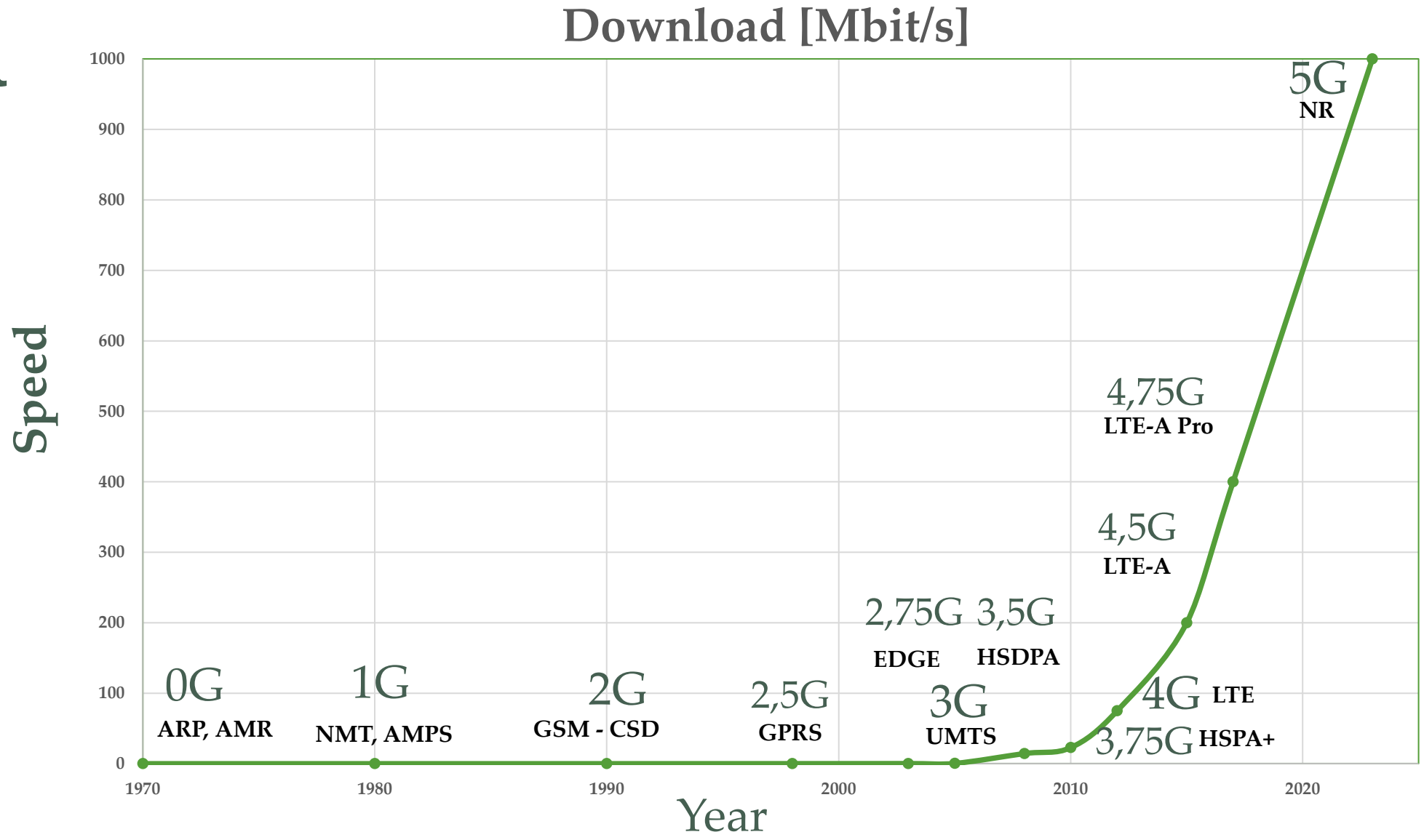
network security

Ing. Michal Poupa
ČVUT CIIRC
e-mail: michal.poupa@gmail.com

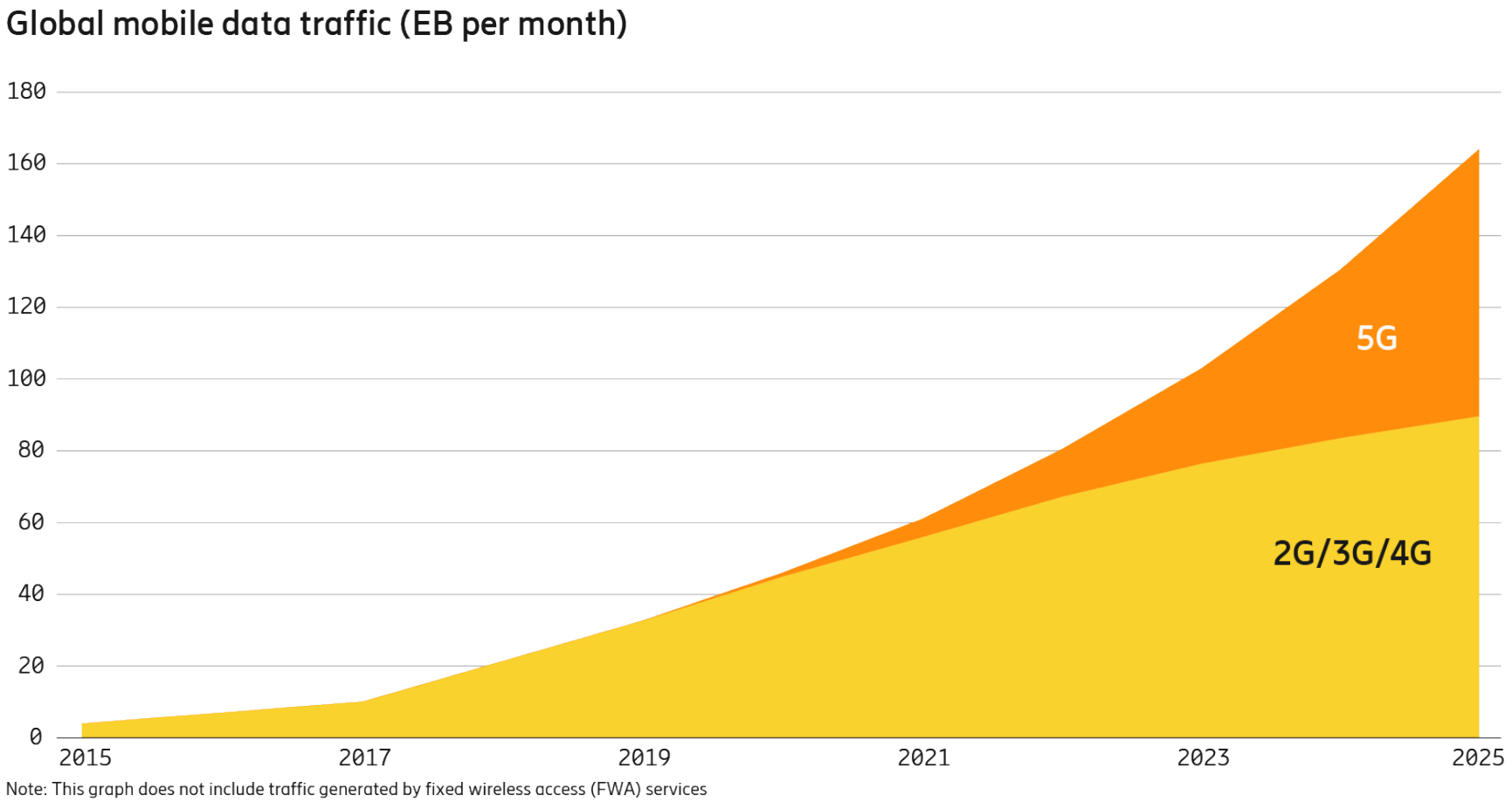
Data


Download [Mbit/s]
Speed
Year
1000
900
800
700
600
500
400
300
200
100
0
1970
1980
1990
2000
2010
2020
0G
ARP, AMR
1G
NMT, AMPS
2G
GSM - CSD
2,5G
GPRS
2,75G
EDGE
3,5G
HSDPA
3G
UMTS
4G
LTE
3,75G
HSPA+
4,5G
LTE-A
4,75G
LTE-A Pro
5G
NR

5G net forecast to carry nearly half of the world's mobile data traffic in 2025

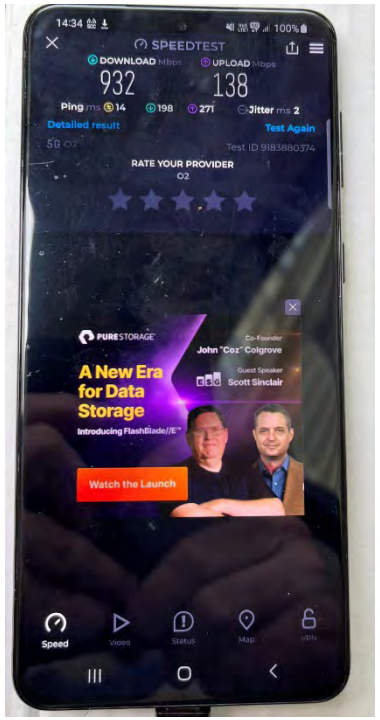
164 EB

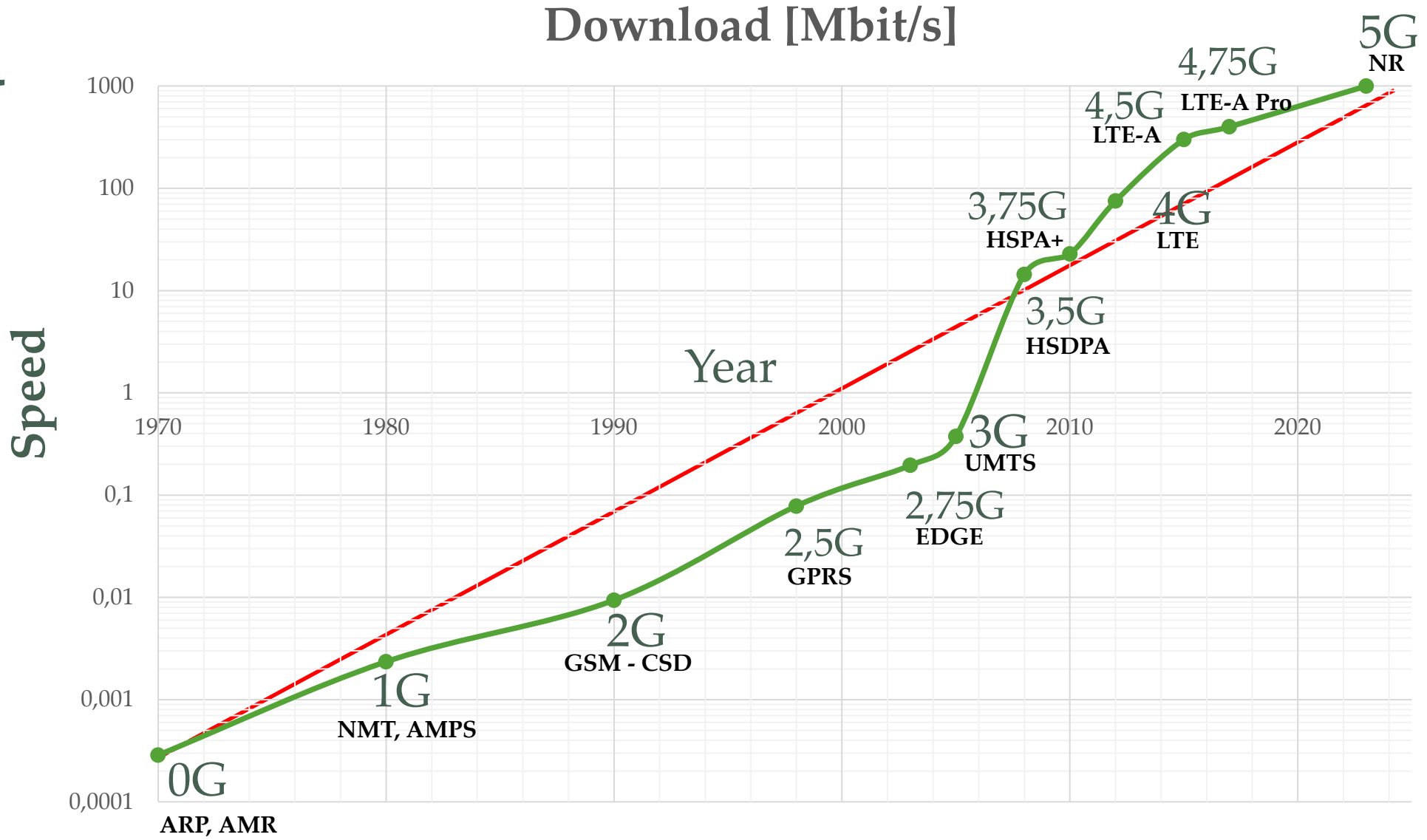
Total traffic predicted to reach 160 exabytes per month in 2025.



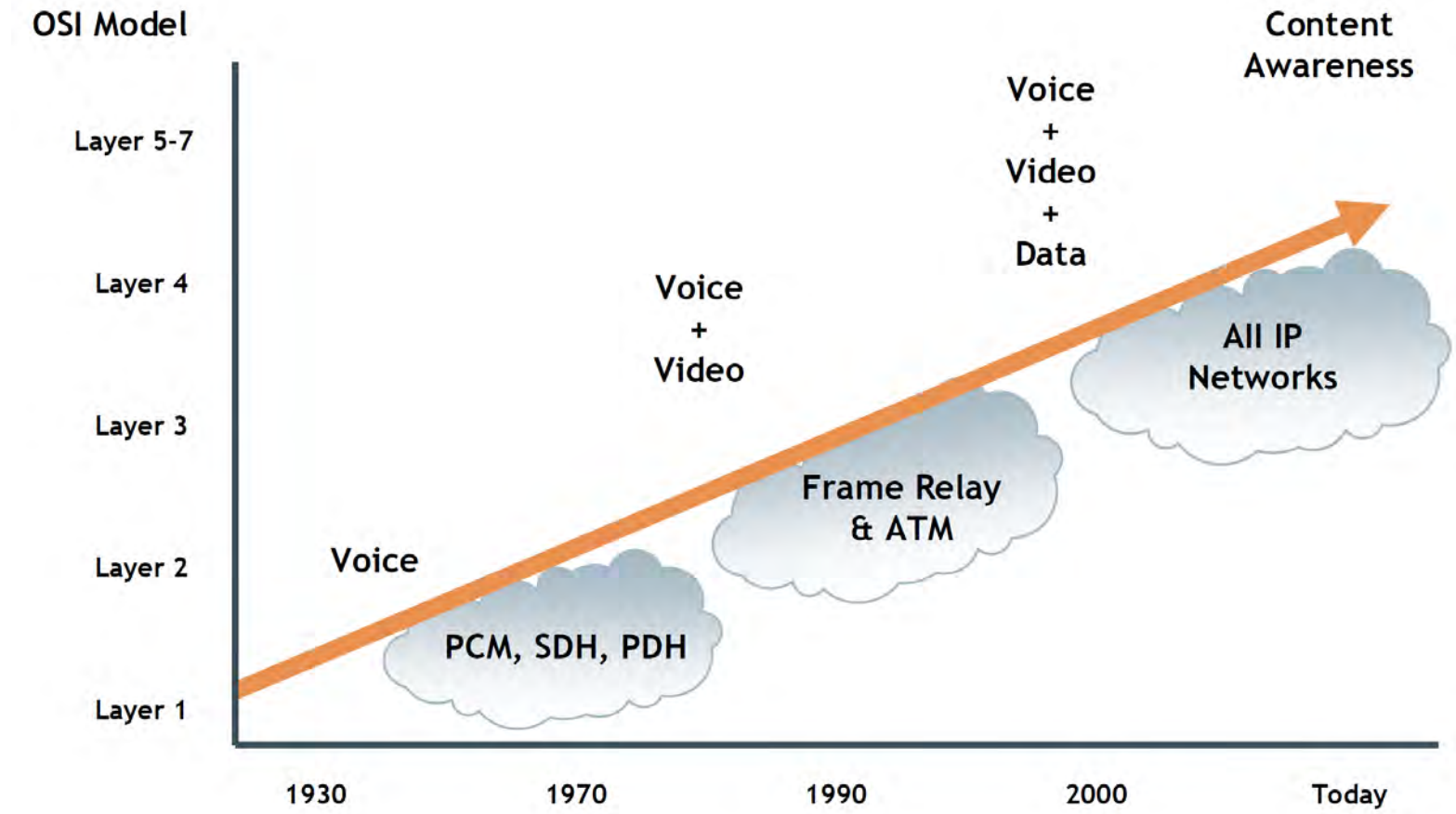
Note: This graph does not include traffic generated by fixed wireless access (FWA) services

Data


SPEEDTEST
DOWNLOAD Mbps
UPLOAD Mbps
932
138
Ping ms 14
198
271
Jitter ms 2
Detailed result
Test Again
RATE YOUR PROVIDER
PURESTORAGE
A New Era for Data Storage
Introducing FlashBlade//E™
Co-Founder
John "Coz" Colgrove
Guest Speaker
Scott Sinclair
Watch the Launch
Speed

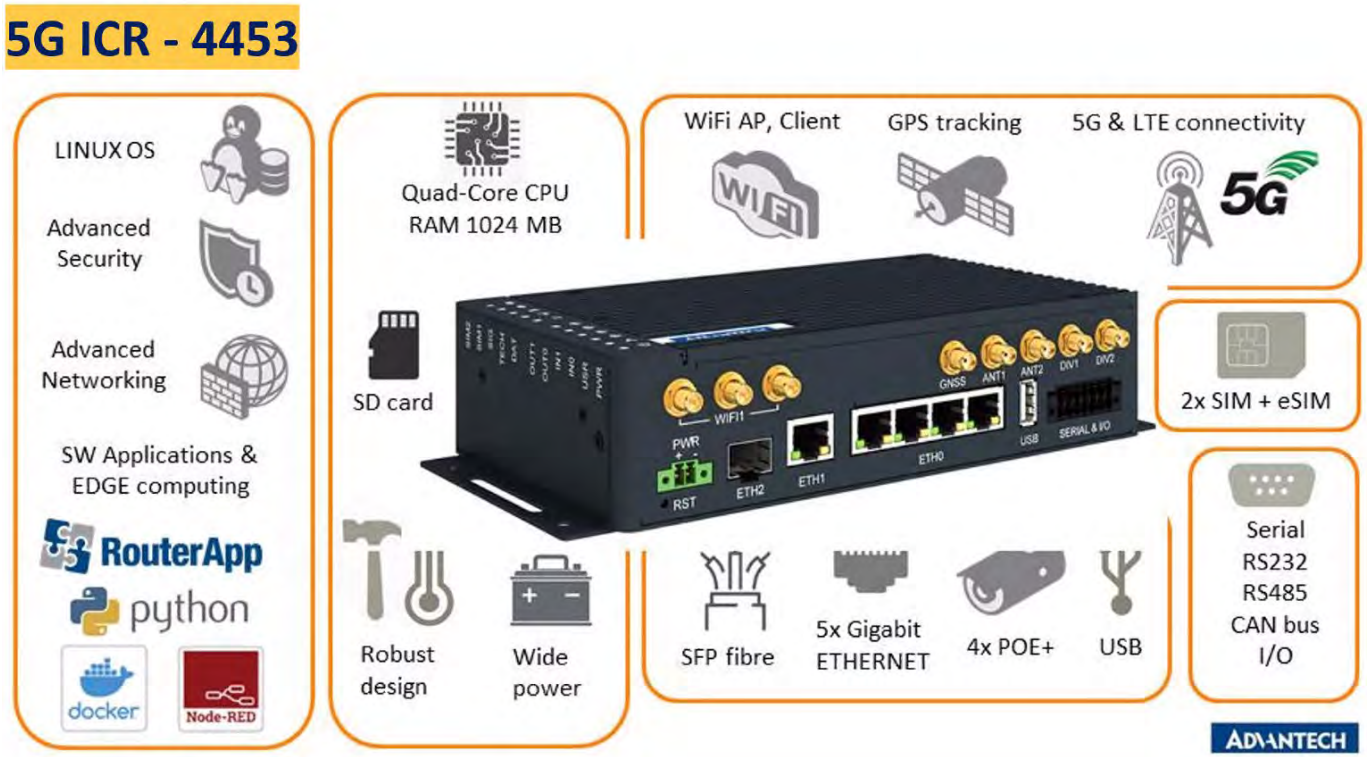

Download [Mbit/s]
Speed
1000
100
10
1
0,1
0,01
0,001
0,0001
Year
1970
1980
1990
2000
2010
2020
0G
ARP, AMR
1G
NMT, AMPS
2G
GSM - CSD
2,5G
GPRS
2,75G
EDGE
3G
UMTS
3,5G
HSDPA
3,75G
HSPA+
4G
LTE
4,5G
LTE-A
4,75G
LTE-A Pro
5G
NR

