Sítě páté generace z hlediska bezpečnosti

Verze 0.9.0

k doplnění a připomínkám

kolektiv autorů VNICTP ve spolupráci s akademickou sférou

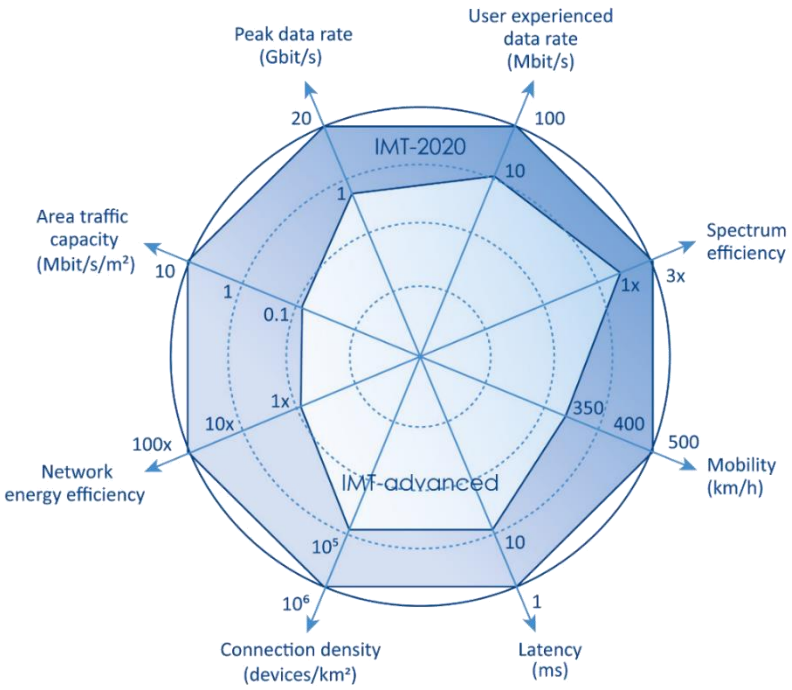
Proč potřebujeme mobilní sítě páté generace

Datový provoz v mobilních sítích velmi rychle roste, je to způsobeno především díky streamování videa. S více zařízeními má každý uživatel rostoucí počet připojení. Internet věcí (IoT) bude vyžadovat sítě, které budou muset zvládat připojit další miliardy zařízení. S rostoucím počtem mobilních telefonů a rostoucím datovým provozem potřebují mobilní zařízení i sítě zvýšit i svou energetickou účinnost. Provozovatelé sítí jsou pod tlakem, aby snížili provozní výdaje, protože uživatelé si zvykli na paušální tarify a nechtějí platit více.

Sítě páté generace nabízí nové možnosti použití (např. pro aplikace které potřebují velmi nízkou latenci nebo vysokou spolehlivostí). Technologie 5G by tedy měla přinést výrazně vyšší provozní výkon (např. zvýšenou spektrální účinnost, vyšší datové rychlosti, nízkou latenci) a také vynikající uživatelskou zkušenost.

Mobilní sítě páté generace

5G (neboli pátá generace bezdrátových sítí) je telekomunikační standard mobilní sítě, který technicky navazuje na standard 4G LTE. Hlavním přínosem nové technologie je významné, přibližně desetinásobné zvýšení přenosové rychlosti a podstatné snížení doby odezvy oproti standardu 4G, což kromě obsloužení více zařízení a zákazníků také umožňuje využívat nové technologie (online dálkové ovládání různých zařízení, vysoká kvalita multimédií, vysokorychlostní přístup, nízkou latenci, vysokou dostupnost a spolehlivost, QoS apod.). Základní požadavky na systém 5G byli definovány v IMT-2020 a pro 4G LTE-A to bylo IMT-advanced viz obrázek 1. kde jsou shrnuty požadavky na uživatelskou rychlost (User experience data rate), spektrální účinnost (Spectrum efficiency), mobilitu (Mobility), latenci (Latency), hustotu připojení/zařízení (Connection density), energetická účinnost sítě (Network energy efficiency), plošnou kapacitu sítě (Area traffic capacity) a špičkovou rychlost přenosu dat (Peak data rate).

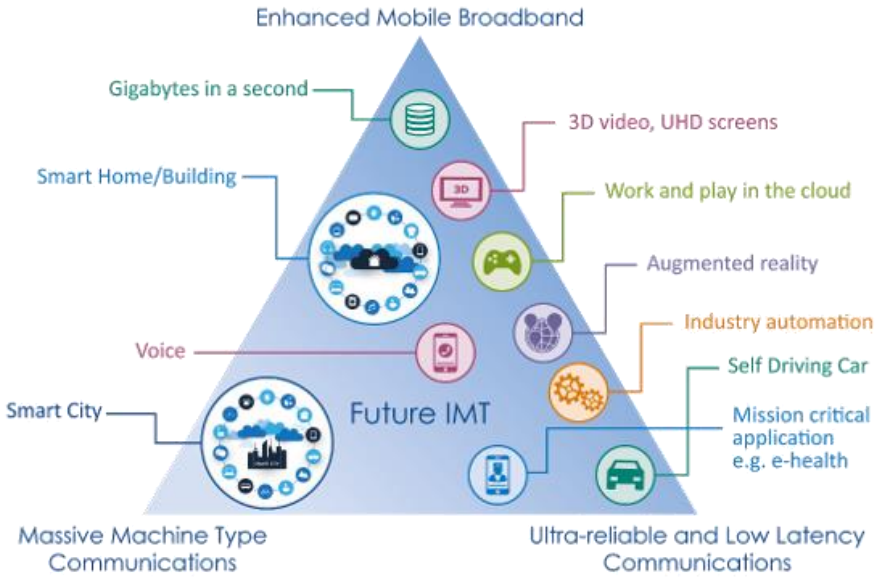


Obrázek 1 Porovnání klíčových vlastností IMT-advanced (4G LTE-A) s IMT-2020 (5G)

Jak je vidět z porovnání se 4G sítí LTE advanced (IMT-advanced) tak některé parametry se mění o jeden řád a některé dokonce až o dva řády. Podobně jako u předchozích sítí je jasné že ne všechny požadavky a parametry budou splněny na začátku, ale postupně se budu vylepšovat tak jak budou uvolňovány další specifikace (release) 5G sítě.

Nové služby 5G sítí (viz. obrázek 2) jsou definovány jako:

- eMBB – Enhanced Mobile Broadband – Vylepšené mobilní širokopásmové připojení
- mMTC – Massive Machine-type Communications – Strojová komunikace v masivním měřítku
- uRLLC – Ultra-Reliable Low Latency Service – Vysoce spolehlivá služba s nízkou latencí



Obrázek 2 Služby 5G sítě dle 3GPP

Enhanced Mobile Broadband (eMBB)

Vylepšené mobilní širokopásmové připojení (eMBB) 5G sítí je nejviditelnějším rozšířením schopností LTE. eMBB nabídne podstatně větší datové rychlosti, vysokou hustotu uživatelů a velmi vysokou kapacitou, a vysokou mobilitu. Vyšší rychlosti jsou důležité zejména pro streamování, videokonference a virtuální realitu. Nejvyšší rychlosti budou dostupné v malých buňkách s omezenou mobilitou koncových uživatelů, jako jsou například chodci.

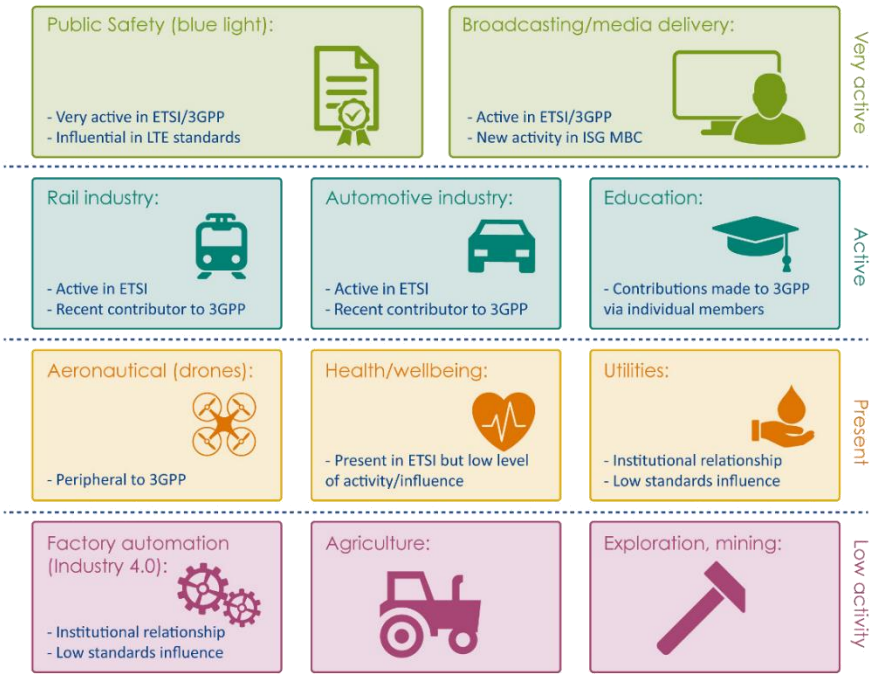
Massive Machine-type Communications (mMTC)

Strojová komunikace v masivním měřítku. tato služba je určena pro Internet věcí (IoT), vyžadující nízkou spotřebu energie a nízké datové rychlosti pro velmi velký počet připojených zařízení.

