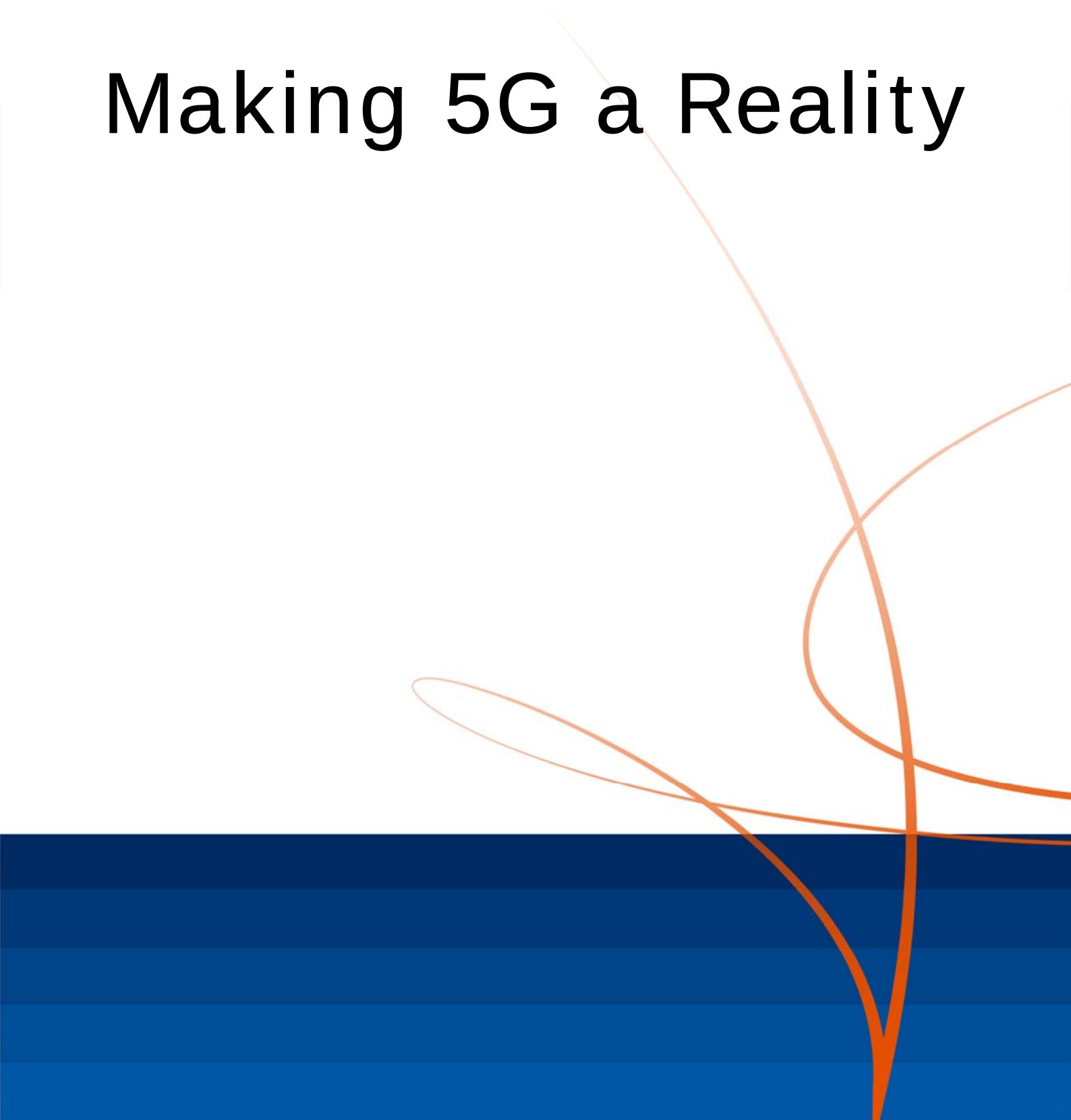
Orchestrating a brighter world NEC

Making 5G a Reality



First set of 5G specifications by 3GPP are completed thus opening doors for 5G deployment in near future; “Making 5G a Reality”. Technology is already present to fulfill 5G market requirements such as partnership, flexibility, cost reduction and personalization. Based on given technologies, 5G specifications respond to market requirements with new radio, APIs for partners, options for authentication, service based architecture and slicing. Market requirements will also be reflected by Business Support Systems / Operational Support Systems (BSS/OSS). In this technical white paper we present all aspects of 3GPP 5G specifications and impact on BSS/OSS as well as opinion from NEC where necessary.

Preface

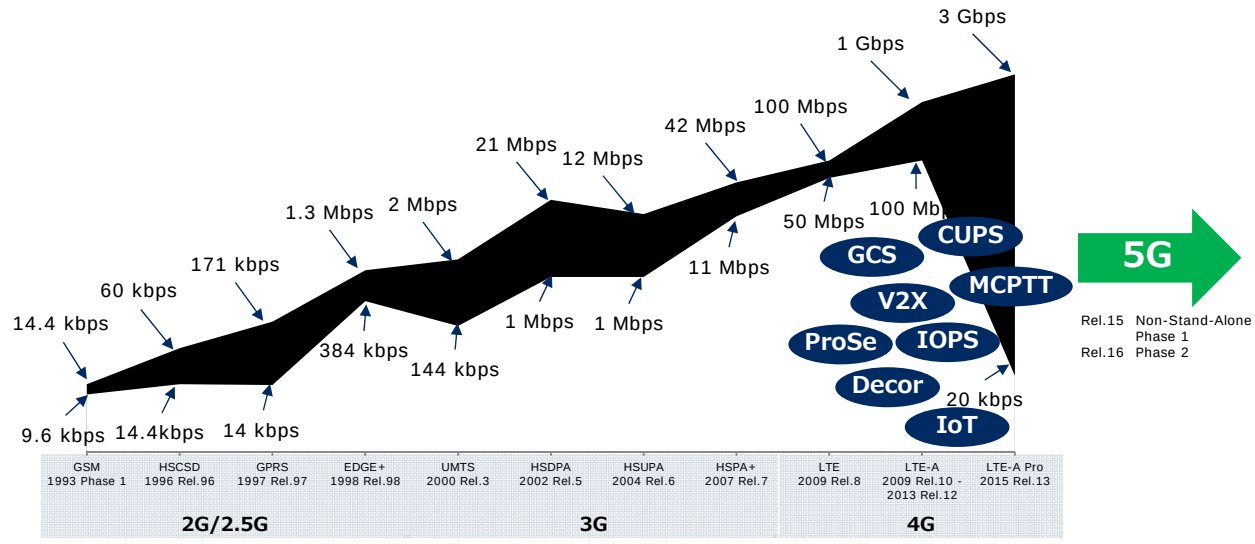
Mobile communication has seen tremendous growth with significant impact on society and economy. This has happened due to continuous evolution of mobile communication systems with each new generation and increasing penetration in the society. Every new generation of mobile communication systems has brought higher data-rates but 4G and its evolution also brought other enhancements that require lower data-rates such as services related to Internet-of-Things (IoT); depicted in figure below. Market demands for variety of services, range of data-rates and cost consciousness together with technology enhancements has brought us to the stage where the 5th Generation (5G) of mobile communication system can be a reality.

The Third Generation Partnership Project (3GPP), the mobile communication system specification group, started developing 5G specifications already a while back. First 5G technical specifications from 3GPP is already concluded thus “Making 5G a Reality”.

The goal of this whitepaper is to bring information regarding 5G from 3GPP standardization perspective and implications on Business Support System / Operations Support System (BSS/OSS). This whitepaper is meant for a wide audience ranging from CEOs to 5G product developers.

The whitepaper starts with introduction in Chapter 1 covering market and technology factors leading to 5G and 3GPP standardization overview together with time-line. The 2nd Chapter covers 5G radio, Radio Access Network (RAN), system architecture and security aspects. Chapter 3 discusses migration and interworking. In Chapter 4 we describe the impact of 5G on BSS/OSS including orchestration and security.

This whitepaper is developed by NEC group companies including NEC Corporation, NEC Labs China, NEC India and Netcracker. All NEC standardization delegates have contributed with expert inputs on 5G technology while Netcracker team has provided input from BSS/OSS perspective.



IOPS: Isolated E-UTRAN for Public Safety **MCPTT**: Mission Critical Push to Talk for LTE **ProSe**: Proximity based Services **GCS**: Group Comm. Service
Decor: Dedicated core network **CUPS**: Control & User Plane Separation **IoT**: Internet Of Things **V2X**: Vehicle to everything

Table of contents

Preface i

Table of contents ii

1 Introduction: Path to 5G 1

1.1 Market and Technology Factors 1

1.2 5G and 3GPP 3

1.3 Whitepaper Overview 3

2 The 5th Generation Communication System 4

2.1 NR Aspects 4

2.2 The NG-RAN Architecture 4

2.3 5G System – Key Features 6

2.3.1 Overview 6

2.3.2 Network Slicing 8

2.3.3 Service Based Architecture 9

2.3.4 Deployment options 9

2.4 Security 10

3 Migration and Interworking 13

3.1 EN-DC – Reuse of existing networks 13

3.2 Radio Access Network 14

3.3 Core Network 15

3.4 Security 15

4 5G Impact on BSS/OSS 16

4.1 Impacts on BSS 17

4.2 Impacts on OSS 18

4.2.1 End-to-end Service Orchestration 19

4.2.2 5G Infrastructure Management & Orchestration 19

4.2.3 MANO Security 20

5 Summary 23

Abbreviations 24

Bibliography 28

1 Introduction: Path to 5G

The 5th Generation (5G) of mobile communications system will bring huge changes to the industry and society at large. First flavor of 5G is expected to be available in 2018 with the complete solution available in the market by 2020. With digitalization on its way to touch every aspect of our lives, Internet of Things (IoT) will be an integral part of 5G; this is unlike 4G where IoT came later. However, there are still a lot of open questions: whether there is market demand for 5G, whether the technology is ready to address the market demand and industry readiness for 5G adoption. In this chapter we will touch the questions of market and technology readiness followed by introduction to current 5G activities in 3GPP that gives a glimpse on industry readiness towards 5G adoption.

1.1 Market and Technology Factors

Referring to the figure in the preface, a basic trend in mobile communications has been increase in data-rates with introduction of new generation. During 2G the main service was voice communication over circuit switched (CS) network. Increasing demand for data meant provisioning of data services over CS and then packet switched (PS) networks. Increasing demand for data also means increase in data-rates as we moved from 2G to 2.5G, 3G and 4G. Moving from 3G towards 4G various forms of services became available over mobile systems leading to higher data-rates as well as lower data-rates for some IoT type services. Several other enhancements happened during 4G such as device-to-device communication over licensed spectrum using Proximity based Services (ProSe) and Vehicle to Everything (V2X) communication. In this section we present market and technology factors leading towards 5G.

There is increasing demand for services provisioned by the mobile industry due to digitalization or mobile operator partnership with players of other industry such as media and over the top (OTT) service providers. Another reason is also the increase in data-rate of mobile communication systems and the necessity for the mobile industry to diversify their business due to flattening Average Revenue Per user (ARPU). One can from this the possibility of inter-industry or inter-verticals Merger and Acquisition (M&A) and different forms of partnership between mobile industry and other verticals enabling delivery of various services; NBIoT network is one such example of partnership between verticals and provisioning of new services over the mobile system. Technically this means that partner companies should be able to configure mobile network to fulfill their service requirements, provision services to correct subscribers and have means for correct charging.

Flattening of ARPU and expanding need of investment also necessitates cost optimization which can be achieved by network sharing and use of open-source implementations. Virtualization and cloud technologies allow multi-tenancy enabling ever simplified network sharing. Open-source implementation of mobile network functions running on off-the-shelf hardware allows further cost reduction.

Market demand for new services equates to mobile networks capable of provisioning services flexibly including launching and tearing-down of network based on customer needs. Such market requirement can be fulfilled by softwarization of network functions that are independent of hardware and through better techniques to manage or orchestrate the network. Softwarization, virtualization and cloud also enables automation in network that leads to further cost reduction as it minimizes human resource involvement. These technologies and open Application Programming Interface

(API) also makes it simpler to change partners thus increasing competition.

IoT will form a key part of 5G. IoT, i.e. anything or everything having connectivity, also requires solutions for identification used for authentication and also cost minimization. Subscriber identification and authentication is achieved today by Subscriber Identification Module (SIM), commonly known as SIM-card, which stores subscription credentials. With large number of IoT devices we need simpler methods for provisioning and managing the subscription. This leads to need for softwarization of SIM-card. For cost reduction, another solution of storage is needed potentially in the form of embedded storage of subscription credentials.

Another aspect of IoT is the wide variety of IoT services with varying requirements on data-rates and delays. 5G will cater for these as well.

