAP SendRoutingInfo_for_SM vagy a DIAMETER Send-Routing-Info-for-SM-Request üzenet használatával érhető el. A címzett előfizető telefonszáma (MSISDN) szerepel az SRI_for_SM üzenetben, amelyet a HLR/HSS lekérdezésben kell használni.

1. A keresés után a HLR visszaadja az SRI_for_SM választ a kérdező SMSC-nek ami lehet akár honos, de lehet idegen SMSC is. MAP szinten ez az üzenet a következőket tartalmazza:
   - Az SMS-t fogadó előfizetőt kiszolgáló aktuális MSC/VLR pontkódja (címe)
   - Az SMS-t fogadó előfizető nemzetközi mobil előfizető azonosítója (IMSI)
2. A keresés után a HSS visszaküldi a Send-Routing-Info-for-SM-Answer (SRA) választ a kérdező SMSC-nek. A Diamaternél ez az üzenet a következőket tartalmazza:
   - Az SMS-t fogadó előfizetőt kiszolgáló MME pontkódja (címe)
   - Az SMS-t fogadó előfizető nemzetközi mobil előfizető azonosítója (IMSI)

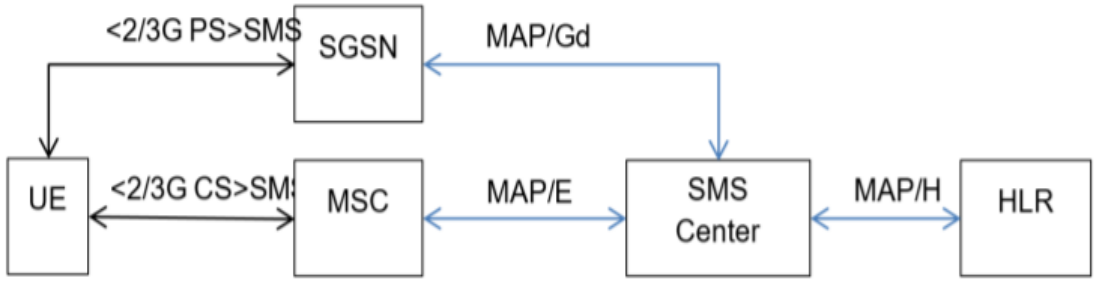
A fő probléma az, hogy a szolgáltatók évekkel korábban visszaküldték az előfizető IMSI-jét, miután megkapta a kérést, ahelyett, hogy egy úgynevezett hamis IMSI- és SMSC-címet küldött volna vissza.
Megoldás: A külföldi SMSC és a honos hálózat között be kell tenni egy Home Router dobozt ami elrejti a külföldi hálózat elől az előfizető valós IMSI-ét és tartózkodási helyét.



SMS küldés 2G rádió hálózaton

Főbb jellemzői:

- GSMA név: **SMS over MAP**
- Az SMS over MAP (Mobile Application Part) egy olyan technológia, amely az SS7 (Signaling System No. 7) protokollrendszeren belül működik és az SMS-ek továbbítását teszi lehetővé GSM vagy UMTS hálózatokon keresztül. Ez a megoldás a klasszikus SMS továbbításának alapját képezi és a mobilhálózati komponensek közötti kommunikációhoz használatos.
- Az SMS over MAP technológia a mai modern IP-alapú megoldások mellett is széles körben használatos a hagyományos mobilhálózatokban.
- Két fajtája létezik: **2G CS SMS over MAP** és a **2G PS SMS over MAP**. Az utóbbit a Yettel nem használja, mivel minden ügyfél aki 2G-n van fent azok a CS Core hálózatba regisztrálnak, így ott az üzenet mindig leküldhető



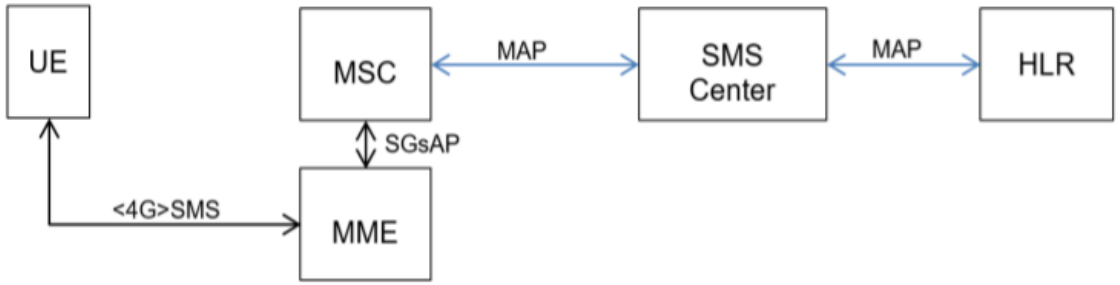
Főbb jellemzői:

- GSMA név: **SMS over DIAMETER**
- Az SMS over Diameter over 2G egy ritkább de létező megoldás, amely az SMS-ek továbbításához a Diameter protokollt és a hagyományos GSM hálózatok kombinációját használja. Ez általában olyan hibrid hálózatokban fordul elő, ahol a Diameter protokollt az LTE/IMS infrastruktúrában vezették be de a GSM hálózati komponensek még működésben vannak.
- Yettel ezt a SMS küldési megoldást nem implementálta, mivel minden ügyfél aki 2G-n van fent azok a CS Core hálózatba regisztrálnak, így ott az üzenet mindig leküldhető MAP-en keresztül.