Masivní komunikace strojového typu rozšiřuje možnosti internetu věcí LTE – například NB-IoT – a podporuje obrovské množství zařízení s nižšími náklady, lepším pokrytím a dlouhou výdrží baterie. Jak je uvedeno v cílech ITU níže, 5G bude podporovat desetkrát více zařízení v oblasti než LTE.

Ultra-reliable and Low Latency Communications (URLLC)

Ultra-spolehlivá komunikace s nízkou latencí (uRLLC) je určena pro kritické aplikace a aplikace kritické z hlediska bezpečnosti. Díky vysoké spolehlivosti a extrémně krátké době průchodu sítí umožní uRLLC, označované také jako „kritická“ komunikace, průmyslovou automatizaci, řízení dronů, nové lékařské aplikace, autonomní vozidla nebo například zabezpečení železniční dopravě. Někdy bývá uRLLC také označována jako kritická komunikace typu stroje (cMTC).



Obrázek 3 Služby v 5G sítí dle 3GPP

První spuštění komerčního provozu 5G sítí bylo roku 2019 v Jižní Koreji. 5G sítě poskytují telekomunikačním operátorům potenciál nabízet nové služby novým kategoriím uživatelů.

Rádiová část - 5G NR New Radio

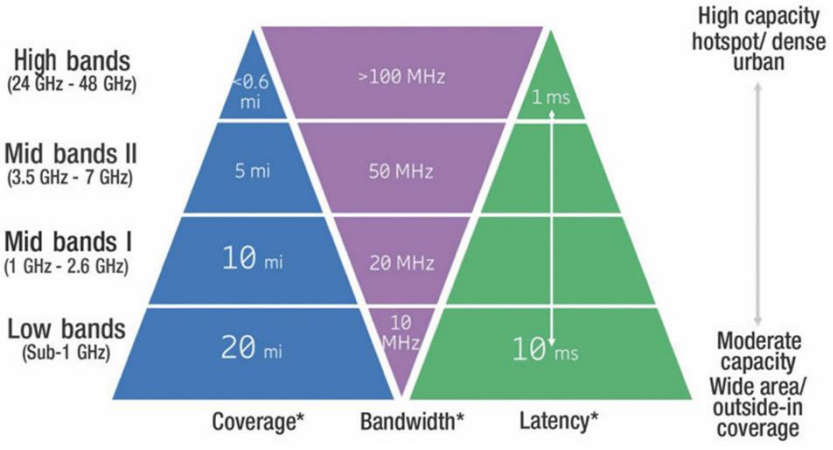
5G NR (anglicky 5th Generation New Radio) je nová rádiová přístupová technologie (RAT) vyvinutá konsorciem 3GPP jako globální standard nového rádiového rozhraní pro mobilní sítě páté generace. (Pojmy RAN a RAT jsou částečně zaměnitelné.)

Technické detaily technologie 5G NR a 4G LTE popisují doporučení 3GPP řady 38. Rádiové rozhraní 5G NR využívá techniku OFDMA (Orthogonal Frequency Division Multiple Access) a modulaci až 1024 QAM. Společně s rozšiřujícími se bloky spektra využitelnými v pro aplikace 5G očekáváme znatelné navýšení přenosových kapacit sítí.

Základní rozdělení kmitočtových pásem pro 5G NR je následující:

- Frequency Range 1 (FR1) zahrnuje pásma v rozsahu od 410 MHz až 7,125 GHz (vlnové délky 42-732 mm), Maximální šířka pásma kanálu definovaná pro FR1 je 100 MHz, kvůli nedostatku spojitého spektra v tomto přeplněném frekvenčním rozsahu. Nejpoužívanější pásmo pro 5G NR v tomto frekvenčním rozsahu je 3,3 – 4,2 GHz a frekvenční pásma po 2G, 3G a 4G.

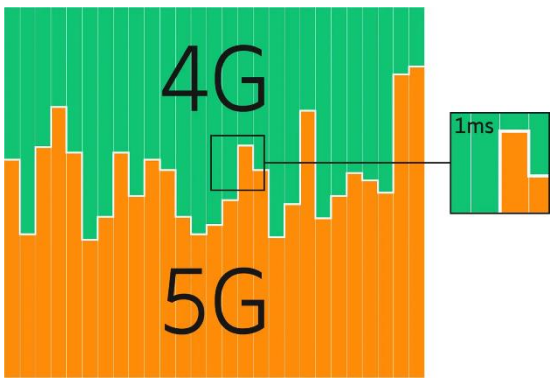
- Frequency Range 2 (FR2), zahrnuje pásma v rozsahu od 24,250 GHz až 52,600 GHz s vlnovými délkami 5,7-12,5 mm. Minimální šířka pásma kanálu definovaná pro FR2 je 50 MHz a maximální je 400 MHz, přičemž dvoukanálová agregace je podporována v 3GPP Release 15. Čím vyšší frekvence, tím větší je schopnost podporovat vysoké rychlosti přenosu dat. Vyšší frekvence znamenají ale menší porytí a vyžadují vyšší hustotu (počet) výstavby vysílačů. Pásmo FR 2 je označováno také jako mmWave tedy milimetrové vlny.



Obrázek 4 Pásma 5G sítí – pokrytí, kapacita a latence

Dynamické Sdílení Spektra (DSS)

V rozsahu FR1 mohou mobilní operátoři pro lepší využití vložených investic využívat také dynamické sdílení rádiového pásma pomocí technologie DSS. Technologie DSS umožňuje dynamicky sdílet pásmo mezi technologiemi 4G LTE a 5G NR. Rádiové spektrum je tedy časově multiplexováno pomocí technologie TDM (Time Division Multiplex) mezi oběma generacemi mobilních sítí, a pro řídicí funkce se stále používá síť 4G LTE dle poptávky uživatelů. Existující zařízení 4G LTE, která jsou kompatibilní s 5G NR, mohou používat Dynamické sdílení spektra (DSS). Přitom stačí, aby s DSS byl kompatibilní pouze 5G NR terminál. Dynamické sdílení spektra má však určitou režii a s potřebuje tedy část kapacity (21 % režie ve srovnání pouze s LTE bez DSS a 41 % režie ve srovnání pouze s 5G bez DSS). DSS je tedy řešení pro současný souběh sítí 4G LTE a 5G NR po přechodné období.



Obrázek 5 Dynamické sdílení spektra

Zavádění 5G sítí

5G síť nabízí dva základní režimy – Nesamostatný režim (NSA)– kdy je rádiové rozhraní 5G NR spuštěno jako podružené ke 4G LTE na jádru sítě 4G EPC a to pouze za účelem navýšení kapacity.

Samostatný režim tedy standalone (SA) mode 5G je zcela nová síť s novým rádiovým rozhraním i novým jádrem sítě.

Nesamostatný režim

Nesamostatný (NSA) tedy non-standalone režim 5G je pouze nasazení nového rádiového rozháraní tedy 5G NR, při kterém se pro řídicí funkce stálé využívá řídicí rovina (signalizace) stávající 4G LTE sítě, zatímco 5G NR je zaměřen výhradně na uživatelskou rovinu (data) za účelem navýšení kapacity. Veškerá signalizace (řídící rovina) se přenáší v režimu LTE. Rádiové spektrum mezi 4G LTE a 5G NR lze dynamicky sdílet pomocí technologie DSS. Prioritizaci zavádění 5G NR NSA má ovšem negativní dopad na rychlost zavádění nové sítě 5G NR SA, což někteří operátoři a dodavatelé kritizují.

Samostatný režim

Samostatný (SA) režim 5G NR znamená, že pro signalizace (řídící rovina) i přenos dat (uživatelská rovina) se používají pouze 5G buňky gNB (gNode-B) a radiové rozhraní 5G NR. V tomto je místo 4G Evolved Packet Core použita nová architektura jádra sítě tedy 5G Packet Core. Nové 5G jádro sítě umožňuje nasazení 5G sítě samostatně bez LTE sítě a poskytuje nové služby které 4G LTE sítě nejsou schopny zajistit. Oprávněně lze očekávat, že s budoucím rozvojem sítí 5G SA dosáhne 5G nižší ceny a zároveň lepší efektivitu. To je nezbytné pro vývoji nových služeb a efektivní nasazení nových a aplikací.