Finally there is a visible change in customers. Not only enterprises but also the end consumer is becoming very sophisticated and demand personalized service. Ever demanding services such as gaming, Augmented Reality (AR) and Virtual Reality (VR) are appearing; demanding in terms of network resources and end-to-end latency. These two items in essence require similar technology as discussed earlier, together with higher data-rate and lower delays.

Mobile communication in 5G era will also reach parts of world that did not have connectivity before. This brings requirements such as higher coverage to reduce deployment cost, energy efficiency for areas not well connected with the grid and availability.

These market and technology factors are depicted in Figure 1 from the perspective of business, network, spectrum, end-device, security (subscription) credentials and user-space.

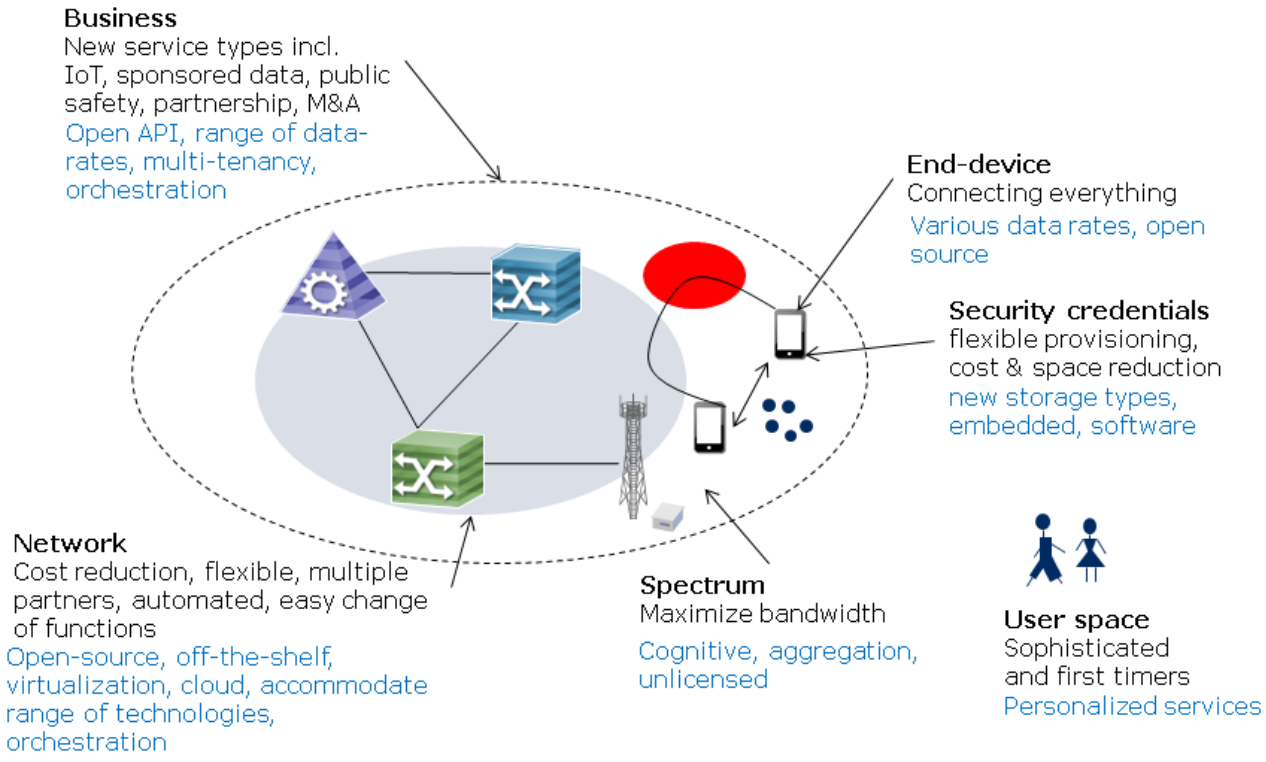


Figure 1: Market and technology factors leading towards 5G.

1.2 5G and 3GPP

5G activity in 3GPP started in Release 14, which concluded in March 2017, with study on key issues and requirements; see Figure 2. Specifications from 3GPP will be available in following steps:

Non-Stand-Alone (NSA): 3GPP decided to develop non-stand-alone specifications in Release-15 so as to bring 5G early in market with specification completion in December 2017. The purpose of NSA being to specify only the radio and associated enhancements. The 5G radio will work with 4G core network and is expected to give hotspot coverage with 4G providing the overlay network. This is also known as E-UTRA-NR Dual Connectivity (EN-DC).

Phase 1: The first phase of complete 5G specification will cover the radio, core, security and all associated specifications. This phase of specification is regarding Enhanced mobile Broadband (eMBB) as given by International Telecommunications Union (ITU). Specifications will be completed in June 2018.

Phase 2: Rest of the technology specifications for Massive Machine-Type Communication (MMTC) and Ultra-Low Latency Communication (URLLC) will be ready in the second phase. Specification is expected in December 2019.

1.3 Whitepaper Overview

With the goal to bring overview of 5G from 3GPP standardization perspective, Chapter 2 of this whitepaper presents the NR –the new radio- for 5G, Radio Access Network (RAN), the Core Network (CN) and security. After the system description, Chapter 3 presents migration and interworking aspect that is necessary for deployment of any new technology. We then look at the implications of 5G on Business Support System / Operations Support System (BSS/OSS), orchestration and associated security in Chapter 4. The whitepaper is concluded in Chapter 5 with a summary.

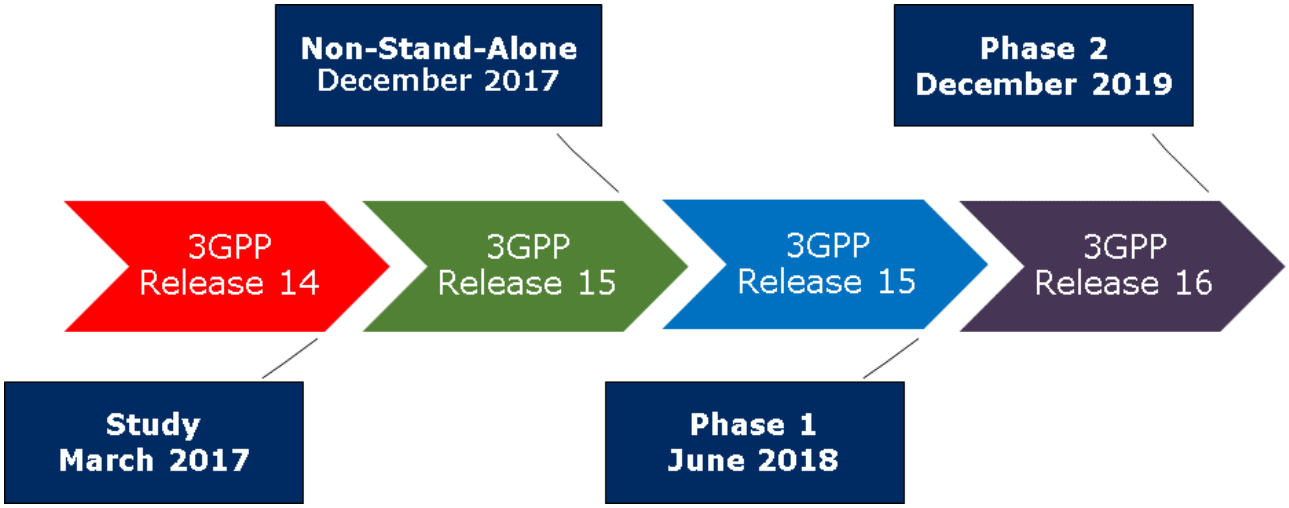


Figure 2: Time-plan, 3GPP 5G activities.

2 The 5th Generation Communication System

5G brings several technical enhancements that aim to cater for market factors presented in Chapter 1. The NR is expected to support much higher data-rates with lower latency while the base-station, gNB, will be split in two (central unit, gNB-CU, and distributed unit, gNB-DU). The system architecture of 5G brings enhancements such as slicing and service based architecture (SBA) allowing enhanced flexibility together with simpler means for business partners. 5G will also see several enhancements from security perspective. All these aspects associated with 5G are discussed in this chapter.

2.1 NR Aspects

5G NR will support both high frequency (>6 GHz) and low frequency (<6 GHz) bands. The Key Performance Index (KPI) defined by 3GPP for overall 5G, i.e. both Phase 1 and 2, requires peak data-rates of 20Gbps for down-link and 10Gbps for uplink when using eMBB. Latency for URLCC is expected to be 0.5ms, while for eMBB it is expected to be 4ms. MMTC solutions should provision for 15 years battery life. NR has to cater for all these KPIs. In this section we present information regarding the first version of NR specification to be concluded in June 2018 in Release 15 of 3GPP.

A number of key features of 5G have been determined for NR in Phase 1. These key features include (a) support for multiple numerologies which equates to a bigger selection of data-rates, options for latency, different coverage possibility and also scalability depending on bandwidth needs; (b) self-contained frame structure which can support low latency; (c) massive Multiple Input Multiple Output (MIMO) with large numbers of controllable antenna elements allows communication in high interference environment with beamforming bringing stable data-rate and thus improved Quality of Service (QoS); (d) Low Density Parity Check (LDPC) and polar code for the channel coding leads to lower error rates in-turn leading to better service quality, improved coverage and performance at cell edge; (e) modulation allows choice of data-rates and low error rates and (f) Long Term Evolution-NR (LTE-NR) coexistence bringing an overlay network in-case 5G coverage is not available.

These key features of NR allow a huge variety of services to be provisioned over 5G including very high quality video, AR, VR or low data-rate IoT services. It also shows that NR is usable in various environments; be it factory, fast moving vehicle or rural environment with low density population. Various options also allow granular deployment to maximize cost effectiveness (both capital and operating expenses, CAPEX and OPEX) of radio element deployment. One can easily notice the benefit of Artificial Intelligence (AI) to achieve optimized deployment.

For those who are interested in details of radio aspects, differences between NR and LTE radio parameters are listed in Table 1. Note that NR is only the radio part of the 5G base-station. The 5G base-station with all other protocol layers included is known as gNB.

2.2 The NG-RAN Architecture

One of the biggest change in the 5G Radio Access Network (RAN), known as Next Generation RAN or NG-RAN, architecture is the distributed concept from the very beginning. NG-RAN comprises of gNBs and can comprise of ng-eNB, i.e. enhanced 4G base-station. The gNB (5G base-station) is split in gNB-Central Unit (CU) and gNB-Distributed Unit (DU) where the CU can be placed in the cloud infrastructure. This architecture allows easier and cost effective deployment as well as management,

Table 1: Radio parameters comparison of LTE and NR.

Item	LTE	NR
Subcarrier spacing	Unicast + MBMS • 15 KHz MBMS dedicated carrier • {7.5 kHz, 1.25 kHz}	Below 6 GHz • {15 KHz, 30 kHz, 60 kHz} Beyond 6 GHz • {60 kHz, 120 kHz, 240 kHz (*1)}
Minimum/Maximum channel bandwidth	1.4 MHz / 20 MHz	Below 6 GHz • 5 MHz / 100 MHz Beyond 6 GHz • 50 MHz / 400 MHz
Maximum number of carrier aggregation	Up to 32 CC	Up to 16 CC
Frame structure	• 1 radio frame = 10 ms • 1 subframe= 1ms • 1 slot = 0.5 ms • Slot format: pre-defined in the specification	• 1 radio frame = 10 ms • 1 subframe= 1ms • 1 slot = {1 ms, 0.5 ms, 0.25 ms, 0.125 ms} depending on subcarrier spacing • Slot format: semi-statically and dynamically configurable
Channel coding	• Turbo coding (Data) • TBCC (Control)	• LDPC (Data) • Polar (Control)
Multiplexing scheme	• Downlink: OFDM • Uplink: DFT-S-OFDM	• Downlink: OFDM • Uplink: {OFDM, DFT-S-OFDM}
MIMO	• 8 antenna ports for SU-MIMO • 2 antenna ports for MU-MIMO	• 8 antenna ports for SU-MIMO • 16 antenna ports for MU-MIMO
HARQ	• TB based transmission & retransmission	• TB based transmission & retransmission • Code block group based transmission & retransmission
Carrier frequency	• 450 MHz ~ 3.8 GHz • Unlicensed band (5GHz)	• 600 MHz ~ 40 GHz

*1: 240 kHz subcarrier spacing is not applicable to data transmission

simpler network sharing, flexibility in adding new functions and provisioning of services much closer to the end-user or device. Closer to end-users or devices equates to lower latency fulfilling requirement for several services especially those related URLLC such as autonomous vehicle. In the following we look at further details regarding NG-RAN.

The NG-RAN architecture, as depicted in Figure 3, consists of logical nodes gNB and ng-eNB. gNBs provide the NR User-plane (UP) and Control-plane (CP) protocol termination towards the User Equipment (UE) and ng-eNBs provide the LTE UP and CP protocol termination towards the UE. The difference from LTE base-station is that the ng-eNB can work with 5G Core (5GC). We discuss 5GC in latter part of the whitepaper.