SMS küldés 4G rádió hálózaton

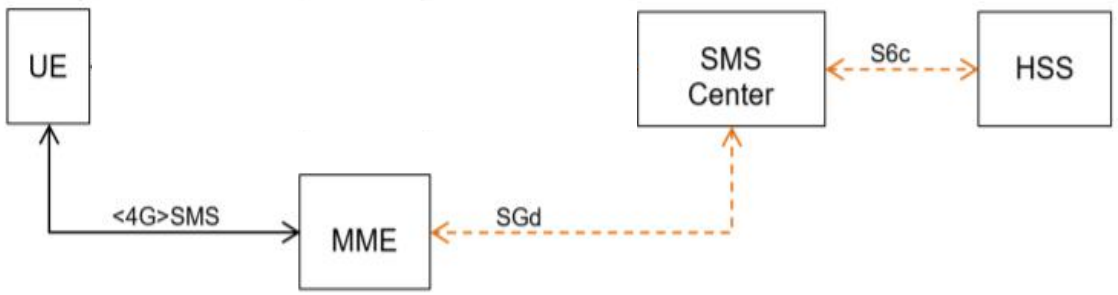
Főbb jellemzői:

- GSMA név: **SMS over SGsAP and MAP**
- Az SGsAP interface az LTE hálózatokon belül alkalmazott interfész, amely az LTE hálózatot a hagyományos CS hálózattal köti össze. Az SMS over SGsAP lehetővé teszi a szöveges üzenetek küldését és fogadását egy LTE-hálózaton keresztül, miközben a hagyományos CS alapú SMS-funkciókat használja.
- A megoldást abban az esetben használják amikor a nem VoLTE-s előfizető 4G alatt van vagy ha technikai probléma miatt nem működik az (IMS) SMS over MAP/Diameter megoldás, de mindenképpen el akarjuk kerülni a CSFB-t.



Főbb jellemzői:

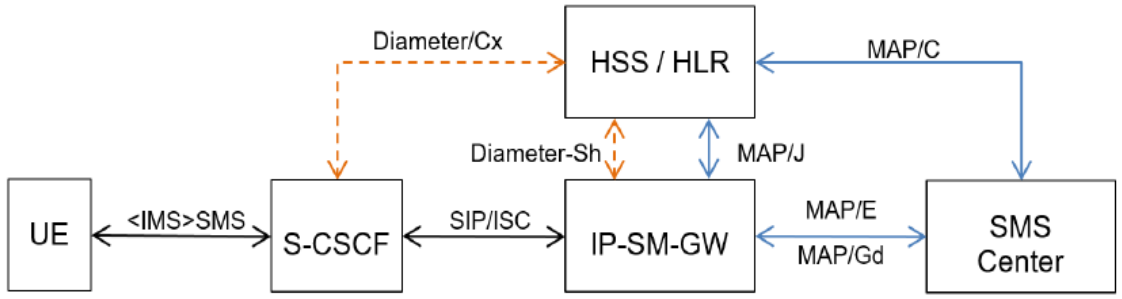
- GSMA név: **SMS over DIAMETER** (over MME)
- Az SMS over Diameter (over MME) üzenetküldés egy modern megközelítés, amely lehetővé teszi az SMS-ek továbbítását az LTE hálózaton keresztül.
- Yettel ezt a SMS küldési megoldást sem implementálta, mivel minden ügyfél aki 4G-n van fent azok elsődlegesen IMS-en keresztül kapják meg az üzenetet (VoLTE képes ügyfelek). Ha nem VoLTE képes előfizetőről van szó, akkor az SMS over SGsAP and MAP-et használjuk.



SMS küldés 4G és 5G rádió hálózaton

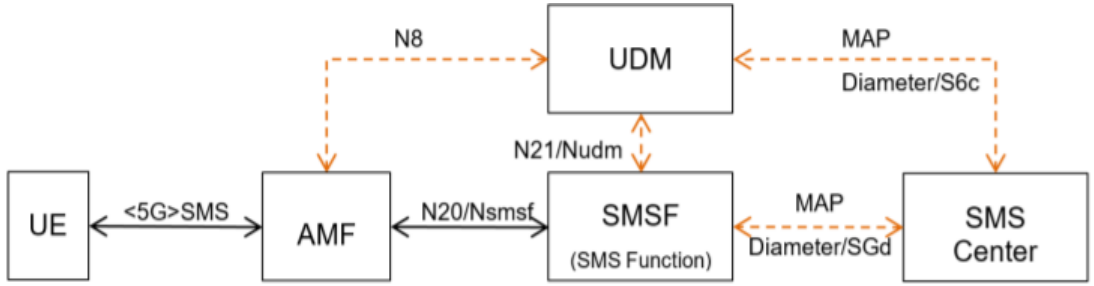
Főbb jellemzői:

- GSMA név: **(IMS) SMS over MAP/Diameter (SMS over IMS)**
- Az SMS over IMS (IP Multimedia Subsystem) egy modern megközelítés az SMS-ek továbbítására, amely teljes mértékben az IP-alapú LTE/NR hálózatok infrastruktúrájára épül.
- Az SMS-t az IMS hálózaton keresztül továbbítják. Ehhez egy külön elem kerül telepítésre ami az IP-SM-GW.
- Az IP-SM-GW fő feladata a protokoll konverzió MAP és SIP között valamint a Service Domain Selection támogatása (hol kerüljön az SMS kiküldésre?: IMS-en, vagy CS Core-on keresztül).
- Forgalom szempontjából a legtöbbet használt megoldás.



