Nemzeti Média- és Hírközlési Hatóság

Az 5G hálózatok biztonsági kihívásai

Dr. Bartolits István
Technológiaelemző Főosztály

Információbiztonság aktuális kihívása
PTE-NMHH-HTE-NJSZT tudományos konferencia 2023. október 25.

TARTALMI VÁZLAT

- Az 5G rendszer célkitűzései
- Az 5G rendszertechnikából adódó biztonsági kérdések
- Az 5G kezdeti konfigurációjából adódó biztonsági kérdések
- A RAN hálózat biztonsági kihívásai
- A hálózatszeletelés és a biztonság

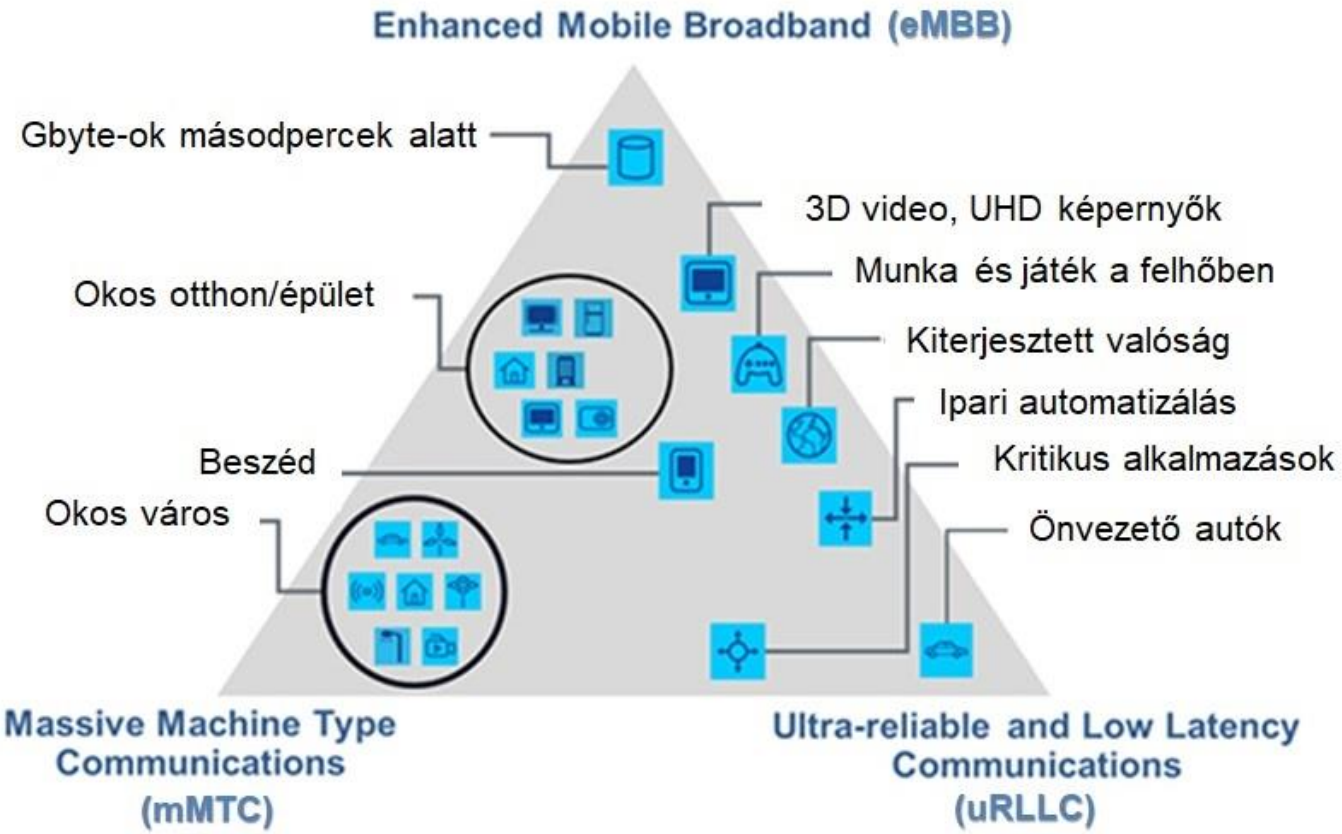
Az 5G rendszer célkitűzései

AZ 5G RENDSZERREL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK

Az IMT-2020 legfontosabb célkitűzései (ITU-T Focus Group, 2015) :

- Magas felhasználói adatsebesség
- Igen nagy felhasználó-sűrűség kiszolgálása
- Igen kicsi késleltetés és magas megbízhatóság
- Tárgyak nagy tömegben történő hálózatra kapcsolása (IoT)
- Nagy sebességű mozgás (mobilitás) esetén is változatlan minőség
- Emelt szintű multimédia szolgáltatás
- Konvergens alkalmazások differenciált kezelése