Note: UP carries user traffic, e.g. voice, Internet traffic, while CP carries control messages used for signaling in the mobile network.

With reference to Figure 3, the NG-RAN architecture consists of NG interface, Xn interface and F1 interface. The NG interface provisions, among others, functions such as handover and bearer management used for communication in the radio interface. For those familiar with LTE, NG interface is similar to S1 interface. Xn interface, similar to X2 interface in LTE, provisions functions such as handover between gNBs and dual

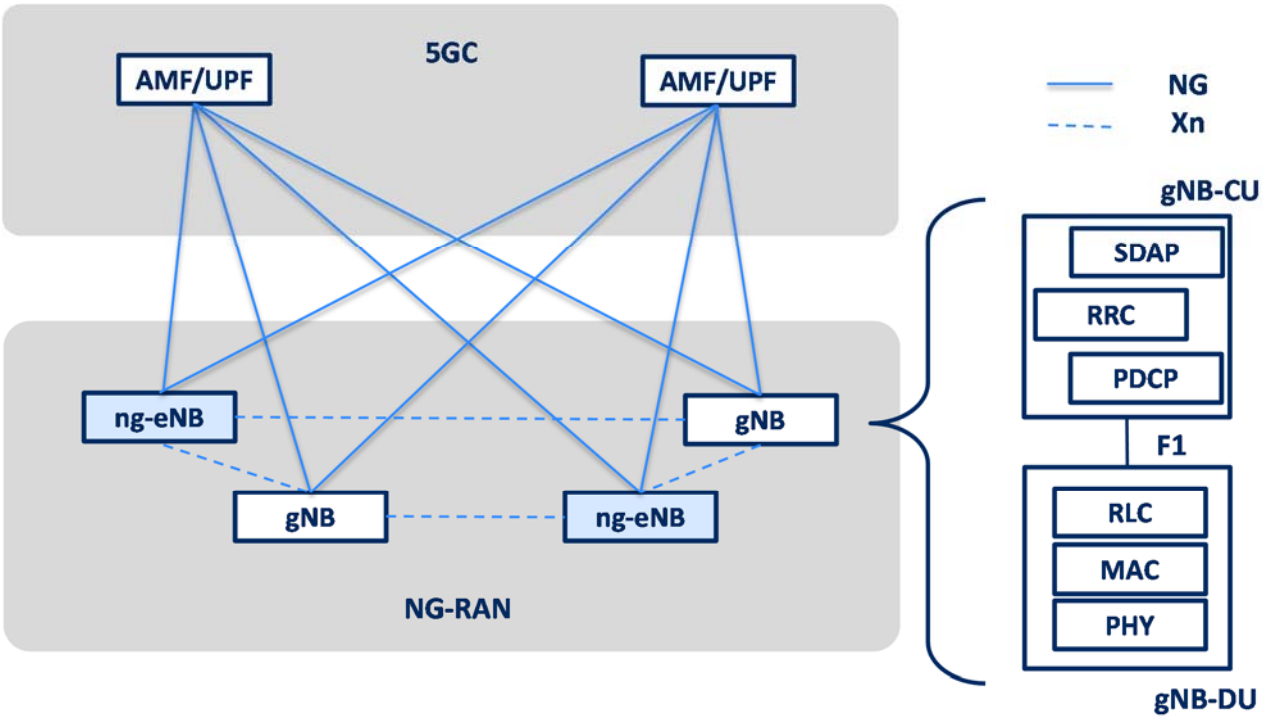


Figure 3: NG-RAN overall architecture

connectivity between different radio technologies. The F1 interface, which is internal to gNB, carries UP in the GPRS Tunneling Protocol for user data (GTP-U). CP is also carried on F1 interface for UE context management, Bearer management to setup/modify/release bearers. Cell configuration is done by Operations and Management (O&M).

The Central Unit or gNB-CU, see Figure 3, is a logical node that hosts higher layer protocols such as Radio Resource Control (RRC), Service Data Adaptation Protocol (SDAP) and Packet Data Convergence Protocol (PDCP). The Distributed Unit or gNB-DU is a logical node that hosts Radio Link Control (RLC), Medium Access Control (MAC) and Physical (PHY) layers. One gNB-DU supports one or multiple cells. One cell is supported by only one gNB-DU.

It is possible to have a flat gNB without CU-DU split. Also, it is possible to deploy gNB-CU by splitting into CP gNB-CU and UP gNB-CU. For example UP gNB-CU could be deployed in cloud or collocated with gNB-DU for delay sensitive application.

2.3 5G System – Key Features

The 5G System (5GS) is designed based on new network technologies, such as Network Function Virtualization (NFV) and Software Defined Networking (SDN), in order to make 5GS more agile and flexible. These have led to standardization of several features in 5G. We will present two unique features of 5G Phase 1, i.e. network slicing and service based architecture, in this section followed by a discussion on deployment options.

2.3.1 Overview

The 5G system architecture is depicted in Figure 4. A brief overview of all the functions of the architecture is given here.

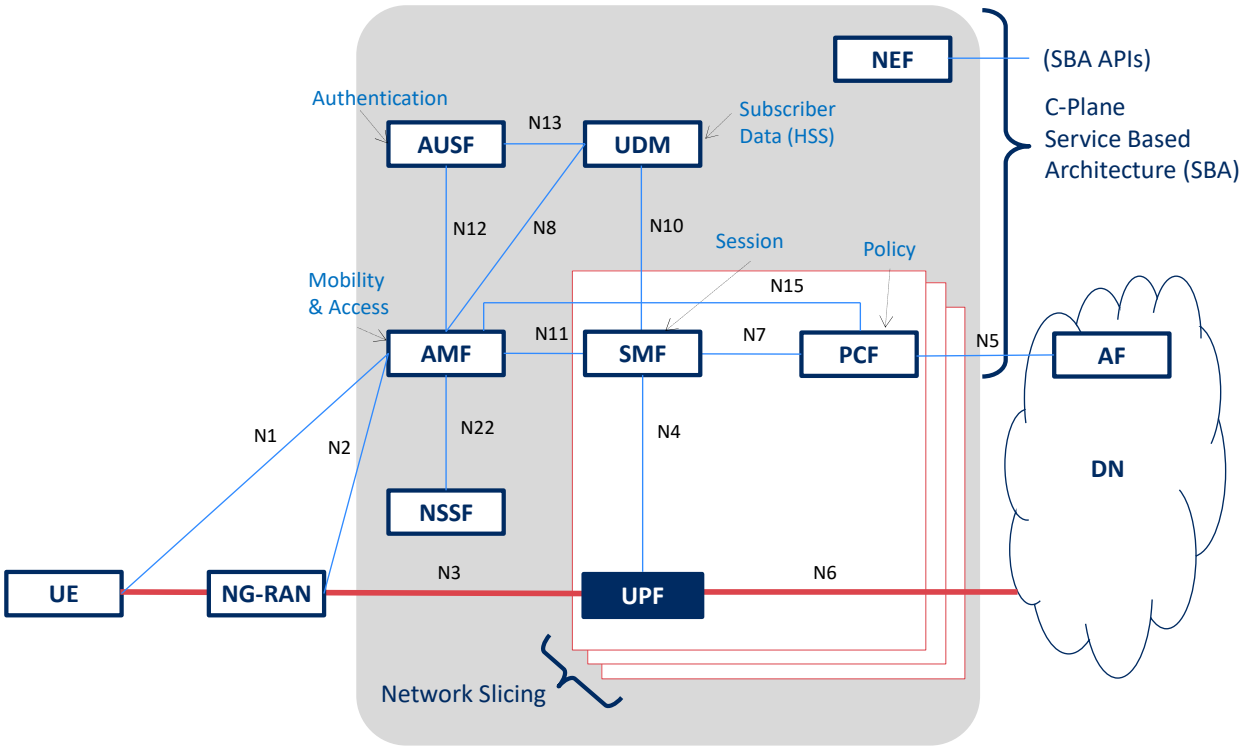


Figure 4: 5G System (5GS) architecture

Starting from left of Figure 4, User Equipment (UE) is a general terminology used in 3GPP specification for any device connected to the mobile network. The UE constitutes of a Mobile Equipment (ME) and a subscription credential storage module, mentioned as SIM-card in Chapter 1. In 5G-era the SIM-card could be embedded in the ME as we are discussing about various types of UEs starting from those requiring 15years battery life to smartphones and going up to vehicles. NG-RAN is already discussed in earlier sections thus we present rest of the functions here. Security is discussed in Section 2.3.

In Figure 4, the network functions in the grey rectangle form the core network (CN) of 5G. The Access and Mobility Function (AMF) is the control function in the architecture with functions such as mobility within the CN as well RAN and supporting authentication of the UEs. The Authentication Function (AUSF) takes care of authentication of the UE together with AMF and Unified Data Management (UDM) where subscriber data is stored. The UDM is similar to the Home Subscriber Subsystem (HSS) in earlier generation. Every session in 5G is managed by the Session Management Function (SMF) that receives the policy from Policy Control Function (PCF) – so does the AMF. The Network Slice Selection Function (NSSF) supports network slicing. There is also a Network Exposure Function (NEF) that exposes the network, using APIs to interact with the network functions and with partner companies for new business opportunities as discussed in Chapter 1. You will also notice that a partner company could input policies to the PCF through the Application Function (AF). AMF, AUSF, UDM, SMF, PCF, NEF and AF together form the CP or control part of the 5G system. For user plane there is only one function, i.e. the User Plane Function (UPF), which connects to the external parties over the Data Network allowing various service provisioning and partnership.

Cloud, NFV and SDN brings business advantages such as flexibility in deployment, cost effectiveness and aspects as discussed in Chapter 1. Modular architecture makes it possible for different parties to own parts of a network thus enabling new business models. Interface with external parties and a core network catering for NR, LTE and non-3GPP (example WiFi) allows new partnership and businesses to develop.

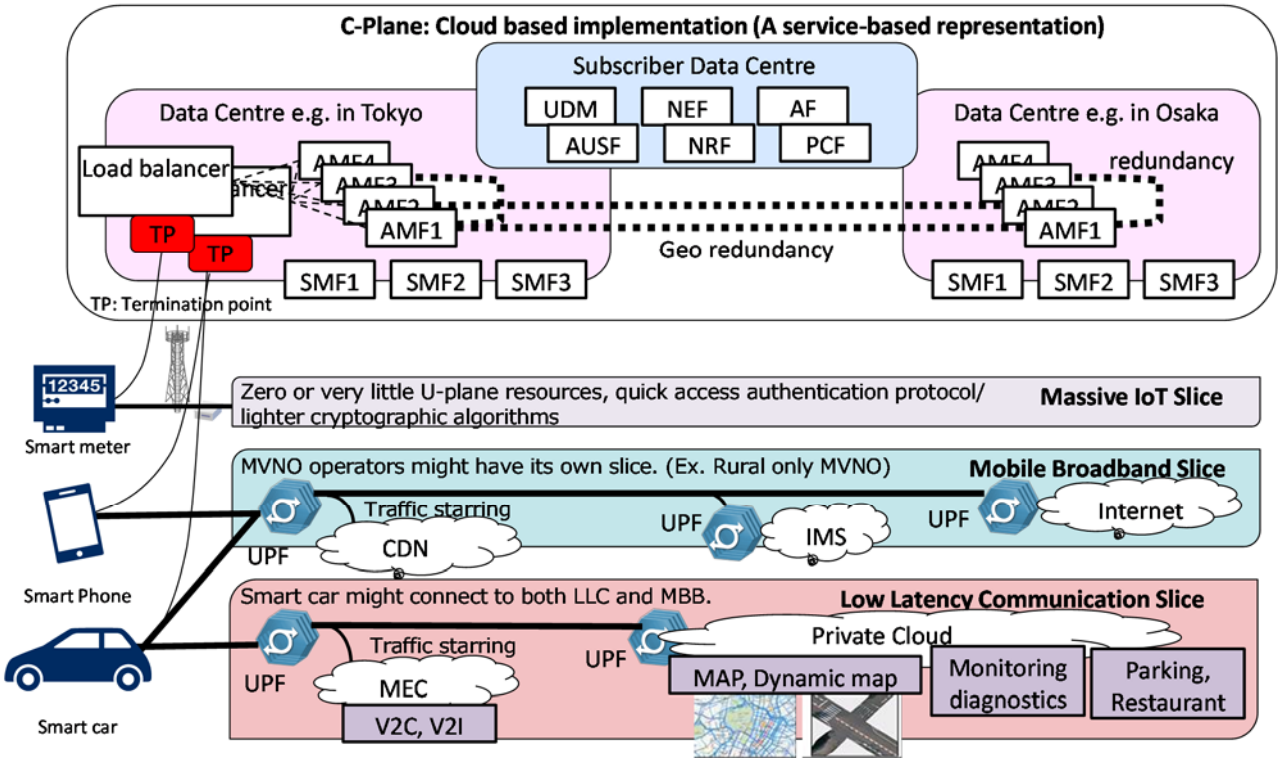


Figure 5: 5G system (5GS) implementation example

2.3.2 Network Slicing

There is strong interest in market to use 5G for enabling new business models while also strengthening and maintaining the existing business. For example, operators might establish a partnership with a 3rd party to provide a network dedicated to the given party. Another example is that operators can run the 5GS for supporting public safety. These use cases can be considered as new revenue streams for operators. The solution for this is to provision network slices for given party or service.