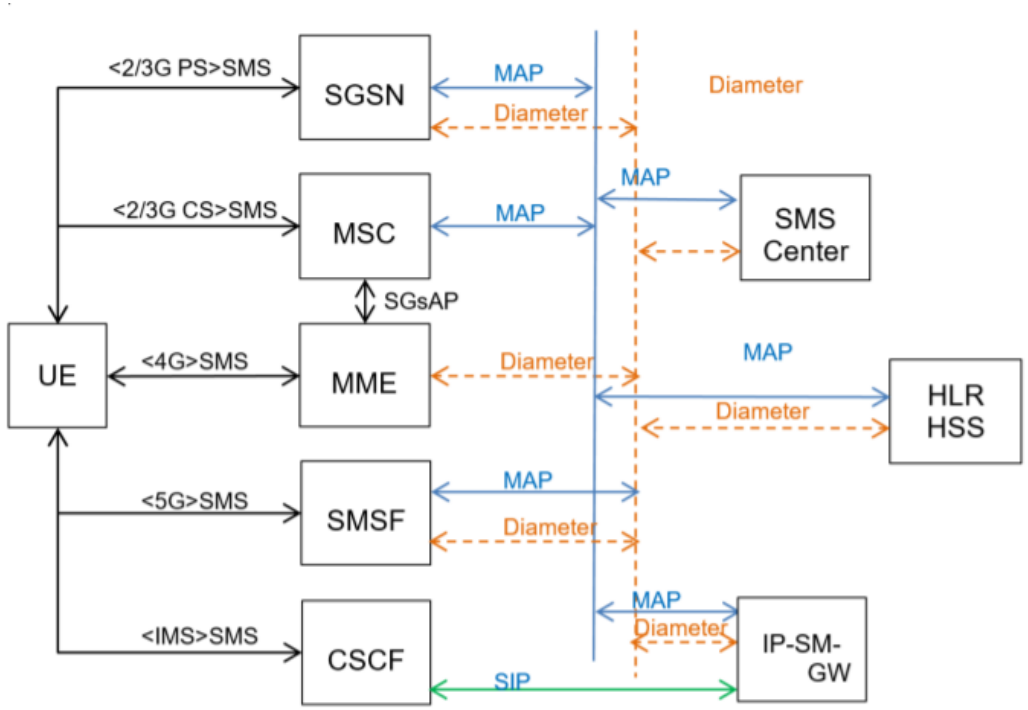
Főbb jellemzői:

- GSMA név: **(5G) SMS in MAP/Diameter (SMS over SMSF)**
- Az SMS over SMSF (Short Message Service Function) egy 5G-specifikus megoldás az SMS-ek továbbítására, amely az 5G hálózat alapvető komponenseit és az új architektúráját használja. Az SMSF lehetővé teszi az SMS-küldést és fogadást teljesen IP-alapú 5G hálózatokban a hagyományos CS infrastruktúra szükségessége nélkül.
- Az SMS-t az 5GC Core hálózaton keresztül továbbítják. Ehhez egy külön elem kerül telepítésre ami az SMSF.
- Az SMSF fő feladata a protokoll konverzió MAP és http2 között valamint a Service Domain Selection támogatása (hol kerüljön az SMS kiküldésre?: SMSF-en keresztül, vagy IMS-en).
- Fő driver: SMS küldés Data Centric készülékek esetében és alternatíva az SMS over IMS megoldáshoz.