The Evolution of Infrastructure & Shifting service



Field telephone

5G router ICR-4453



- 5G NR (NSA i SA),
- 2 x USIM, 1 x eSIM
- CPU ARM Cortex-A72
- 5 x ETH 10/100/1000 Mbit/s
- 4 x PoE
- SFP, USB
- RS232, RS485, CAN, IO
- 9 až 48 V

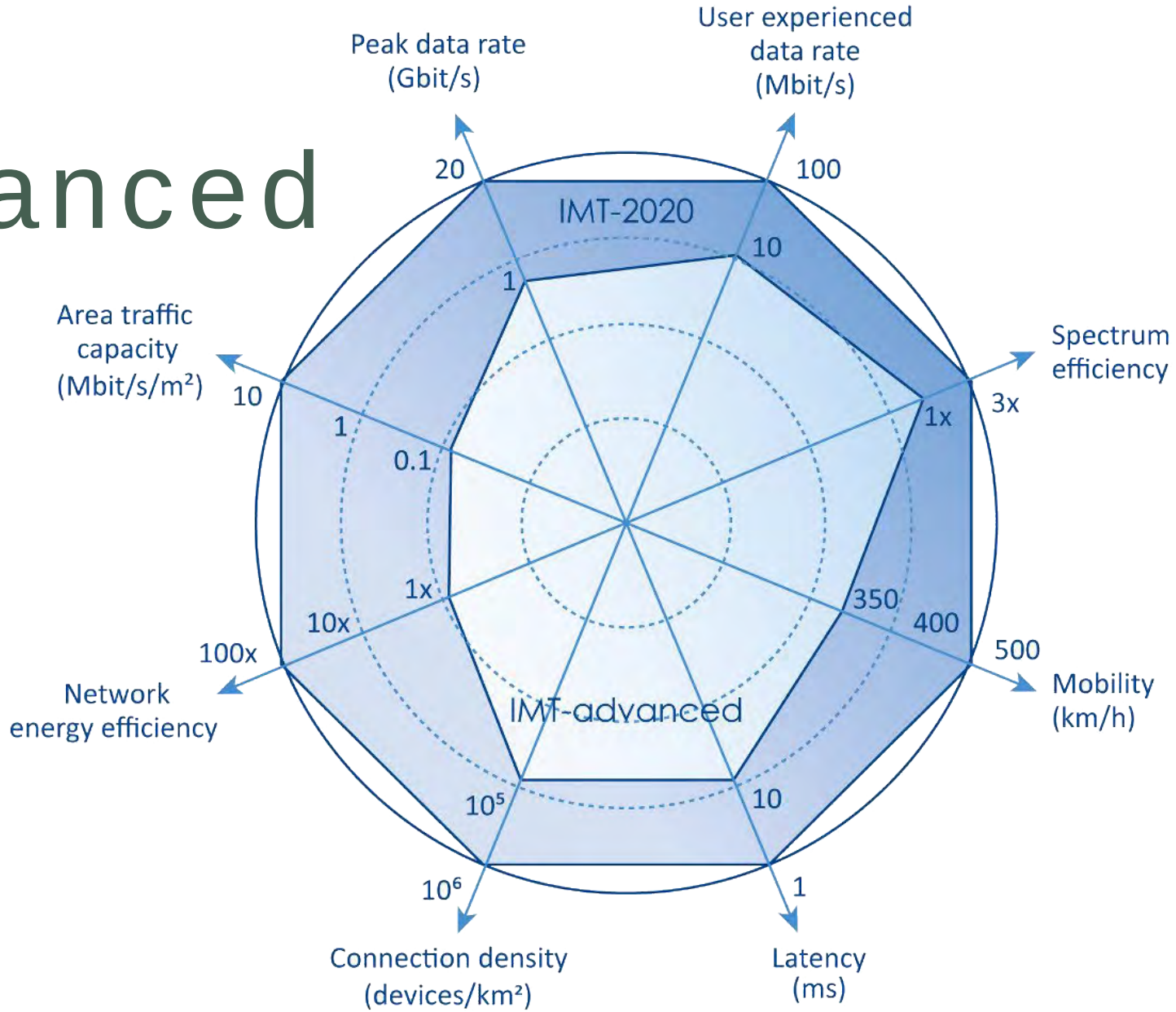
The Evolution of mobile networks

Circuit-only	Circuit & Packet	Packet-only
CS Voice, SMS, (CS Data)	Voice, SMS, (CS Data)	
	PS Data	Data, Voice, SMS VoLTE, VoNR
GSM	GPRS, EGRS, UMTS	EPS, 5G core
2G	2,5G – 3,75G	4G LTE, 5G NR

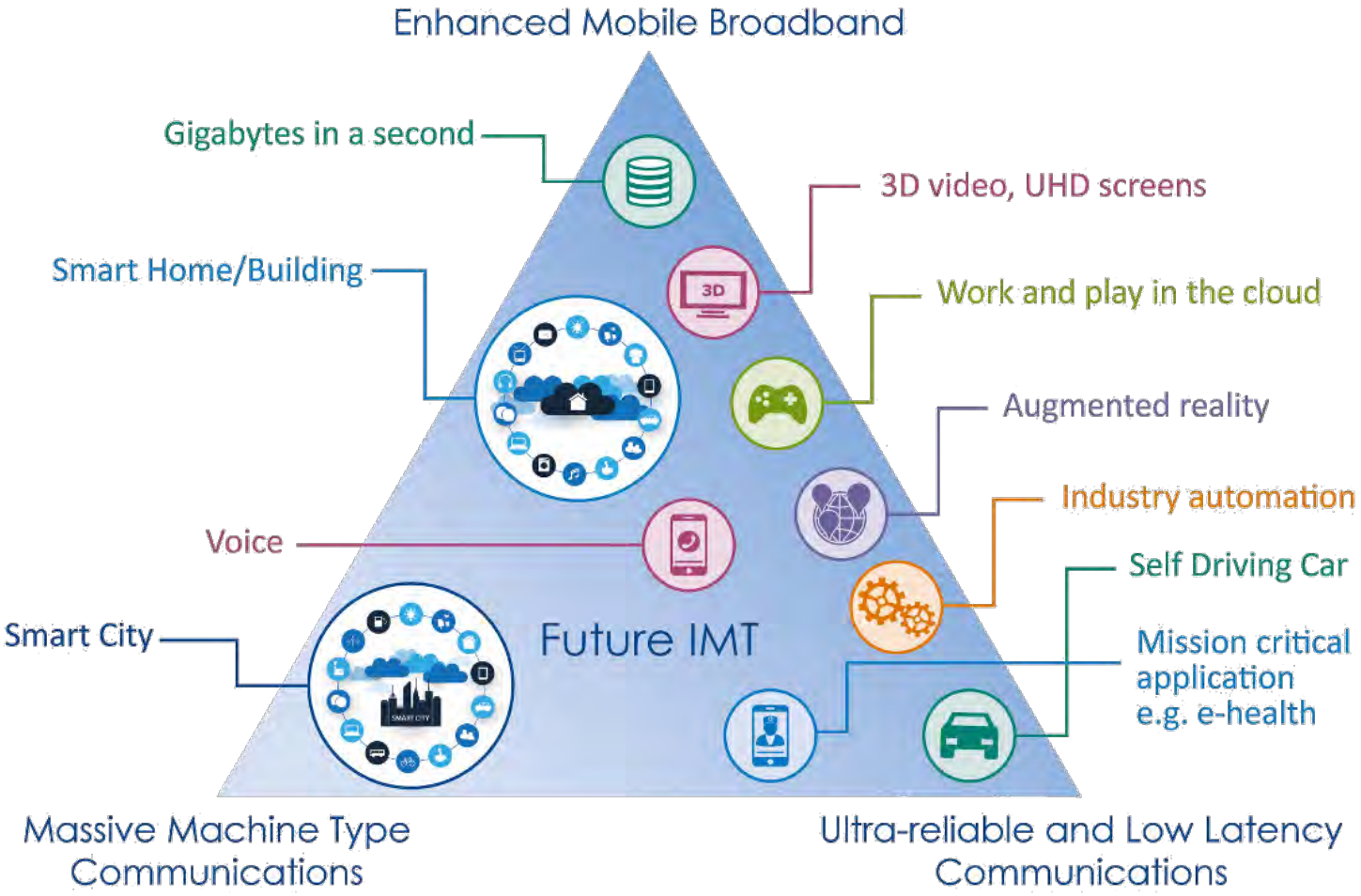
5G – Main Requirements

- 1-10 Gbit/s connections to end points in the field (not theoretical maximum)
- 1 millisecond end-to-end round-trip delay – latency
- 1000x bandwidth per unit area
- 10-100x number of connected devices
- Perception of 99.999% availability
- Perception of 100% coverage
- 90% reduction in network energy usage
- Up to 10 years battery life for low power, machine-type devices

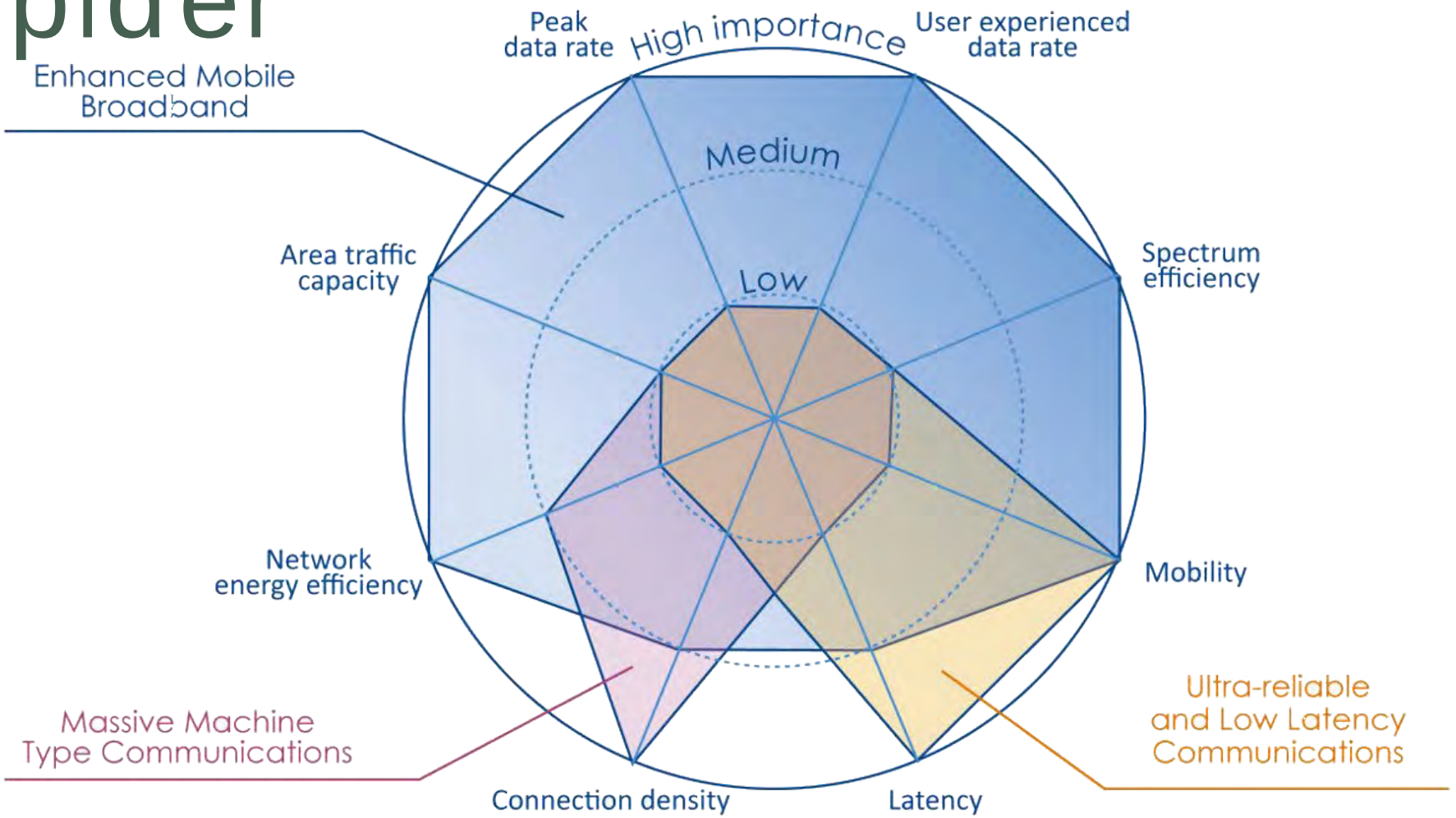
IMT-2020
IMT-advanced



5G – type of communication



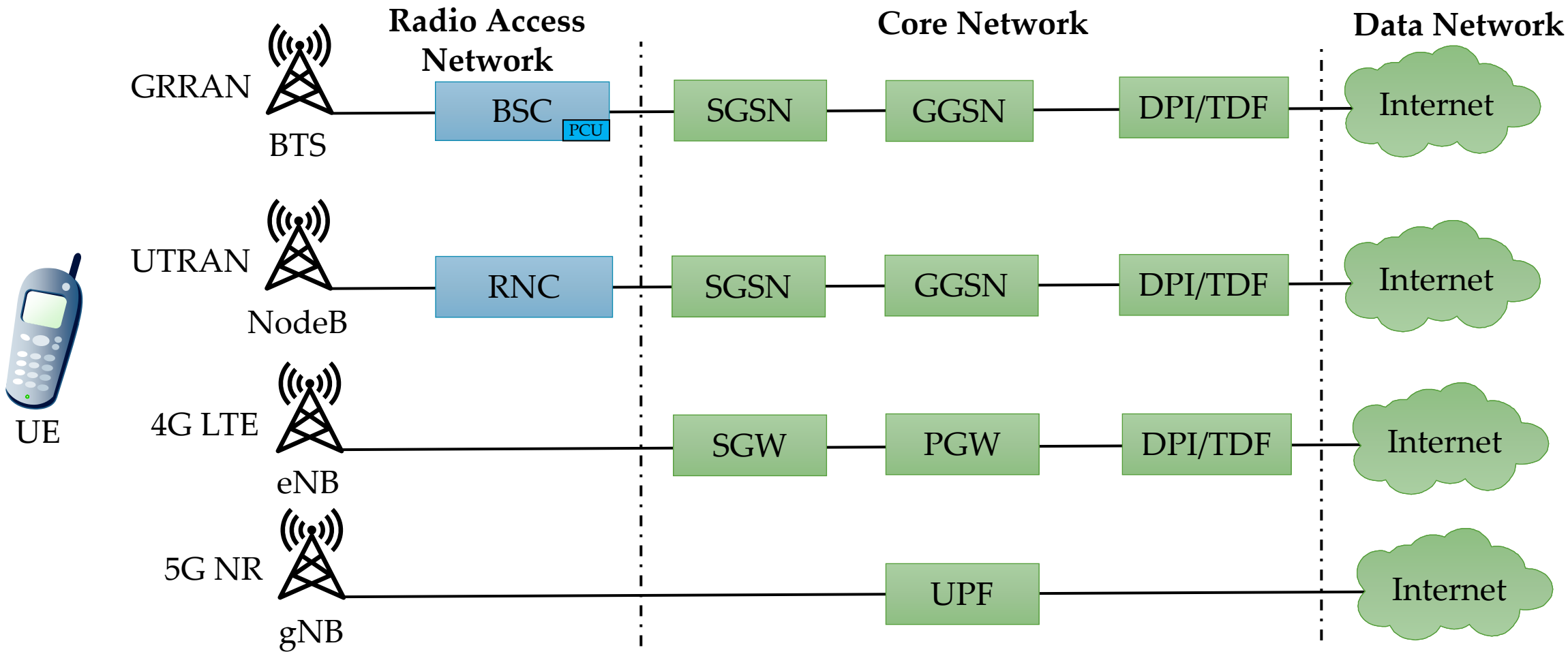
5G – Spider


Peak data rate
High importance
User experienced data rate
Enhanced Mobile Broadband
Medium
Area traffic capacity
Low
Spectrum efficiency
Network energy efficiency
Mobility
Massive Machine Type Communications
Ultra-reliable and Low Latency Communications
Connection density
Latency

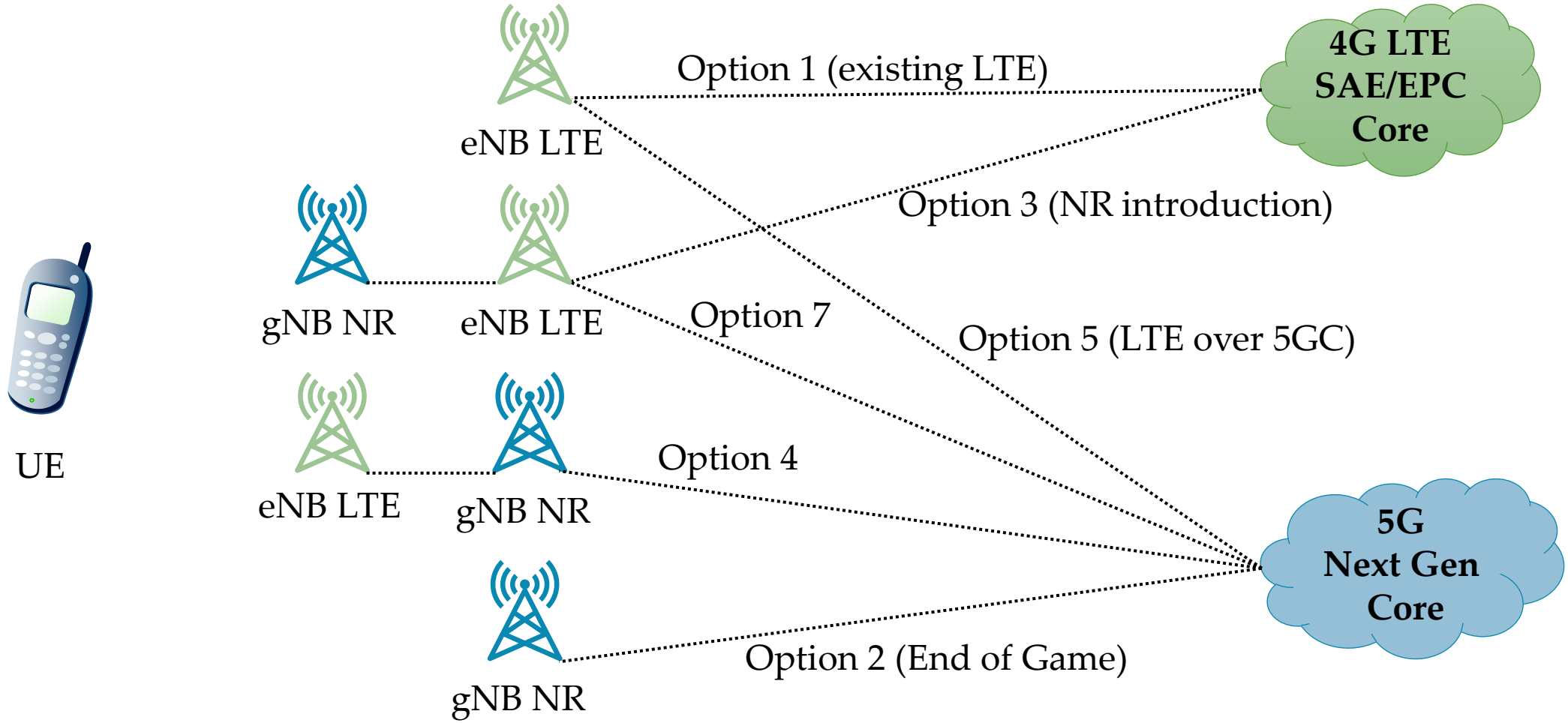
5G Cases according ITU-R

- **Enhanced Mobile Broadband (eMBB**) to deal with hugely increased data rates, high user density and very high traffic capacity for hotspot scenarios as well as seamless coverage and high mobility scenarios with still improved used data rates
- **Massive Machine-type Communications (mMTC)** for the IoT, requiring low power consumption and low data rates for very large numbers of connected devices
- **Ultra-reliable and Low Latency Communications (uRLLC)** to cater for safety-critical and mission critical applications

