1

Introduction

1.1 Overview

The 5G Explained presents key aspects of the next, evolved mobile communications system after the 4G era. This book concentrates on the deployment of 5G and discusses the security-related aspects whilst concrete guidelines of both topics for the earlier generations can be found in the previously published books of the author in Refs. [1, 2].

The fifth generation is a result of long development of mobile communications, the roots of its predecessors dating back to the 1980s when the first-generation mobile communication networks started to convert into a reality [3]. Ever since, the new generations up to 4G have been based on the earlier experiences and learnings, giving the developers a base for designing enhanced security and technologies for the access, transport, signaling, and overall performance of the systems.

Regardless of the high performance of 4G systems, the telecom industry has identified a need for faster end-user data rates due to constantly increasing performance requirements of the evolving multimedia. 5G systems have thus been designed to cope with these challenges by providing more capacity and enhanced user experiences that solve all the current needs even for the most advanced virtual reality applications. At the same time, the exponentially enhancing and growing number of IoT (Internet of Things) devices requires new security measures such as security breach monitoring, prevention mechanisms, and novelty manners to tackle the vast challenges the current and forthcoming IoT devices bring along.

The demand for 5G is reality based on the major operators' interest to proof the related concepts in global level. Nevertheless, the complete variant of 5G is still under development, with expected deployments complying with the full set of the strict performance requirements taking place as of 2020.

As there have been more concrete development and field testing activities by major operators, as well as agreements for the forthcoming 5G frequency allocation regulation by International Telecommunications Union (ITU) World Radio Conference (WRC) 19, this book aims to summarize recent advances in the practical and standardization fields for detailing the technical functionality, including the less commonly discussed security-breach prevention, network planning, optimization, and deployment aspects of 5G based on the available information during 2018 and basing on the first phase of the 3rd Generation Partnership Project (3GPP) Release 15, which is the starting point for the gradual 5G deployment.

5G Explained: Security and Deployment of Advanced Mobile Communications, First Edition.
Jyrki T. J. Penttinen.

1.2 What Is 5G?

The term 5G refers to the fifth generation of mobile communication systems. They belong to the next major phase of mobile telecommunications standards beyond the current 4G networks that will comply with the forthcoming International Mobile Telecommunications (IMT)-2020 requirements of ITU-R (radio section of the International Telecommunications Union). 5G provides much faster data rates with very low latency compared to the current systems up to 4G. It thus facilitates the adaptation of highly advanced services in wireless environment.

The industry seems to agree that 5G is, in fact, a combination of novel (yet to be developed and standardized) solutions and existing systems basing on 4G Long-Term Evolution (LTE)-Advanced, as well as non-3GPP access technologies such as Wi-Fi, which jointly contributes to optimizing the performance (providing at least 10 times higher data rate compared to current LTE-Advanced networks), lower latency (including single-digit range in terms of millisecond), and support of increased capacity demands for huge amounts of simultaneously connected consumer and machine-to-machine, or M2M, devices. Because of the key enablers of 5G, some of the expected highly enhanced use cases would include also the support of tactile Internet and augmented, virtual reality, which provide completely new, fluent, and highly attractive user experiences never seen before.

At present, there are many ideas about the more concrete form of 5G. Various mobile network operators (MNOs) and device manufacturers have been driving the technology via concrete demos and trials, which has been beneficial for the selection of optimal solutions in standardization. This, in turn, has expedited the system definition schedules. While these activities were beneficial for the overall development of 5G, they represented proprietary solutions until the international standardization has ensured the jointly agreed 5G definitions, which, in turn, has led into global 5G interoperability.

The mobile communication systems have converted our lives in such a dramatic way that it is hard to imagine communication in the 1980s, when facsimiles, letters, and plain old fixed-line telephones were the means for exchanging messages. As soon as the first-generation mobile networks took off and the second generation proved the benefits of data communications, there was no returning to those historical days. The multimedia-capable third generation in the 2000s, and the current, highly advanced fourth generation offer us more fluent always-on experiences, amazing data rates, and completely new and innovative mobile services. The pace has been breathtaking, yet we still are in rather basic phase compared to the advances we'll see during the next decade. We are in fact witnessing groundbreaking transition from the digital world toward truly connected society that will provide us with totally new ways to experience virtual reality and ambient intelligence of the autonomic IoT communications.

The ongoing work on the development of the next big step in the mobile communications, the fifth generation, includes the IoT as an integral part. Although one of the key goals of the 5G is to provide considerably higher data rates compared to the current 4G systems, with close to zero delays, at least an equally important aspect of the new system will be the ability to manage huge amount of simultaneously communicating IoT devices – perhaps thousands under a single radio cell.

1.3 Background

The term *5G* is confusing. During 2016–2017, there were countless public announcements on the expected 5G network deployments while the 4G deployment was still in its most active deployment phase. Up to the third-generation mobile communication networks, the terminology has been quite understandable, as 3G refers to a set of systems that comply with the IMT-2000 (International Mobile Telecommunications for 3G) requirements designed by the ITU. Thus, the cdma2000, Universal Mobile Telecommunications System (UMTS)/High Speed Packet Access (HSPA) and their respective evolved systems belong to the third generation as the main representatives of this era.