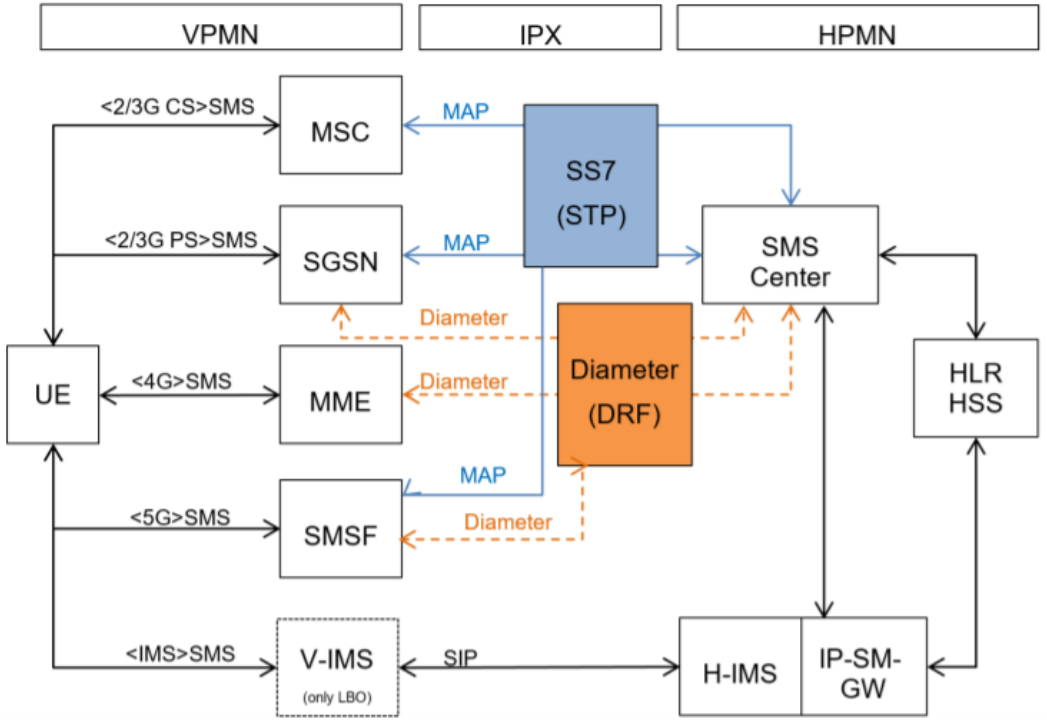


SMS küldési lehetőségek - Összefoglaló

Non-Roaming Case



Roaming Case



SMS visszaélések csoportosítása

Előfizetők megtévesztését vagy megkárosítását célzó üzenetek	Fizetős csatornák kikerülése	Speciális parancsokat tartalmazó üzenetek	Előfizetői adatbázis feltérképzése
Linket tartalmazó üzenetek	Grey route	OTA üzenetek	Előfizetői adatbázis feltérképezése
Emelt díjas SMS szolgáltatások	SIM farmok	Távvezérléshez használt csaló üzenetek	
Hamis feladóval küldött üzenetek	SCCP screening		
Alfanumerikus feladóval küldött üzenetek			
SMS KiberPajzs elődleges prioritása	SMS KiberPajzs másodlagos prioritása	SMS KiberPajzs szolgáltatók belső prioritása	

Megjegyzés: A fenti csoportosítás egy kiinduló lehetőség és célja struktúrába helyezni a problémás területeket. Ez a terület további egyeztetést igényel majd minden érintett bevonásával

Linket tartalmazó üzenetek

Az SMS használata során többféle visszaélési forma létezik, amelyek célja a mobil szolgáltató előfizetőinek megtévesztése vagy megkárosítása. Egyik legelterjedtebb formája ha az SMS linket tartalmaz. Néhány példa:

1. **Phishing** (Adathalászat): Az elkövetők hamis SMS-eket küldenek, amelyek úgy tűnnek, mintha hivatalos szervezetektől (pl. bank, mobil szolgáltató, kormányzati szerv) érkeznének. Az üzenetekben jellemzően arra kérik az áldozatot, hogy adja meg személyes adatait, jelszavait, vagy kattintson egy linkre. Példa: „Tisztelt Ügyfelünk! Fiókja biztonsági okokból zárolásra került. Kérjük, kattintson ide [hamis link], hogy újraaktiválja."
2. **Smishing**: Az SMS-ekkel végzett adathalászat egy formája, ahol az üzenet célja az, hogy az áldozatot egy hamis weboldalra irányítsa, vagy rávegye, hogy érzékeny adatokat osszon meg. Példa: „Gratulálunk, nyert egy okostelefont! Igényléshez kattintson ide: [hamis link]"
3. **Malware-terjesztés**: Az SMS-ekben található linkek kártékony programokat tölthetnek le a telefonra, amelyek érzékeny adatokat lophatnak el, például banki információkat vagy jelszavakat. Példa: „Frissítse most az alkalmazását! Kattintson ide: [rosszindulatú link]"
4. **Hamisan sürgető üzenetek:** Az elkövetők sürgős vagy vészhelyzeti érzetet keltenek, például azt állítják, hogy a telefonos szolgáltatás megszűnik, ha az előfizető nem cselekszik azonnal. Példa: „Az előfizetése 24 órán belül lejár. Fizessen most: [hamis link]"
5. **Csaló nyereményjátékok:** Az SMS-ekben hamis nyereményeket ígérnek, és azt kérik, hogy az áldozat adja meg személyes vagy banki adatait a „nyeremény átvételéhez". Példa: „Gratulálunk, Ön az 1.000. ügyfelünk! Nyereményéért kattintson ide."

- Szabályozás szempontjából a legérzékenyebb terület mert biztosítani kell, hogy a szolgáltatók belenézhessenek a nemzetközi hálózatból érkező üzenetek tartalmába és ha abba előre meghatározott linket vagy egyéb információt talál akkor blokkolni kell az üzenet.
- Fontos, hogy az fekete listás adatbázis tartalmát központilag kell meghatározni, majd ahhoz hozzáférést kell biztosítani a szolgáltatóknak (KRA típusú működés).

Hamis feladóval vagy rossz formátummal küldött üzenetek

- Sok esetben a linket tartalmazó üzeneteket hamis feladóval adják fel, de az is a megtévesztés eszköze lehet ha ugyan nincs link az üzenetben de azt hamis feladóval adják fel a csalók.
- Távvezérléshez használt csaló üzenetek esetében egyértelműen hamis feladóval indítják az üzenet küldést, annak érdekében, hogy például SMS üzenettel lehessen egy riasztó kikapcsolni (ez esetben sokszor nem is lényeges az SMS tartalma).
- SMS fogadás esetében előfordul, hogy rossz formátumban (ami leginkább kevés vagy sok karaktert tartalmaz, ideértve a rövid kódokat is) érkezhet SMS a nemzetközi irányból.

SMS Kiber Pajzs érintettségi példa:

- Egy csaló a nemzetközi hálózatban felad egy SMS-t, ahol a címzett előfizető egy Yetteles előfizető aki a számát a Telekomtól hordozta át a Yettelhez. Az üzenetben a feladó száma pedig egy One-hoz tartozó szám. A külföldi SMSC és a GT címek megfelelőek, azok miatt nem kell blokkolni az üzenet kézbesítését.
- A külföldi hálózat elküldi az SRI for SM üzenetet a Telekomnak. Mivel a szám hordozott, ezért a Telekom az SRI for SM-et továbbítja a Yettelnek. A Yettel Home Router visszaküldi a saját címét és egy fake IMSI-t Telekomnak, aki azt továbbítja a feladónak. A feladó a Yetteltől kapott Home Router cím alapján a Forward SM üzenetet közvetlenül a Yettelnek küldi el. Mivel a Forward SM tartalmazza a feladó számát, ezért cask a Yettel tudja annak jogosságát ellenőrizni.
- Jelen esetben a feladó szám egy One-os szám, ezért a Yettel MAP-en megkérdezi a One-t, hogy jogos-e a küldés vagy sem. A One ellenőrzi, saját előfizetője státuszát és vagy továbbr engedi az SMS-es kézbesítését vagy blokkolja azt.