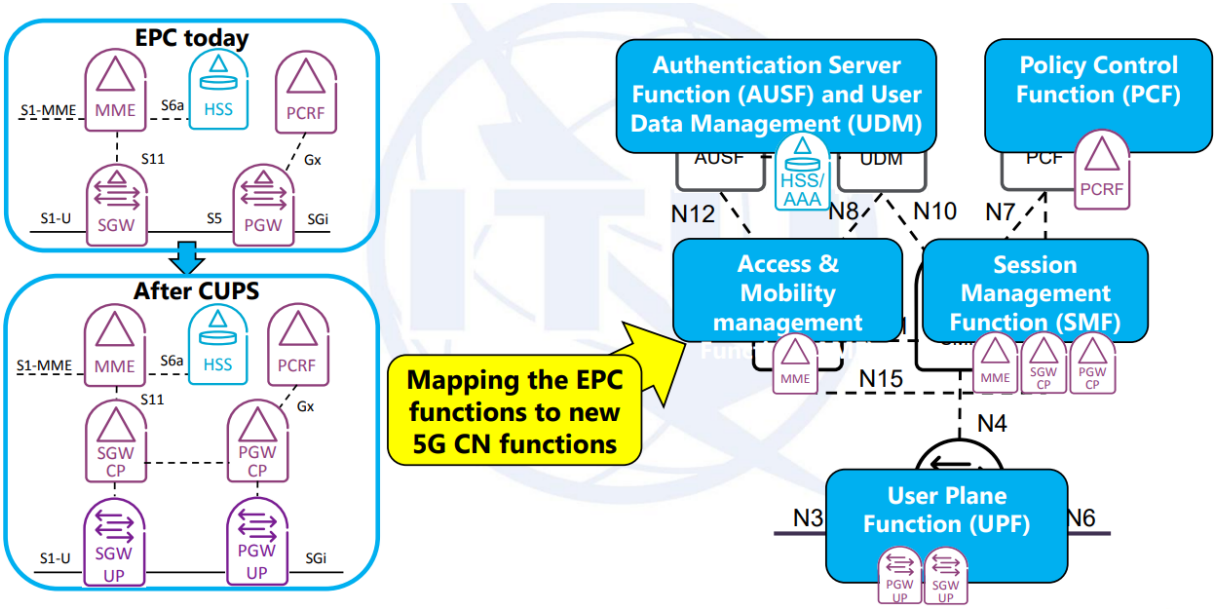
Nové jádro sítě

Tak aby sítě páté generace mohli nabízet nové služby jako jsou eMBB (Extreme Mobile Broadband), mMTC (Massive Scale Communication) a uRLLC (Ultra-Reliable Low Latency Service) někdy také uváděnou jako cMTC (critical Machine-Type Communications) je třeba vyměnit nejen rádiové rozhraní sítě (5G NR) tedy vlastní rádia, antény atd.. ale i vlastní jádro sítě (5GC). Zcela nové jádro 5G sítě je označováno jako 5GC a je založeno moderních technologiích virtualizace síťových technologií tedy SDN (Software-Defined Networking), NFV (Network Functions Virtualization), cloudových, webových technologiích a rozhraní a protokolu HTTP2 s RESTful API.

Oddělení řídící a uživatelské roviny v sítích 4G a 5G

Oddělení uživatelské a řídící roviny jádra sítě anglicky CUPS (Control and User Plane Separation) je popsáno v doporučení 3GPP R14 a bylo zaváděno již v sítích čtvrté generace. Sítě čtvrté generace byly původně navrženy ještě bez architektury CUPS, ale později se ukázalo, že oddělení řídící roviny a uživatelské roviny je velmi výhodné z hlediska rozšiřování, provozu a řízení. U jádra sítí páté generace (5GC) tato architektura již tvoří funkční základ.

Sítě páté generace mají definováno kompletně své nové jádro s požadavkem na snadné vytváření nových služeb tedy – Service Based Architecture. Jádro sítí páté generace je již od počátku navrženo s oddělením řídící (dříve označované jako signalizace) a uživatelské roviny tedy uživatelských dat (aplikací). Architektura CUPS zde nabízí mnoho výhod.



Obrázek 6 EPS, EPS s CUPS a 5G CN – zdroj ITU

Jak bylo již popsáno Control User Plane Separation (CUPS) v jádru mobilních sítích označuje úplné oddělení funkcí řídící roviny (control plane) tedy signalizace (které se starají o správu připojení uživatelů, o zásady QoS, zajištění autentizace uživatele, podporu mobility atd.) a uživatelské roviny (user plane), která se zabývá směrováním vlastního datového provozu a kde se odehrává vlastní přenos uživatelských dat.

Hlavní motivací pro oddělení řídící a uživatelské roviny je nezávislé škálování funkcí uživatelské roviny, což operátorům umožňuje mnohem flexibilnější nasazení a dimenzování sítě. Pokud se například stoupne datový provoz, lze přidat více uzlů datové roviny (například prvků UPF), aniž by to ovlivnilo funkce řídicí roviny. Další výhodou oddělní řídící a uživatelské roviny je také vyšší úroveň bezpečnosti tím že řízení sítě je kompletně odděleno od uživatelských dat.

Architektura CUPS byla poprvé byl představena ve verzi R14 3GPP u sítí čtvrté generace SAE (System Architecture Evolution) kde je jádro sítě nazvané jako EPC (Evolve Packet Core). U sítí čtvrté generace s architekturou CUPS došlo k rozdělení prvků („specializovaných routerů“) jádra sítě SGW (Serving Gateway) na SGW-CP (Serving Gateway-Control Plane) a SGW-UP (Serving Gateway-User Plane) a u prvků PGW (PDN Gateway) na PGW-CP (PDN Gateway-Control Plane) a PGW-UP (PDN Gateway-User Plane).

Klíčové principy architektury 5G:

- Upřednostnění rozhraní pro podporu integrace s více dodavateli
- Nezávislé škálování funkcí UP (User Plane) a CP (Control Plane) díky architektuře CUPS
- Umožnění flexibilního nasazení UP oddělené od CP
- Podpora autentizace pro identity založené na IMSI (International Mobile Subscriber Identity) i identity bez použití IMSI
- Umožňuje různé konfigurace sítě v různých částech sítě – Network Slicing
- Abstraktní transportní vrstva z 3GPP NFs

5G nové koncepty

- Oddělení řídící roviny-vrstvy (Control Plane - CP) a uživatelské roviny-vrstvy (User Plane - UP) – architektura CUPS
- Network slicing
- Service Based Architecture (SBA)

Network Slice

5G network slicing je síťová architektura, která umožňuje multiplexování virtualizovaných a nezávislých logických sítí na stejné fyzické síťové infrastruktuře. Každý segment sítě je izolovaná síť typu end-to-end přizpůsobená tak, aby splňovala různé požadavky požadované konkrétní aplikací.

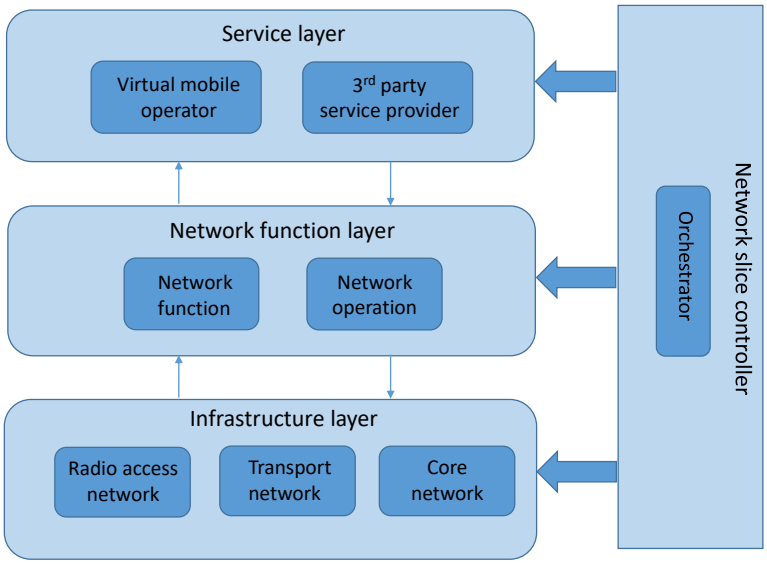
Logická část sítě tedy slouží pouze pro daný účel nebo daného zákazníka.

Technologie network slicing tedy přebírá ústřední roli při podpoře mobilních sítí 5G , které jsou navrženy tak, aby efektivně zahrnovaly nepřeberné množství služeb s velmi odlišnými požadavky na úroveň služeb (Service Level Requirements - SLR). Realizace tohoto servisně orientovaného pohledu na síť využívá koncepty softwarově definovaných sítí (Software Defined Networking – SDN) a virtualizace síťových funkcí (Network Function Virtualization – NFV), které umožňují implementaci flexibilních a škálovatelných síťových segmentů v rámci společné síťové infrastruktury.

Z pohledu obchodního modelu je každý segment sítě spravován operátorem mobilní virtuální sítě (Mobile Virtual Network Operator MVNO). Poskytovatel infrastruktury (vlastník telekomunikační infrastruktury) pronajímá své fyzické zdroje MVNO, kteří sdílejí základní fyzickou síť. Podle dostupnosti přidělených zdrojů může MVNO autonomně nasadit více síťových segmentů, které jsou přizpůsobeny různým aplikacím poskytovaným jeho vlastním uživatelům.

Network Slicing je klíčovým spouštěčem, který podporuje

- Oddělení jednotlivých poskytovatelů, uživatelů
- Rozdílné případy použití a požadavky
- Umožňuje vícenásobné instance stejné funkce
- Umožňuje rychlejší vytvoření a uvedení služeb na trh tedy TTM (Time To Market)



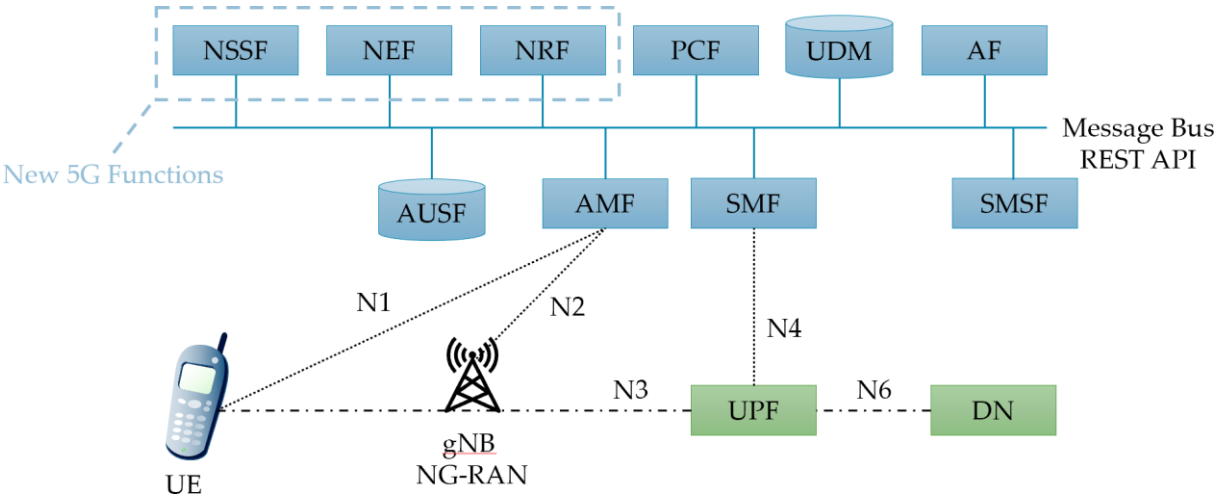
Obrázek 7 5G network slicing

Network slicing vlastnosti:

- Logická síť a je spravovaná poskytovatelem
- Je to aktivátor pro další služby, nikoli samostatná služba
- Je určen jak pro mobilní, tak i pevné sítě
- Zdroje mohou být fyzické nebo virtuální, vyhrazené nebo sdílené (rádio, přenos a jádro sítě)
- Je nezávislý a izolovaný, ale může sdílet zdroje
- Může integrovat služby od jiných poskytovatelů, usnadňující např. agregace a roaming
- Může zahrnovat manažerské funkce a možné vystavení ovládání/řízení zákazníkovi

Jádro sítě 5G a kritické části 5G sítě

Jednotlivé prvky v jádře 5G sítě mají rozhraní RESTful API (Application Programming Interfaces) - tato architektura je u 5G označována jako 5G Service Based Architecture (SBA) a jsou propojeny navzájem pomocí tzv. Message Buss.



Obrázek 8 5G síť, Service Based Architecture

Jádro sítě 5G neboli 5GC se skládá z následujících prvků:

AMF (Access and Mobility Management Function)

Access and Mobility Management Function má na starosti Mobility management tedy zajišťuje hlavně podporu mobility. Mezi jeho hlavní úkoly patří: Správa registrace, Správa připojení, Správa dosažitelnosti, Správa mobility a různé funkce související se zabezpečením a správou přístupu a autorizací. AMF má podobnou funkci jako prvek MME (Mobility Management Entity) ve 4G EPC.

AUSF (Authentication Server Function)

Jako hlavní část 5G jádra sítě AUSF je zodpovědný za provádění bezpečnostních procesů. AUSF má funkci ověřování a identifikaci UE a ukládání ověřovacích klíčů. Podobně jako AuC (Authentication Center) u sítí 2G a 3G nebo HSS (Home Subscriber Server) u 4G.

SMF (Session Management Function)

SMF (Session Management Function) - Funkce správy relací systému 5G má na starost nastavení konektivity pro UE směrem k datovým sítím a také za správu uživatelské roviny pro tuto konektivitu. Prvek SMF řídí router UPF pomocí rozhraní N4. SMF je řídicí funkce, která spravuje uživatelské relace včetně vytváření, modifikace a uvolňování relací a může přidělovat IP adresy pro relace IP PDU. SMF komunikuje nepřímo s UE přes AMF, který přenáší zprávy týkající se relace mezi zařízeními a SMF.

NEF (Network Exposure Function)

Network Exposure Function umožňuje bezpečný, robustní přístup třetích stran k síťovým službám 5G sítě. NEF tedy nabízí možnost vývojářům třetích stran, firmám vytvářet a přizpůsobovat jejich vlastní síťové služby pro 5G sítě. NEF poskytuje ekosystémem a podhoubí pro tyto nové služby. Dále NEF také bezpečně poskytuje data z UDR pro tyto služby třetích stran.

UDR (Unified Data Repository)

HSS v sítích 4G plní podobnou funkci jako UDR. Ukládá data zákaznického profilu a autentizační informace spolu s šifrovacími klíči. V 5G sítích je funkce HSS rozdělena na funkci autentizačního serveru (AUSF), UDM a UDR. AUSF ověřuje servery a poskytuje šifrovací klíče. UDM ukládá a spravuje data do UDR.

Přechod od HSS k UDM a UDR je jednou z mnoha změn přicházejících v přechodu ze sítí čtvrté generace na sítě páté generace.

UDR je konvergované úložiště (databáze) informací o předplatitelích a lze jej použít pro ukládání řady síťových funkci ne jen 5G sítí.

UDR muže být implementován jako cloudová nativní funkce a nabízí sjednocenou databázi pro ukládání informací o aplikaci, předplatném, autentizaci, autorizaci služeb, datech zásad (policy), relacích a stavech aplikací. UDM nabízí rozhraní RESTful API založené na protokolu HTTP2 pro přístup k uloženým datům.

Například prvek 5G sítě UDM (Unified Data Management) používá UDR k ukládání a načítání dat předplatného.

Také PCF (Policy Control Function) používá UDR k ukládání a získávání dat souvisejících s politikou tedy zásadami pro jednotlivé předplatitele.

Z pohledu CIoT (Cellular Internet of Things) může NEF (Network Exposure Function) používat UDR k ukládání dat souvisejících s předplatitelem, která mohou být bezpečně poskytována aplikacím třetích stran.

V terminologii 3GPP se databáze, která uchovává data související s předplatným, již nějakou dobu nazývá User Data Repository (UDR). Bohužel stejná zkratka – UDR – se také objevuje v prostředí 5G: jako databáze informací o předplatném specifických pro 5G. Zkratka „UDR“ však v prostředí 5G znamená „Unified Data Repository“, nikoli „User Data Repository“, jak tomu bylo dříve u 4G.

Data v 5G UDR

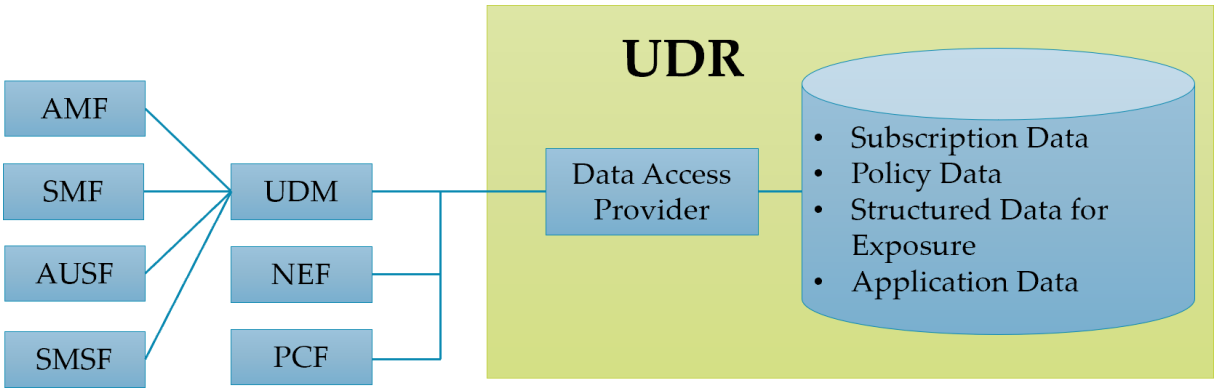
Unified Data Repository ukládá data strukturovaně do různých sestav informací souvisejících s předplatným:

- Údaje o účastnících – funkce jako HLR, HSS
- Data zásad – policy (jako databáze SPR ve 4G)
- Strukturovaná data pro aplikace třetích stran
- Další aplikační data

Tyto čtyři různé struktury parametrů jsou zpřístupněny dalším funkcím sítě 5G:

- Údaje o účastnících jsou zpřístupněna prostřednictvím front-endu UDM (Unified Data Management) řadě NF (Network Function), které řídí aktivity UE v rámci sítě: AMF, SMF, AUSF, …
- Data zásad jsou zpřístupněna (přímo prostřednictvím rozhraní N36) pro prvek PCF (Policy Control Function) – což znamená, že UDR plně nahrazuje dřívější databázi SPR (Subscription Profile Repository) kde byla u 4G sítí uložena politika účastníka.
- Aplikační data jsou vkládána do UDR externími aplikacemi tedy AF (Application Function) prostřednictvím funkce NEF (Network Exposure Function), tak aby tato data mohla být zpřístupněna všem 5G NF, které potřebují – a jsou oprávněni žádat – informace související s předplatitelem.

Další zajímavou funkcí v 5G UDR je skutečnost, že v roamingových scénářích může navštívený UDR lokálně ukládat parametry roamingových uživatelů. Uchovává tedy data o politice i data pro vystavení roamingových UE mohou být uložena v UDR v navštívené síti a zpřístupněna místně příslušným NF – díky tomu je jeho funkce velmi podobná jako registr VLR u 2G/3G sítí.



Obrázek 9 Architektura UDR

UDM (Unified Data Management)

Unified Data Management (UDM), je analogický s Home Subscriber Server (HSS) v architektuře EPC 4G a zavádí koncept User Data Convergence (UDC), který odděluje úložiště uživatelských dat (UDR), které ukládá a spravuje informace o předplatitelích od frontendu, který zpracovává informace o účastnících.

Unified Data Management je tedy centralizovaný způsob řízení uživatelských dat síti páté generace. UDM má podobnou funkci jako HSS u sítí čtvrté generace, ale je nativně podporován v cloudu a je navržen pro 5G sítě.

Stavové informace jsou ukládány přímo do UDM. Bez stavová data jsou ukládána pomocí UDM do jednotného úložiště dat (UDR). UDM má odpovědnost za správu přístupu uživatelů, spravuje data pro autorizaci přístupu, registraci uživatelů a profily datových sítí.