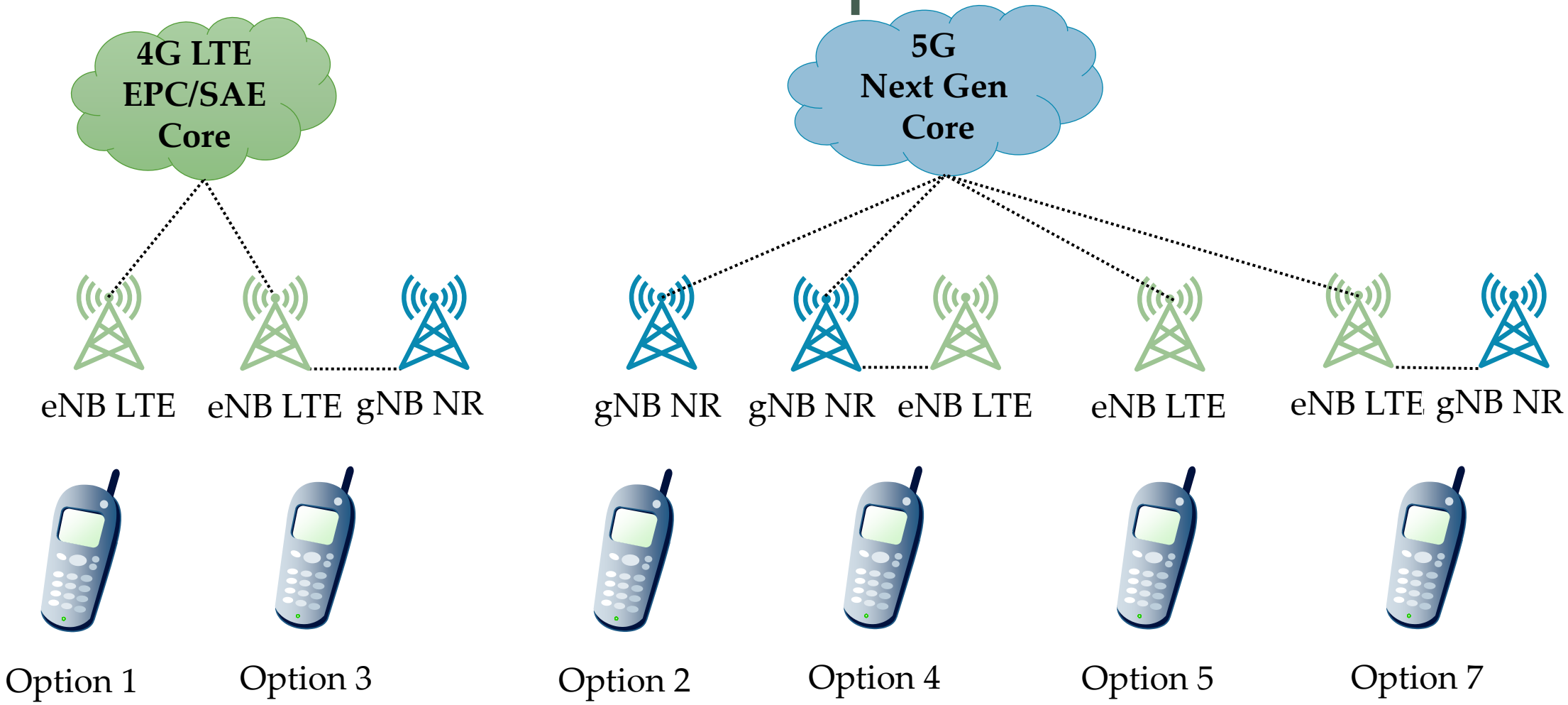
Architecture 2G, 3G, 4G & 5G



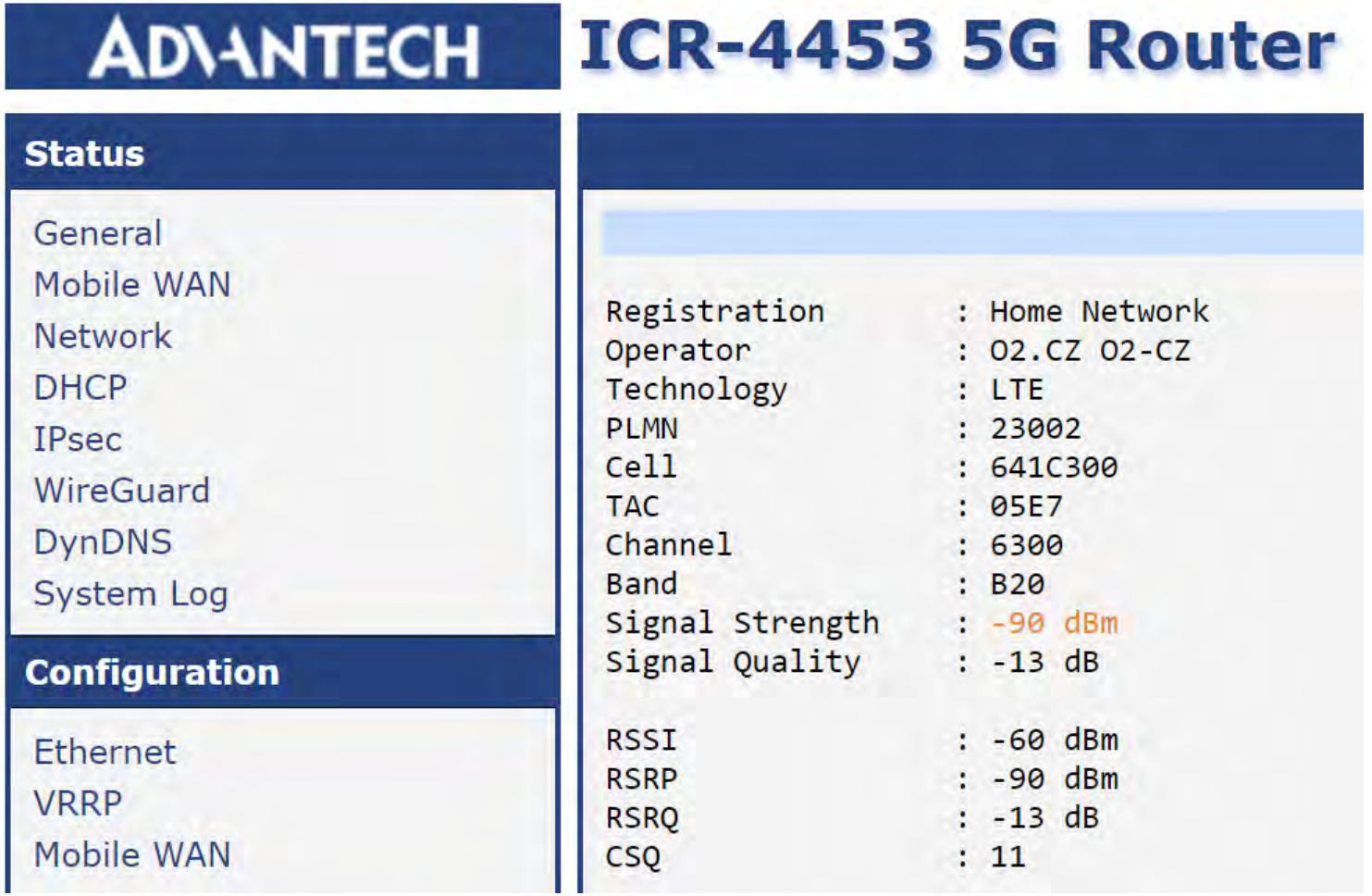
5G architecture options



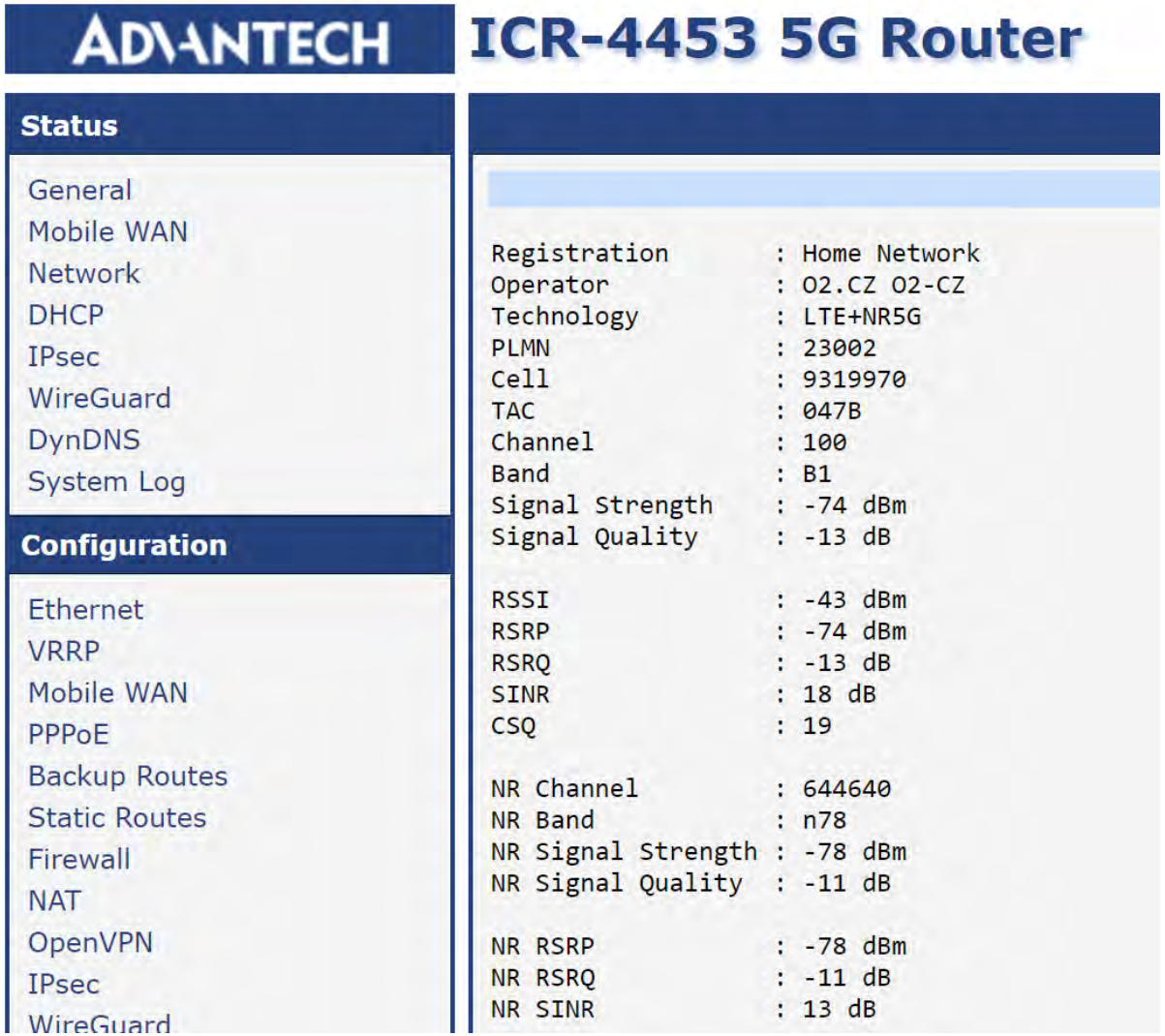
From 4G to 5G / Options



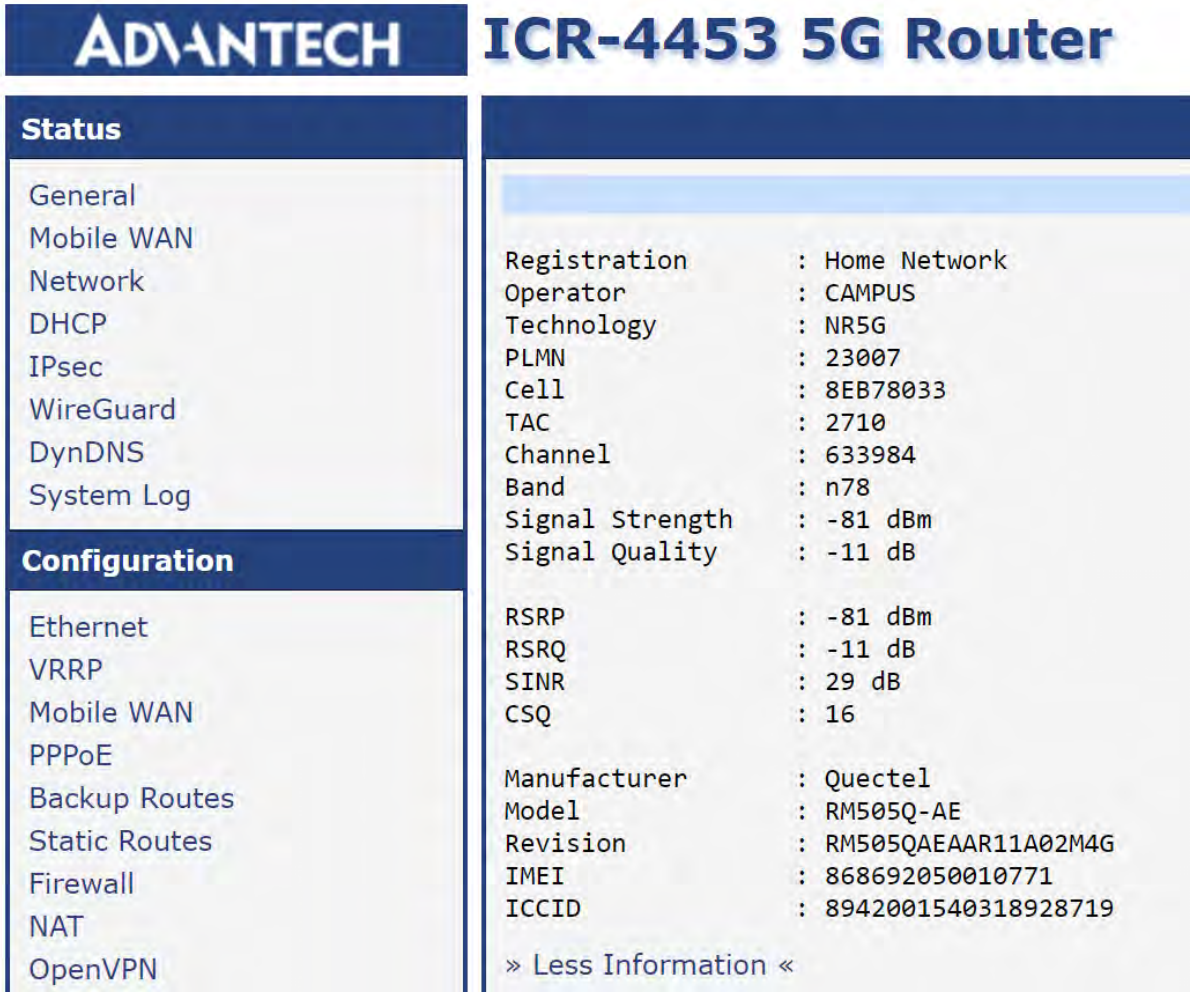
Long-Term Evolution (LTE)



LTE+5G NR Non-Standalone Mode (NSA)



5G NR Standalone Mode (SA)



ping & jitter SA network

```
PACKET JITTER v1.5 & RFC 1889
PING 10.81.40.97 (10.81.40.97): 56 data bytes
64 bytes from 10.81.40.97: seq=0 ttl=254 time=10.862 ms
64 bytes from 10.81.40.97: seq=1 ttl=254 time=10.233 ms jitter=0.629 ms avg=0.629 ms rfc_jitter=0.676 ms
64 bytes from 10.81.40.97: seq=2 ttl=254 time=9.686 ms jitter=0.547 ms avg=0.588 ms rfc_jitter=0.668 ms
64 bytes from 10.81.40.97: seq=3 ttl=254 time=10.278 ms jitter=0.592 ms avg=0.589 ms rfc_jitter=0.663 ms
64 bytes from 10.81.40.97: seq=4 ttl=254 time=9.654 ms jitter=0.624 ms avg=0.598 ms rfc_jitter=0.661 ms
64 bytes from 10.81.40.97: seq=5 ttl=254 time=10.263 ms jitter=0.609 ms avg=0.600 ms rfc_jitter=0.657 ms
64 bytes from 10.81.40.97: seq=6 ttl=254 time=9.681 ms jitter=0.582 ms avg=0.597 ms rfc_jitter=0.653 ms
64 bytes from 10.81.40.97: seq=7 ttl=254 time=10.289 ms jitter=0.608 ms avg=0.599 ms rfc_jitter=0.650 ms
64 bytes from 10.81.40.97: seq=8 ttl=254 time=9.685 ms jitter=0.604 ms avg=0.599 ms rfc_jitter=0.647 ms
64 bytes from 10.81.40.97: seq=9 ttl=254 time=10.331 ms jitter=0.646 ms avg=0.605 ms rfc_jitter=0.647 ms

--- 10.81.40.97 ping statistics ---
9 jitters count
jitter min/avg/max = 0.547/0.605/0.646 ms, RFC1889 jitter 0.647 ms
rtt-1 min/avg/max = 9.654/10.011/10.331 ms
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 9.654/10.096/10.862 ms
```

ping & jitter SA network

```
PACKET JITTER v1.5 & RFC 1889
PING 1.1.1.1 (1.1.1.1): 56 data bytes
64 bytes from 1.1.1.1: seq=0 ttl=56 time=12.369 ms
64 bytes from 1.1.1.1: seq=1 ttl=56 time=10.522 ms jitter=1.847 ms avg=1.847 ms rfc_jitter=0.840 ms
64 bytes from 1.1.1.1: seq=2 ttl=56 time=9.786 ms jitter=0.736 ms avg=1.292 ms rfc_jitter=0.834 ms
64 bytes from 1.1.1.1: seq=3 ttl=56 time=11.488 ms jitter=1.702 ms avg=1.428 ms rfc_jitter=0.888 ms
64 bytes from 1.1.1.1: seq=4 ttl=56 time=10.677 ms jitter=0.811 ms avg=1.274 ms rfc_jitter=0.883 ms
64 bytes from 1.1.1.1: seq=5 ttl=56 time=8.780 ms jitter=1.897 ms avg=1.399 ms rfc_jitter=0.947 ms
64 bytes from 1.1.1.1: seq=6 ttl=56 time=11.190 ms jitter=2.410 ms avg=1.567 ms rfc_jitter=1.038 ms
64 bytes from 1.1.1.1: seq=7 ttl=56 time=9.386 ms jitter=1.804 ms avg=1.601 ms rfc_jitter=1.086 ms
64 bytes from 1.1.1.1: seq=8 ttl=56 time=10.586 ms jitter=1.200 ms avg=1.551 ms rfc_jitter=1.093 ms
64 bytes from 1.1.1.1: seq=9 ttl=56 time=8.892 ms jitter=1.694 ms avg=1.567 ms rfc_jitter=1.131 ms

--- 1.1.1.1 ping statistics ---
9 jitters count
jitter min/avg/max = 0.736/1.567/2.410 ms, RFC1889 jitter 1.131 ms
rtt-1 min/avg/max = 8.780/10.145/11.488 ms
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 8.780/10.367/12.369 ms
```