- A Kiber Pajzs Hanghoz hasonlóan SMS esetében is vizsgálni kell a nemzetközi összeköttetéseken, hogy az SMS küldő szám milyen szám (magyar vagy külföldi, megfelelő formátumú vagy nem), illetve ha magyar szám akkor mi a státusza (nem létező, roamingol, nem elérhető, honos hálózaton van, …), majd annak alapján blokkolni kell az üzenet kiküldését. Itt kérdés, hogy a blokkolást visszajelezzük-e a feladónak, vagy a ne.
- A működéshez elegendő a FORWARD_SM vizsgálata amiben megjelenik a feladó száma ami alapján le ehet futtatni a vizsgálatot.
- A vizsgálatot annak a szolgáltatónak kell elvégeznie aki a Forward_SM üzenetet fogadja nemzetközi irányból.

Alfanumerikus feladóval küldött üzenetek

Alfanumerikus karakterek használatát két csoportra kell bontani:

- belföldi használat, amire a magyar jogszabályok vonatkoznak
- külföldi használat, amire a nemzetközi és az adott ország jogszabályai vonatkoznak

Belföldi használat esetén releváns jogszabály-részletek: a 14/2020 NMHH rendeletből:

- „25. § (1) Számfüggő elektronikus hírközlési szolgáltatások igénybevétele során, a szolgáltatás igénybevételét kezdeményező azonosítására szolgáló hívó azonosító (a továbbiakban: hívó azonosító) csak a nemzetközi és nemzeti számozási tervben meghatározott módon és formátumban alkalmazható. Számfüggő elektronikus hírközlési szolgáltatások igénybevétele során a hívás és üzenetküldés kezdeményezésekor a hívó azonosítójaként a számjegyeken és a + karakteren kívül más karakter nem használható."
- „25. § (9) A számfüggő elektronikus hírközlési szolgáltatások igénybevételénél hívás, üzenetküldés és más kommunikáció kezdeményezésére a számjegyeken és a + karakteren kívül más karakter nem használható."
- A belföldi szám hossza 8, 9 vagy 12 számjegy. A mobilszám szolgáltatáskijelölő számból és előfizetői számból áll: AB abc defg, ahol AB = mobil rádiótelefon szolgáltatást jelölő SHS, abc defg = előfizetői szám 000 0000 – 999 9999 között.

Nemzetközi használat esetén (bejövő hívásokra és SMS-ek esetén) érvényes jogszabály-részletek:

- „A nemzetközi szám hossza legfeljebb 15 számjegy. A használat feltételei: A belföldi számok használati feltételeit az adott ország nemzeti számozási terve határozza meg. A belföldi számok használatát az adott ország nemzeti szabályozó szervezete/hatósága engedélyezi."

- A fentiekből egyértelmű, hogy Magyarországon semmiképp nem lehet alfanumerikus karaktereket használni. Ha ilyet tapasztal egy szolgáltató, akkor az üzenetet nem szabd kikézbesíteni.
- Nemzetközi esetben nem zárható ki teljesen, hogy a feladó szám a numerikus karaktereken kívül mást is tartalmazhat, ha az adott ország hatósága engedélyezi ezt. Ennek ellenére a nemzetközi linkeken bejövő SMS-ek esetében is blokkolni kell(ene) az SMS kézbesítését.

Fizetős csatornák kikerülése

Nemzetközi irányból érkező SMS-ek esetében a csalók és a költségeket elkerülni kívánó szolgáltatók gyakran különböző technikákat alkalmaznak annak érdekében, hogy megkerüljék a hivatalos, fizetős csatornákat. Ezek a megoldások lehetővé teszik számukra, hogy csökkentsék a költségeket, vagy kihasználják a gyengébb szabályozással rendelkező infrastruktúrát.

- **Grey Route (Szürke útvonalak használata)**
  A legelterjedtebb módszer a grey route használata, amely során az üzeneteket nemzetközi aggregátorokon vagy nem hivatalos csatornákon keresztül küldik.
  Hogyan működik?: A csalók vagy nem hivatalos aggregátorok egy másik ország szolgáltatóján keresztül küldik el az SMS-t. Az üzenet formálisan nemzetközi SMS-ként érkezik meg, de valójában olcsóbb belföldi tarifák alapján számlázzák. Példa: Egy SMS a célországban belföldi üzenetként érkezik, de az eredeti forrás egy másik országból származik. Cél: Az operátorok közötti nemzetközi roaming díjak és tranzitköltségek kikerülése.
- **SIM farmok alkalmazása**
  A SIM farmok használata egy másik gyakori módszer, amely során nagyszámú, belföldi SIM-kártyát helyeznek el egy automatizált rendszerben.
  Hogyan működik?: A csalók nagy mennyiségű belföldi SIM-kártyát vásárolnak. Ezeket a SIM-kártyákat egy központi eszközbe helyezik (SIM farm), amely lehetővé teszi az üzenetek belföldi hálózatokon keresztüli továbbítását. Az üzenetek belföldi SMS-nek tűnnek, de valójában nemzetközi forrásból származnak. Cél: Az üzenetek belföldi tarifával történő továbbítása, az országon belüli díjak kihasználása.
- **SCCP screening**
  Megvizsgálja az SCCP üzenetekben található Global Title (GT) címeket (a küldő és fogadó fél címei), hogy azok hitelesek és jogosultak-e az üzenetküldésre. Biztosítja, hogy csak megbízható hálózatokból és szolgáltatóktól érkező üzenetek jussanak el a célállomásra. A GT (Global Title) az üzenetek irányítására és továbbítására használt címek egyik formája a SS7 protokollban. Ezek a címek lehetővé teszik, hogy SMS-ek nemzetközi hálózatokon keresztül érkezzenek meg a fogadó félhez. Hamisítók gyakran visszaélnek más szolgáltatók GT-címeivel, hogy megtévesszék a címzettet.
  Hogyan működik?: Nem létező címekről küldik az üzeneteket agy az elszámolás nem megoldható, mert nem tudni ki is a valós küldő.