Unified Data Management (UDM) zahrnuje podporu pro následující funkce:

- Generování 3GPP AKA autentizačních pověření
- Zpracování identifikace uživatele (např. ukládání a správa SUPI pro každého účastníka v systému 5G)
- Oprávnění přístupu na základě předplatitelských dat (např. omezení roamingu).
- UE Serving NF Registration Management (tedy například uložení obsluhujícího AMF pro UE, uložení obsluhujícího SMF pro UE PDU Session)
- Podpora kontinuity služby/relace, např. zachováním SMF (Session Management Function) / DNN (Data Network Name) přiřazení probíhajících relací.
- Podpora doručení MT-SMS (Mobile Terminating SMS)
- Funkce zákonného odposlechu LI (Lawful Interception) – zejména v případě odchozího roamingu, **kde je UDM jediným kontaktním místem pro LI**
- Správa předplatného
- Správa SMS

K poskytování této funkce používá UDM data předplatného (včetně ověřovacích dat), která mohou být uložena v UDR, v takovém případě UDM implementuje aplikační logiku a nevyžaduje interní úložiště uživatelských dat a poté může stejnému uživateli sloužit několik různých UDM. v různých transakcích.

UPF (User Plane Function)

UPF (User Plane Function) je základní prvkem architektury systému infrastruktury 5G core.UPF je vlastně router v 5G síti.

UPF představuje evoluci v oddělení datové roviny podle architektury CUPS (Control and User Plane Separation), která byla poprvé představena jako rozšíření existujících EPC (Evolved Packet Core) ve specifikacích 3GPP Release 14. Oddělení řídící uživatelské roviny ve 4G EPC rozděluje prvek PGW (Packet Gateway) na PGW-UP (User Plane) a PGW-CP (Control Plane). Prvek PGW-UP se v 5G Core nazývá UPF a PGW-CP je nazývá SMF (Session Management Function).

Architektura CUPS umožňuje zpracování paketů zejména pak směrování a agregaci provozu provádět blíže k účastníkovy, což zvyšuje efektivitu i šířku pásma a zároveň redukuje velikost sítě a počet prvků v ní a tím snižuje i latenci.

Řídící rovina tedy signalizace, kterou zajišťuje prvek SMF zůstává dále v jádru sítě.

Funkce UPF:

- UPF je propojovací bod mezi mobilní infrastrukturou a datovou sítí (DN). Tedy UPF provádí zapouzdření pomocí protokolu GPT (GPRS Tunneling Protocol) pro uživatelskou rovinu (GTP-U).
- UPF je koncový bod relace PDU pro poskytování mobility rámci a mezi technologiemi rádiového přístupu (RAT), včetně odesílání paketů do gNB.

Směrování a předávání paketů, včetně plnění role Uplink Classifier / UL-CL (směrování toků do konkrétních datových sítí na základě filtrů pro přizpůsobení provozu) a Branching point, když funguje jako prostřední UPF tedy (I-UPF) s více domovy více než jedna PDU session anchor (PSA).

Detekce aplikací pomocí šablon filtru provozu Service Data Flow (SDF) nebo 3 n-tice (protokol, adresa IP na straně serveru a číslo portu) Popis toku paketů (PFD) přijaté z SMF.

Manipulace s QoS za tok, včetně značení paketů na úrovni transportu pro uplink (UL) a downlink (DL), omezení rychlosti a reflektivní značení QoS (DSCP) na DL.

Hlášení o využití provozu pro fakturaci a sběrné rozhraní zákonného odposlechu (LI).

Funkce uživatelské roviny má čtyři různé referenční body:

- N3: Rozhraní mezi RAN (gNB) a (počátečním) UPF.
- N9: Rozhraní mezi dvěma UPF (tj. Intermediate I-UPF a UPF Session Anchor)
- N6: Rozhraní mezi datovou sítí (DN) a UPF
- N4: Rozhraní mezi funkcí správy relací (SMF) a UPF

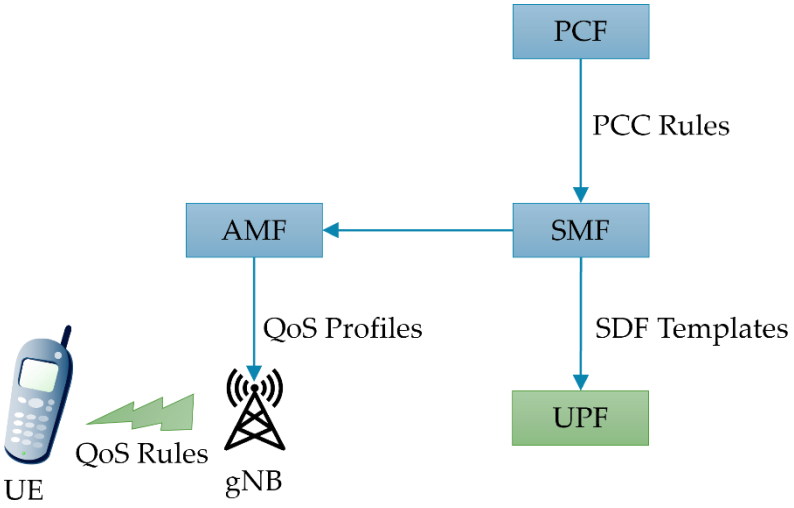
Network Repository Function (NRF)

Různé síťové funkce NF (Network Functions) jsou propojeny prostřednictvím jednotného rozhraní SBA. Kromě toho se individuální NF skládá z menších jednotkových funkcí nazývaných služby NF a služba NF v určitém NF může přímo přistupovat ke službě NF v jiném NF, aniž by musela komunikovat s dalším uzlem. Funkce síťového úložiště (NRF) poskytuje funkci zjišťování pro služby NF. Network Repository Function (NRF) funguje jako centralizované úložiště pro všechny funkce sítě 5G NF v síti operátora. NRF umožňuje 5G NF registrovat se a vzájemně se objevovat prostřednictvím rozhraní API založeného na standardech.

Policy Control Function (PCF)

Funkce kontroly zásad (PCF) zahrnuje následující funkce:

- Podporuje jednotnou politiku pro QoS (Quality of Service), řízení a chování sítě
- Poskytuje pravidla zásad pro řídící rovinu (Control Plane)
- Přístup k informacím o předplatném relevantním pro rozhodnutí o zásadách v Unified Data Repository (UDR)



Obrázek 10 Funkce PCF pro QoS a řízení sítě

Network Data Analytics Function (NWDAF)

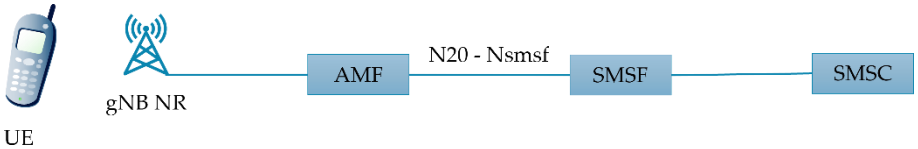
Funkce analýzy dat sítě (NWDAF) je navržena tak, aby monitorovala v jak tečou data v core network a generovala statistiky, umožnila optimalizovat nastavení sítě a tím zlepšit end-user-experience uživatelů 5G sítě.

NWDAF má tyto funkce:

- Rozhraní sběru dat ze síťových uzlů
- Předdefinované analytické statistiky
- Rozhraní pro prezentaci dat
- Rádiová část 5G – 5G NR

Short Message Service Function (SMSF)

V 5G sítích jsou dva možné způsoby přenosu SMS. První způsob se nazývá SMSoIP (SMS over IP) je realizován pomocí IMS (IP Multimedia Subsystem) a IP-SM-GW. Druhý způsob přenosu SMS se nazývá SMS Function. Zde je SMS přenášena pomocí signalizace z UE do SMSF přes AMF. Způsob SMSoIP se používá v 5G sítí kde je podpora hlasu a hlas přenášen pomocí IMS. Naopak u 5G sítí které nepodporují přenos hlasu (např průmyslové 5G sítě) se používá metoda SMS Function.

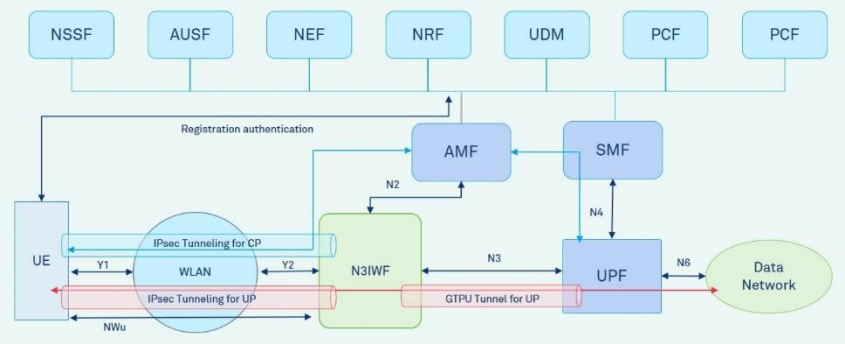


Obrázek 11 Přenos SMS pomocí SMSF

Non-3GPP Inter Working Function (N3IWF)

N3iWF zajišťuje přístup do jiných než 3GPP sítí – tedy nedůvěryhodných sítí pomocí IPsec tunelu. Například připojení pomocí Wi-Fi či pevných sítí.

N3IWF podporuje je připojen k 5G jádru pomocí rozraní N2 k AMF, pomocí N3 a protokolu GTPU k UPF. Směrem k zařízení je N3IWF připojeno pomocí IPSec. Jeden IPSec tunel slouží pro signalizaci – řídící rovina a druhý pro datové přenosy – uživatelská rovina.