AZ 5G RENDSZER KÖVETELMÉNYHÁROMSZÖGE



ÚJ ALAPELVEK, ÚJ BIZTONSÁGI KIHÍVÁSOK

- Az 5G rendszer összetettebb funkciókat fog betölteni, mint a korábbi mobil rendszerek
- Az 5G rendszer sokkal szélesebb szolgáltatási palettát fog nyújtani, mint a korábbi rendszerek
- Az 5G rendszer sokkal több adatot fog kezelni – és így sokkal több adatot is őrizhet, társíthat – mint az előző mobil rendszerek

Következmény: A biztonság kulcskérdéssé válik, meg kell őrizni a bizalmat

- ITU-T SG17: Security tanulmányi csoport

AZ ITU-T 5G VÉGTŐL-VÉGIG BIZTONSÁGI VÁZA

Végberendezés biztonság	Hozzáférési hálózat biztonság	Maghálózat biztonság	Szolgáltatás és alkalmazás biztonság
Malwares Side channel attacks Zombies	Air interface security Fronthaul & backhaul security MEC security SDN/NFV security Cloud security	Network capability exposure security Inter network security SBA security Network slicing security SDN/NFV security Cloud security	Service security Big data security Web security Information security Cloud security

Általános biztonsági eszközök		
	Cryptography (including Quantum-safe Cryptogr.)	IDM PKI AI/ML (DLT)
	Security situation awareness	Authentication technologies (incl. Biometrics)
	Security emergency response	Threat intelligence handling
		Security testing and certification

AZ ITU-T 5G VÉGTŐL-VÉGIG BIZTONSÁGI VÁZA

Végberendezés biztonság	Hozzáférési hálózat biztonság	Maghálózat biztonság	Szolgáltatás és alkalmazás biztonság
Malwares Side channel attacks Zombies	Air interface security Fronthaul & backhaul security MEC security SDN/NFV security Cloud security	Network capability exposure security Inter network security SBA security Network slicing security SDN/NFV security Cloud security	Service security Big data security Web security Information security Cloud security

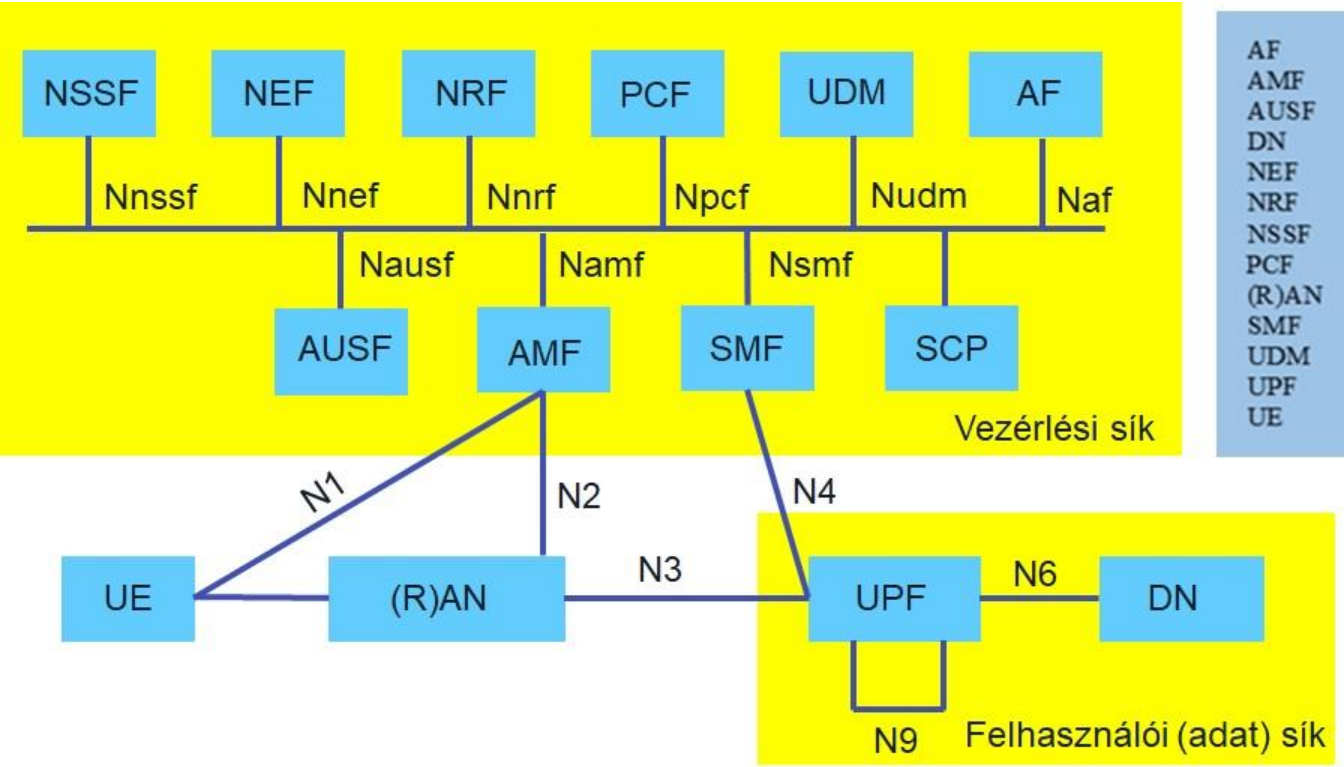
Általános biztonsági eszközök		
	Cryptography (including Quantum-safe Cryptogr.)	IDM PKI AI/ML (DLT)
	Security situation awareness	Authentication technologies (incl. Biometrics)
	Security emergency response	Threat intelligence handling
		Security testing and certification