- A bemutatott példák szűrése alap mobil szolgáltatói érdek, ezt a Yettel folyamatosan, napi szinten végzi annak érdekében, hogy minimalizálja az SMS végződtetéssel járó veszteségeket valamint, hogy ne legyen téves árazás a roaming partnerek felé.
- Ezen a területen nem látjuk szükségesnek szabályokat hozni, mert a szolgáltatók saját érdekből is megteszik a szükséges beállításokat.

Előfizetői adatbázis feltérképezése

Tömeges SRI for SM üzenetek küldése különböző telefonszámokra

A válaszokból a következő információk nyerhetők ki ha nincs Home Router:

- Mi az előfizető IMSI azonosítója
- Az előfizető aktív-e a hálózatban
- Melyik központ kezeli az adott előfizetőt. Ha ismert, hogy egy adott MSC vagy VLR milyen földrajzi területeket fed le, akkor a válaszok alapján térképezhető a felhasználók elhelyezkedése (Magyarországon ez nem releváns a poolba rendezett hálózati elemek miatt).
- A számhordozhatósági információk. Ha egy számot egy másik hálózat kezel, az SRI válaszban egy Routing Number jelenik meg, amelyből következtetni lehet a számhordozhatóságra.

Egy mobilhálózat előfizetőinek feltérképezése az SRI for SM üzenetek tömeges lekérdezésével jogi és etikai aggályokat vet fel, mivel személyes és helymeghatározási adatokhoz lehet hozzáférni. Az ilyen műveletek végrehajtása engedély nélkül jogellenes lehet és súlyos adatvédelmi következményekkel járhat.

A fenti problémák mellett a tömeges lekérdezés jelentős terheléseket is okozhatnak bizonyos időszakban, ezért is célszerű az ilyen típusú lekérdezéseket már a mobil hálózatok határán megfogni.

- Nemzetközi irányból bejövő tömeges SRI for SM-ek esetében amikor látszik, hogy a cél az előfizetői adatbázis feltérképezése, akkor ott érdemes a feladó cím automatikus blokkolásán elgondolkozni. Pl, ha 1 percen belül 1000 darab SRI for SM érkezik ugyanarról a címről és a lekérdezésben szereplő MSISDN szám nem létező, akkor feltételezhető, hogy visszaélésről van szó. Ezt hívják úgy hogy Rate Limit figyelés.

Nemzetközi példák

INT call blocking in UK

A letiltás a fogadott, Egyesült Királyságbeli számot tartalmazó PAID (P-Asserted-Identity) tartalmán alapul, az alábbiak szerint:

- A +447-es tartományból származó CLI-vel érkező hívásokat nem szabad blokkolni. Ezzel biztosítható, hogy a tengerentúlon barangoló brit mobilügyfelek vissza tudjanak hívni az Egyesült Királyságba.
- A mobilállomás barangolási szám (MSRN)/nemzetközi barangolási szám (IRN) tartományon belüli célszámokra irányuló hívásokat nem szabad letiltani. Ez annak biztosítására szolgál, hogy az Egyesült Királyságbeli számokról érkező, az Egyesült Királyságba barangoló tengerentúli ügyfelekre irányuló hívások ne legyenek blokkolva.
- Ha az Egyesült Királyságon kívüli hálózatok az alábbi vonatkozó feltételek valamelyikének megfelelő hívásokat küldenek, akkor a fogadó Egyesült Királyságbeli szolgáltatónak meg kell kérnie, hogy az összekapcsolást az Egyesült Királyságból származó és nem az Egyesült Királyságból származó forgalomra szegmentálják. Csak az utóbbi útvonalon szabad a forgalmat blokkolni.

  A vonatkozó feltételek a következők:

  - A forgalom az Egyesült Királyság hálózatáról indult, vagy
  - A forgalom tengerentúli csomópontokon tárolt Egyesült Királyságbeli ügyfelektől származik, ill
  - A forgalom a felhőszolgáltatásokon üzemeltetett brit ügyfelektől származik.

Source: NICC ND 1447

USA megoldás

2019-ben az Egyesült Államok Kongresszusa elfogadta a „Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act” („TRACED Act”) törvényt, amely az év végén lépett hatályba. A TRACED törvény arra utasította a Szövetségi Kommunikációs Bizottságot (FCC), hogy kötelezze az iparágat a hívófél-azonosító hitelesítési eljárások kidolgozására, és olyan szabályok kibocsátására, amelyek megvédik az előfizetőket a nem kívánt hívásoktól vagy szöveges üzenetektől, amelyek nem hitelesített hívóazonosítót használnak.