Obrázek 12 Funkce N3IWF a IPsec tunely

Rádiová část sítě

gNB (g node-B)

gNB patří do RAT (Radio Access Technology) někdy také zvaně jako RAN (Radio Access Network) jedná se tedy o základnovou stanici v síti 5G. gNB je podle architektury CUPS rozdělena na řídící rovinu/část tedy gNB-CU a uživatelskou část/ rovinu tedy gNB-DU. Dále je možno u gNB použít network slicing a je možno gNB virtualizovat.

Virtualizace gNB

gNB může být implementována jako D-RAN tedy distributed RAN (Radio Access Network) kdy je vlastní základnová stanice složena ze dvou částí – BBU (Baseband Unit) a RRH (Remote Radio Head). BBU je umístěna většinou v kontejneru pod věží a RRH na stožáru. Další možnost je Centralized RAN (C-RAN) kdy BBU je centralizována. Centralizovanou BBU je možno dále virtualizovat a pak mluvíme o Cloud RAN tedy (C-RAN) a virtual BBU.

RRH a virtuál BBU jsou propojeny pomocí rozehranní Common Public Radio Interface (CPRI)

Bezpečnost 5G sítí

S popisu 5G sítě vyplívá že jádro 5G sítě (řídící rovina - signalizace) je pomocí architektury CUPS již plně oddělené od uživatelské roviny a data o uživatelích používají centrální úložiště UDR (Unified Data Repository).

Jádro 5G sítě je již v návrhu plně připraveno na virtualizaci a je možno ho provozovat pomocí virtualizace a v cloudu. Všechna komunikace v jádru 5G sítě je založena na protokolu RESTful API.

Rádiovou část je možno také částečně virtualizovat pomocí jednotky BBU (Baseband Unit) a připojit pomocí rozhranní CPRI (Common Public Radio Interface) připojit k RRH (Remote Radio Head).

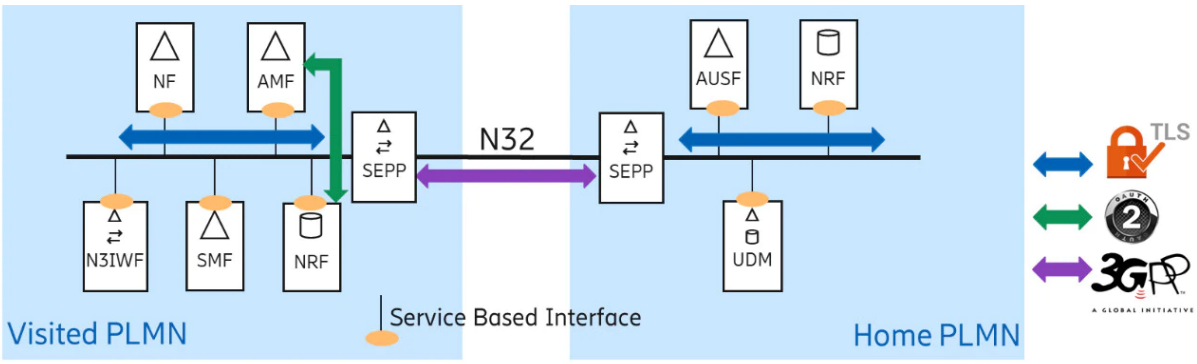
Komunikace mezi gNB a UPF (rozhraní N3) je šifrována a přenášena pomocí GTP-U tunelu.

Zabezpečení jádra sítě 5G

Použití SBA (Service Based Architecture) také zavedlo ochranu na vyšších protokolových vrstvách (tj. transportní a aplikační), navíc k ochraně komunikace mezi entitami jádrové sítě na vrstvě internetového protokolu (IP) (typicky IPsec). Proto funkce základní sítě 5G podporují nejmodernější bezpečnostní protokoly, jako je TLS 1.2 (Transport Layer Security) a TLS 1.3 pro ochranu komunikace na transportní vrstvě a rámec OAuth2 na aplikační vrstvě, aby bylo zajištěno, že přístup k nim budou mít pouze autorizované síťové funkce.

Pokud komunikace probíhá mezi dvěma různými jádry v různých sítích tedy například v případě roamingu tak komunikace probíhá prostřednictvím SEPP (Security Edge Protection Proxy). Veškerá signalizace mezi operátory bude procházet těmito bezpečnostními proxy. Dále je vyžadována autentizace mezi jednotlivými SEPP. To umožňuje efektivní filtrování provozu přicházejícího z mezioperátorského propojení.

Nové bezpečnostní řešení aplikační vrstvy na rozhraní N32 mezi SEPP bylo navrženo tak, aby poskytovalo ochranu citlivých datových atributů a zároveň umožňovalo mediační služby v celém propojení.



Obrázek 13 Propojení 5G sítí pomocí SEPP

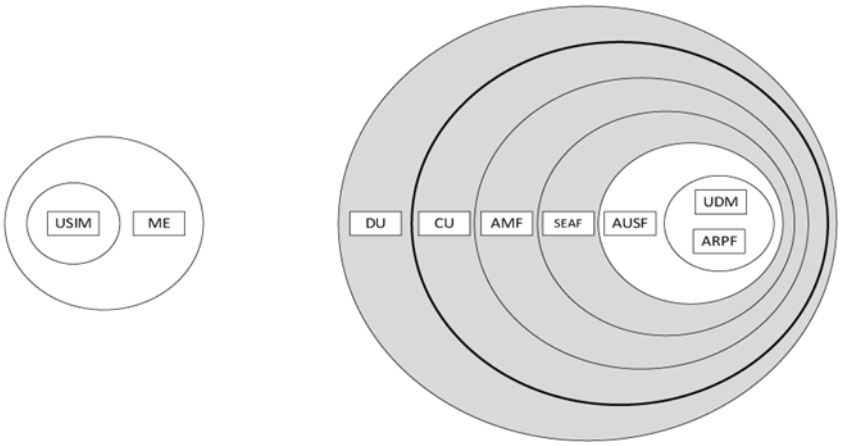
Hlavními součástmi zabezpečení SBA jsou autentizace a ochrana přenosu mezi síťovými funkcemi pomocí TLS, autorizační rámec využívající OAuth2 a vylepšené zabezpečení propojení pomocí nového bezpečnostního protokolu navrženého 3GPP (při komunikaci mezi sítěmi).

Modelu důvěry v 5G sítích a jeho evoluce

Po přechodu od NSA (Non-Standalone architecture) 5G sítí v SA (Standalone architecture) 5G sítě se model důvěry vyvinul. Důvěra v rámci sítě se považuje za klesající, čím dále se člověk vzdaluje od jádra. To má dopad na rozhodnutí přijatá v návrhu zabezpečení 5G.

Model důvěry v UE je přiměřeně jednoduchý: existují dvě důvěryhodné domény, karta UICC (Universal Integrated Circuit Card), která je odolná proti neoprávněné manipulaci, na které je nahrána aplikace USIM (Universal Subscriber Identity Module) ve které jsou umístěny privátní klíče a mobilní zařízení ME (Mobile Equipment). ME a USIM dohromady společně tvoří UE (User Equipment).

Model důvěry v 5G sítích je více vrstvý a lze si jej představit jako cibuli.



Obrázek 14 Model důvěry v 5G sítí

Rádiová přístupová síť RAN (Radio Access Network) je rozdělena na jednotky gNB-DU (gNodeB-Distributed Unit) a řídící jednotky gNB-CU (gNodeB-Control Unit). Dohromady gNB-DU a gNB-CU společně tvoří celou gNodeB základnovou stanici pro 5G sítě. Jednotka gNB-DU nemá žádný přístup k zákaznické datové komunikaci a proto může být nasazen na nekontrolovaných místech sítě.

Následný uživatel nemá žádný přístup ke komunikaci se zákazníky, protože může být nasazen na nehlídaných místech. CU a Non-3GPP Inter Working Function (N3IWF – neznázorněno na obrázcích), která ukončuje zabezpečení Access Stratum (AS), budou nasazeny na místech s omezenějším přístupem. gNB-CU a jednotka N3IWF (non-3GPP Interworking Function), která ukončuje zabezpečení AS (Access Stratum), by měli být nasazeny v lokalitách s omezenějším přístupem.

V jádru sítě slouží jednotka AMF (Access Management Function) jako koncový bod signalizace pro zabezpečený NAS (Non-Access Stratum). V současné době, tj. ve specifikaci 3GPP 5G Phase 1, je AMF spojen s funkcí SEAF (SEcurity Anchor Function), která drží kořenový klíč (známý jako kotevní klíč – anchor key) pro navštívenou síť. Bezpečnostní architekturu je možno do budoucna rozvíjet, protože umožňuje oddělení SEAF a AMF, což by mohlo být možné v budoucím vývoji systémové architektury.

V jednotce AUSF (AUTHentication Function) je uchováván klíč pro opětovné použití, odvozený po ověření, v případě současné registrace UE v různých technologiích přístupové sítě, tj. v přístupových sítích 3GPP a přístupových sítích jiných než 3GPP, jako je například IEEE 802.11 WLAN tedy Wi-Fi.

Authentication credential Repository and Processing Function (ARPF) uchovává autentizační údaje tedy klíče, podobně jako USIM na straně klienta.

Všechny informace o účastnících jsou uloženy v uložišti (UDR) Unified Data Repository. UDM (Unified Data Management) využívá předplatitelská data uložená v UDR a implementuje aplikační logiku k provádění různých funkcí, jako je generování autentizačních pověření, identifikace uživatele, kontinuita služeb a relace atd. Bezdrátové rozhraní, aktivní i pasivní útoky jsou brány v úvahu jak na úrovni kontroly, tak na úrovni uživatele. Soukromí se stává stále důležitějším, což vede k tomu, že trvalé identifikátory jsou udržovány v tajnosti přes bezdrátové rozhraní.