There are a few key factors why network slicing is the key for enabling above mentioned , use-cases: (a) network slicing enables isolation which is necessary to guarantee Service Level Agreement (SLA) with a 3rd party by dedicating network resources for given service. In order to support resource provisioning, the 5GS can assign dedicated network logical nodes (AMF, SMF, UPF, etc. as in Figure 5) to the 3rd party; (b) security can be provisioned per slice, which is unlike 4G where same security is provisioned to all UEs regardless of service type. While the 4G approach is reasonable, for some cases 4G security could be considered weak, for example for Mission Critical (MC) services, while for others it could be considered a overkill, for example simple IoT services. In 5GS (potentially in Phase 2), security strength can vary according to security requirements for the slice. For example, faster authentication, lighter cryptographic algorithms and protocols apply to IoT services while quick access and strong authentication protocol, strong encryption algorithms and credential management could apply to MC services.

Figure 5 illustrates a 5G system implementation example. Control plane nodes adapt using the latest cloud technologies in order to be agile and flexible without any service disruption. The geo-redundant configuration makes the 5GC resilient against any possible system-wide-failures, for example due to earthquakes.

User plane nodes can be designed based on services running on a dedicated slice. As each slice can be dynamically transformed, i.e. instantiated, deleted, capability updated,

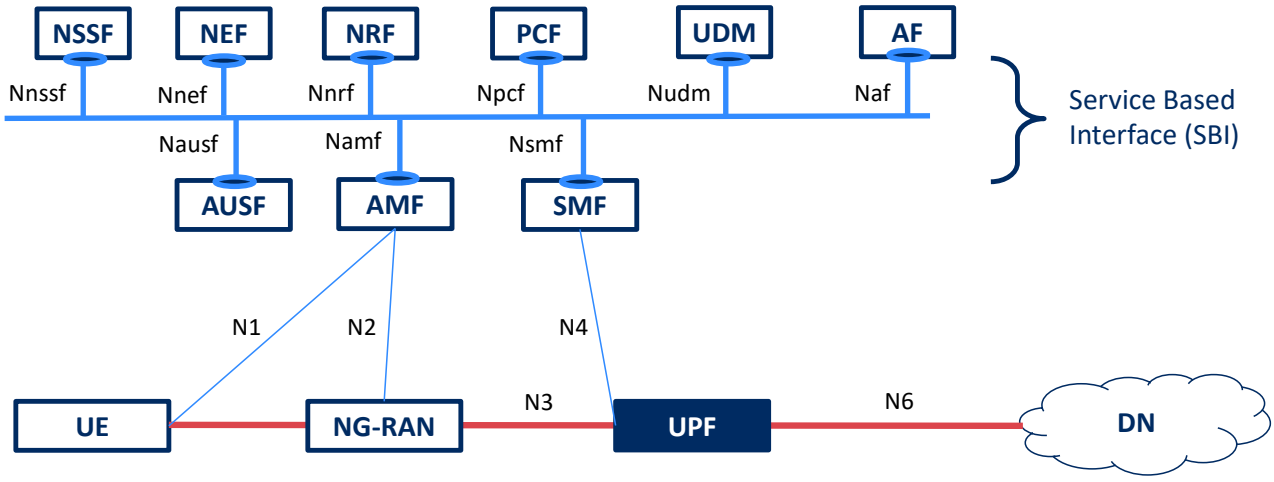


Figure 6: Service Based Architecture (SBA)

using NFV technology, operators can provide adequate service quality, i.e. user plane resources, to SLA with minimal capital expense (CAPEX). In addition, as all user plane nodes in a slice are totally separated from ones in the other slices, user plane resource isolation and slice based security are guaranteed.

2.3.3 Service Based Architecture

The control plane architecture in 5GC is drastically enhanced as compared to 4G; see Figure 6. The 5GC adopts so-called Service Based Architecture (SBA) that enables the control plane nodes to access any services that other logical nodes provide. Since all control plane nodes are connected by bus-type interface, known as Service Based Interface (SBI), each control plane function can communicate directly with each other. This network topology contributes a lot to simplify control plane signaling to introduce new functionalities achieved by coordination of control plane functions. For example, in 4G the Packet Data Network Gateway (PDN GW) has to communicate to the Mobility Management Entity (MME) though the Serving GW (SGW) since there is no direct reference point defined in the 4G core network, i.e. Evolved Packet Core (EPC). Meanwhile, the control plane functions in 5GC can serve their functionalities as services to other functions. Also, SBI adopts web-based technology on HTTP/2 which enables more flexible and rapid service development.

All network functions are same as that shown in Figure 4 as it is the same architecture. A new function, Network Resource Function (NRF), is used as a registry of all functions in the architecture somewhat like a Domain Name Server (DNS).

2.3.4 Deployment options

5GS can be deployed with standalone NR; known as Option 2 in 3GPP. There are deployment options that use both LTE and NR at the same time using dual connectivity technology; so called as non-stand-alone as given in Chapter 1. Non-Stand-Alone or EN-DC is depicted in Figure 10 and discussed further in Chapter 3.

Figures 7 and 8 depict other typical deployment options. As described in Figure 7, the 5GS connects to NR as primary radio technology and to LTE as secondary technology (NE-DC); this is known as Option 4. The example in Figure 8, known as Option 7, is the opposite of Option 4, i.e. LTE is primary with 5G CP capability and NR is secondary radio (NG-EN-DC).

Note that other possible deployment options can be seen in 3GPP TR 38.801: "Study on new radio access technology: Radio access architecture and interfaces".

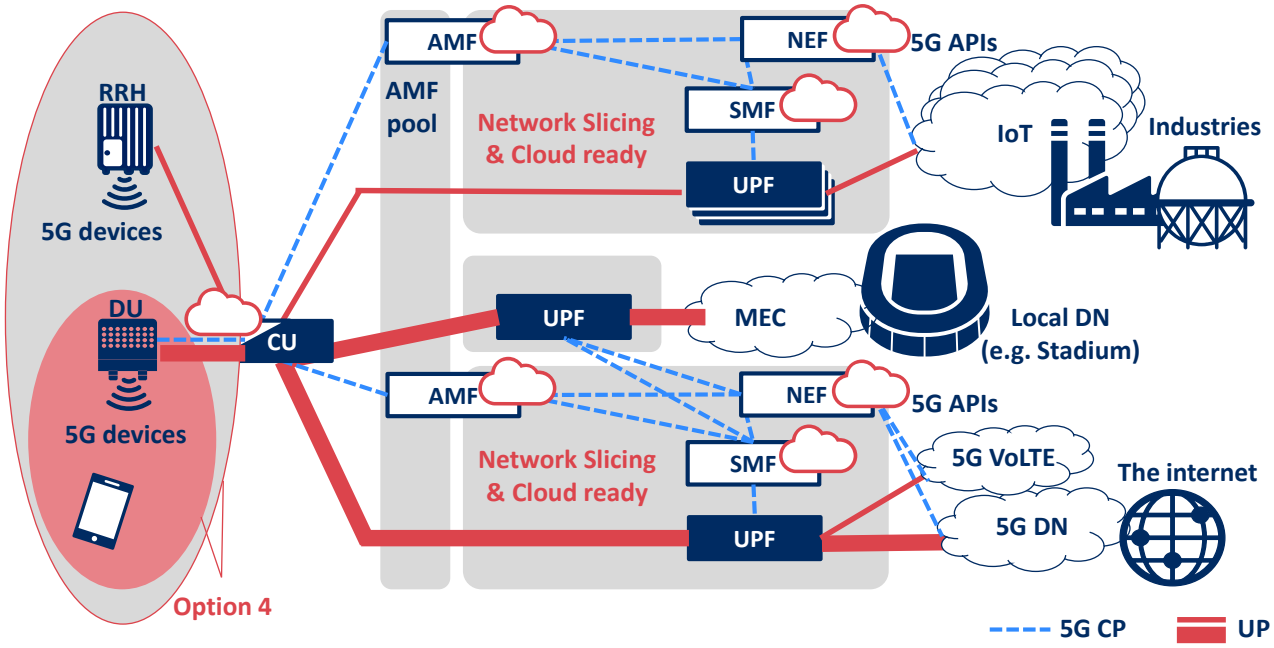


Figure 7: NR-E-UTRA (NE-DC) architecture (Option 4)

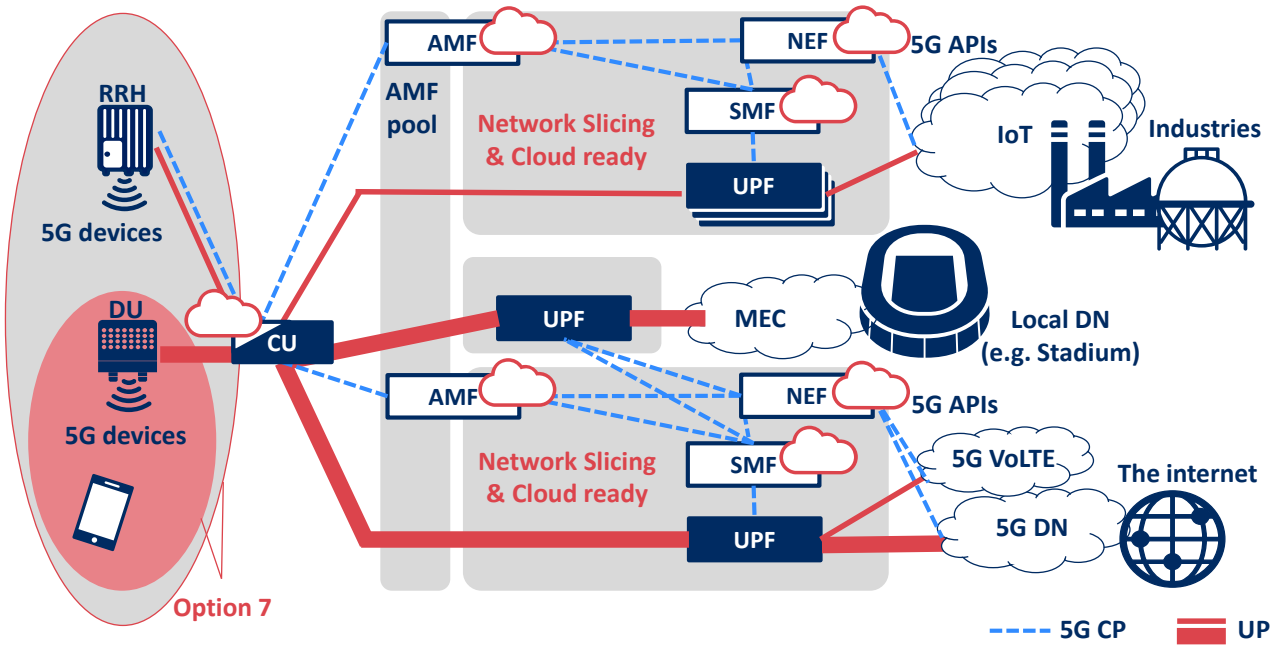


Figure 8: NG-RAN EN-DC (NG-EN-DC) architecture (Option 7)

2.4 Security

Security is dependent on both business requirements and system architecture. Given that there are several changes in 5G from both market, i.e. business, and architecture aspects, we have to expect changes in security as well. At the same time security solutions have to cater for issues identified in previous generations.