A TRACED törvény végrehajtása érdekében az FCC számos határozatot hozott, amelyek a következőkhöz vezettek:

- A Robocall mérséklési adatbázis létrehozása – Az Egyesült Államokban működő hangszolgáltatóknak nyilatkozatot kell regisztrálniuk az adatbázisban arról, hogy teljes mértékben megvalósítják a STIR/SHAKEN keretrendszert, vagy dokumentálják ésszerű eljárásaikat a nem kívánt hívások csökkentésére. 2021. szeptember 18-tól az egyesült államokbeli székhelyű hangszolgáltatók már nem fogadhatnak hívásokat közvetlenül az adatbázisban nem szereplő egyesült államokbeli szolgáltatóktól.
- Az egyesült államokbeli összes hangszolgáltatónak 2021. június 30-ig teljes mértékben be kellett vezetnie a STIR/SHAKEN szabványt. Ez magában foglalta a 100000-nél kevesebb előfizetői vonallal rendelkező kis szolgáltatók számára a mentesítést, eredetileg 2023. június 30-ig. Ezt a határidőt később lerövidítették. 2022. június 20. A megrendelés a kisméretű, nem IP-szolgáltatókra vonatkozó folyamatos mentességet is tartalmazott.
- 2023. június 30. óta a nemzetközi átjáró-szolgáltatóknak regisztrálniuk kell a Robocall Mitigation Database-ben, és be kell vezetniük a SHAKEN/STIR-t, ha az Egyesült Államokban az észak-amerikai számozási terv (NANP) CLI-jeivel kívánnak hívást befejezni. Az Egyesült Államokban működő hangszolgáltatóknak tilos lesz NANP CLI-hívásokat fogadniuk az adatbázisban nem regisztrált átjárókról.

2023 végétől a köztes szolgáltatóknak regisztrálniuk kell a Robocall-mérséklési adatbázisban, SHAKEN/STIR hitelesítést kell alkalmazniuk azoknál a hívásoknál, amelyeket a kezdeményező szolgáltató nem hitelesített, és az „Ismerd meg az ügyfelet” átvilágítást a upstream szolgáltatóknál.

Francia megoldás

A francia elektronikus hírközlési, postai és nyomtatott sajtót szabályozó hatóság (ARCEP) számos szabványos előírást vezetett be a CLI-hamisítás (E.164 + kezelt tiltólisták) leküzdésére. Ezen túlmenően a 2019-0954 határozat [5] hivatkozik a „STIR/SHAKEN" protokollokra, amelyek valószínűleg egy hosszú távú megoldás alapját képezik a hívóazonosító szám hitelesítés iránti növekvő igény kielégítésére. A tesztelés érdekében az ARCEP már bevezetett bizonyos tartományokat (földrajzi, mobil és nem földrajzi számokhoz), amelyek a hitelesített számoknak vannak fenntartva.

A törvény további, 2020. július 24-től hatályos kiegészítése előírja, hogy az üzemeltetőknek le kell tiltaniuk azokat a hívásokat, amelyek francia CLI-vel rendelkeznek, de olyan szolgáltatóhoz kapcsolódnak, amely általában nem nyújt távközlési szolgáltatásokat a végfelhasználóknak Európában. Ezenkívül a törvény előírja, hogy minden szolgáltató 36 hónapon belül alkalmazzon valamilyen híváshitelesítési módszert.

Az ARCEP által vezetett MAN (Mécanisme d'Authentification des Numéros) munkacsoport legutóbbi döntései a következők:

- Néhány kezdeti fenntartás ellenére a STIR/SHAKEN-t választották preferált megoldásként Franciaországban, mivel kereskedelmi forgalomban kapható és viszonylag megvalósítható az integrációhoz. A STIR/SHAKEN bevezetésének kezdeti dátumát 2023. július 24-re tűzték ki. Az MAN munkacsoport azonban elismeri, hogy ez a technológia nem lesz képes kezelni az összes CLI-manipulációs esetet, és további fejlesztést igényel. 2023 után további fejlesztésekre lesz szükség.
- Határokon átnyúló: Az MAN munkacsoport és a francia hatóságok elismerik, hogy a CLI-hamisítás határokon átnyúló együttműködést igénylő probléma. A CLI-k határokon átnyúló érvényesítésének szükségességét hallgatólagosan elismerik, de jelenleg nincsenek konkrét javaslatok ezen a területen.

Lengyel megoldás

A Lengyel Miniszterek Tanácsa 2022. november 15-én elfogadta az elektronikus hírközlésről szóló törvénytervezetet, amely végrehajtja az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló (EU) 2018/1972 irányelvet. Az új szabályozás kiterjed a hagyományos távközlési üzletágakra, de a felsőbb szintű szolgáltatások üzemeltetőire is. A CLI érvényesítésének már bevezetett módszerei a következők:

- Roaming állapotellenőrzés – ez a megoldás a hívások befejezésére vonatkozik, amikor a mobilfelhasználó CLI-jét ellenőrzik a roaming állapotával. Az állapotot a nemzeti szolgáltatók és a CAMEL segítségével ellenőrzik a mobilfelhasználó állapotának ellenőrzése a kimenő látogatott mobilhálózatban.
- Szabványos gyakorlatok, beleértve a kezelt tiltólistákat és az ITU-T E.164. ajánlásának való megfelelést.