Az 5G rendszertechnikából adódó biztonsági kihívások

RENDSZERTECHNIKAI CÉLKITŰZÉSEK

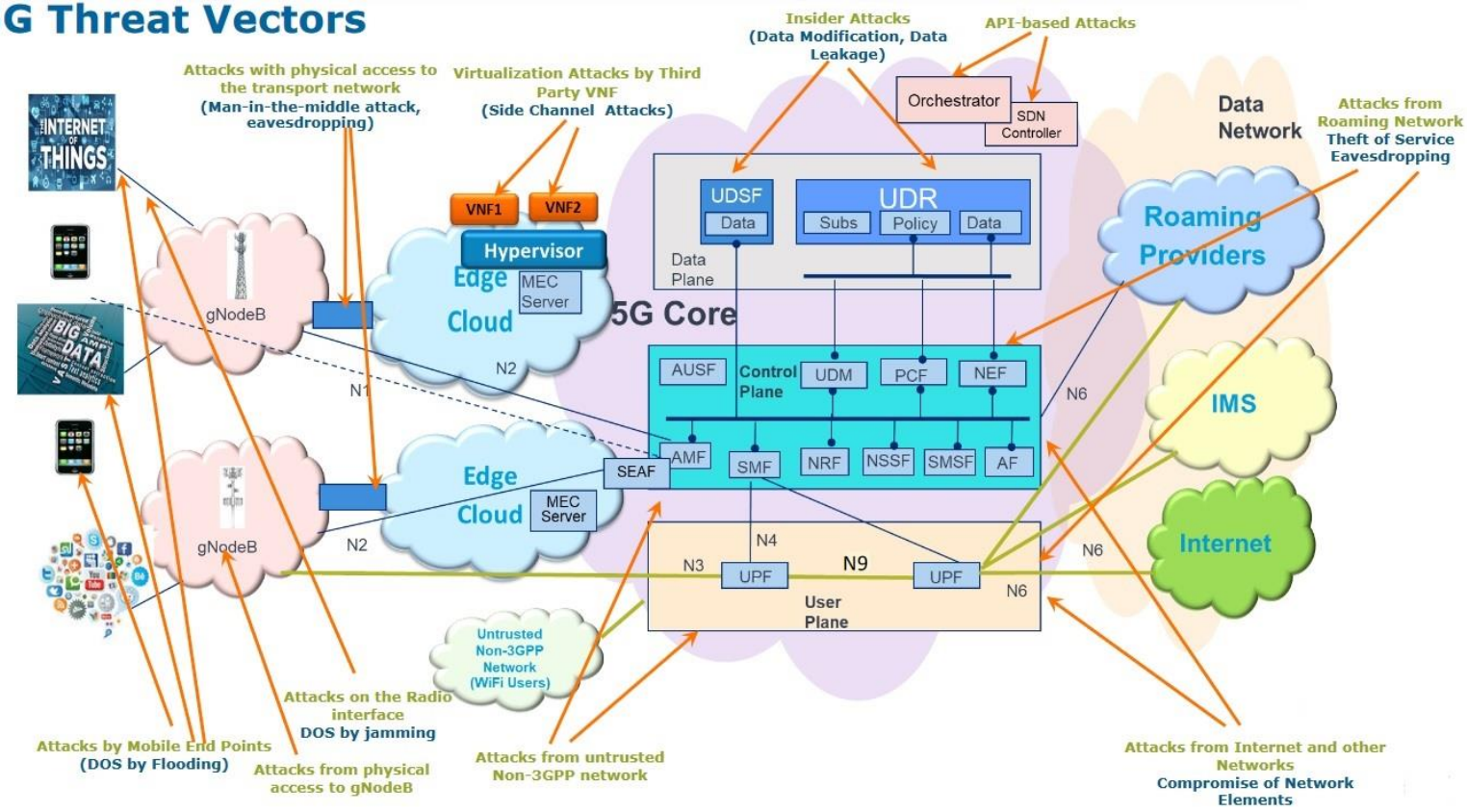
- Az 5G rendszertechnika alapvető célkitűzései
  - Lapos hálózati architektúra
  - Az SDN és NFV alapelvek maximális használata
  - A vezérlési sík (control plane) és az adatsík/felhasználói sík (user plane) elválasztása
  - Minden funkció önálló egységbe szervezése – felhőnatív megoldások támogatása
  - Erőforrások optimális kihasználása az alkalmazásoknak megfelelően – hálózatszeletelés (network slicing)
  - Magasszintű koordináció – orkesztráció (orchestration) a teljes 5G rendszer felett

AZ 5G REFERENCIAMODELL ÉS A SERVICE-BASED ARCHITECTURE (SBA)



AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
DN	Data Network
NEF	Network Exposure Function
NRF	NF Repository Function
NSSF	Network Slice Selection Function
PCF	Policy Control Function
(R)AN	(Radio) Access Network
SMF	Session Management Function
UDM	Unified Data Management
UPF	User Plane Function
UE	User Equipment

TÁMADÁSI PONTOK AZ 5G RENDSZERTECHNIKÁBAN



Forrás: Dr. Ashutos Dutta, AT&T

A 3GPP FELADATMEGOSZTÁSA ÉS MUNKACSOPORTJAI

Rádiós hozzáférési hálózat (RAN) TSG	Szolgáltatási/Rendszer Aspektusok (SA) TSG	Maghálózat & végberendezés (CT) TSG
RAN WG1 Layer 1 (Physical) space	SA WG1 Service requirements	CT WG1 Mobility management, Call control, Session management
RAN WG2 Layer 2 and 3 protocols	SA WG2 Architecture	CT WG2 Policy, QoS and interworking
RAN WG3 Access network interfaces +O&M	SA WG3 Security	CTWG3 Network protocol
RAN WG4 Performance requirements	SA WG4 Codecs, multimedia system	CT WG4 Smart card application
RAN WG5 UE conformance testing	SA WG5 Telecom management	
RAN WG6 Legacy RAN	SA WG6 Mission-critical services	

A MULTI-ACCESS EDGE COMPUTING (MEC)

- A kis késleltetésű rendszerek kulcsa az információ közeli ponton történő feldolgozása.
- A lehetséges megoldás: Multi-access Edge Computing, korábban: Mobile Edge Computing (MEC)
- A hálózat peremén működő autonóm feldolgozó egység
- Szerepe lehet pl. a közlekedési infrastruktúrában (önvezető autók, váratlan közlekedési információk stb.)
- Közvetlenül a RAN hálózat adatainak a feldolgozása a központi rendszer beavatkozása nélkül Igen kis késleltetés (!)
- A teljes hálózat számára csak az aggregált adatok kerülnek megadásra – itt már a késleltetés nem lényeges
- Több helyen nevezik „fog computing”-nak is

A MEC ÉS AZ EDGE CLOUD BIZTONSÁGA

- A hálózaton akár több száz vagy több ezer MEC is működhet
- Lehetséges támadási pontok:
  - Nem biztonságos felhordóhálózat a MEC és a RAN hálózat elemei között
  - Amennyiben a MEC és a maghálózat nyilvános interneten van összekapcsolva, akkor támadás az internet felől
  - Megosztott infrastruktúra használata harmadik felek alkalmazásainál