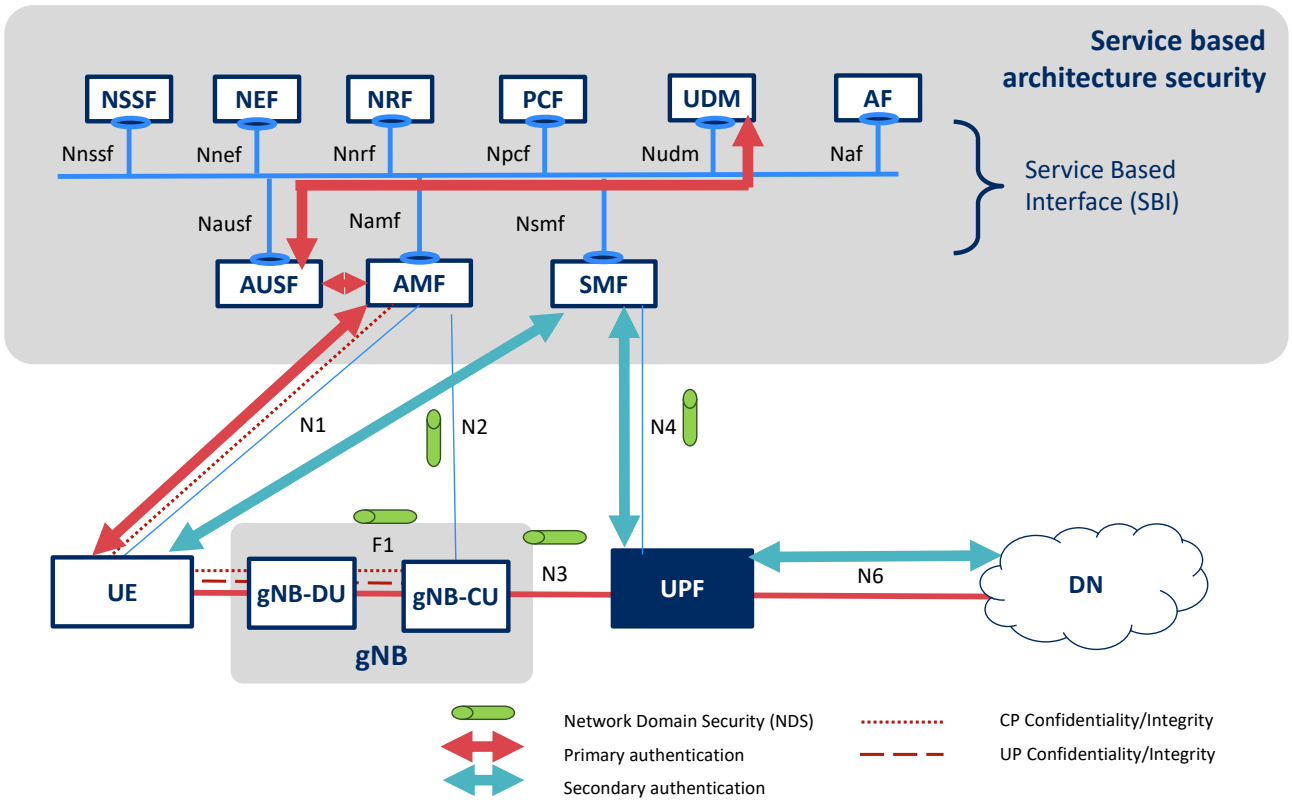


Figure 9: 5G security overview

With the above in mind, some of the changes in 5G security in Phase 1 are depicted in Figure 9: (a) key hierarchy suitable for the new architecture; (b) new options for authentication known as primary authentication; (c) options for secondary authentication for UE communication with external Data Network (DN) which can be associated to a slice; (d) options for security credentials storage in the UE; (e) privacy for subscription identity. Of course there is also security for SBA including inter-operator interconnect security and security for external interfaces that also includes APIs. In the following we discuss some details of few of these points.

Primary authentication is performed between the UE and the network, i.e. mutual authentication. Relation with business is that the operator can correctly identify the subscriber and thus correctly charge for services used. Two authentication mechanisms mandatory for 5G are (i) 5G Authentication and Key Agreement (5G-AKA), which is an enhancement of AKA used in 4G with the feature of increasing home network control and (ii) The second method is Extensible Authentication Protocol-AKA' (EAP-AKA'), which enables unified authentication framework for 3GPP and non-3GPP access technologies. Other EAP based authentication methods are also optionally allowed for primary authentication in 5G. EAP is a wrapper that allows any kind of authentication method to be carried on it thus opening mobile network to several authentication options for the first time. Cryptographic algorithms to be used are same as that for 4G, i.e. Advanced Encryption Standard (AES), SNOW-3G and ZUC, other algorithms might be added in Phase 2. Although not shown in Figure 9, non-3GPP authentication (e.g. WiFi) runs via a function known as Non-3GPP Inter-Working Function (N3IWF).

The purpose of the secondary authentication is to authenticate the UE's access to the 3rd party Data Network (DN) via the SMF, which acts as the authenticator. EAP based method is also agreed as the secondary authentication framework but exact authentication method is left open.

The protection of IP based interfaces for 5GC and NR-RAN will be done using Network Domain Security / Internet Protocol (NDS/IP) specification defined by 3GPP a while back. NDS/IP is based on IP security (IPsec). Traffic on interfaces carrying control plane signaling shall be integrity protected according to NDS/IP. In addition to the mandatory integrity protection, traffic carrying subscriber specific sensitive data, e.g. cryptographic keys, shall also be confidentiality protected according to NDS/IP. Specification leaves it on the operator to decide whether to use NDS/IP.

As mentioned earlier, 5G also provides solution for privacy of subscriber identity. In the 5Gs, the globally unique 5G subscription permanent identifier is called SUbscription Permanent Identifier (SUPI). In addition to that there is Subscriber Concealed Identifer (SUCI) that is used for privacy preserving. The UE generates SUCI using the public key from the home operator that was securely provisioned. The AMF supports primary authentication using SUCI.

In 5G the inter-operator interconnect (IPX network) will also be protected, this falls under SBA security. For this purpose a new function known as Security Edge Protection Proxy (SEPP) is being defined that will be placed at the edge of the operator network; not shown in Figure 9. The SEPP will provision confidentiality and integrity protection on the signaling traffic exchanged between different operators and also enforces security policies for topology hiding and firewall based filtering. Two-tier security model is being considered (1) application-layer security for end-to-end (e2e) protection of signaling messages or parts of the security-sensitive Information Elements (IEs) (2) transport layer security for hop-by-hop security between adjacent nodes in the IPX networks.

In addition to 3GPP specified security, usage of open source, cloud, NFV and SDN will require several non-standard (not defined in standard) security as well. All open source solutions will have to be security tested and so will the hardware used as they will be mainly off-the-shelf. Additional security for NFV will be required as discussed in Chapter 4. Bringing cloud, NFV and SDN will also allow enhanced security provisioning and thus business opportunities in the form of security as a service.

3 Migration and Interworking

It is obvious that 5G will not provide 100% coverage from day one. Thus migration steps from 4G to 5G are necessary. At the same time, 5G should work with 4G network thus interworking solution is required. The starting step defined by 3GPP is Non-Stand-Alone or NSA, also known as E-UTRA-NR Dual Connectivity (EN-DC), as discussed in Chapter 1. In this chapter we discuss 5G migration and interworking aspects for RAN, core network and security.

3.1 EN-DC – Reuse of existing networks

The EN-DC architecture, also known as Option 3 or non-stand-alone, is designed as early adaptation of the new 5G radio targeting a market launch before 2020. The key feature of the EN-DC is the ability to utilize existing LTE and EPC, thus making new 5G-based services available without network replacement. EN-DC uses LTE as the master radio access technology, while the new radio access technology (i.e. NR) serves as secondary radio access technology with UE connected to both radios thus dual connectivity.

In order to support EN-DC, the EPC (the 4G core network) requires minimal upgrade in 3GPP Release 15 timeframe. For example, the EPC supports low latency communications in addition to enhanced mobile broadband and massive machine type communications. In order to guarantee low latency communications, the EPC is enhanced with new capability to handle new standardized QoS class identifier (QCI). For example, new QCI may have a packet delay budget less than 10 msec. With this system-wide coordination, the EN-DC can support new contents-rich and real-time based services such as VR and AR without waiting full 5G system to be rolled-out.

With this approach, operators can provide high data rate services and radio capacity to smart devices in order to support continuously growing media services, e.g. video streaming, rich content sharing etc.

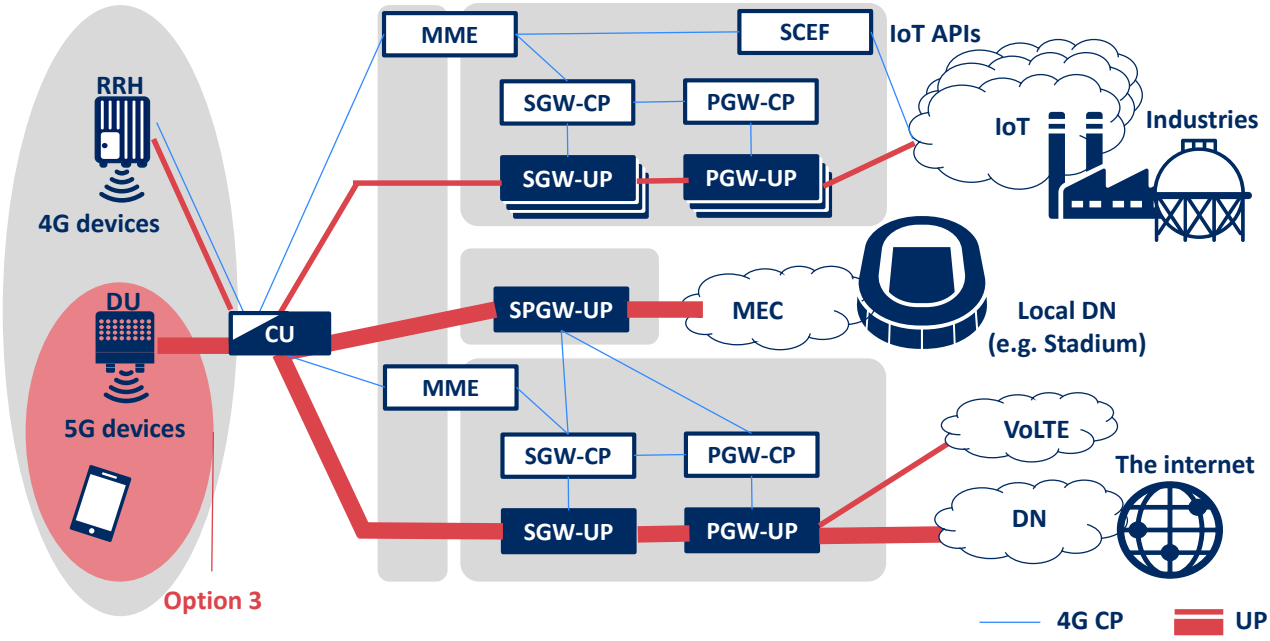


Figure 10: E-UTRA-NR Dual Connectivity (EN-DC) architecture, i.e. non-stand-alone

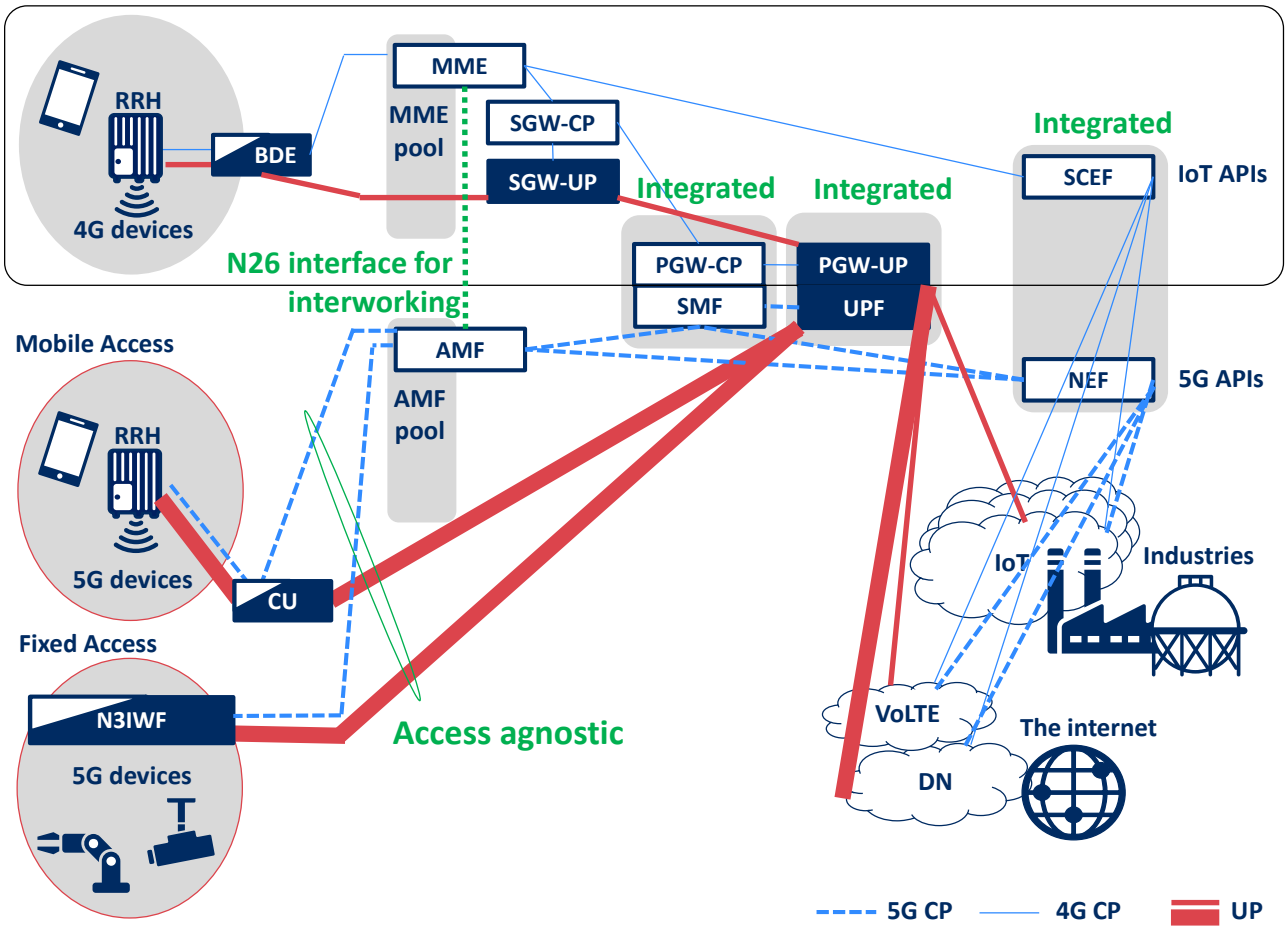


Figure 11: EPS – 5GS interworking deployment

3.2 Radio Access Network

The current 4G system can evolve via 2 types of migration path. The first path is to leverage the LTE radio and gradually introduce the NR, i.e. the EN-DC. The 5G service will then be available only in areas where the NR is available. Those areas can be determined by operators based on the expected traffic load or possible service requirements. In exchange for the relatively limited coverage of 5G services, operators can quickly provide the 5G service to users, reduce the investment cost for installing the new NR-RAN nodes (i.e. gNBs) and delay the 5GC installation in the early phase of the 5G availability in the market.