V roamingové architektuře jsou domácí a navštívená síť propojeny prostřednictvím proxy SEPP (SEcurity Protection Proxy) které zajišťuji propojení řídicí roviny (signalizace) mezi sítěmi. Tato vylepšená architektura se zavádí v 5G kvůli počtu útoků, které se množí, jako jsou krádeže klíčů a útoky v signalizační SS7 síti, falšování zdrojové adresy v signalizačních zprávách v DIAMETER, které zneužívaly důvěryhodnou povahu mezisíťového propojení.

Ochrana integrity uživatelské roviny

V 5G byla jako nová funkce zavedena ochrana integrity uživatelské roviny (UP) mezi zařízením (UE) a základnovou stanicí (gNB). Stejně jako funkce šifrování je podpora funkce ochrany integrity povinná na zařízeních i gNB, zatímco použití je volitelné a pod kontrolou operátora.

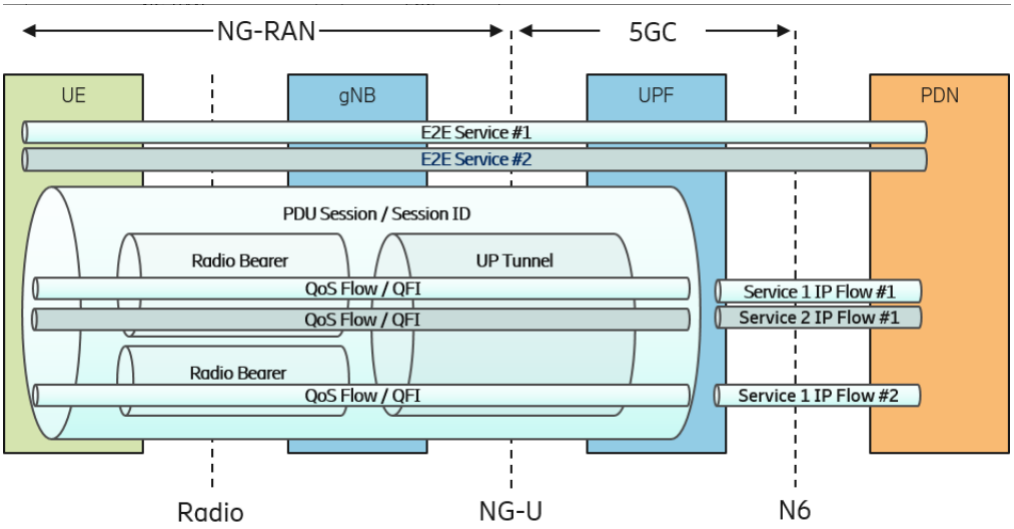
Je dobře známo, že ochrana integrity je náročná na zdroje a že ne všechna zařízení ji budou schopna podporovat při plné rychlosti přenosu dat. Systém 5G proto umožňuje vyjednávání o tom, které sazby jsou pro danou funkci vhodné. Pokud například zařízení udává maximální datovou rychlost 64 kbit/s pro provoz chráněný integritou, pak síť zapne ochranu integrity pouze pro připojení UP, kde se neočekává, že rychlost přenosu překročí limit 64 kbit/s.

Bezpečnost 5G sítí na rádiovém rozhraní

V telekomunikačních systémech operátor sítě přiděluje každé SIM kartě jedinečný identifikátor, známý od 2G až do 4G jako IMSI (International Mobile Subscriber Identity) a pro 5G sítě jako SUPI (Subscription Permanent Identifier). Protože autentizace mezi uživatelem a jeho poskytovatelem sítě je založena na sdíleném symetrickém klíči, může k němu dojít až po identifikaci uživatele. Pokud jsou však hodnoty IMSI/SUPI odesílány jako prostý text prostřednictvím rádiového přístupového spojení, lze uživatele identifikovat, lokalizovat a sledovat pomocí těchto trvalých identifikátorů.

Aby se předešlo tomuto narušení soukromí, mobilní síť přiděluje USIM kartě dočasné identifikátory (v sítích 2G a 3G jako TMSI (Temporary Mobile Subscriber Identity) a GUTI (Global Unique Temporary Identifier) pro systémy 4G a 5G. Tyto často se měnící a dočasné identifikátory se pak používají pro účely identifikace přes rádiový interface. Existují však určité situace, kdy autentizace pomocí dočasných identifikátorů není možná, např. když se uživatel poprvé registruje do mobilní sítě, a ještě mu není přidělen dočasný identifikátor. Jiný případ je, když navštívená síť nedokáže identifikovat uživatele (tedy jeho IMSI či SUPI) prezentovaného TMSI/GUTI.

Aktivní protivník typu „man-in-the-middle“ může záměrně simulovat tento scénář, aby donutil nic netušícího uživatele odhalit jeho dlouhodobou identitu. Tyto útoky jsou známé jako „IMSI catching“ útoky a přetrvávají v dnešních mobilních sítích včetně 4G LTE/LTE-Advanced.



Obrázek 15 NG-RAN a 5GC

Řešení IMSI Catchers v 5G

Útok zachycení IMSI ohrožuje všechny generace mobilních sítí (2G/3G/4G) po celá desetiletí. V důsledku zpětné kompatibility tento problém ochrany osobních údajů přetrvává i v 4G sítích. 3GPP se však rozhodl tento problém řešit u 5G, i za cenu zpětné kompatibility. V případě selhání identifikace prostřednictvím 5G-GUTI, na rozdíl od dřívějších generací, bezpečnostní specifikace 5G neumožňují přenosy SUPI v prostém textu přes rádiové rozhraní. Namísto toho se přenáší eliptické křivky integrované šifrovací schéma (ECIES) – založené na identifikátoru pro ochranu soukromí, který obsahuje skryté SUPI. Toto skryté SUPI je známé jako SUCI (Subscription Concealed Identifier)

SUPI (Subscription Permanent Identifier) je globálně jedinečný identifikátor přidělený každému účastníkovi a definovaný ve specifikaci 3GPP TS 23.501. SUPI je uloženo u účastníka na jeho USIM a v mobilní síti na UDM/UDR v 5G Core.

Platné SUPI může mít následující formát:

- IMSI (International Mobile Subscriber Identifier) definovaný v TS 23.503 pro 3GPP RAT
- NAI (Network Access Identifier), jak je definováno v RFC 4282 na základě identifikace uživatele, definovaný v TS 23.003 pro non-3GPP RAT

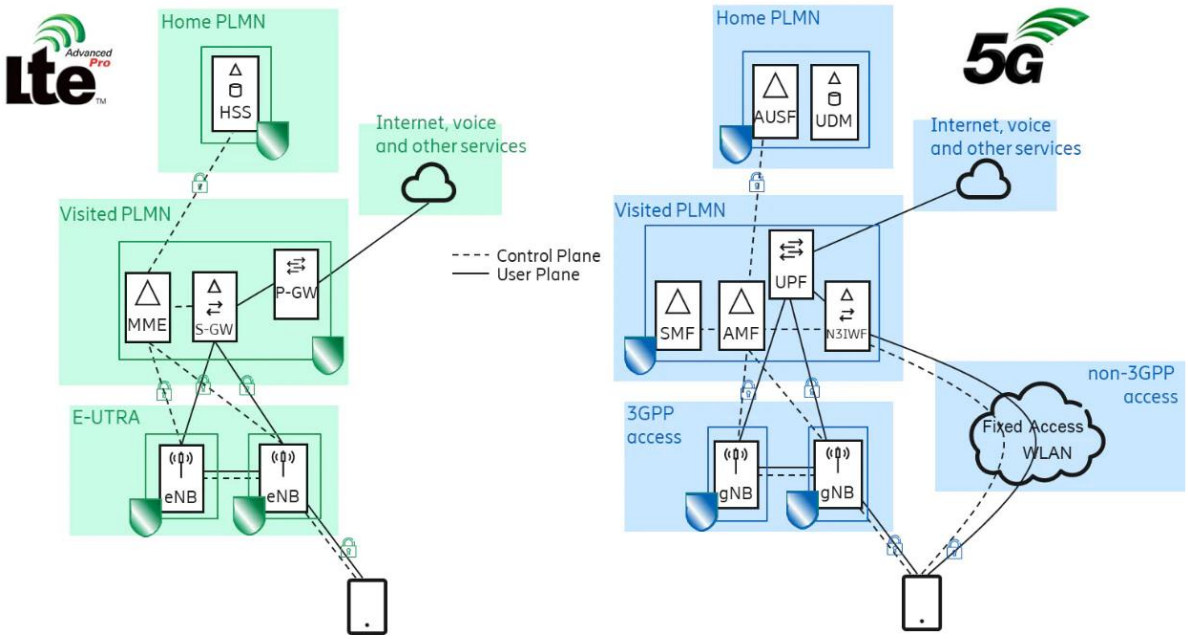
SUPI je obvykle řetězec 15 desetinných číslic. První tři číslice představují mobilní kód země (MCC), zatímco další dvě nebo tři tvoří kód mobilní sítě (MNC) identifikující operátora sítě v dané zemi. Zbývající (devět nebo deset) číslic jsou známé jako Mobile Subscriber Identification Number (MSIN) a představují jednotlivého účastníka konkrétního operátora. SUPI je tedy ekvivalent IMSI, které jedinečně identifikuje mobilní zařízení.