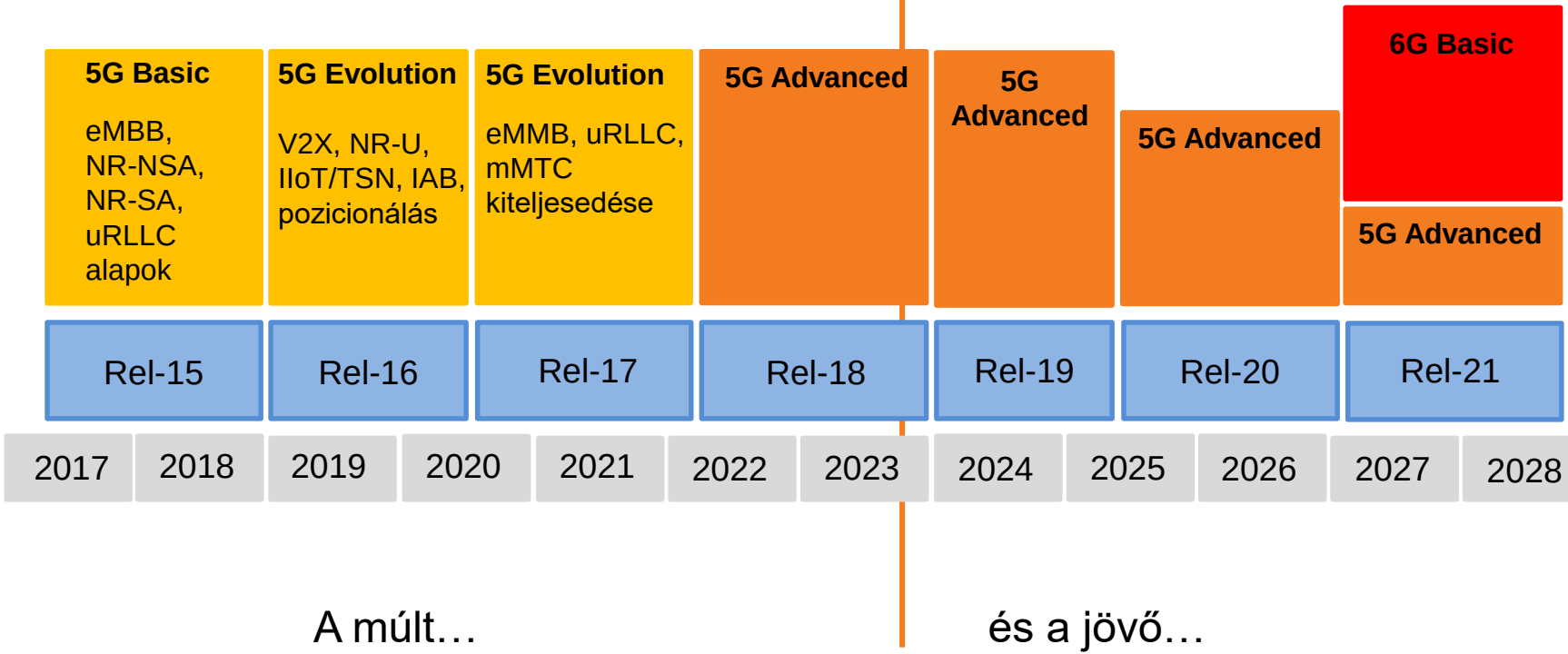
A KVANTUMBIZTOS KRIPTOGRÁFIA BELÉPÉSE

Küszöbön áll a kvantumszámítógépek kereskedelmi megjelenése

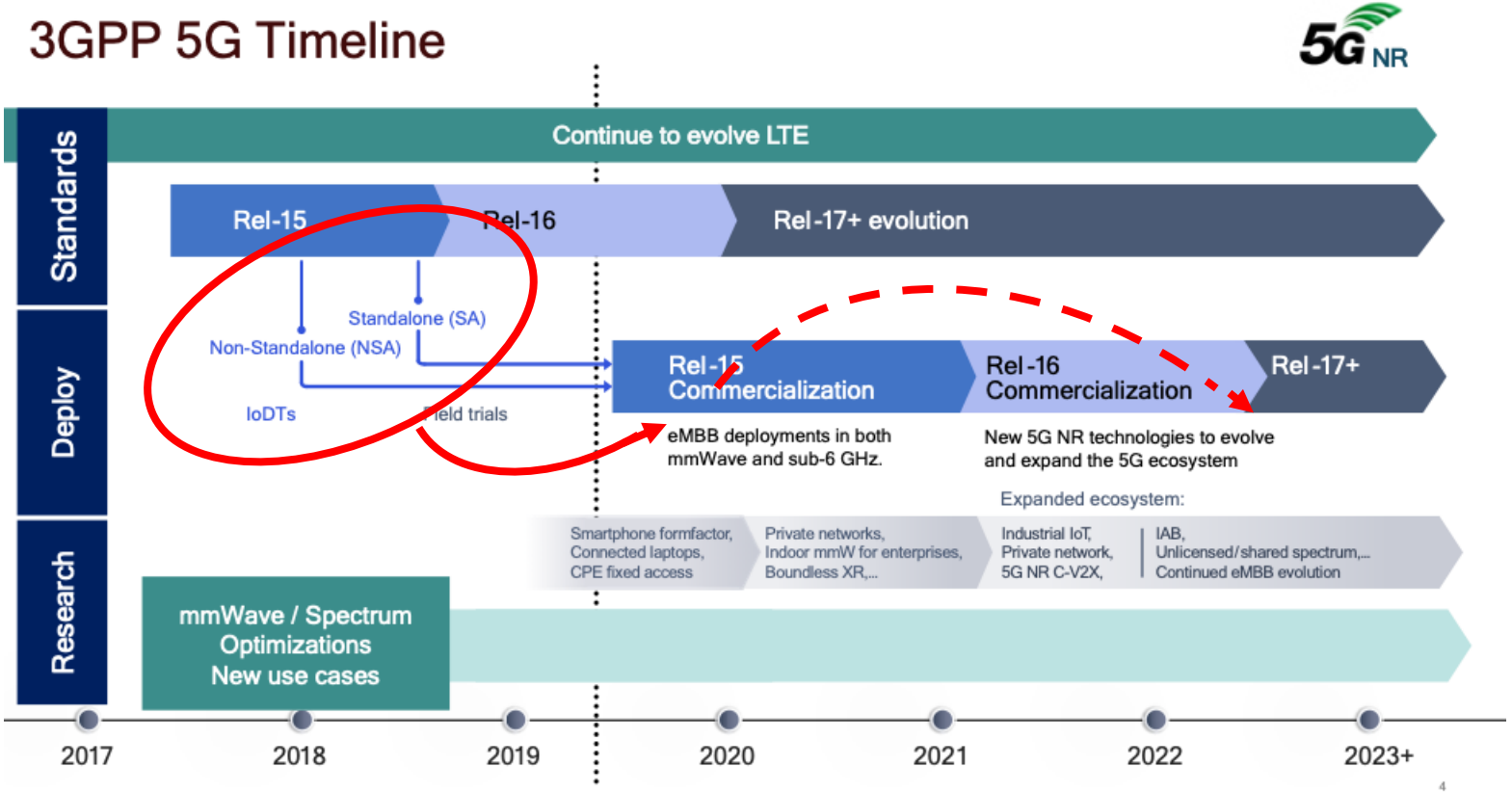
- A jelenlegi rendszerekhez képest drasztikus kapacitás- és sebességnövekedés
- A nagy számítási igény által védett kriptográfiai megoldások ezzel pillanatok alatt feltörhetővé válnak
- Peter Shor (1994): az RSA, az ECDSA, az ECDH és a DSA törhetővé válik
- Helyettük poszt-kvantum titkosításra van szükség
- Erre 2021 végén már született hazai jogszabály is (2013. évi L. tv. módosítása)
- A világ első poszt-kvantum 5G SIM kártyája: IDEMIA 2021. dec.