5G current state

- Current 5G / NSA - 4G SAE/EPC core & new gNB 5G NR (option 3)
- Standalone (SA) x NonStandalone (NSA)
- Standalone only private / 5G campus network
- 5G core x 4G EPC core
- Band FR1 – 700 MHz; 2 GHz; 3,5 GHz; 5 , 6 & 7 GHz
- Bands over existing 2G, 3G and 4G networks,
- Dynamic Spectrum Sharing (DSS) 4G LTE & 5G NR
- New Bands mmWave, FR2 – 26, 28, 39 & 41 GHz
- Carrier aggregation & Dual connectivity

2G, 3G & 4G security

SIM contains a secret key Ki which is also stored in HLR AuC (2G, 3G) or HSS (3G, 4G)

Algorithms that are used for encryption in GSM:

- A3 – authentication algorithm
- A5 – encryption algorithm (only – 54 bits)
- A8 – Kc key generator for voice communication

2G security

Anonymity – good: temporary identity via TIMSI

Authentication – poor: only one-way

- fake-BTS (one way authentication)
- voice encrypted only between UE and BTS
- short key – 54 bits only
- authentication data including KC key is transmitted in open form between mobile networks

Integrity of data – none

Signaling: SS7 no protection

3G UMTS security

Anonymity – the same as in GSM (via temporary identity)

Encryption – better than GSM

- Better algorithm, long enough keys
- Voice encrypted only between UE and NodeB
- Data encrypted only between NodeB and 3G SGSN
- New f8, f9 algorithms
- Integrity – better than in GSM (f1)

UMTS and GSM compatibility

- GSM users have UMTS level security GSM

4G LTE security

Very similar to 3G UMTS:

- Same authentication
- Different encryption algorithm
- No end-to-end security, only between UE and network
- For end2end security must be used higher layers protocols like: TLS, SSH, IPsec, OpenVPN, …

Signaling is partially protected via EPC-DIAMETER protocol

Security – Authentication Vectors

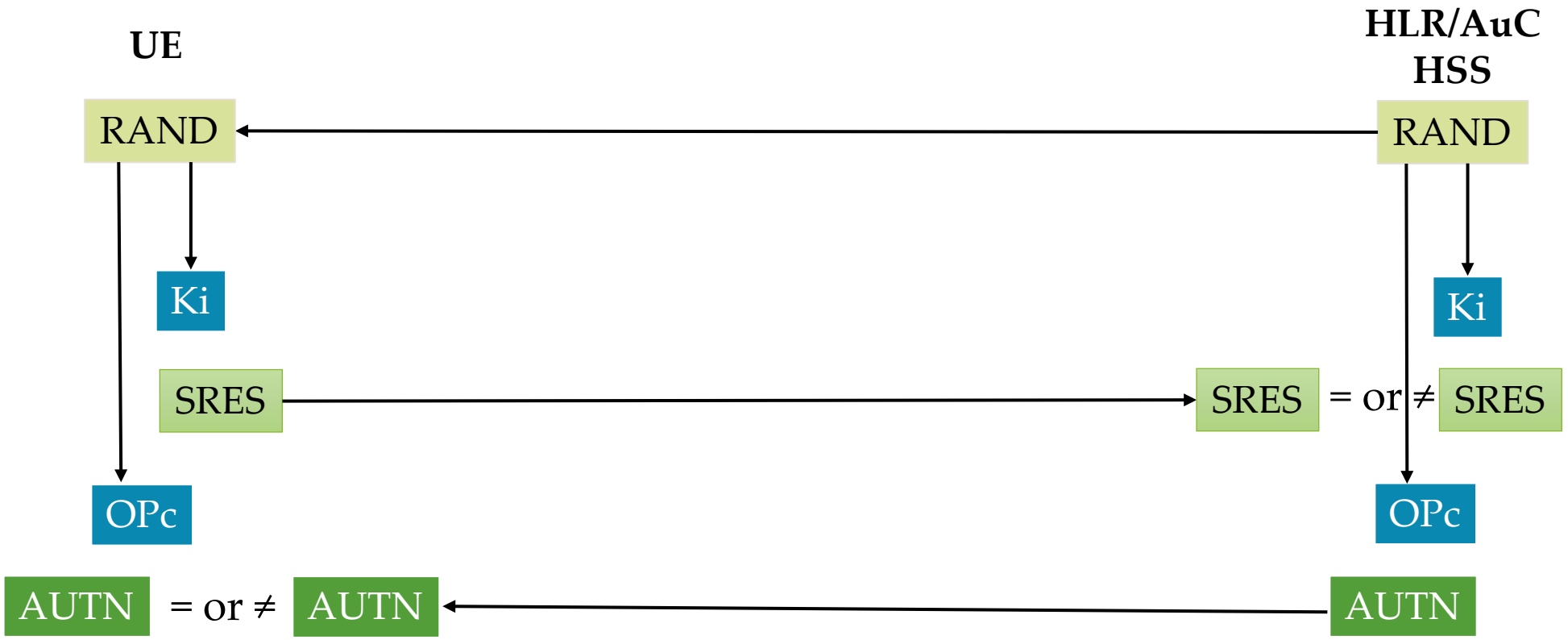
GSM (R98) : Triplet / SIM 2G, 3G

- RAND – network challenge (128 bits)
- SRES – expected user response (32 bits)
- K (Ki) – cipher or secret key (64 bits)

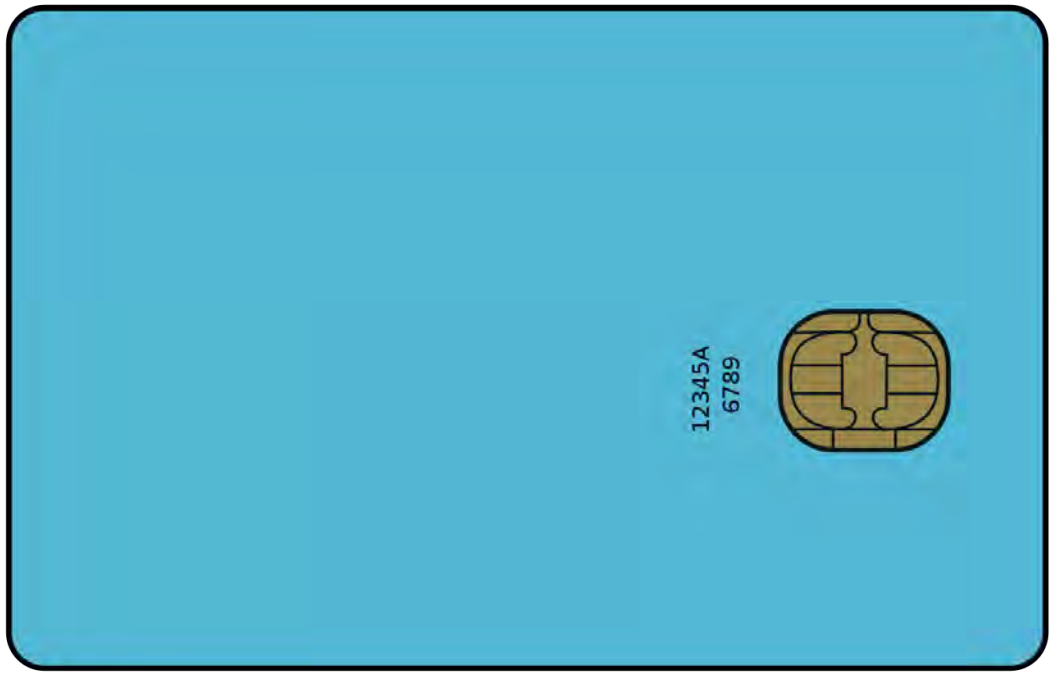
UMTS (R99) : Quintet / USIM 4G, 5G

- RAND – network challenge (128 bits)
- XRES – expected user response (32 – 128 bits)
- K (Ki) – cipher or secret key (128 bits)
- OPc (Operator key) or IK (Integrity Key) (128 bits)
- AUTN – network authentication token (128 bits)

Authentication Vectors 2G, 3G & 4G



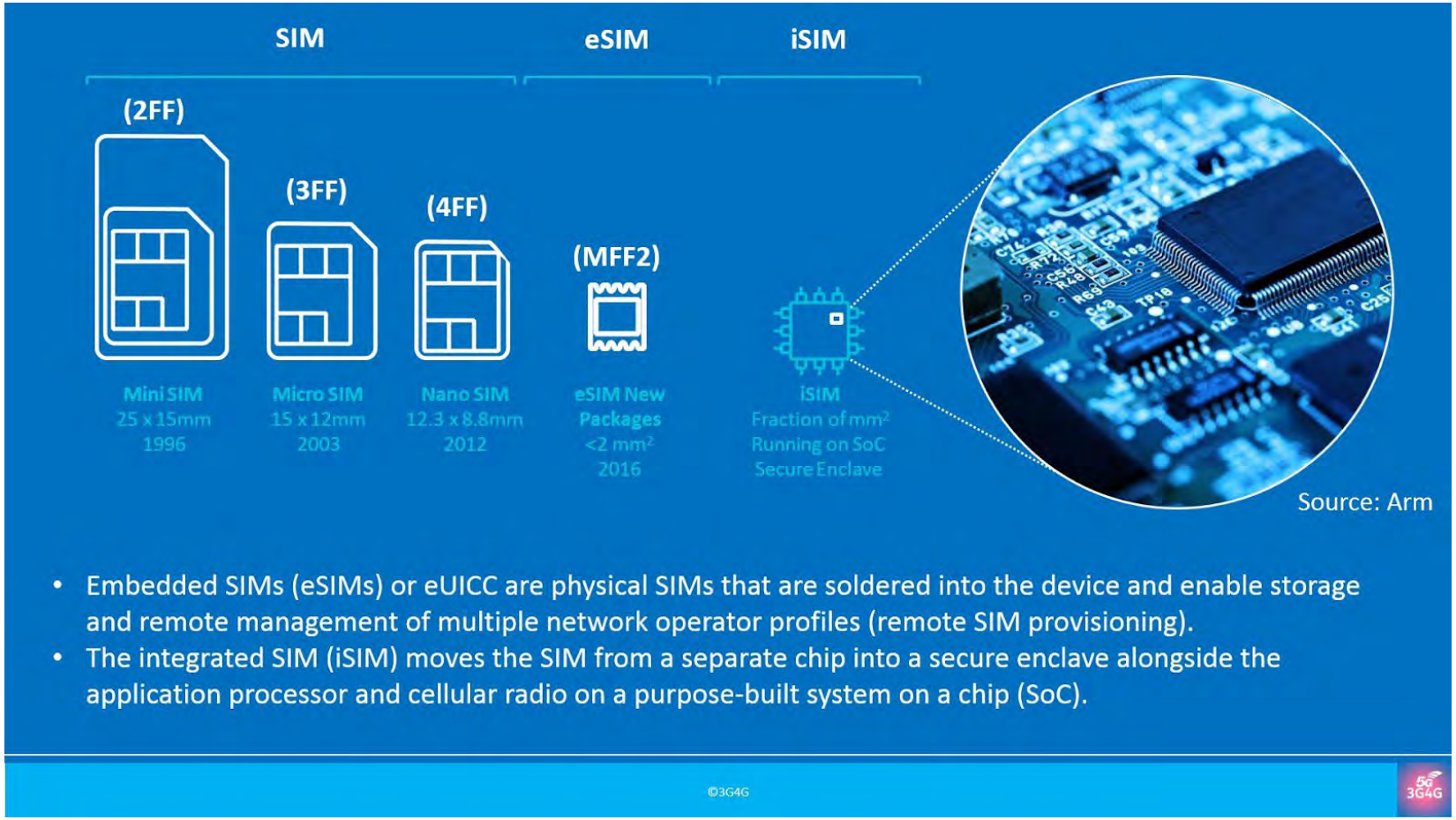
Full-size, Mini, Micro, Nano



Format	Year
Full-size (1FF)	1991
Mini-SIM (2FF)	1996
Micro-SIM (3FF)	2003
Nano-SIM (4FF)	2012
Embedded-SIM (eSIM)	2016

FF (Form Factor)

Full-size, Mini, Micro, Nano



SIM, USIM, UICC, Smart Cards

- **SIM –** When GSM was already in use, the specifications were further developed and enhanced with functionality such as SMS and GPRS. These development steps are referred as releases by ETSI. Within these development cycles, the SIM specification was enhanced as well: new voltage classes, formats and files were introduced.

- **USIM (Universal Subscriber Identity Module) –** In GSM-only times, the SIM consisted of the hardware and the software. With the advent of UMTS, this naming was split: the SIM was now an application and hence only software. The hardware part was called UICC. This split was necessary because UMTS introduced a new application, the USIM. The USIM brought, among other things, security improvements like mutual authentication and longer encryption keys and an improved address book.

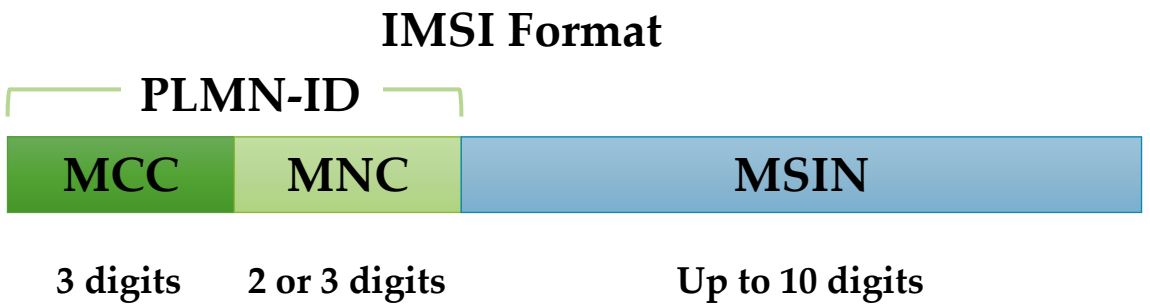
- **UICC (Universal Integrated Circuit Card) - Smart card** - "SIM cards" in developed countries today are usually UICCs containing at least a SIM application and a USIM application. This configuration is necessary because older GSM only handsets are solely compatible with the SIM application and some UMTS security enhancements rely on the USIM application.

SIM vs eSIM (embedded-SIM)

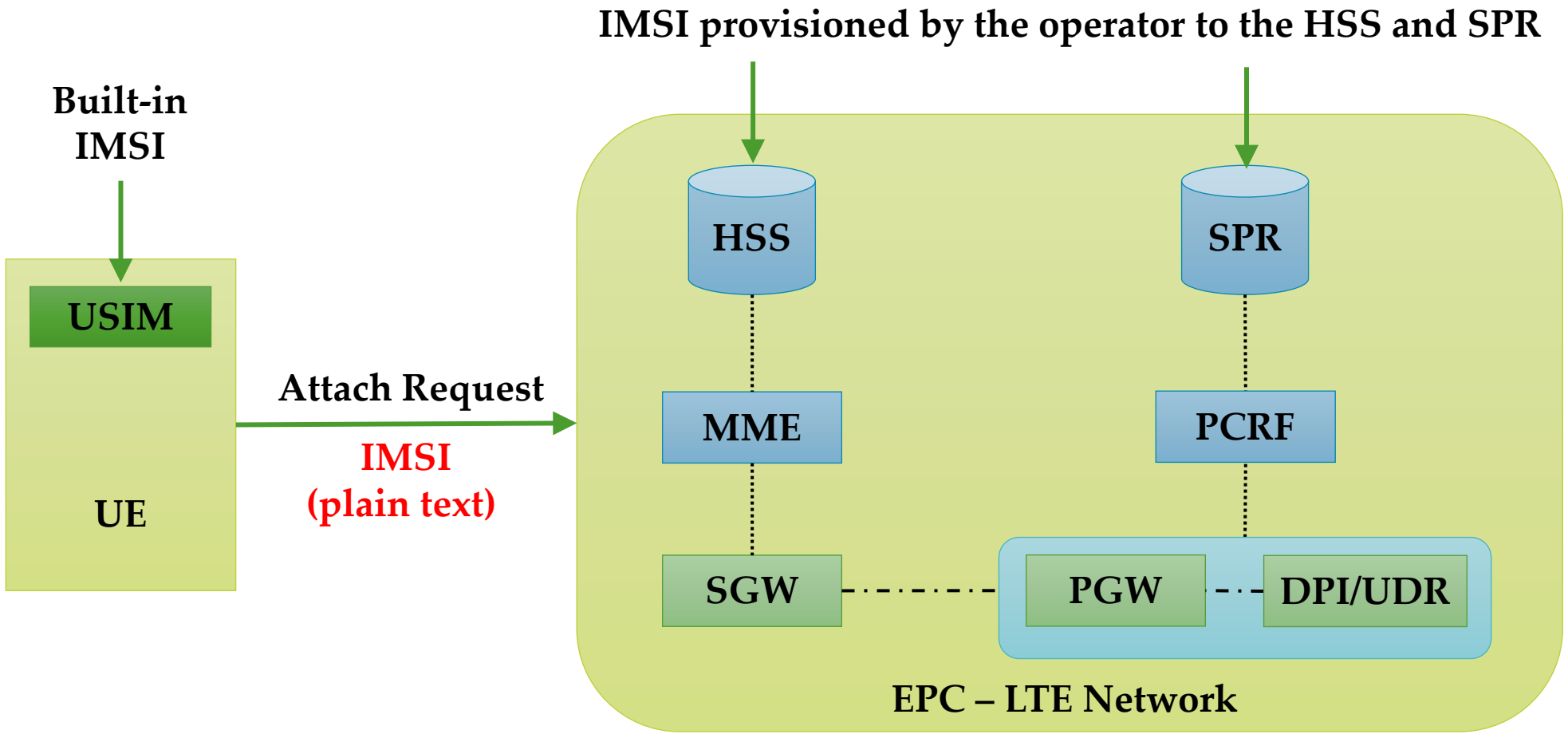
- An embedded-SIM (eSIM), or embedded universal integrated circuit card (eUICC), is a form of programmable SIM that is embedded directly into a device.
- A first version of the standard was published in March 2016, followed by a second version in November 2016.
- eSIM is a global specification by the GSMA that enables remote SIM provisioning of any mobile device. GSMA defines eSIM as the SIM for the next generation of connected consumer devices.
- Provisioning via QR code – need connectivity e.g. Wi–Fi

International Mobile Subscriber Identity

- International Mobile Subscriber Identity (IMSI)
- Main identifier – Built in SIM or USIM
- Mobile Subscription Identification Number (MSIN)
- MSIN first two digits usually umber of HLR/HSS/UDM
- Example MCC 230
- Example MNC 01, 02, 03