Subscription Concealed Identifier (SUCI) je identifikátor chránící soukromí obsahující skryté SUPI. UE generuje SUCI pomocí schématu ochrany založeného na ECIES s veřejným klíčem domovské sítě, který byl bezpečně poskytnut USIM během registrace USIM.

Ochranným schématem je skryta pouze MSIN část SUPI, zatímco identifikátor domácí sítě, tj. MCC/MNC, je přenášen v prostém textu.

Pokud jsou v 5G síti použity identifikátory SUCI (Subscription Concealed Identifier) a SUPI (Subscription Permanent Identifier) a šifrování 5G pak nehrozí problém který měli sítě 2G, 3G a 4G – odchycení IMSI v případě 2G sítí falešná tedy fake BTS (základnová stanice).

Identifikátor SUPI (tedy vlastně IMSI) se tedy v mobilní síti páté generace nikdy nepřenáší v otevřené formě jako tomu bylo u sítí 2G, 3G a 4G.



Obrázek 16 Zabezpečení 4G LTE a 5G sítí

Nové bezpečnostní prvky 5G sítí

- Nové šifrování a ověřování uživatele založený na 3GPP / non-3GPP (EPA-AKA / 5G-AKA)
- Architektura založená na službách využívající IPsec a autorizaci pomocí 0Auth2.0
- Integrita a bezpečnost ochrany signalizace (řídící roviny) a uživatelské roviny
- Bezpečné propojení a spolupráce mezi VPLMN a HPLMN na síťové a aplikační vrstvě pomocí SEPP (Security Edge Protection Proxy)
- Ochrana soukromí (SUPI je vždy chráněno veřejným klíčem a není přenášeno textově)

Možné útoky v 5G síti

Je třeba chránit celý 5G Core (zejména pak prvky UDM, UDR, AUSF, AMF, UPF, PCF, SMF) jak pomocí FW tak při mezi operátorském propojení pomocí SEPP (Security Edge Protection Proxy). Všechny prvky v 5G core jsou v architektuře SBA (Service-Based Architecture) připojeny pomocí sběrnice SBI (Service Based Interface). Jádro sítě je chráněno důsledným oddělením od uživatelské roviny a je zde použito šifrování IPsec a autorizace pomocí 0Auth2.0.

Rádiové rozhraní 5G NR je bezpečnější díky šifrovanému přenosu identity – SUPI které je vždy šifrováno veřejným klíčem takže nehrozí jeho odchycení. Pokud je tedy v síti správně nastavené šifrování EPA-AKA nebo 5G-AKA pak nehrozí možnost zachycení hovoru nebo čísla případně datové komunikace.

Otázky a odpovědi relevantní k zabezpečení sítí 5G

Otázka 1

Je tedy bezpečné ve všech scénářích (neuvažujeme scénář, kdy dodavatel je zároveň provozovatel sítě) používat RAN součásti sítě? (gNodeB, Access)

Odpověď:

Ano, používání gNB části sítě je bezpečné, protože veškeré přenosy jsou šifrované a klíče jsou uloženy na straně zařízení v USIM a na straně sítě core network nikoliv v gNB (gNodeB).

Dle specifikace 5G Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.3.0 Release 16) podle odstavce 5.3.2 (https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf)

Důvěrnost uživatelských dat a dat signalizace u gNodeB (gNB):

- gNB musí podporovat šifrování uživatelských dat mezi UE a gNB
- gNB aktivuje šifrování uživatelských dat na základě bezpečnostní politiky zaslané SMF
- gNB musí podporovat šifrování RRC (Radio Resource Control) signalizace
- gNB musí implementovat následující šifrovací algoritmy:
  NEA0, 128-NEA1, 128-NEA2, jak je definováno v příloze D této normy
- gNB může implementovat následující šifrovací algoritmus:
  128-NEA3, jak je definováno v příloze D této normy

Ochrana důvěrnosti uživatelských dat mezi UE a gNB je volitelná.
Ochrana důvěrnosti signalizace RRC (Radio Resource Control) je volitelná.
Ochrana důvěrnosti by měla být používána vždy, když to předpisy umožňují.

Integrita uživatelských a signalizačních dat u gNB:

- gNB musí podporovat ochranu integrity a ochranu před přehráváním uživatelských dat mezi UE a gNB
- gNB aktivuje ochranu integrity uživatelských dat na základě bezpečnostní politiky zaslané SMF
- gNB musí podporovat ochranu integrity a ochranu před přehráním RRC signalizace.
- gNB bude podporovat následující algoritmy ochrany integrity:
  NIA0, 128-NIA1, 128-NIA2, jak je definováno v příloze D této normy
- gNB může podporovat následující algoritmus ochrany integrity:
  128-NIA3, jak je definováno v příloze D tohoto dokumentu
- Ochrana integrity uživatelských dat mezi UE a gNB je volitelná a nesmí používat NIA0 (Null Integrity Protection algorithm)

Otázka 2

Je tedy bezpečné ve všech scénářích (neuvažujeme scénář, kdy dodavatel je zároveň provozovatel sítě) používat CORE součásti sítě?

Odpověď

Ne zcela, v Core network jsou uloženy šifrovací klíče a probíhá ze ověřování a šifrování (prvky UDR, UDM, AUSF), dále je v core network uložena politika sítě a její řízení (prvky UDR, UDM, PCF). Core network také zajišťuje mobilitu a veškerou signalizaci (AMF a SMF).

Otázka 3

Je tedy bezpečné ve všech scénářích (neuvažujeme scénář, kdy dodavatel je zároveň provozovatel sítě) ošetřovat propojovací infrastrukturu sítě? Transportuji data prostřednictvím sítí třetích stran.

Odpověď

Není to potřeba od uživatelského zařízení UE, přes gNB až do domovského UPF jsou data i signalizace šifrovány pomocí 128-bitových klíčů které jsou uloženy na USIM a v jádru sítě.

Otázka 4

V EU 5G Toolboxu se mluví o tom, že by stát měl:

- Stanovit pro příslušné vnitrostátní orgány a provozovatele mobilních sítí rámec s jasnými kritérii se zohledněním rizikových faktorů uvedených v bodě 2.37 celounijně koordinovaného posouzení rizik a s doplněním informací o jednotlivých zemích (např. posouzení hrozeb ze strany národních bezpečnostních služeb), a to s cílem:
    - provést důkladné posouzení rizikového profilu všech příslušných dodavatelů na vnitrostátní úrovni a/nebo na úrovni EU (například společně s ostatními členskými státy nebo s jinými provozovateli mobilních sítí),
    - v návaznosti na posouzení rizikového profilu uplatňovat příslušná omezení vůči dodavatelům, kteří jsou považováni za vysoce rizikové, včetně nezbytných vyloučení za účelem účinného zmírnění rizik, pokud jde o klíčová aktiva označená v celounijně koordinovaném posouzení rizik jako kritická a citlivá (např. funkce páteřní sítě, funkce správy a orchestrace sítě a funkce přístupu k síti),
    - přijmout opatření k zajištění toho, aby provozovatelé mobilních sítí zavedli náležité kontroly a postupy k řízení možných zbytkových rizik, jako jsou pravidelné audity a posuzování rizik dodavatelského řetězce, spolehlivé řízení rizik a/nebo specifické požadavky na dodavatele založené na jejich rizikových profilech;

Která aktiva jsou podle vás “klíčová”?

Odpověď

Velmi citlivé je jádro sítě 5GC, zejména pak šifrovací klíče UDR, UDM/ARPF, AUSF, AMF, dohled, orchestrace, správa, distribuce USIM, eSIM a klíčů.

Otázka 5

V případě přístupové sítě, se v celounijně koordinovaném posouzení rizik uvádí toto: “Access network functions were also rated with relatively high sensitivity. However, the assessment of the degree of sensitivity of specific elements within the access functions varies according to a number of factors. Furthermore, in the coming development phases of 5G, traditionally less sensitive parts of the

network are gaining importance and becoming more sensitive, such as for instance certain elements in the radio access part of the network, depending on the extent to which they handle user data or perform smart or sensitive functions. Moreover, when edge computing is introduced, certain core network functions are expected to be moved physically farther out in the network, closer to the access sites."

český překlad: "Funkce přístupové sítě byly rovněž hodnoceny s poměrně vysokou citlivostí. Hodnocení míry citlivosti konkrétních prvků v rámci přístupových funkcí se však liší v závislosti na řadě faktorů. V nadcházejících fázích vývoje 5G navíc tradičně méně citlivé části sítě nabývají na významu a stávají se citlivějšími, jako například některé prvky v rádiové přístupové části sítě, a to v závislosti na tom, do jaké míry zpracovávají uživatelská data nebo vykonávají inteligentní či citlivé funkce. Navíc se očekává, že po zavedení edge computingu se některé funkce hlavní sítě fyzicky přesunou dále v síti, blíže k přístupovým místům."

Jak hodnotíte tento popis (z roku 2019) z hlediska reálné podoby 5G sítí v současnosti i do budoucna?

Odpověď:

V současné době dochází teprve k začátku implementace 5G sítí a většina 5G sítí je zatím provozována v režimu Non-Standalone.

Otázka 6

Je pravda tvrzení, že "se zvyšuje význam tradičně méně citlivých částí sítě"?

Odpověď:

Ne, nemyslíme si. Naopak dochází k velmi silnému oddělení řídících částí sítě a uživatelské části sítě.

Otázka 7

Je podle vás fyzická přítomnost funkcí jádra sítě blíže k přístupové části sítě zvýšením rizika z hlediska kybernetické bezpečnosti u přístupové části sítě?

Odpověď:

Ne není, je to přesně naopak. V sítích 5G je důsledněji rozdělena řídící rovina a uživatelská rovina.