Az 5G kezdeti konfigurációjából adódó biztonsági kihívások

A SZABVÁNYOSÍTÁSI MENETREND KÉT FONTOS KÖVETKEZMÉNYE

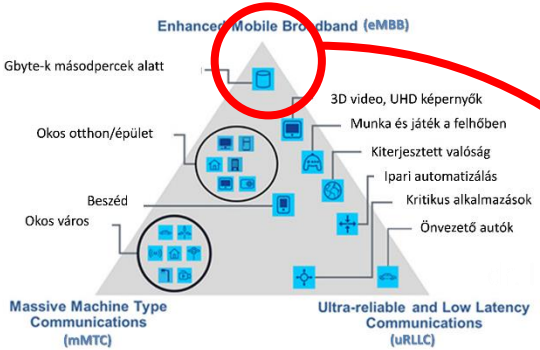


A TYÚK VAGY A TOJÁS PROBLÉMA ÉS MEGOLDÁSA
5G Non Standalone és 5G Standalone New Radio



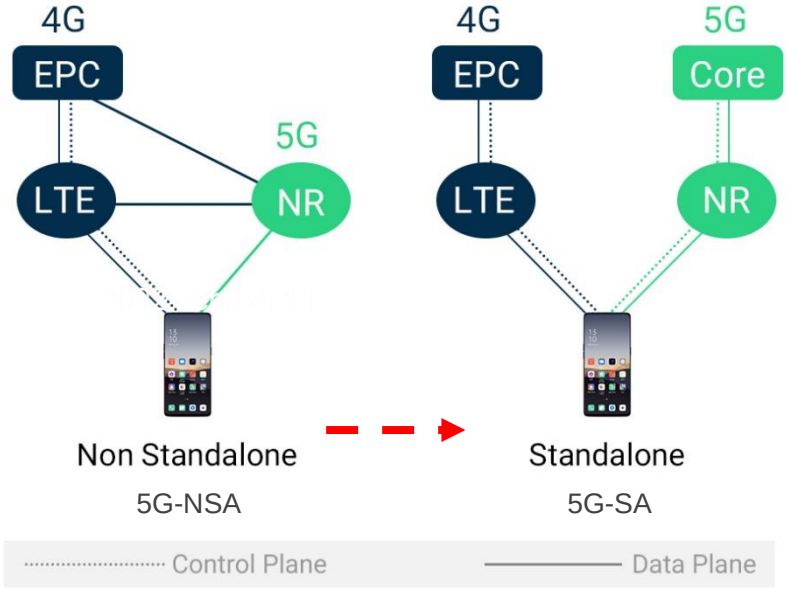
A TYÚK VAGY A TOJÁS PROBLÉMA ÉS MEGOLDÁSA

5G Non Standalone és 5G Standalone hálózat



ITU-T követelmények

4G hálózat + 5G NR (New Radio)
ez legyen a kezdeti megoldás



- A megoldás tökéletes az induláshoz, de megtartja a 4G hálózat korlátait.
- Amíg ezek a korlátok nem zavaróak, addig növelhető az eMBB, a mobil szélessáv élménye.
- Az 5G többi előnye viszont csak az 5G standalone hálózaton tud érvényesülni.

A SZABVÁNYOSÍTÁSI MENETREND KÉT FONTOS KÖVETKEZMÉNYE

Első következmény:

- A Non Standalone rendszerek még a 4G rendszer biztonsági szintjét képviselik, csak a rádiós hozzáférési hálózatban jelenik meg az 5G rendszer. Az összes 5G maghálózati védelem ebből még hiányzik!!!

Második következmény:

- A teljes – végtől végig terjedő – biztonsági megoldások csak a Release 17 telepítése után lesznek jelen a hálózatban
- A Release 17 2022-ben elkészült, de még nem kezdték meg a szolgáltatók a telepítését
- Továbbra is főként 5G NSA rendszerek üzemelnek a világban