IMSI Allocation

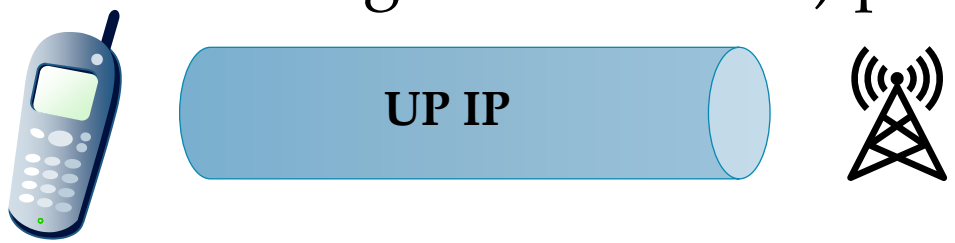


Fundamental security features of 2G, 3G, 4G & 5G

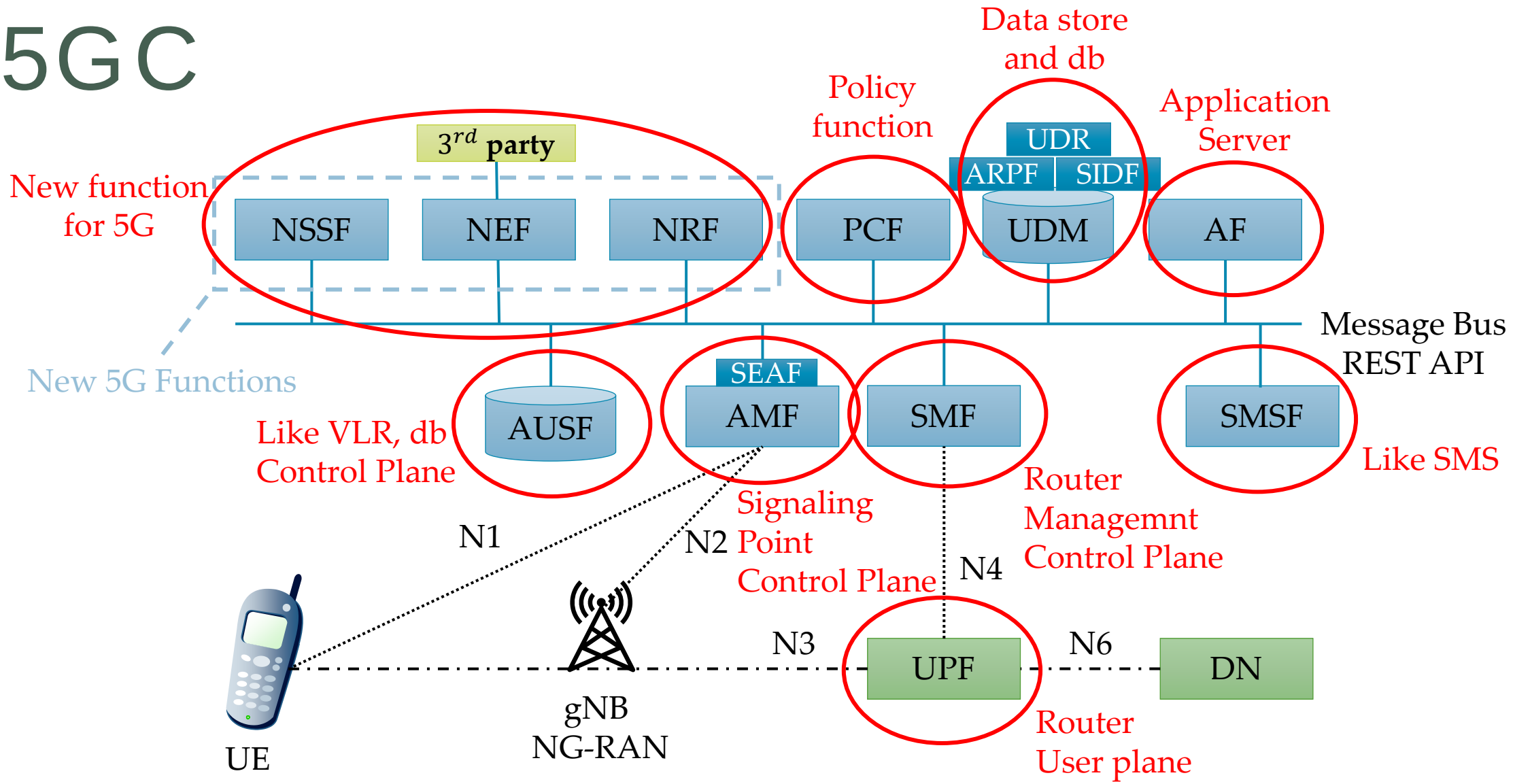
Security features/Mobile Technology	2G	3G	4G	5G
Subscriber/device authentication to network	Y	Y	Y	Y
Network authentication to Device/Subscriber	N	Y	Y	Y
Interconnect Authentication	N	N	N	Y
IPSec	N	Optional	Optional	Y
Data Origin End to End – Integrity	N	N	N	Y
Data Encryption End to End – Confidentiality	N	N	N	Y
The Subscriber Identity De-concealing Function	N	N	N	Y

5G Security enhancements

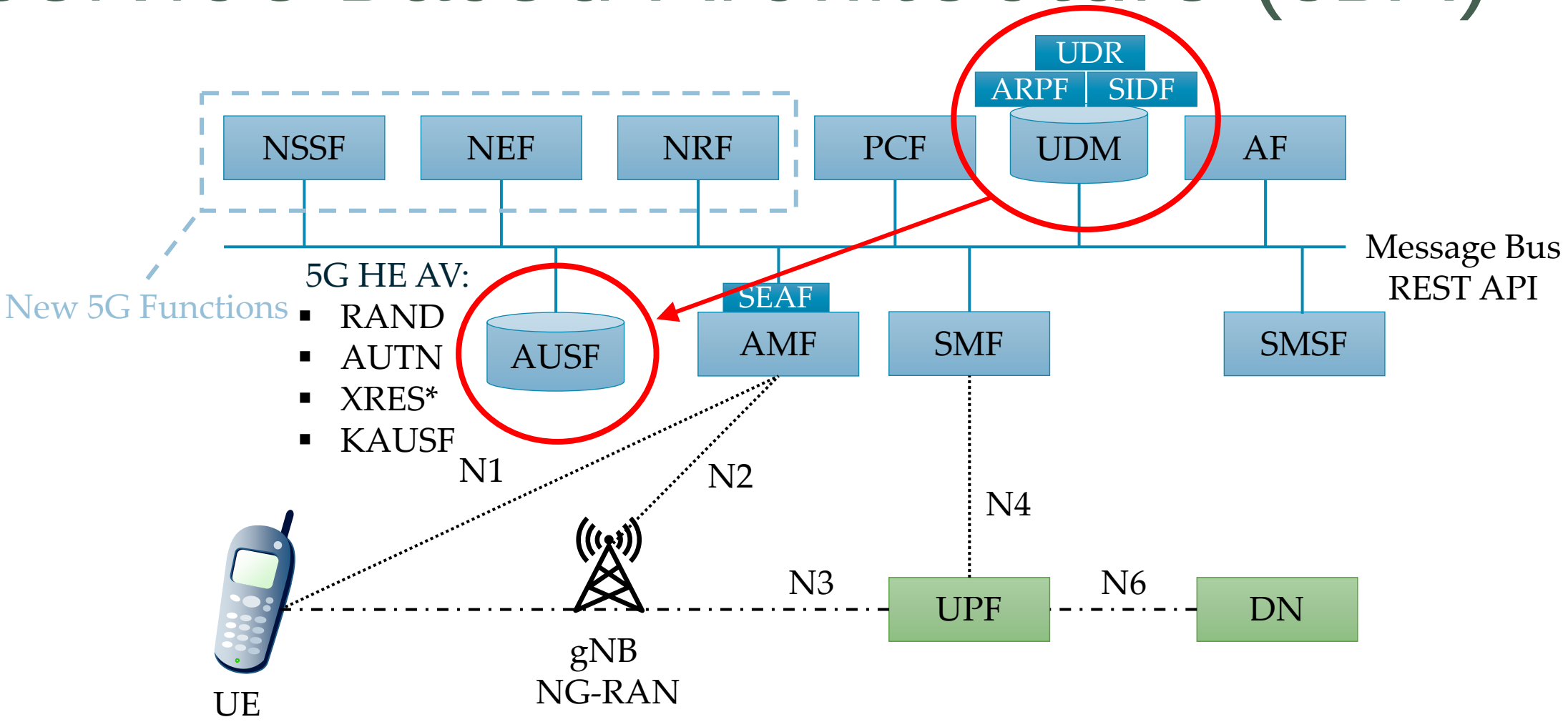
- Improved key hierarchy, algorithm flexibility (5G AKA, EAP-AKA)
- Subscriber policy – SUCI/SUPI (Subscription Concealed Identifier / Subscription Permanent Identifier), Subscriber paging by SUCI
- Interconnect security SEEP (Security Edge Protection Proxy) CP signaling and UP GTP attack
- Service Based Interface Security
- User plane Integrity Protection UP IP (serious 4G/LTE problem)
- 5G introduce PDCP (Packet Data Convergence Protocol) protection (in 4G LTE CP only)



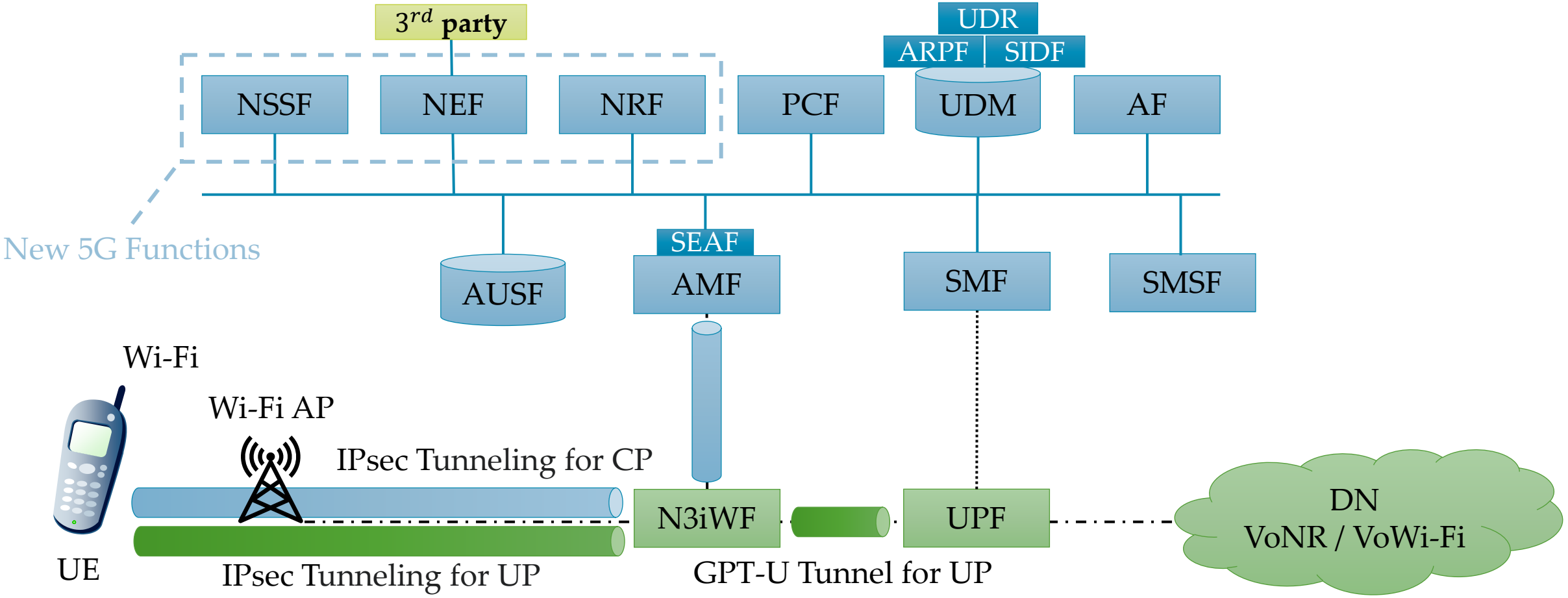
5GC


Data store
and db
Policy
function
Application
Server
New function
for 5G
3rd party
UDR
ARPF
SIDF
NSSF
NEF
NRF
PCF
UDM
AF
Message Bus
REST API
New 5G Functions
SEAF
AUSF
AMF
SMF
SMSF
Like VLR, db
Control Plane
Like SMS
Router
Managemnt
Control Plane
Signaling
Point
Control Plane
N1
N2
N4
N3
N6
UPF
DN
gNB
NG-RAN
UE
Router
User plane

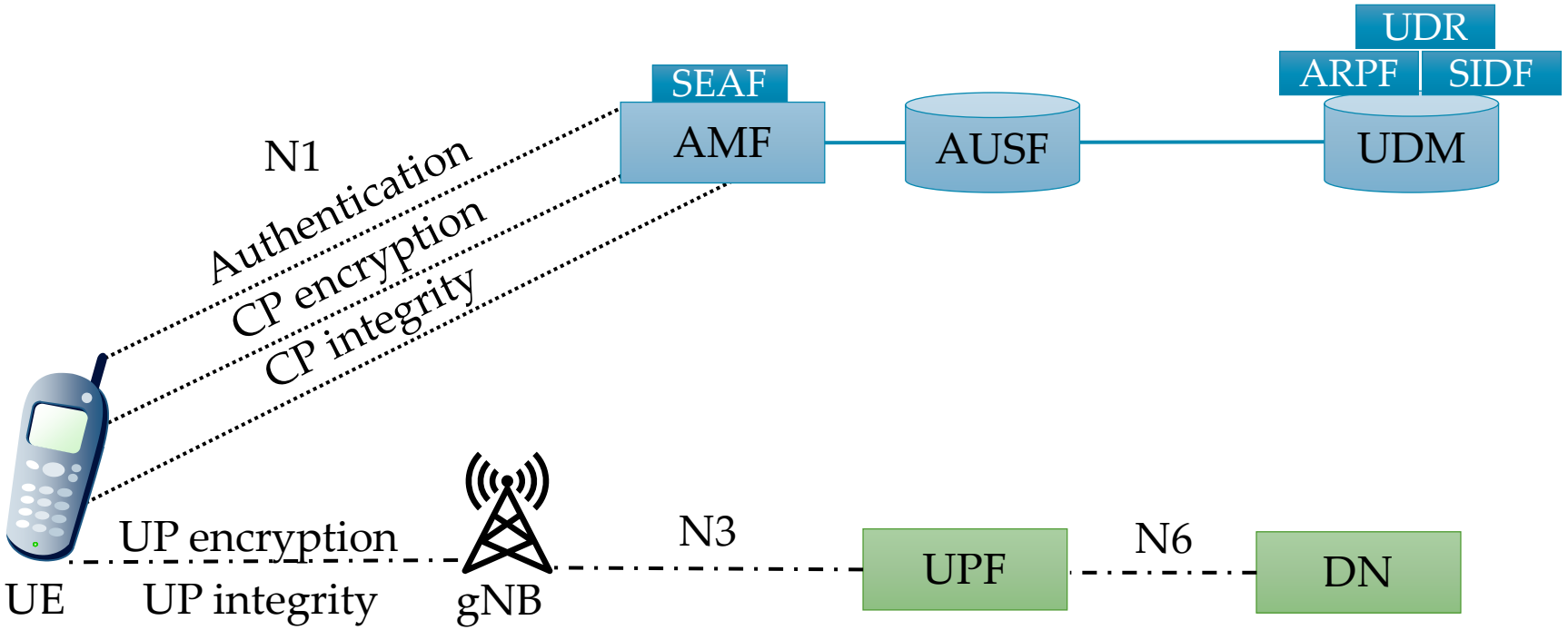
Service Based Architecture (SBA)



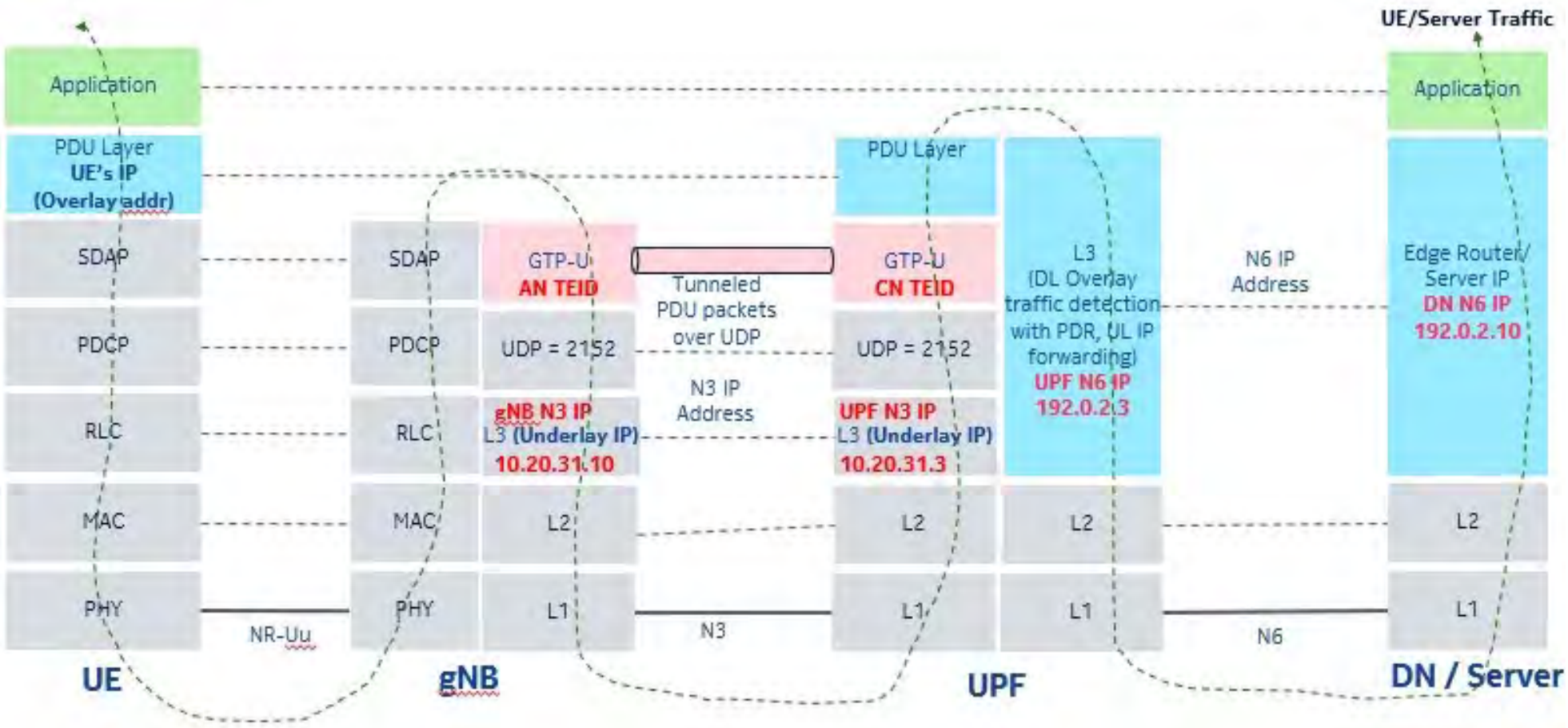
Wi-Fi GTPU and IPsec Tunnel in 5G



5GC security functions



GPT-U in 5G


UE/Server Traffic
Application
PDU Layer
UE's IP
(Overlay addr)
SDAP
PDCP
RLC
MAC
PHY
NR-Uu
UE
SDAP
PDCP
RLC
MAC
PHY
gNB
GTP-U
AN TEID
UDP = 2152
gNB N3 IP
L3 (Underlay IP)
10.20.31.10
L1
L2
Tunneled
PDU packets
over UDP
N3 IP
Address
N3
PDU Layer
GTP-U
CN TEID
UDP = 2152
UPF N3 IP
L3 (Underlay IP)
10.20.31.3
L1
L2
UPF
L3
(DL Overlay
traffic detection
with PDR, UL IP
forwarding)
UPF N6 IP
192.0.2.3
L1
L2
N6
N6 IP
Address
Application
Edge Router/
Server IP
DN N6 IP
192.0.2.10
L1
L2
DN / Server