This first path could be further evolved by replacing the EPC with the 5GC, i.e. the NG-EN-DC (aka Option 7) as discussed in Section 2.2, where the new QoS handing and the network slicing can be utilized. This transition will bring additional flexibility, better user experience and more business opportunities for the “verticals”.

During the transition period, two types of RAN-CN connections, the LTE eNB connected to the EPC and the LTE eNB connected to the 5GC, will co-exist in the network. Service continuity can be ensured by introducing seamless mobility between the EPC and the 5GC. Finally, the system can evolve to the standalone NR operation (i.e. Option 2).

The second path is directly introducing the NR with the 5GC, i.e. the NR standalone (aka Option 2). Operators can provide the 5G services to users with extremely good performance due to the new QoS handling and the network slicing, in exchange for large initial investment required for nationwide support of the 5G services. On the other hand,

this path can be evolved further by using also the LTE radio, i.e. the NE-DC (aka Option 4, see Section 2.2), with little effort.

With the above, operators can select the appropriate migration path to the 5G according to their business plan and service requirements.

3.3 Core Network

From the view point of the core network, its migration will be conducted along with RAN's migration path. Note that the Options 2, 4 and 7 (as discussed in Sections 2.2 and 3.2) require 5GC. During the migration to these options, operators could manage both EPC and 5GS. Also, as a result of migration, Fixed Access may be served by 5GC thanks to the 5GC's access agnostic design.

To reduce unnecessary deployment during the migration, 5GS entities can be integrated with existing EPC entities. Optionally an inter-system interface between MME and AMF can assist smooth interworking between systems. Figure 11 is an example of the overall architecture consisting of integrated entities.

3.4 Security

From security point of view during migration it is important to consider that there will be a wide variety of UEs. Therefore, when a UE connects to 5G network or NR, the UE's capability including its security capability and the UE's access right to the network should be checked.

In case of EN-DC (or Option 3) a Master eNB (MeNB) checks whether the UE has 5G NR capability to access the Secondary gNB (SgNB) and the access right to SgNB. The MeNB derives and sends the key to be used by the SgNB for secure communication over NR; the UE also derives the same key. Unlike dual connectivity in 4G network, RRC messages are exchanged between UE and SgNB, thus keys used for integrity and confidentiality protection of RRC messages as well as UP data are derived. Although integrity protection for UP data is supported in 5G network, it will not be used in EN-DC case. Use of confidentiality protection is optional for both UP and CP. Security procedures for EN-DC basically follows the specifications of dual connectivity security for 4G.

On the other hand, security procedures in 5G such as authentication, key hierarchy and CP, UP security are required for Options 4 and 7, where UE connects to 5G core network via LTE and NR. The overall 5G security is presented in Section 2.4.

In case of interworking between 4G and 5G networks, UE's capability including security and access rights are checked not only when attaching to 4G or registering to 5G network, but also during handover between the two networks. At the handover, an intermediate security key is derived at the source network (AMF or MME) and the key is sent to target network via the N26 interface defined between AMF and MME. The security key in the target network is derived from the intermediate key followed by CP and UP security keys for integrity and confidentiality protection.

4 5G Impact on BSS/OSS

5G opens up unparalleled business opportunities for operators to step into new areas, acquire new customers and differentiate in the highly competitive telecom market. 5G services and business models will rely on 4 key principles:

- Offerings will become more complex, bundling products and services with different requirements towards quality of service, rating, billing and fulfilment. This will become especially prominent in enterprise offerings with complex end-to-end vertical solutions. Resulting in 5G offerings being more complex to fulfill, rate and bill requiring new capabilities from order management and product catalog.
- New services will be provided over any type of network whether it is fixed, wireless or WiFi
- Services will become real-time and on-demand with customers able to order them, consume and deactivate with a single click through any touchpoint,
- The partner ecosystem will become a key element of complex multi-component 5G offerings such as Connected Cars, Smart Home and vertical solutions.
- To capitalize on the 5G opportunity, service providers will have to make sure that their Business Support Systems/Operational Support Systems (BSS/OSS) ecosystem, as depicted in Figure 12, is ready to deliver and monetize the new fixed-wireless, complex, on-demand, partner-enabled services.

Based on these principles, in this chapter we present 5G impacts on BSS, OSS, orchestration and security aspects.

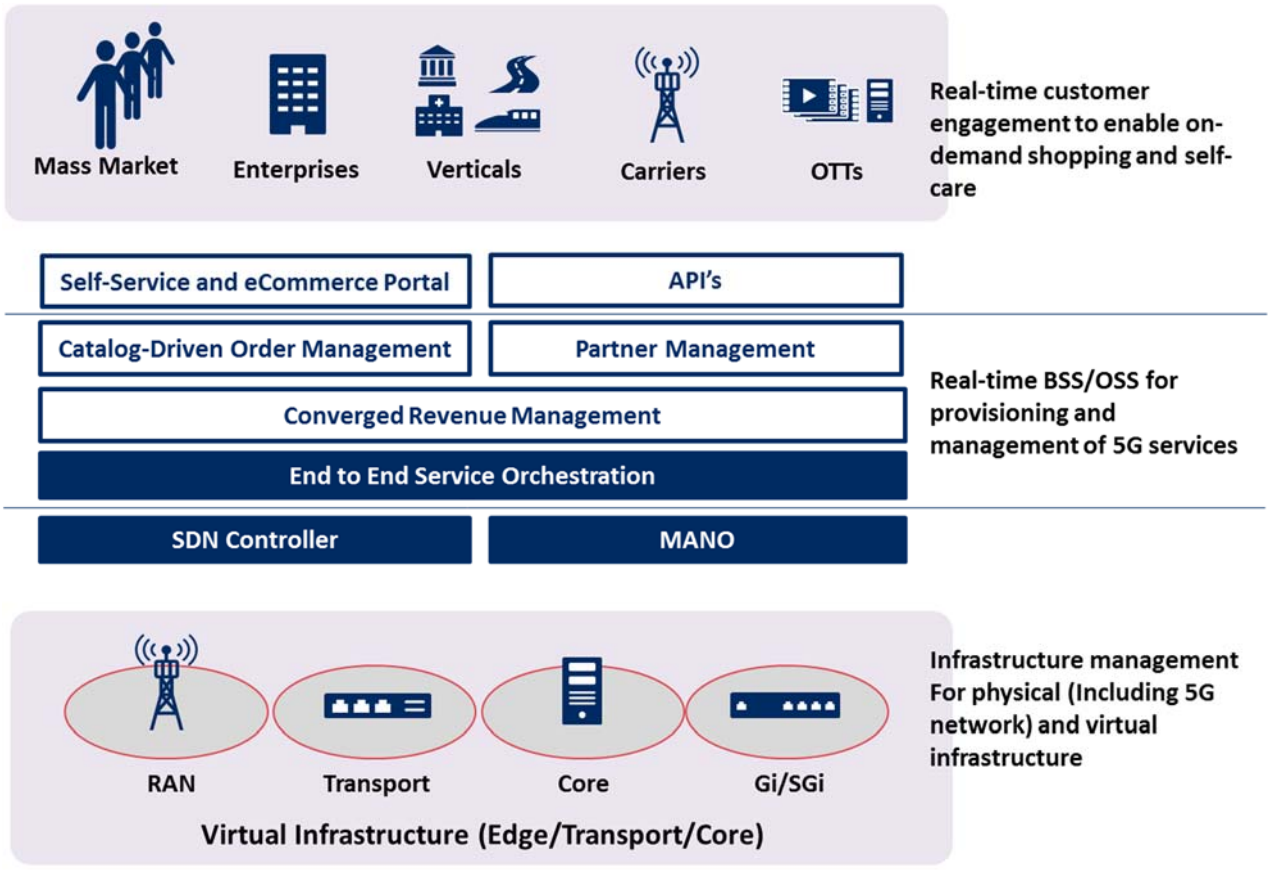


Figure 12: End-to-end 5G BSS/OSS Ecosystem

4.1 Impacts on BSS

The changes on BSS side will be driven by on-demand nature of 5G business models, openness of the 5G ecosystem and increased offer complexity. Emphasis will be put on enabling customers to manage services and infrastructure in real-time through either self-service capabilities or API's. BSS applications will have to be seamlessly integrated to-deliver the needed responsiveness and agility.

Impact of 5G on BSS applications will be significant across all core domains:

- Self-service based Sales and Care. To efficiently sell on-demand 5G offerings, service providers will have to provide customers with the ability to order services and manage them effortlessly with just a couple of clicks. Because of this, service providers will need to move away from siloed self-service applications with lack of BSS integration to a pre-integrated omni-channel ecosystem that is able to drive lifetime value-oriented customer experience. On top of traditional channels 5G will enable many new touchpoints such as IoT devices, Connected Cars and many others. This will require service provider to deliver self-service capabilities through these touchpoints by exposing shopping and care API's.
- Order Management will play a bigger role as it will have to enable the ordering of complex 5G services. Fixed-wireless will enable enhanced mobility allowing enterprises to have their complex enterprise fixed-line services over their mobile network. This along with increased offering complexity will require new order management capabilities form service providers. Order Management will have to support real-time delivery of these complex multi-component on-demand services for business and mass market consumers. It will have to rely on a dynamic product catalog which will enable real-time creation of service offerings taking into account a variety of network parameters including current network capacity, demand and partner incentives. The product catalog will have to support diverse partner-enabled business models:
  - Service provider bundling partner services with own services and selling bundles to the end customer
  - Partners bundling service provider services with own services and selling them to end-customers
  - Service provider white-labelling partner services and selling them to end customers
- To accelerate time-to-market for new offerings, service provider will have to enable quick offerings design, creation, deployment and management. This will require extensive configuration capabilities in product catalog and a user-friendly interface for non-technical users.
- Due to an increased number of services, Revenue Management will have to be flexible and quick to change to provide accelerated time-to-market. It will have to support pre-paid like capabilities for post-paid customer to enable real-time pricing and quotation of on-demand 5G services. As these services will reside in different network slices with different QoS requirements, Revenue Management will have to be slice-aware and support rating based on diverse parameters. Since many 5G services will be partner-enabled, Revenue Management will have to support complex revenue sharing schemes across partners that are involved in the service delivery.
- Partner management will play critical role in the complex partner-enabled 5G business models. Service providers will have the capability to onboard partners quickly through APIs and integrate partner offerings into the product catalog. In the 5G ecosystem partner onboarding will become a day-to-day process, it will

leverage Continuous Integration/ Continuous Testing/ Continuous Delivery methodologies to ensure the necessary speed to market. As partner ecosystem will constantly expand, service provider will need robust partner management capabilities to support diverse partners with different business models.

- The API Ecosystem will play a major role in enabling diverse 5G use-cases. Enabling 5G Infrastructure-as-a-Service will require exposure of network management and orchestration capabilities to 3rd parties and customers. These parties will be able to leverage 5G network programmability to create new slices and sub-slices, change them, and manage their parameters including SLA's, services and users. Another important role for API's is to enable cross-operator network orchestration for complex scenarios including federated slicing for 5G roaming and cross-operator infrastructure sharing. This means that to enable a 5G ecosystem service providers will need to rely on a set of out-of-the box 5G-ready API's.