TOVÁBBI BIZTONSÁGI MEGFONTOLÁSOK

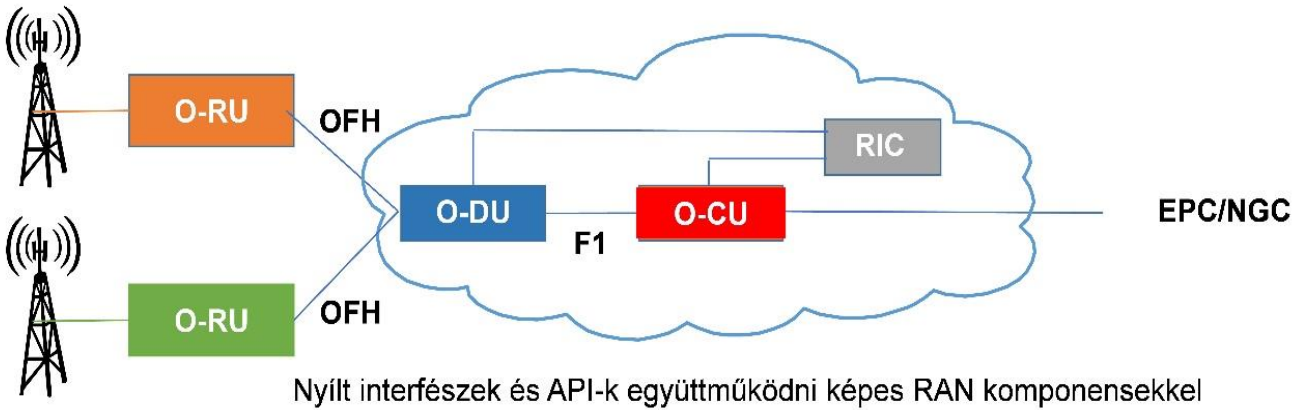
- Az LTE rendszer a korábbi RADIUS helyett bevezette a DIAMETER protokollt az autentikáció, az autorizáció és a számlázás rendszerében. A DIAMETER rendelkezett néhány biztonsági problémával, de az 5G is a DIAMETER-t használja
- Az 5G az SDN és az NFV bevezetésével a HTTP és a REST API protokollokat is használja – ezeket a weben is sikerrel támadják a hackerek
- Az 5G a megfogalmazott követelményeknek megfelelően flexibilis és erőteljesen konfigurálható , de ez rejtett biztonsági problémákat hozhat elő a későbbiekben
- A későbbiekben várható több millió IoT eszköz a botnetek sokaságával támadhatja a rendszert

A RAN hálózat biztonsági kihívásai

AZ OPEN RAN KEZDEMÉNYEZÉS HÁTTERE

- A beszállítók rendszerei olyan specifikus interfészeket használnak a megosztott RAN hálózatban, ahol a belső interfészek nem egységesek
  - Következmény: a kiválasztott beszállító kvázi monopolhelyzetbe kerül
  - Megoldására magalakult az O-RAN Alliance és olyan interfészt dolgoztak ki, ahol a RAN hálózat elemei beszállító-függetlenek
- Az EU Toolbox on 5G cybersecurity egyik kívánalma:
  - Biztosítják, hogy minden szolgáltató megfelelő, több értékesítőre kiterjedő stratégiával rendelkezzen **az egyetlen beszállítótól** (vagy több, hasonló kockázati profillal rendelkező beszállítótól) **való jelentős függés elkerülése vagy korlátozása érdekében**, így biztosítva nemzeti szinten a beszállítók közötti megfelelő egyensúlyt és **elkerülve a magas kockázatúnak tekintett beszállítóktól való függést**; ehhez el kell kerülni az egyetlen beszállítótól való függést, többek között a berendezések nagyobb interoperabilitásának előmozdítása révén;

AZ O-RAN MEGOLDÁS ALAPGONDOLATA



Nyílt interfészek és API-k együttműködni képes RAN komponensekkel
NFV modulok és referencia architektúra
Intelligencia és automatizmus a Plug and Play számára

O-RU – Open Remote Unit
OFH – Open Fronthaul
O-DU – Open Distributed Unit
RIC – RAN Intelligent Controller
O-CU – Open Centralized Unit

AZ OPEN RAN BIZTONSÁGI KÉRDÉSEI

Az O-RAN Alliance intenzíven dolgozik a specifikáción
A felmerülő biztonsági kérdések:

- Az RU és a DU közötti integritás megteremtése biztonsági résektől mentesen, megfelelő titkosítási algoritmusok használata
- Egységes biztonsági rendszer kidolgozása a megosztott funkciókra
- Az egységes menedzsment rendszer biztonságos kialakítása TLS (Transport Layer Security) és digitális aláírás használatával
- Az O-RAN platformok, komponensek és alkalmazások teljes mértékű biztonsági rendszere

Ezeknek és más felmerülő biztonsági kérdéseknek a kezelésére az O-RAN Alliance külön biztonsági csoportot hozott létre.

AZ OPEN RAN BIZTONSÁGI KÉRDÉSEI

Az Európi Unió friss dokumentuma:

- 2023. május 11.: Report on the cybersecurity of Open RAN, (EB & ENISA közös dokumentum)
- A dokumentum a szabványosítóknak további munkát, a tagországoknak pedig óvatosságot javasol a bevezetést illetően
- Javaslatok az 5G Toolbox eszköztárának a kibővítésére (szabályozási és műszaki jellegű felvetések)

Ezzel együtt az Open RAN kidolgozása halad előre és egyre inkább az intelligens megoldások felé mozdul el – nem lehet leírni a gondolatot, de nem tudni, mikorra lesz érett