4G vs 5G security

		4G Authentication		5G Authentication	
		EPS-AKA	5G-AKA	EAP-AKA	EAP-TLS
Entities Location	UE	USIM		USIM	USIM/Non-SIM
	Serving Network	MME		SEAF	
	Home Network	HSS		AUSF/UDM/APRF/SIDF	
Message Format	UE <--> SN	NAS	NAS	NAS/EAP	NAS/EAP
	SN <--> UE	Diameter		HTTP-based web APIs	
TRUST Model		Shared Symmetric Key	Shared Symmetric Key		Public Key Certificate
UE Identity	UE <--> SN	IMSI/GUTI		SUCI/5G-GUTI	
	SN <--> UE	IMSI		SUCI/SUPI	
Service Network ID		SN ID (MCC+ MNC)	SN Name (MCC+ MNC)		
Authentication Vector Generation By		HSS	UDM/APRF	UDM/APRF	NA
Authentication of UE Decided By		MME	SEAF/AUSF	AUSF	AUSF
Home Network of UE Authentication		No	Yes	Yes	Yes

5GC and NG-RAN related to keys

Access agnostic:

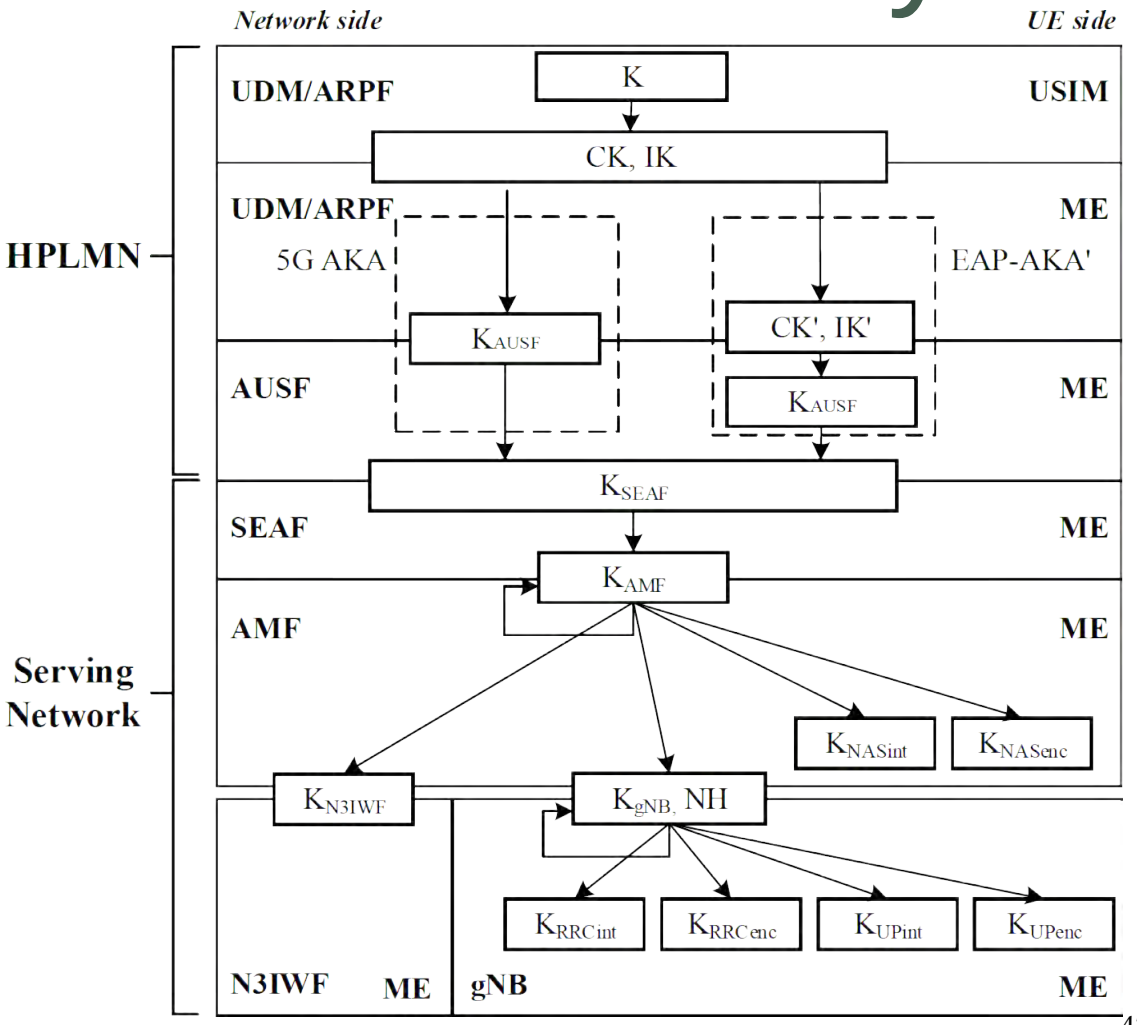
- 3GPP RAN
- Non-3GPP (e.g., Wi-Fi)
- Wireline network

Algorithm flexibility:

- 5G AKA, EAP-AKA

Improved key hierarchy:

- Unified 3GGP/non-3GPP hierarchy
- Decoupled mobility and security
- anchors in the serving network



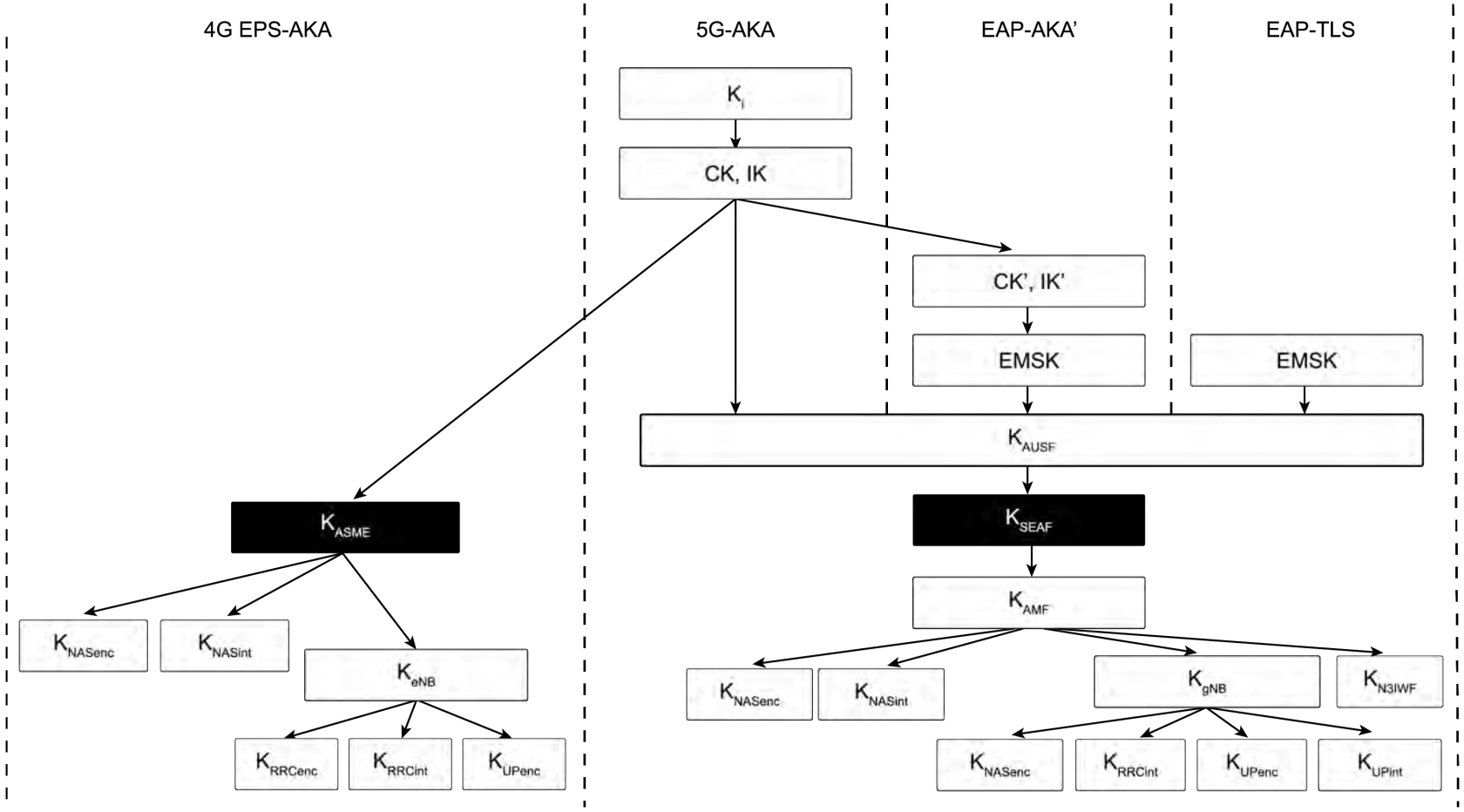
4G vs 5G Authentication

		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <-> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <-> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes
ANCHOR KEY HIERARCHY		K_i -> CK+IK -> K_{ASME}	K_i -> CK+IK -> K_{ASME} -> K_{SEAF}	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}	EMSK -> K_{AUSF} -> K_{SEAF}

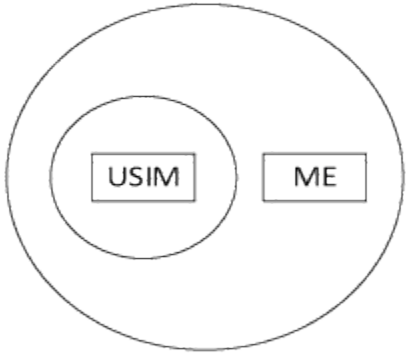
non-SIM authentication EAP-TLS

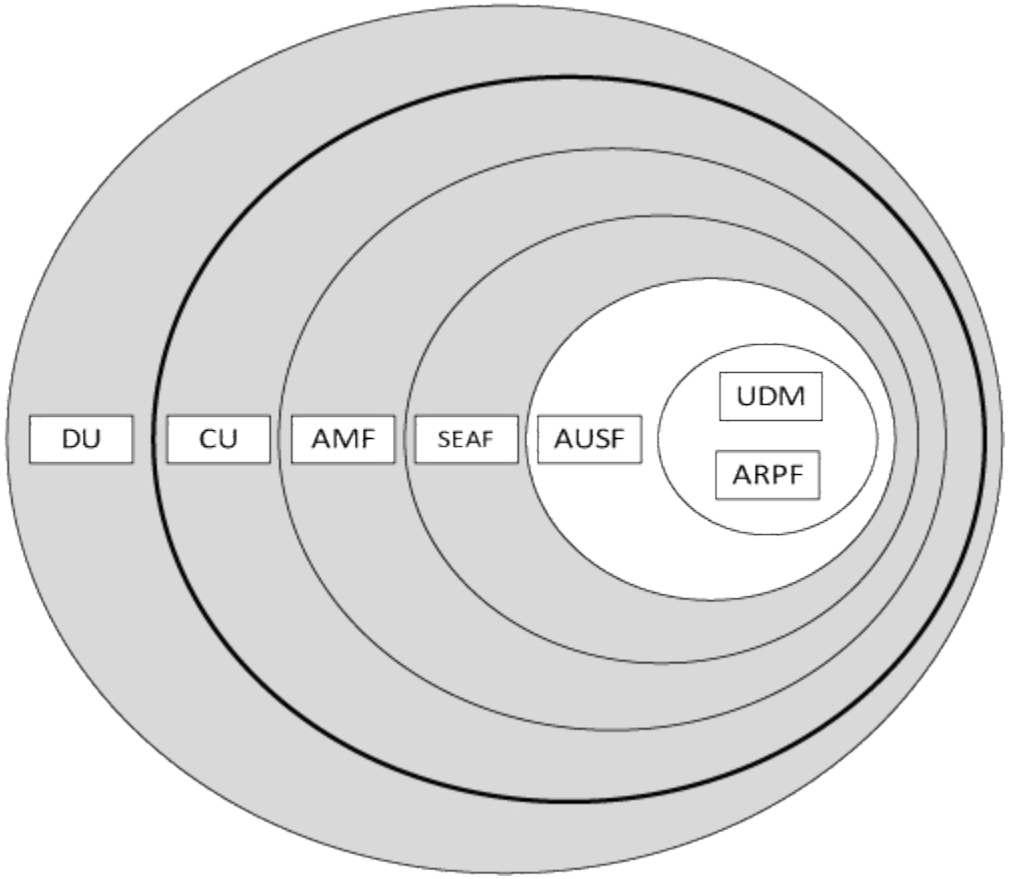
EAP-TLS is defined in 5G for subscriber authentication in limited use cases such as private networks and IoT environments (non-SIM authentication). When selected as the authentication method by UDM/ARPF, EAP-TLS is performed between the UE and the AUSF through the SEAF, which functions as a transparent EAP authenticator by forwarding EAP-TLS messages back and forth between the UE and the AUSF.

Key Hierarchy in 4G and 5G



Trust model 5G – non roaming



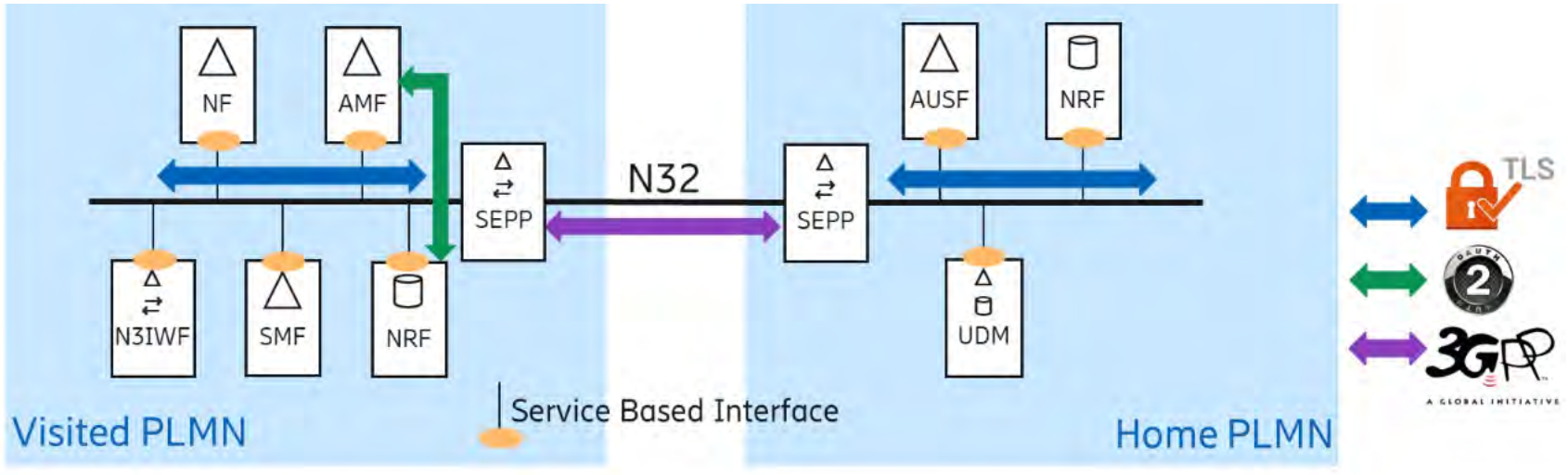


5G Security & 5G interconnection

Security Edge Protection Proxy (SEPP)

Core network:

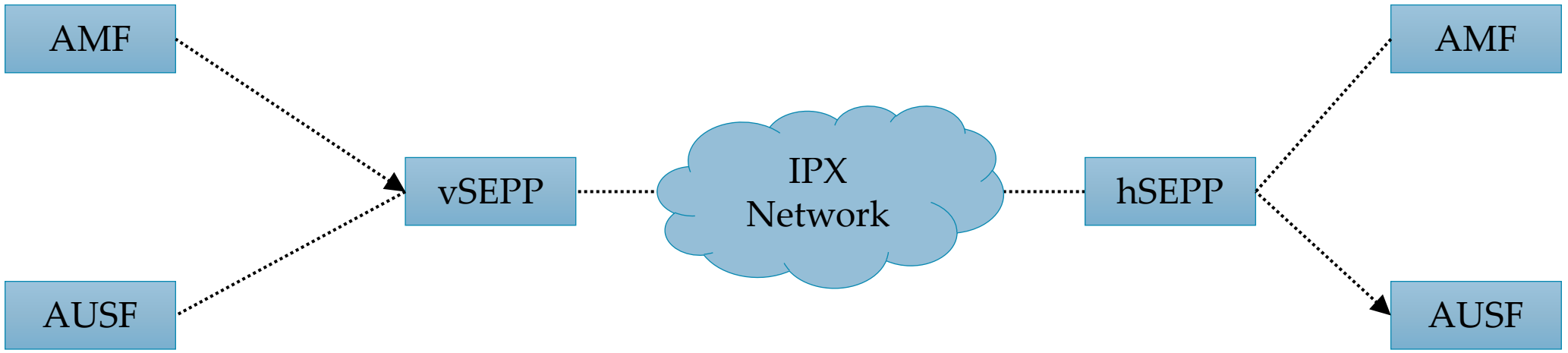
- TLS 1.2 (Transport Layer Security) & TLS 1.3 (transport layer)
- OAuth 2.0 (application layer)
- IPsec



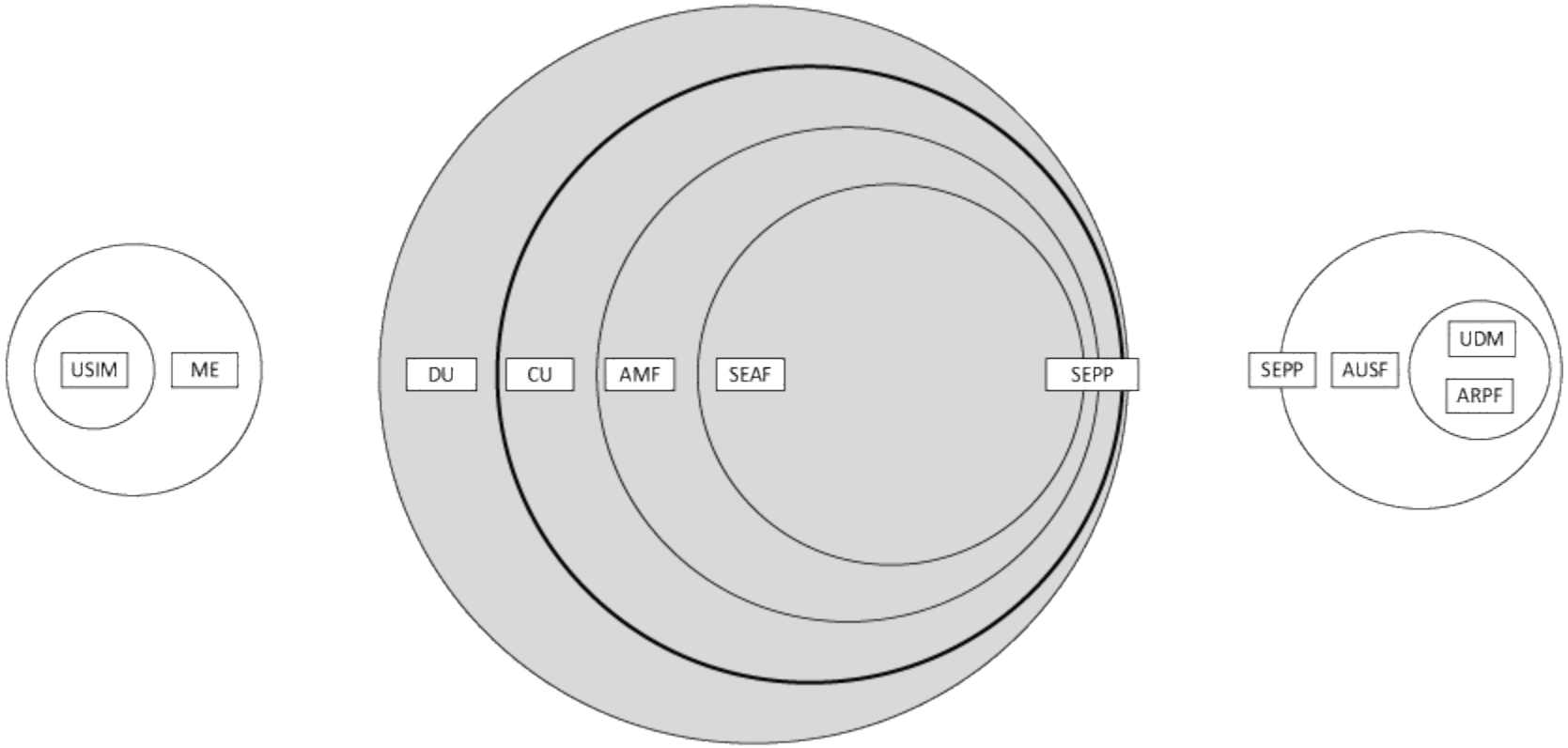
Security Edge Protection Proxy (SEPP)