Németországi megoldás

A 2021. évi német távközlési törvény (TKMG) [11] új megoldást vezetett be a CLI-érvényesítéshez:

- Roaming állapotellenőrzés, ahol minden végződő hívás ellenőrzi, hogy a CLI megfelel-e a roaming állapotnak. Az állapot ellenőrzése a CAMEL (néha CAMEL triggerelésnek is nevezik) segítségével történik a mobilfelhasználó állapotának ellenőrzésére a kimenő látogatott mobilhálózatban.
- Ezenkívül Németország egy sor szabványos gyakorlatot alkalmaz: DNO a segélyhívó és magas biztonsági számok (pl. 112, bankok) számára; ITU-T E.164 ajánlás és kezelt tiltólista.
- A csatlakozásban részt vevő valamennyi nyilvánosan elérhető távközlési szolgáltatónak gondoskodnia kell arról, hogy a német számtartományban országosan jelentős szám csak akkor jelenjen meg a hívó fél számaként, ha a kapcsolat a nyilvános német telefonhálózatról történik.

Ír megoldás

A [omReg ír szabályozó hatóság azt javasolja, hogy a távközlési szolgáltatók hajtsanak végre számos technikai beavatkozást a csaló hívások és szöveges üzenetek leküzdésére, az alábbiak szerint:

- Javított CLI-blokkolás: Megakadályozza, hogy a külföldön elkövetett csalók ír földrajzi számokat (pl. 01-xx) hamisítsanak átverő hanghívások indításához.
- Mobil CLI blokkolás: Megakadályozza, hogy a külföldön elkövetett csalók ír mobilszámokat (pl. 087-xx) hamisítsanak, hogy átverő hanghívásokat indíthassanak.
- Védett számok listája: Megakadályozza, hogy a csalók olyan számokat használjanak, amelyeket még nem használnak, vagy amelyeket még ki kell osztani egy távközlési szolgáltatónak, mielőtt a szolgáltatásba lépnének.
- Nem induló lista: Lehetővé teszi a vállalkozások/szervezetek számára, hogy biztosítsák a kimenő hívásokhoz soha nem használt számaikat azáltal, hogy a távközlési szolgáltatók blokkolják azokat a hívásokat, amelyek úgy tűnik, hogy ezekről a számokról jönnek.
- Hangtűzfalak: A kéretlen hívások blokkolása, bárhol is érkezzenek (Írországban vagy külföldön), és véd a jövőbeni kifinomultabb csalások ellen.

A Comreg egy SMS azonosító nyilvántartás létrehozását is javasolja. Ez lehetővé tenné a vállalkozások/szervezetek számára, hogy regisztráljanak SMS-küldőazonosítót. A távközlési szolgáltatók ezután blokkolnának minden olyan üzenetet, amely küldőazonosítót tartalmaz a nyilvántartásban szereplőktől eltérő forrásokból.

A ComReg egy SMS-átverési szűrő iparági bevezetését is javasolta az átverő SMS-ek blokkolására és a jövőbeli, kifinomultabb csalások elleni védelemre, de ehhez a bevezetést megelőzően alátámasztó jogszabályra lenne szükség..

Finn megoldás

A Finn Közlekedési és Hírközlési Ügynökség, a Traficom 2022. május 16-án elfogadta 28. rendeletének frissített változatát [16], [17]. Új kötelezettségeket ró a távközlési szolgáltatókra, hogy megakadályozzák a hívóazonosító-hamisítást és a csaló hívások átadását a címzettekhez. A frissített rendelet célja, hogy megakadályozza a finn telefonszámok használatát a nemzetközi kiberbűnözésben, és csökkentse a külföldről érkező csaló hívások számát. A hamisított számok használatának megakadályozására vonatkozó kötelezettségek fokozatosan lépnek életbe: a vezetékes telefonszámokra 2022. július 1-től, a mobilhálózati számokra pedig 2023. október 2-tól lépnek hatályba.

Két módszert kínálnak a bejövő nemzetközi hívások CLI-inek érvényesítésére, amelyeket a szolgáltatók számára javasolnak, és amelyek jelentős alapként használhatók a hívásblokkoláshoz:

1. Távközlési szolgáltatók közötti bejövő hívások érvényesítése

a) A nemzetközi hívást végző fogadó távközlési szolgáltató, amelyben a hívó fél száma finn mobilszám, számhordozási lekérdezést hajt végre a hívó számra vonatkozóan.

b) Ha az (a) lépésben a lekérdezés sikeres, a távközlési szolgáltató ellenőrzi, hogy a hívó előfizető éppen hol tartózkodik.

c) A fenti ellenőrzések alapján a távközlési szolgáltató dönti el, hogy a hívott előfizetőhöz kapcsolható-e a hívás. Ha az ellenőrzések sikeresek és a hívó előfizető külföldön tartózkodik, a hívást főszabály szerint minden egyéb intézkedés nélkül hozzá lehet kapcsolni a hívott előfizetőhöz. Más esetekben a hívást más meghatározott intézkedéseken (általában blokkolva) kell elvégezni.

2. A bejövő hívások ellenőrzése proxy szerverrel

a) A hívó fél számára vonatkozó információ elküldésre kerül a proxy szervernek. A kérelmet küldő távközlési szolgáltatónak nem kell ismernie azt a mobilhálózat-szolgáltatót vagy szolgáltatót, amelynek ügyfele az előfizető.

b) A proxyszerver továbbítja a kérést a megfelelő mobilhálózat-szolgáltatónak, amely a kérésre úgy válaszol, hogy elküldi a proxyszervernek az előfizető aktuális roaming állapotát.

c) A proxy szerver a választ továbbítja az eredeti kérelmet benyújtó távközlési szolgáltatónak. A válaszban szereplő információk alapján az üzemeltető eldönti, hogy a hívott előfizetőhöz tudja-e kapcsolni a hívást.