4.2 Impacts on OSS

5G will have significant impact on service provider's OSS environment with network slicing being one of the key game changing concepts. The OSS will have to support delivery of complex partner-enabled services across heterogeneous infrastructure including fixed, wireless, WiFi networks, small cells. It will have to work in real-time to enable seamless quotation, ordering and quality management of on-demand services. The programmable sliced networks will enable on-the-fly management of infrastructure, network functions and network resources. Logical separation of network slices will allow independent management of services, associated per different slices. The network slices shall have exposure through APIs to 3rd party partners for more rapid service onboarding, development and market introduction.

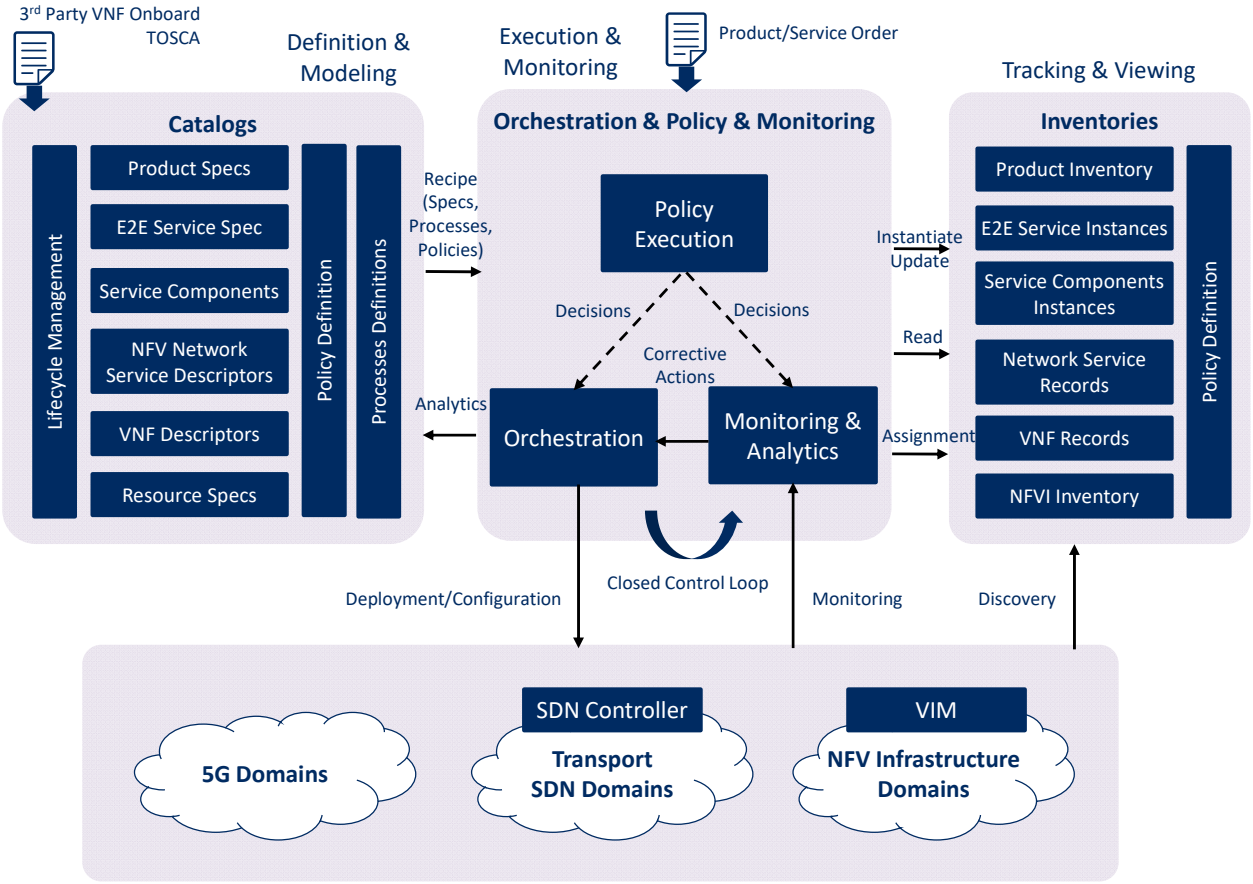


Figure 13: End-to-end Service Orchestration Architecture

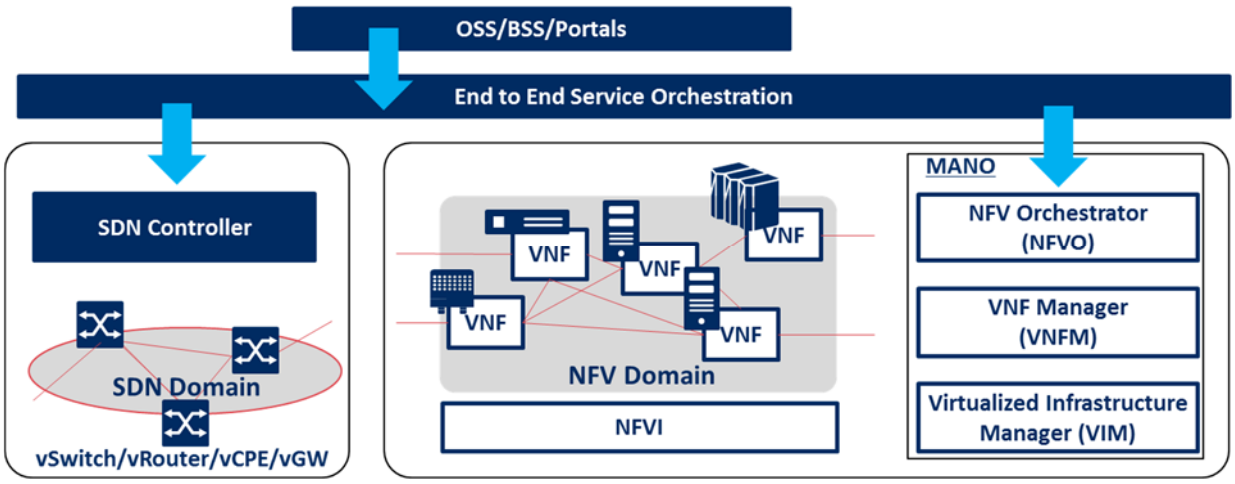


Figure 14: SDN/NFV Architecture as a part of End-to-End BSS/OSS stack

4.2.1 End-to-end Service Orchestration

Management of 5G network will require OSS to rely on end-to-end service orchestration, depicted in Figure 13, to manage physical and virtual infrastructure including complex scenarios like Mobile Edge Computing. End-to-end Service Orchestration will support multi-domain orchestration approach to provide fulfillment of service components within specific network domains by performing required resource assignment logic and configuring corresponding underlying physical and virtual network elements and controllers. It will have to be slice-aware to provision services into specific slices and transition customers between slices in real-time.

End-to-end Service Orchestration will have to include closed-loop analytics-driven service assurance along with real-time Quality of Service management to deliver QoS based services. It will track SLA adherence and heal, scale or modify the underlying services when deviation is detected. Each orchestration layer implements closed control loop (orchestrate change – monitor – detect anomaly – orchestrate change) and includes:

- Orchestration component that performs execution of requests corresponding to the orchestration layer (e.g. E2E Service/Service Component/NFV Network Service/VNF instantiation/modification/scaling/healing/termination requests) in accordance with corresponding specifications/descriptors and associated process definitions and policies provided by Catalog (e.g. E2E Service/Service Components, NS/VNF descriptions). Requests for execution are received from underlying orchestration layer or from Monitoring/Analytics. Requests are decomposed and sent to underlying orchestration layers, network functions and controllers.
- Monitoring/Analytics component monitors state of entities corresponding to the orchestration layer (e.g. E2E Service/Service Component/NS/VNF) by getting events (e.g. alarms, faults) and metrics from underlying orchestration layer or from network functions/Controllers, performs real time and background analytics, including event correlation and processing (e.g. root cause analysis, service impact analysis), aggregates metrics to KPI/KQIs, detect anomalies and trigger resolution actions (e.g. corresponding auto-healing or auto-scaling scenarios) via Orchestration component in accordance with Policies.

4.2.2 5G Infrastructure Management & Orchestration

The 5G system has originally been designed to adapt the latest technologies, e.g. NFV and Cloudification, in order to guarantee the necessary agility. In contrast to the existing EPS, 5G core network entities are designed stateless as much as possible in order to be

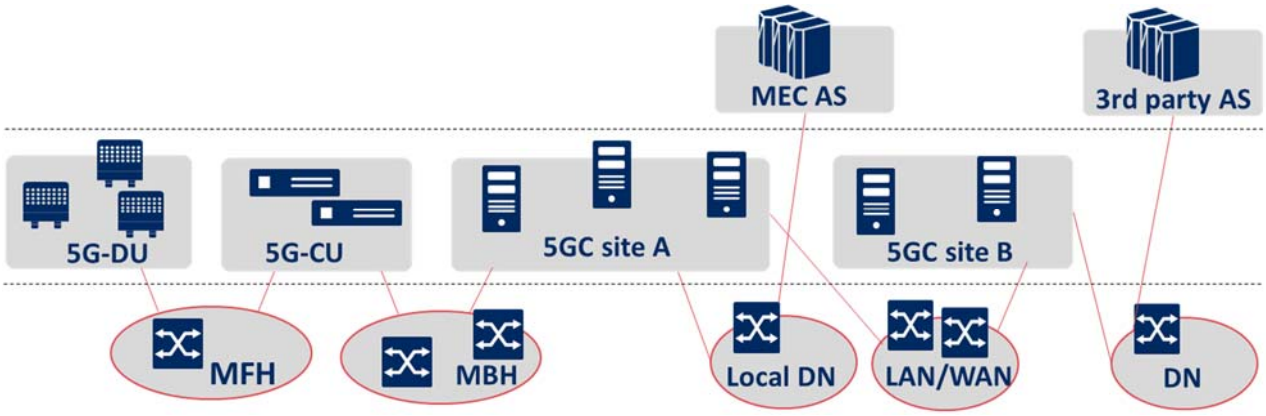


Figure 15: End to end path over the 5GS architecture

able to adapt their capacity dynamically based on their load or even to delete them from the network if not needed any longer. This flexibility can be achieved by adapting the life cycle management mechanism that is defined by the NFV. The Figure 14 illustrates the basic NFV architecture as a part of the end-to-end stack. The VNF, as Virtual Network Function, in the Figure 14 can be a 5G logical entity, like the AMF. Each VNF is dynamically instantiated by using physical resources on NFV Infrastructure (NFVI) under the control of Management and Orchestration (MANO). As the NFV architecture makes it possible for instantiating, deleting, upgrading, downgrading of VNF at any time, holistic network resource management is guaranteed.

On top of the basic NFV architecture as shown in the Figure 14, there are new challenges ongoing to make the end-to-end orchestration possible for the 5G system.

One of the new challenges is to introduce fully automated network management by adapting AI technology together with SDN and NFV. The Figure 15 illustrates the end–to-end connection over the 5G system using SDN and NFV.

As shown in the Figure 15, the distributed RAN can be structured, which consists of 5G-CU entities and 5G-DU entities over the mobile front-haul (MFH). Moreover, 5GC entities and their transport networks (shown as the mobile back-haul (MBH) and LAN/WAN) can be structured as well as the upper Application Servers. These virtualized entities can be connected each other, using new NFV technology, known as "multi-site service over the Wide Area Network". It allows to make transmission paths based on the transport SDN technology and guarantee the data transmission bandwidth between entities over the WAN with taking each entity's capacity into account, for the reliable data transmission.

Then operator can configure its 5G network based on the slices to be instantiated/supported. Depending on the slice characteristics, the network structure required to be instantiated inside the slice varies. For example, if a network slice is used for URLLC (Ultra-Reliable and Low Latency Communications) services, the 3rd party providing the services will benefit from a network structure where all core network entities are located very close to the users in order to guarantee a short delay budget between end to end. The end-to-end forwarding graph technology defined by the ETSI NFV makes it possible to create a tailored network slice configuration based on the SLA with 3rd party. The slice characteristics are described by the standard descriptor that is defined by the NFV.

4.2.3 MANO Security

Security is involved in all levels of NFV MANO components and reference points, including NFV Orchestrator, VNF Manager, and Virtual Infrastructure Manager. Some of

the security issues and requirements addressed in ETSI NFV are remote attestation, dynamic security policy management, security for Lawful Interception (LI) functions, security function lifecycle management, and security monitoring of NFV systems. The lifecycle of MANO component also includes security assurance and security management.