- The SEPP is used to protect control plane traffic that is exchanged between different 5G PLMNs (Public Land Mobile Networks). As such, the SEPP performs message filtering, policing and topology hiding for all API messages.
- A separate security negotiation interface (N32-c) and an end-to-end encrypted application interface (N32-f)
- TLS security as a minimum between two SEPPs for N32c and N32f interfaces
- Optional encapsulation of HTTP/2 core signaling messages using JOSE protection for N32-f transmission (PRINS)

Security Edge Protection Proxy (SEPP)

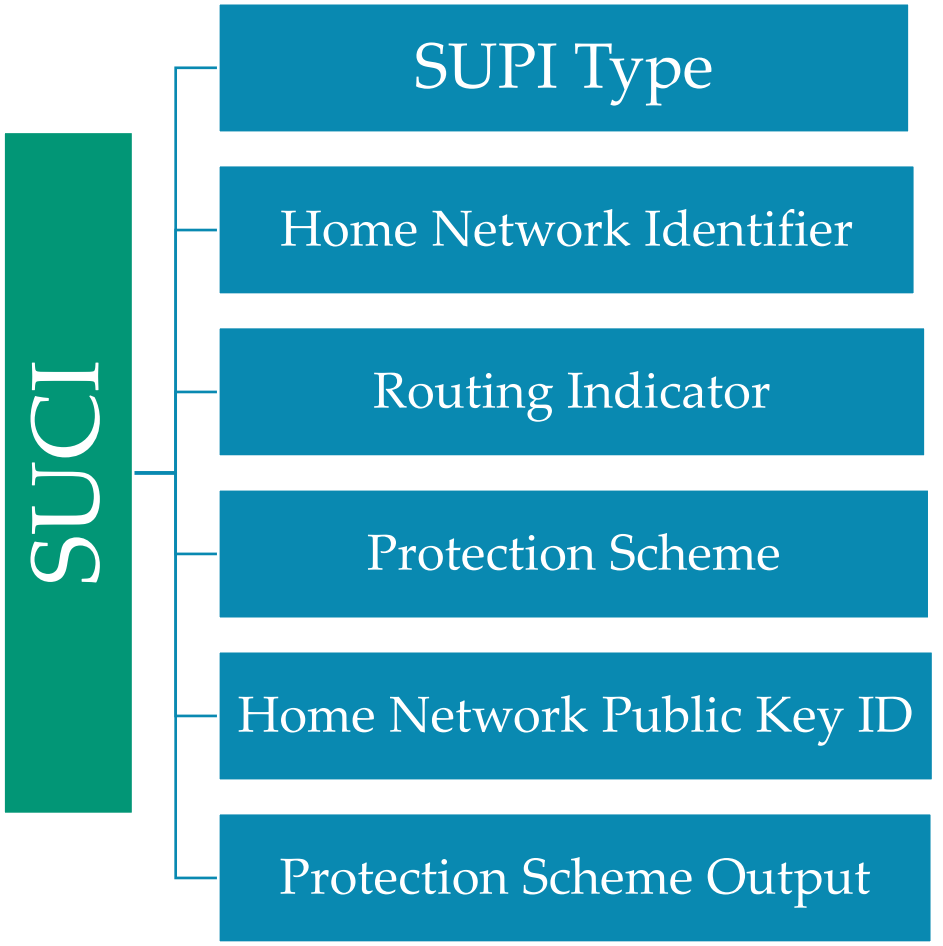


Trust model 5G – roaming



Subscriber Privacy in 5G

- Concealment of **Subscription Permanent Identifiers (SUPI)**
- SUPI ciphering into a **Subscription Concealed Identifier (SUCI)** may be performed in either ME or USIM
- SUCI deciphering on network side performed by the **Subscriber Identity De-concealing Function (SIDF)**, part of the UDM
- 5G further **prohibits** subscriber paging by SUPI



Solution – IMSI Catchers in 5G

5G security specifications do not allow plain-text transmissions of the SUPI over the radio interface.

- 5G NR Global Unique Temporary Identifier (GUTI)
- **SUCI (Subscription Concealed Identifier)**
- **SUPI (Subscription Permanent Identifier)** for 5G – like **IMSI (International Mobile Subscriber Identity)** up to 4G
- The SUPI value is provisioned in USIM and UDM/UDR function in 5G Core.
- SUPI format:
  - IMSI (International Mobile Subscriber Identity)
  - NAI (Network Access Identifier) – like e-mail address

Known vulnerabilities of access network

Problems:

- Fake BTS (2 G)
- Passive IMSI catcher
- Active IMSI catcher

If the IMSI values are sent in plaintext over the radio access link, then users can be identified, located and tracked using these permanent identifiers.

Known vulnerabilities of core network

Problems:

- Hacking SS7 network
- SMS attack
- Fake roaming
- Combined attacks

How to stay safe?

3G USIM is sufficient to support all the new features.
No new SIMs need by LTE and 5G NSA

- Demand 3G, 4G, 5G + USIM
- Turn off 2G mode completely if 3G, 4G, 5G coverage is sufficient (in your phone menu)

Control and User Plane Separation

Control and User Plane Separation (CUPS)

- **Control Plane (CP) = Signalling**
- **User Plane (UP) = Data**

The introduction of CP and UP separation in the 4G EPC is the first step towards the 5G architecture. The SGW and PGW functions were split into a control and data plane component.

- SGW → SGW-C & SGW-U
- PGW → PGW-C & PGW-U
- gNB, eNB → DU & CU (Central Unit & Distributed Unit)

CUPS and EPC

- The Evolved Packet Core (EPC) network is evolving and moving toward Control User Plane Separation (CUPS) based architecture where User Plane and Control Plane are separate nodes for PGW, SGW, and TDF products.
- The User Plane and Control Plane combined to provide the functionality of a node for other elements in the EPC network. However, keeping it separate has numerous advantages from the network point of view – support different scaling for Control Plane and User Plane, support more capacity per session-level in User Plane, and so on.

CUPS allows

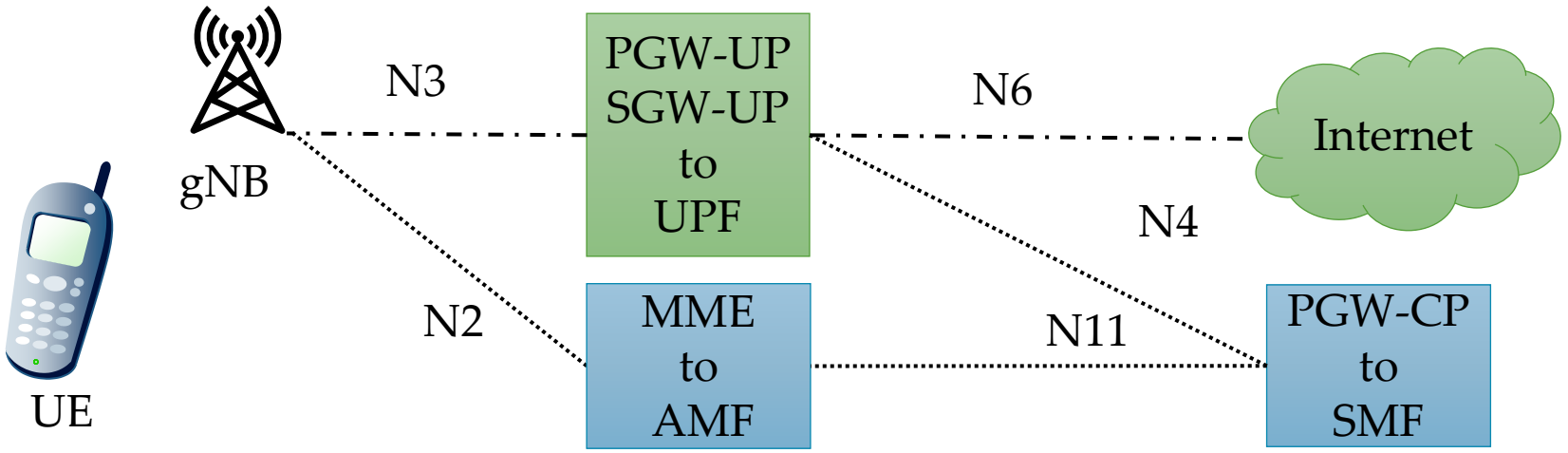
- Reducing Latency on application service, e.g. by selecting User plane nodes which are closer to the RAN or more appropriate for the intended UE usage type without increasing the number of control plane nodes.
- Supporting Increase of Data Traffic, by enabling to add user plane nodes without changing the number of SGW-C, PGW-C and TDF-C in the network.
- Locating and Scaling the CP and UP resources of the EPC nodes independently.
- Independent evolution of the CP and UP functions.
- Enabling Software Defined Networking to deliver user plane data more efficiently.

CUPS

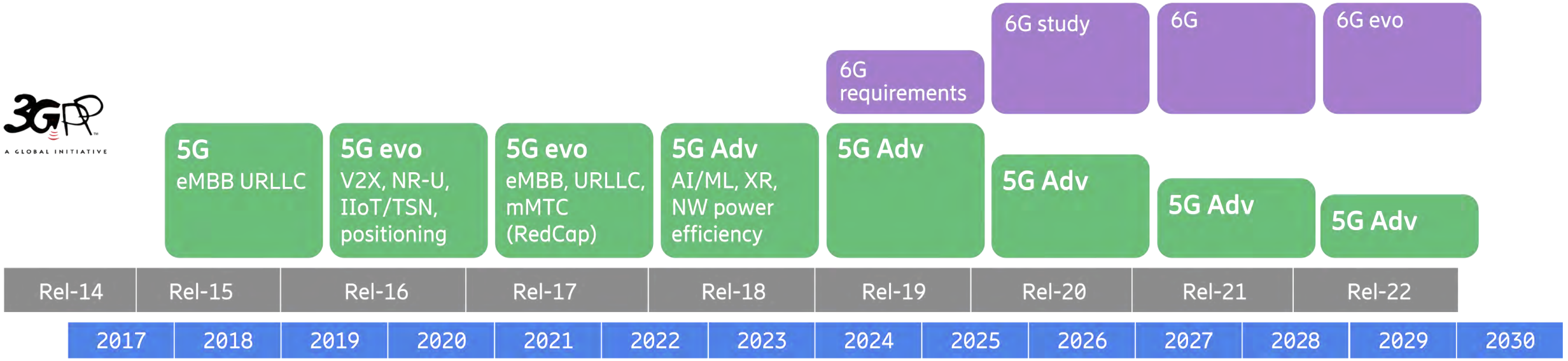
- Independent scalability of the control and user planes
- Ability to specialize the user plane for key applications
- 5G readiness
- Lower backhaul costs
- Traffic offload
- New use-case enablement
- Multi-level CUPS offerings

CUPS in 4G & 5G Network

Control and User Plane Separation is essential to 5G networks because it allows operators to separate the evolved packet core into a control plane that can sit in a centralized location and for the user plane to be placed closer to the application it is supporting.



From 5G Rel 15 to Rel 22



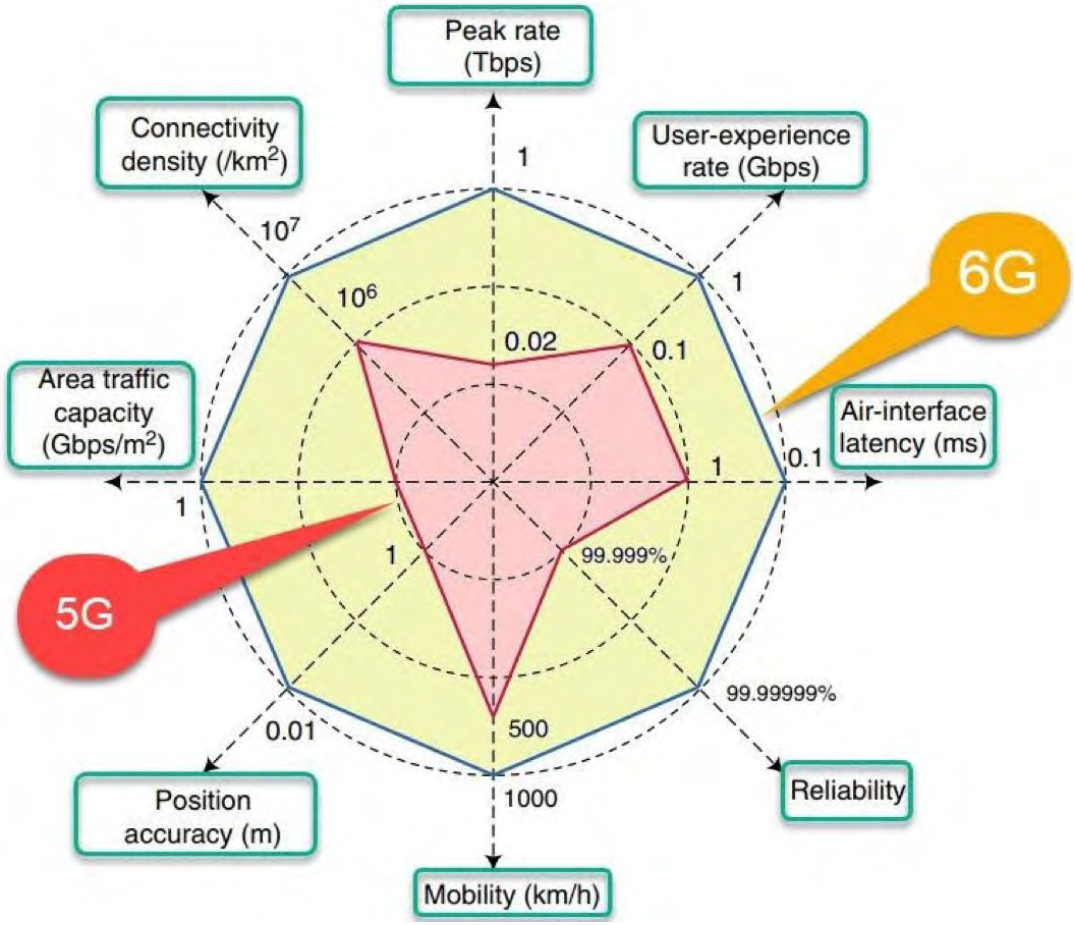
Evolution 4G – 6G

	4G LTE	4G Adv	4G Adv Pro	5G NR	5G Adv	6G
3GPP	Rel 8,9	Rel 10, 11, 12	Rel 13, 14	Rel 15, 16	Rel 17, 18, 19	Rel 23, 24
Service	Data, VoLTE	MBB, VoLTE	MBB, VoLTE	eMBB, VoNR	uRLLC, mMTC, VoNR	?
Bandwidth	20 MHz	100 MHz	640 MHz	400 MHz	800 MHz	1 GHz
Frequency	< 3,7 GHz	< 6 GHz	< 6 GHz	FR1, FR2	FR1, FR2	10 THz
Latency	25 ms	20 ms	15 ms	10 ms	1 ms	0.1 ms

6G – Comparison 5G and 6G

KPIs	5G	6G
Peak data rate	20 Gbit/s	1 Tbit/s
User experienced data rate	100 Mbit/s	1 Gbit/s
Peak spectral efficiency	30 bit/s/Hz	60 bit/s/Hz
Experienced spectral efficiency	0,3 bit/s/Hz	3 bit/s/Hz
Maximum bandwidth	1 GHz	100 GHz
Area traffic capacity	10 Mbit/s/m^2	1 Gbit/s/m^2
Connection density	10^6 devices/km^2	10^7 devices/km^2
Energy efficiency	Not specified	1 Tbit/J
Latency	1 ms	100 µs
Reliability	10^{-5}	10^{-9}
Jitter	Not specified	1 µs
Mobility	500 km/h	1000 km/h

6G Requirements



End

e-mail: michal.poupa@gmail.com
+420 603 404 371

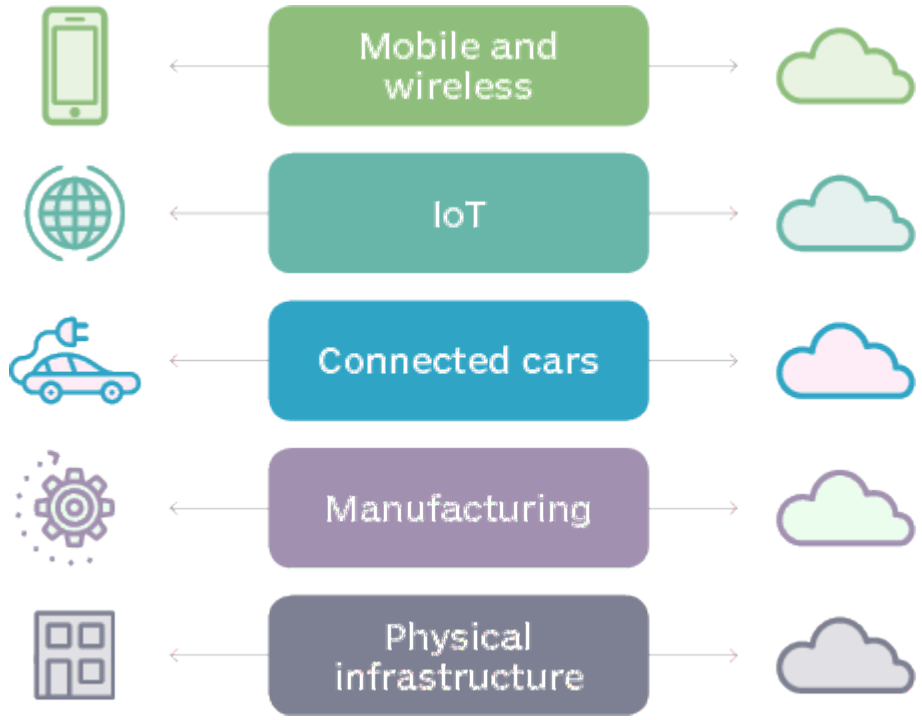
Backup

Network slicing

Network slicing, a mechanism that allows operators to create virtual networks dedicated to a specific service, use case or customer over a common physical network infrastructure, is a potentially key 5G capability. Network slicing is a very attractive tool in operators' quest to address the different needs of enterprise customers. For example, the quality of service requirements of connected car use cases will be vastly different from the needs of agriculture customers.

5G Network Slicing

Network slice is a logical network serving a defined business purpose or customer , consisting of all required network resources configured together. It is created, changed and removed by management functions.