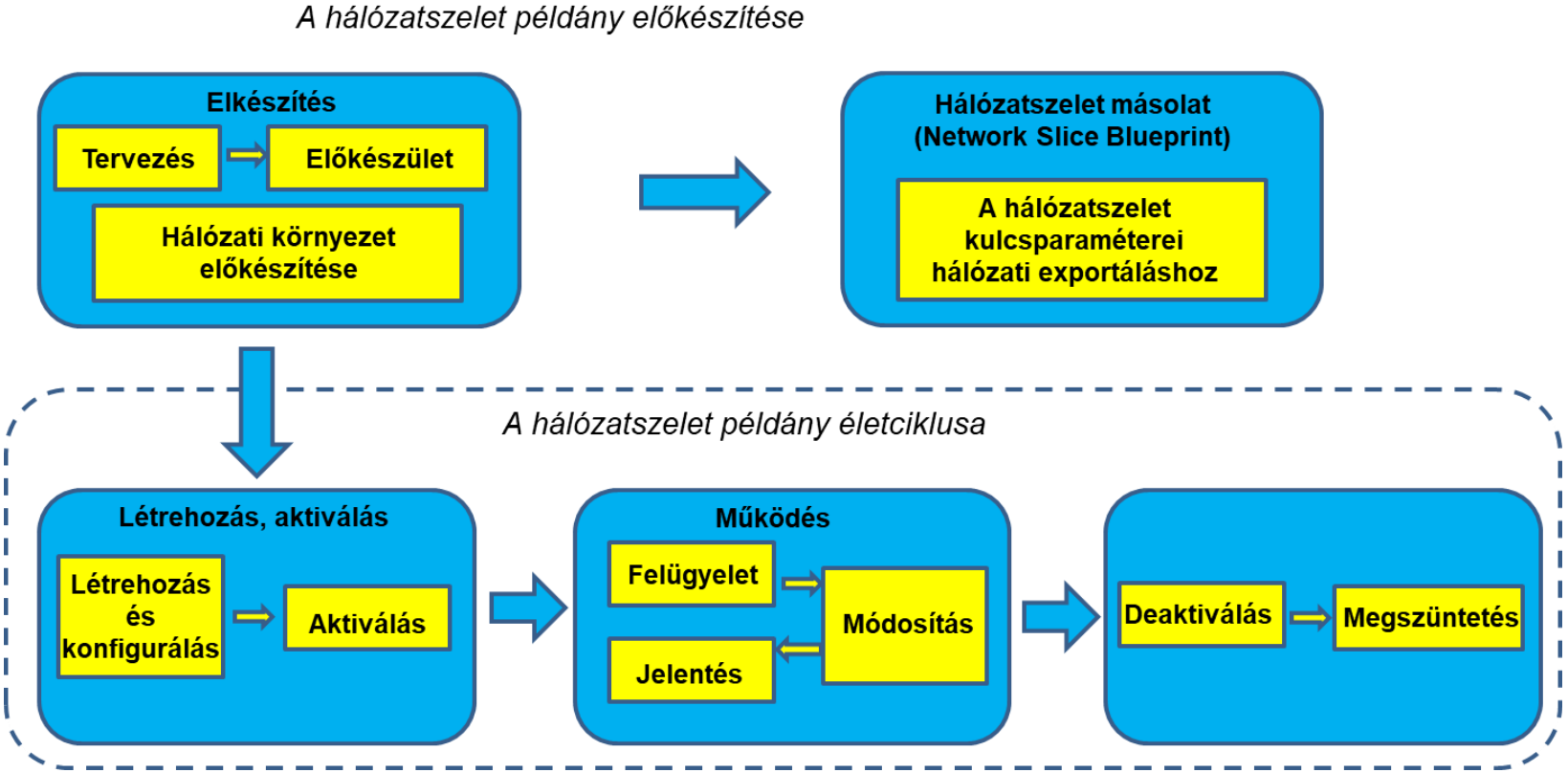
A hálózatszeletelés és a biztonság

AZ ERŐFORRÁSOK OPTIMALIZÁLÁSA: A HÁLÓZATSZELETELÉS (NETWORK SLICING)

Az 5G hálózatoknak az egymással ellentétes követelményeket egyszerre kell kielégíteniük

- Következmény: Olyan hálózat kell, melyben rugalmasan allokálhatók az erőforrások
- Az „ellentmondó” követelmények kezelésére az új elv a Network Slicing, a hálózatszeletelés elve
- A hálózatszeletelés elve lehetőséget ad a szolgáltatóknak arra, hogy az alkalmazási szükségletnek megfelelően optimalizált, végtől-végig terjedő virtuális hálózatot hozzon létre a szükséges mennyiségű erőforrással

AZ 5G HÁLÓZATSZELET ÉLETCIKLUSA



A HÁLÓZATSZELETELÉS ÉS A BIZTONSÁG

A hálózatszeletelés tehát az erőforrások optimális kiosztását hivatott megvalósítani

- Az erőforrások egy része a felhőnatív megoldásokban bővíthető
- Az erőforrások más része ugyanúgy korlátos, mint eddig (pl. átviteli kapacitások)
- Az ideális hálózatszeleteléshez célszerű a mesterséges intelligencia képességeit (is) használni
- Megakadályozandó viszont, hogy szélsőséges vagy hamis igényekkel egy hálózatszelethez indokolatlan mennyiségben rendeljen hozzá erőforrásokat – erre az orkesztrációs rendszernek is fel kell készülnie

Köszönöm a figyelmet!