Figure 16 depicts overall NFV security logical representation which consists of Orchestration, VNF Layer and NFV Infrastructure. Orchestration security is classified as NFV Security Manager (NSM) and Security Orchestration. The NSM is the logical functional block for overall security management including security policies and security requirements for dedicated security functions or security functions embedded within VNFs. The Security Orchestration automates triggering of deployment or activation of Virtual Security Functions (VSFs) and Infrastructure Security Functions (ISFs), to the NFVI, thus creating a pool of virtual security devices. The VSF is a special type of VNF with security functionality (e.g. Virtualized Front-end processor (vFEP), virtual taps (vTap)) running on top of NFVI.

The VNF layer includes Security Element Managers (SEM), VNF Security Engine, NFVI Security Manager and 5G Network functions such as SMF, AMF, UPF, gNB-CU etc. The SEM refers to Element Managers (EMs) managing Security Functions. VNF Security Engine handles all the cryptography algorithms and protocols. The NFVI Security Manager manages multiple Security Monitoring Agents that are deployed across physical hosts within a NFVI.

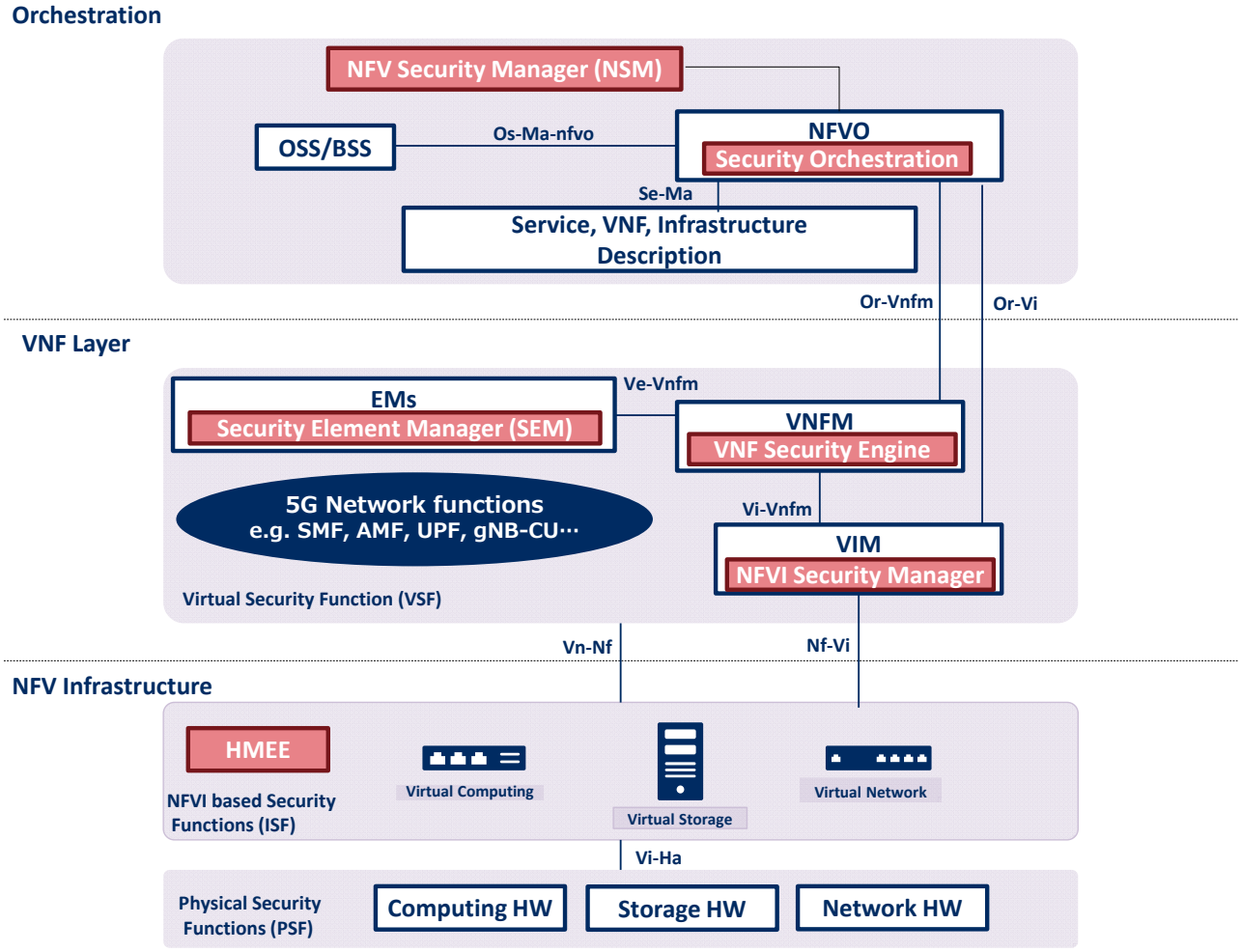


Figure 16: NFV Security logical representation

The NFV Infrastructure includes NFVI-based Security Functions and Physical Security Function. NFVI-based Security Function includes virtualized security appliances (e.g. virtual firewalls) and hardware-based security appliances such as Hardware-Mediated Execution Enclave (HMEE). HMEE is an independent security engine, an exclusive CPU/Memory mode, or an enclave providing memory encryption and code/data execution isolation. Physical Security Function is a security function in the physical part of the network, i.e. non-virtualized.

5 Summary

5G specifications of 3GPP are almost complete. Thus we can surely expect 5G to be available in the market by 2020 if not earlier. This whitepaper brings a timely review of 5G. In this section we summarize some of the key points discussed in the whitepaper.

5G is being developed on the basis of market requirements and the availability of technology that can fulfill these requirements. We are observing market requirements such as reduction of total cost of ownership, provisioning of various types of services, need of partnership with different players or verticals and also sophisticated customer demands. These market requirements induce development of technology to support as well as enable varying data-rates and flexibility, among others.

Cloud, NFV and SDN combined with Open Source Software brings flexibility and also several other benefits such as easier deployment as well as easy sharing of network, i.e. multi-tenancy. Introduction of Open Source Software also requires additional security consideration that goes beyond 3GPP security specifications.

NR technology of 5G allows varying data rates and delays. The NR-RAN is split in a central unit that can exist in cloud and a distributed unit allowing services to be brought closer to the devices.

The core network or 5GS based on NFV/SDN and several other enhancements allows network slicing to provision network uniquely to given service or partner. 5GS is clearly divided in CP and UP. The CP is based on service based architecture that, among others, allows easier interfacing with external parties using API.

To make 5G secure and to enable business, the 5GS provisions several authentication methods that goes beyond any previous generations of mobile systems. Also from security perspective, the UE can have newer means of storing security credentials for subscriber authentication. Security is also provisioned for SBA and external interfaces.

For smooth transition towards complete roll-out of 5G, 3GPP studied various options and concluded on non-stand-alone, also known as EN-DC, as the starting step. In EN-DC the 5G base-station or gNB will be connected to the 4G core network with UE connecting to both 4G and 5G base-stations – dual connectivity.

Changes in 5G will also have significant impacts on BSS/OSS. On demand nature of 5G will mean enabling customers to manage their services flexibly over BSS. Slicing will impact OSS and so will the APIs towards business partners and customers.

NEC's concept is "5G. A Future Beyond Imagination." which constitutes of three key transformations – network, operations and social transformation. For the first key transformation, i.e. network, we need new system and new fundamental technologies. NEC is actively working on this towards development of a more reliable network. The second transformation is in operations. NEC is actively working to utilize NEC's AI capabilities for automation and support of clients' needs. The third is social transformation that includes changes in lifestyle and workstyle; NEC is working on innovations to support social transformation.

"5G. A Future Beyond Imagination."

Abbreviations

2G	Second (2nd) Generation
3G	Third (3rd) Generation
3GPP	The Third Generation Partnership Project
4G	Fourth (4th) Generation
5G	Fifth (5th) Generation
5GC	Fifth (5th) Generation Core
5GS	Fifth (5th) Generation System
AES	Advanced Encryption Standard
AF	Application Function
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
API	Application Programming Interface
AR	Augmented Reality
ARPU	Average Revenue Per User
AS	Application Server
AUSF	Authentication Function
BDE	Base station Digital processing Equipment
BS	Base Station
BSS	Business Support System
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CN	Core Network
CP	Control Plane
CPE	Customer Premises Equipment
CRS	Cell-specific Reference Signals
CSI-RS	Channel State Information Reference Signal
CU	Central Unit
CUPS	Control and User Plane Separation
DC	Data Center
Decor	Dedicated core
DFT	Discrete Fourier Transformation
DMRS	Demodulation Reference Signal
DN	Data Network
DNS	Domain Network Server
DU	Distributed Unit
E2E	End-to-End
EAP	Extensible Authentication Protocol

EM	Element Management
eMBB	enhanced Mobile Broadband
EN-DC	E-UTRA-NR Dual Connectivity
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standards Institute
E-UTRA	Evolved-Universal Mobile Telecommunications System Terrestrial Radio
GCS	Group Communication System
GPRS	General Packet Radio Service
HMEE	Hardware-Mediated Execution Enclave
HSM	Hardware Security Module
HW	Hardware
IMS	IP Multimedia Subsystem
IOPS	Isolated E-UTRAN Operation for Public Safety
IoT	Internet of Things
IP	Internet Protocol
ITU	International Telecommunications Union
KPI	Key Performance Index
KQI	Key Quality Indicator
LDPC	Low Density Parity Check
LI	Lawful Interception
LTE	Long Term Evolution
M&A	Merger and Acquisition
MAC	Medium Access Control
MANO	Management And Network Orchestration
MBH	Mobile Back Haul
MC	Mission Critical
MCC	Mobile Country Code
MCPTT	Mission Critical Push To Talk
MEC	Mobile Edge Computing
MeNB	Master eNB
MFH	Mobile Front Haul
MIMO	Multiple Input Multiple Output
MME	Mobility Management Entity
MMTC	Massive Machine-Type Communication
MNC	Mobile Network Code
MVNO	Mobile Virtual Network Operator
N3IWF	Non-3GPP Inter-Working Function
NBIoT	Narrow Band IoT

NDS	Network Domain Security
NEF	Network Exposure Function
NFV	Network Function Virtualization
NFVM	NFV Manager
NFVO	NFV Orchestrator
NG	Next Generation
NRF	Network Resource Function
NSA	Non-Stand-Alone
NSSAI	Network Slice Selection Assistance Information
NW	Network
O&M	Operations and Management
OFDM	Orthogonal Frequency Division Multiplexing
OSS	Operations System
OTT	Over The Top
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PHY	Physical
ProSe	Proximity-based Services
PTRS	Phase Tracking Reference Signal
PUCCH	Physical Uplink Control CHannel
QCI	QoS class identifier
QoS	Quality of Service
RAN	Radio Access Network
RRC	Radio Resource Control
RRH	Remote Radio Head
SAE	System Architecture Evolution
SAGE	Security Algorithms Group of Experts
SBA	Service Based Architecture
SCEF	Service Capability Exposure Function
SCS	Subcarrier Spacing
SDAP	Service Data Adaptation Protocol
SDN	Software Defined Network
SEPP	Security Edge Protection Proxy
SgNB	Secondary gNB
SGW	Serving Gateway
SIDF	Subscription Identifier De-concealing Function
SIM	Subscriber Identification Module
SLA	Service Level Agreement
SMF	Session Management Function

SPGW	Serving and PDN Gateway
SUCI	SUbscription Concealed Identifier
SUPI	SUbscription Permanent Identifier
TDD	Time Division Duplex
TP	Termination Point
TRS	Total Radiated Power
TS	Technical Specification
UDM	Unified Data Management
UE	User Equipment
UI	User Interface
UL	Up-Link
UP	User Plane
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communication
V2C	Vehicle to Cloud
V2I	Vehicle to Infrastructure
V2X	Vehicle to Everything
vFEP	virtualized Front-end processor
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Function
VNFM	Virtual Network Function Manager
VoLTE	Voice over LTE
VR	Virtual Reality
WAN	Wide Area Network

Bibliography

[1] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[2] 3GPP TS 23.501: "System Architecture for the 5G System ".

[3] 3GPP TS 23.502: "Procedures for the 5G System ".

[4] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[5] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[6] 3GPP TS 36.300: "E-UTRA and E-UTRAN; Overall description".

[7] 3GPP TS 37.340: "E-UTRA and NR; Multi-connectivity".

[8] 3GPP TS 38.300: "NR; Overall description".

[9] 3GPP TS 38.401: "NG-RAN; Architecture description".

[10] 3GPP TR 38.801: "Study on new radio access technology: Radio access architecture and interfaces".

ETSI NFV website: http://www.etsi.org/technologies-clusters/technologies/nfv

3GPP website: http://www.3gpp.

NEC Corporation

7-1, Shiba 5-chome, Minato-ku, Tokyo 108-8001, Japan

Contact: 5G-A-Reality@std.jp.nec.com

http://www.nec.com/en/global/solutions/nsp/5g_vision/