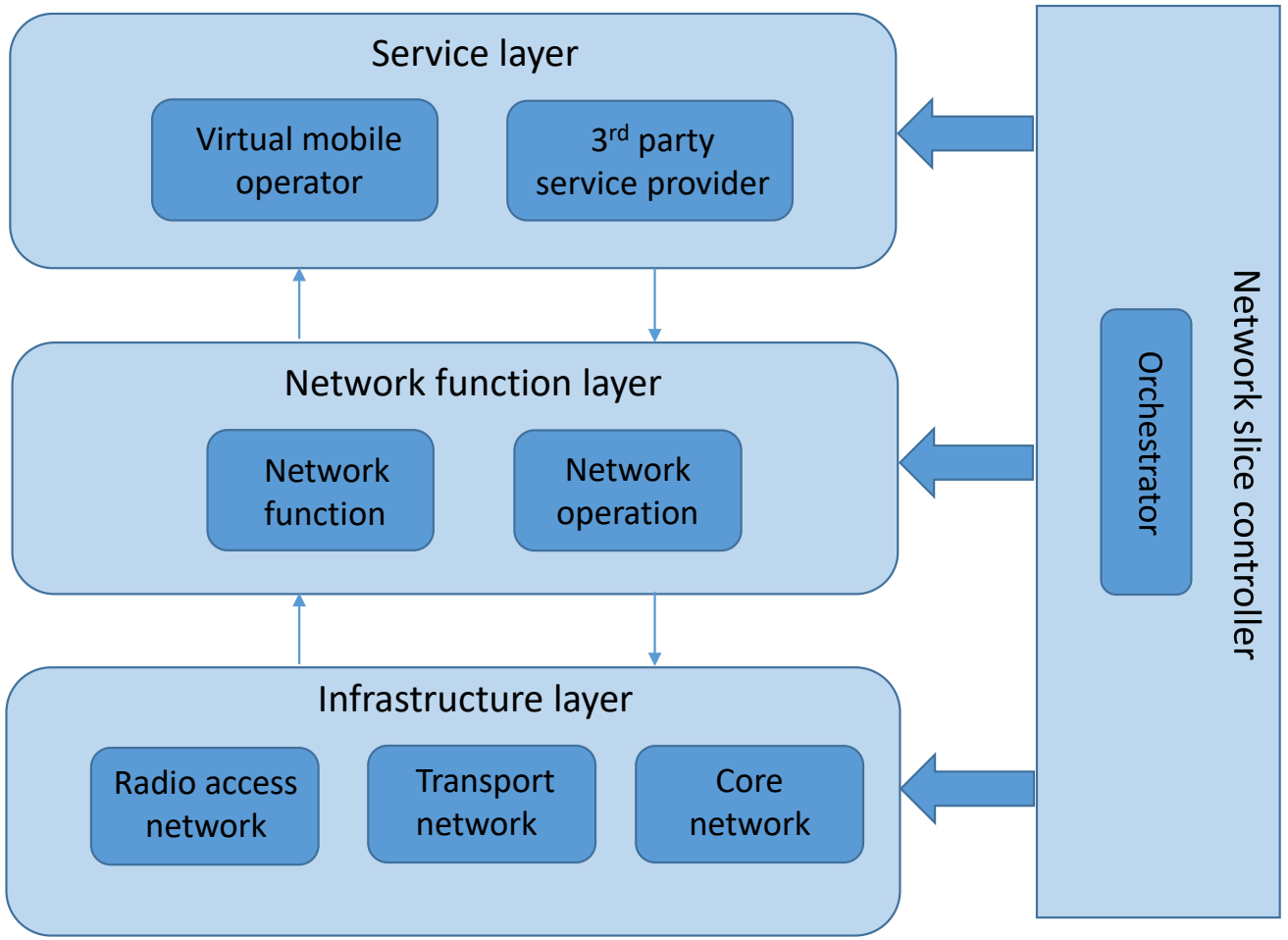
Network Slicing prerequisites

- Next Generation Mobile Networks (NGMN)
- Software Defined Networking (SDN)
- Network Functions Virtualization (NFV)
- Control and User Plane Separation (CUPS)
- Virtualization
- Containerization

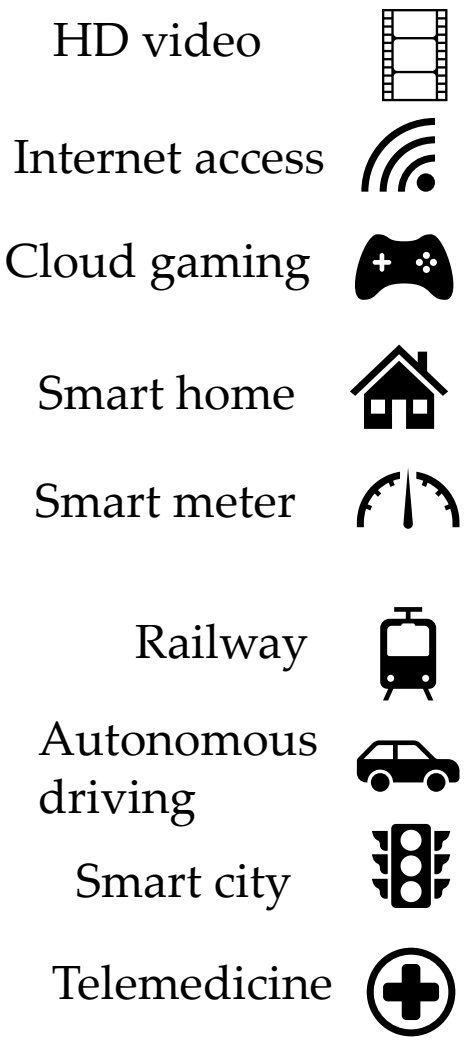
5G Network Slicing

- Separation of concern
- Diverging Use Cases and Requirement
- Multiple instantiations of same functionality
- Reduced Time To Market (TTM)
- Enabler for services, not a service
- Logical network managed by a provider
- Mobile and fixed
- Resources may be physical or virtual, dedicated or shared
- Independent / ”Isolated” but may share resources
- May integrate services from other providers, facilitating e.g. aggregation and roaming
- May include management functions and possible exposure of control/management to customer

5G Network Slicing



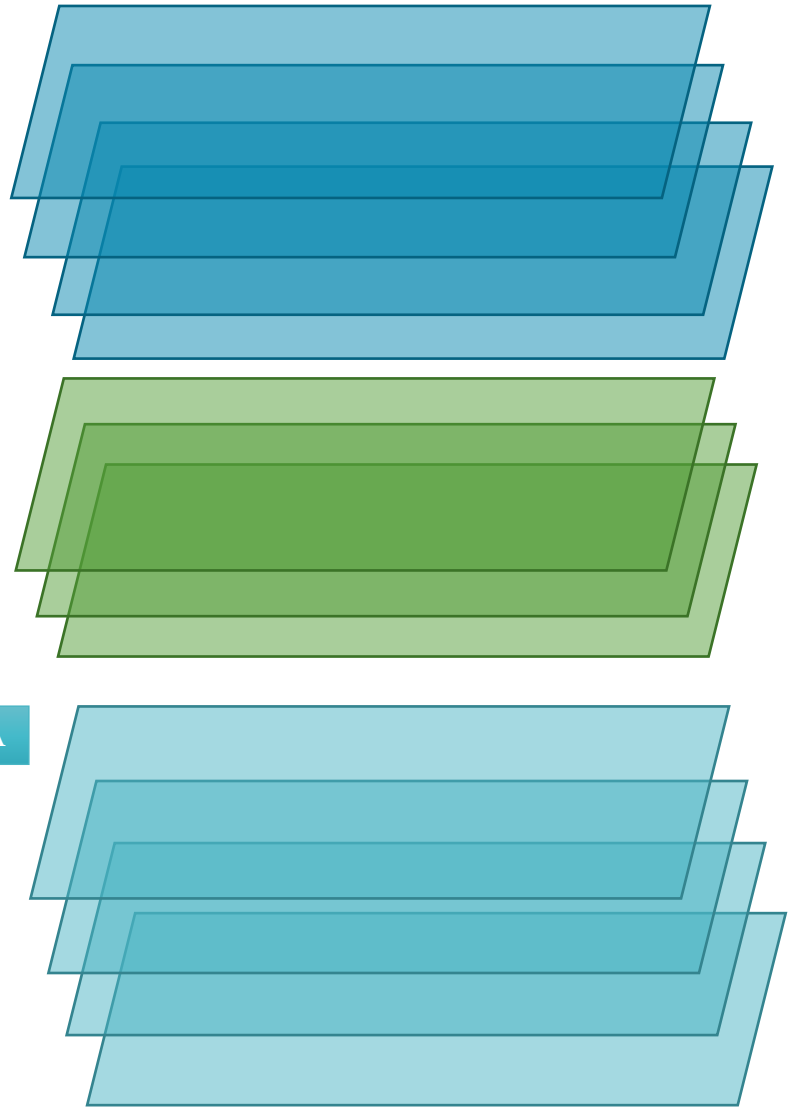
Slicing



Tenant

- Carrier A
- Carrier B
- Carrier C
- Carrier D
- Smart home A
- Power Plant
- Water Plant
- Railway operator A
- Car maker A
- City A
- Hospital A

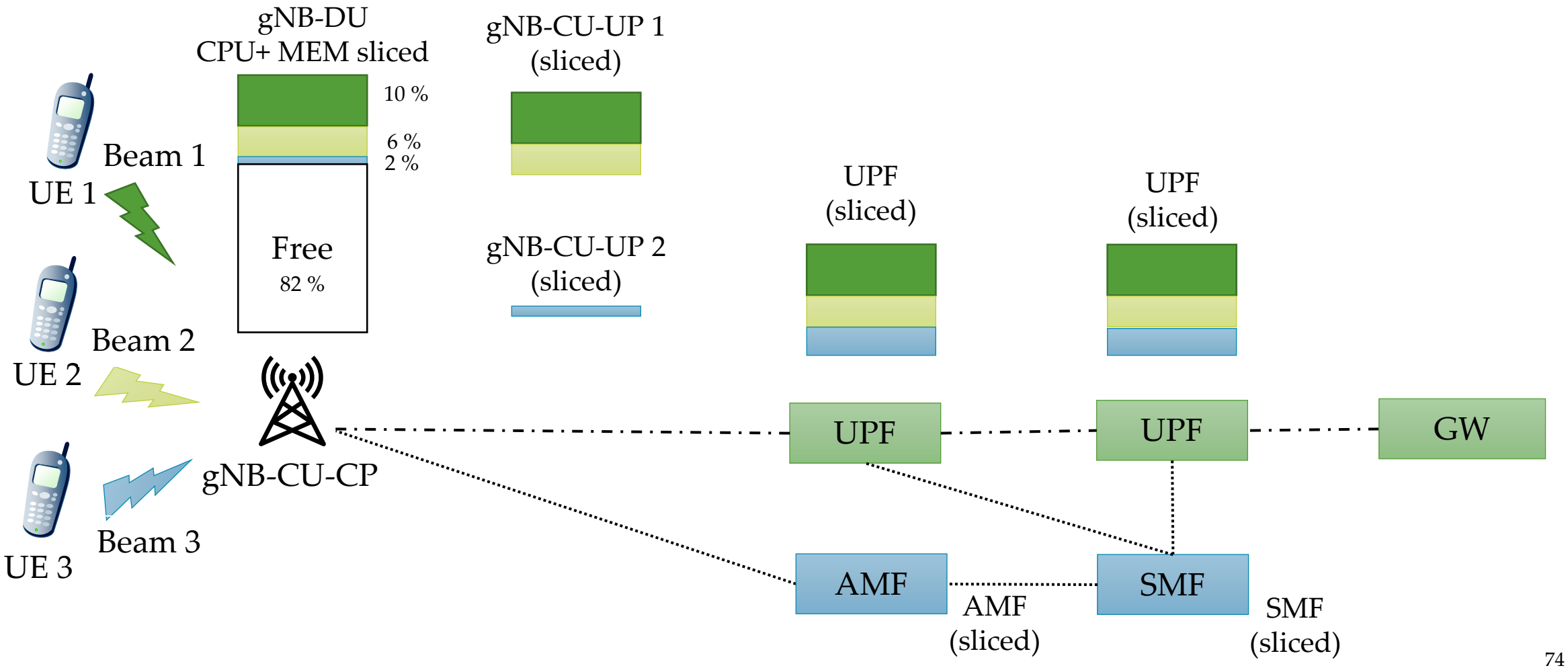
Slice



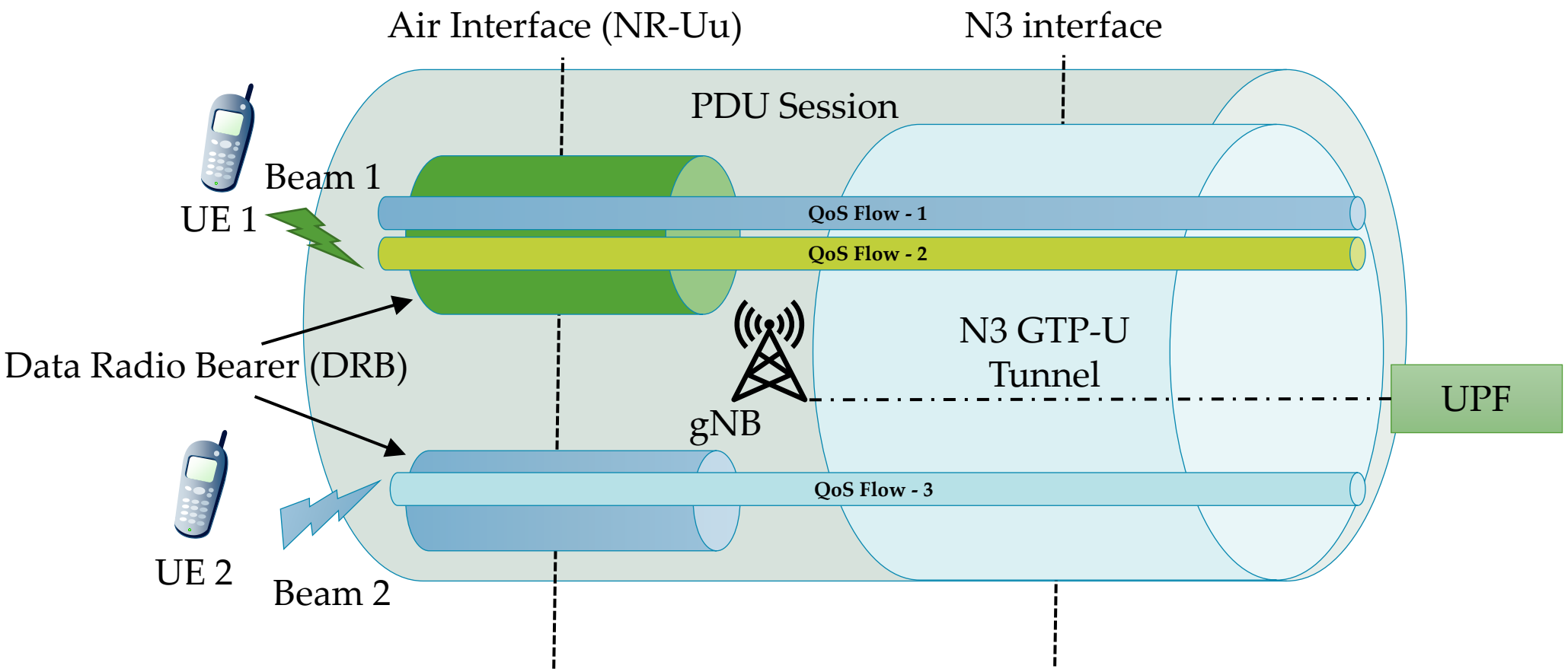
Slice Type

- **Enhanced Mobile Broadband (eMBB)** Ultra High Bandwidth
- **Massive Machine-type Communications (mMTC) Massive IoT**
- **Ultra-reliable & Low Latency Communications (uRLLC) Critical Machine-Type Communications**

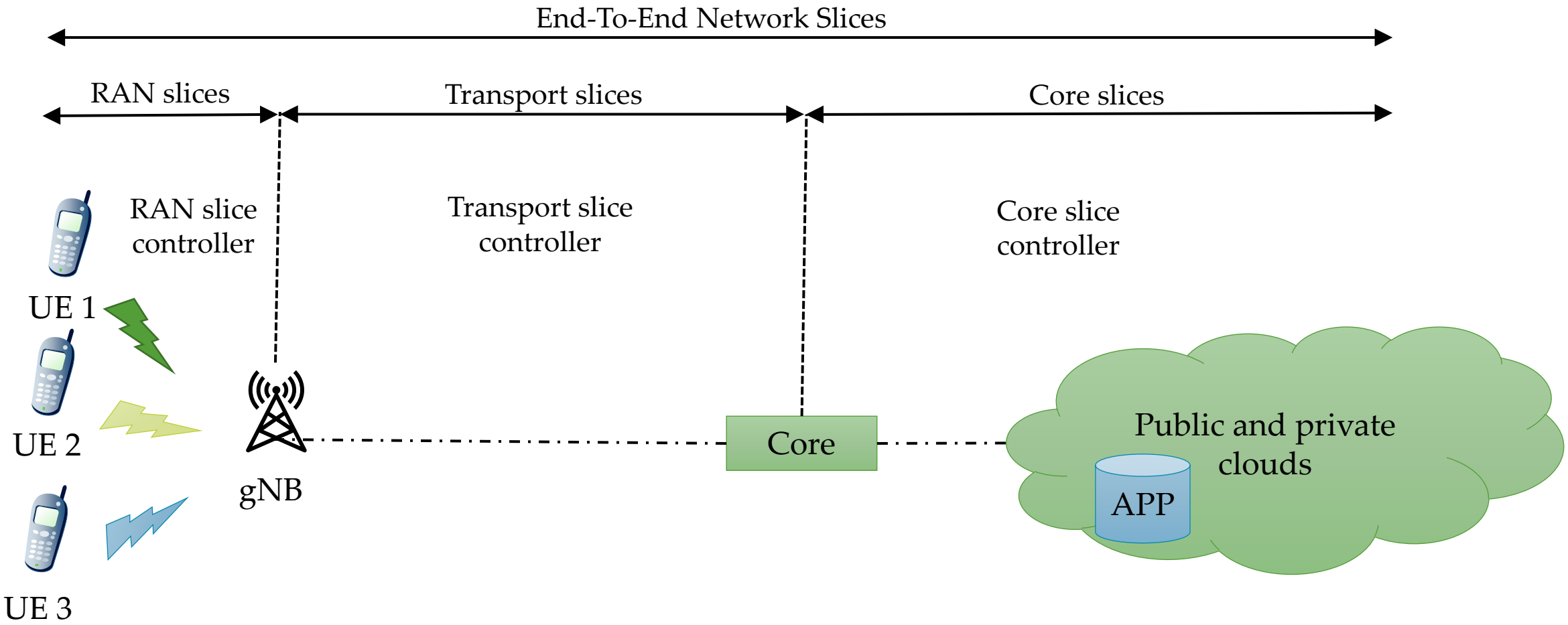
NGMN – 5G Network Slicing



NGMN – 5G Network Slicing



End-To-End-Network Slicing



Standardized SST values

Standardized SST values provide a way for establishing global interoperability for slicing so that PLMNs can support the roaming use case more efficiently for the most commonly used Slice/Service Types.

Slice/ Service type	SST value	Characteristics	Rel
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.	15
uRLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.	15
MIoT	3	Slice suitable for the handling of massive IoT.	15
V2X	4	Slice suitable for the handling of V2X services.	16
HMTC	5	Slice suitable for the handling of High-Performance Machine-Type Communications.	17

SST Slice/Service Type (SST)