The definition of the fourth generation is equally straightforward, based on the ITU's IMT-Advanced requirements. While 3G had multiple representatives in practice, there are only two systems fulfilling the official, globally recognized 4G category as defined in IMT-Advanced, and they are the 3GPP LTE-Advanced as of Release 10, and the IEEE 802.16m referred to also as WiMAX2. The first 3GPP Release 8 and Release 9 LTE networks were deployed in 2010–2011, and their most active commercialization phase took place around 2012–2014. Referring to ITU-terminology, these networks prior to Release 10 still represented the evolved 3G era, which, as soon as they were upgraded, resulted in the fully compatible 4G systems.

While 4G was still being developed, the 5G era generated big interest. The year 2017 was a concrete show-time for many companies for demonstrating how far the technical limits could be pushed. Some examples of these initiations, among many others, included Verizon 5G Technology Forum, which included partners in the Verizon innovation centers [4], and Qualcomm, which demonstrated the capabilities of LTE-Advanced Pro via millimeter-wave setup [5].

These examples and other demos and field trials prior to the commercial deployment of 5G indicated the considerably enhanced performance and capacity that the 5G provides, although fully deployed, Phase 2 of 5G as defined by 3GPP is still set to the 2020 time frame. As soon as available, the 5G era will represent something much more than merely a set of high-performance mobile networks. It will, in fact, pave the way for enabling a seamlessly connected society with important capabilities to connect a large number of always-on IoT devices.

The idea of 5G is to rely on both old and new technologies on licensed and unlicensed radio frequency (RF) bands that are extended up to several GHz bands to bring together people, things, data, apps, transport systems and complete cities, to mention only some – in other words, everything that can be connected. The 5G thus functions as a platform for ensuring smooth development of the IoT, and it also acts as an enabler for smart networked communications. This is one of the key statements of ITU, which eases this development via the IMT-2020 vision.

The important goal of 5G standard is to provide interoperability between networks and devices, to offer high capacity energy-efficient and secure systems, and to remarkably increase the data rates with much less delay in the response time. Nevertheless, the 5th generation still represents a set of ideas for highly evolved system beyond the 4G. As has been the case with the previous generations, the ITU has taken an active role in coordinating the global development of the 5G.

1.4 Research

There are many ideas about the form of 5G. Major operators and device manufacturers have actively conducted technology investigations, demos, and trials aiming to prove the concepts and contributing to the standardization.

There are also several research programs established to study the feasibility and performance of new ideas in academic level. As an example, the European Union (EU) coordinates 5G research programs under various teams. More information about the latest European Commission (EC) funded 5G research plans can be found in EU web page, which summarizes 5G initiatives [6]. As stated by EU, the 5G of telecommunications systems will be the most critical building block of our digital society in 2020–2030. Europe has taken significant steps to lead global developments toward this strategic technology. Furthermore, EU has recognized that the 5G will be the first instance of a truly converged network environment where wired and wireless communications will use the same infrastructure, driving the future networked society. EU states that *5G will provide virtually ubiquitous, ultra-high bandwidth connectivity not only to individual users but also to connected objects. Therefore, it is expected that the future 5G infrastructure will serve a wide range of applications and sectors, including professional uses such as assisted driving, eHealth, energy management, and possibly safety applications.*

The EC study programs include FP7 teams and METIS (Mobile and wireless communications Enablers for Twenty-twenty (2020) Information Society), and other internationally recognized entities. One of the international joint activities is the cooperation between EU and Brazil [7].

As for the 5G radio capacity needs on the current bands, the European Commission aims to coordinate the use of the 700 MHz band for mobile services to provide higher-speed and higher-quality broadband and cover wider areas, including rural and remote regions. The concrete goal of EU is to provide mobile broadband speeds beyond 100 Mb/s.

1.5 Challenges for Electronics

One of the expected key abilities of the 5G networks is the high-energy efficiency to cope with a big amount of low-power IoT devices in the field. The benefits include better cost-efficiency, sustainability, and widening the network coverage to remote areas. Some of the base technologies for facilitating the low energy include advanced beamforming as well as radio interface optimization via user-data and system-control plane separation. Other technologies include reliance on virtualized networks and clouds.

The systems also need to be developed at the component level for both networks and devices. Autonomously functioning remote IoT devices require special attention, as they must function reliably typically several years without human interaction or maintenance. The advances in the more efficient battery technologies are thus in key position. Also, the very small devices such as consumer wearables and M2M sensor equipment may require much smaller electronical component form factors, including tiny wafer-level subscriber modules that still comply with the demanding reliability and durability requirements in harsh conditions. At the same time, the need for enhanced security aspects will require innovative solutions in the hardware (HW) and software (SW) levels.

1.6 Expected 5G in Practice

The 5G is a result of a long development of mobile communications, with roots going back to the 1980s when the first-generation mobile communications networks began to be reality. Ever since the first data services, which the 2G systems started to include around the mid-1990s, the new generations up to 4G have been based on the earlier experiences and learnings, giving the developers a base for designing enhanced technologies for the access, transport, signaling, and overall performance of the systems. Figure 1.1 depicts the development of the data rates of the 3G, 4G, and 5G systems.

However, the telecom industry has identified a further need for considerably faster end-user data rates to cope with the demands of the evolving multimedia. The 5G could handle these challenging capacity requirements to provide fluent user experiences even for the most advanced virtual reality applications. At the same time, the exponentially growing number of the IoT devices require new security measures, including potential security-breach monitoring and prevention.

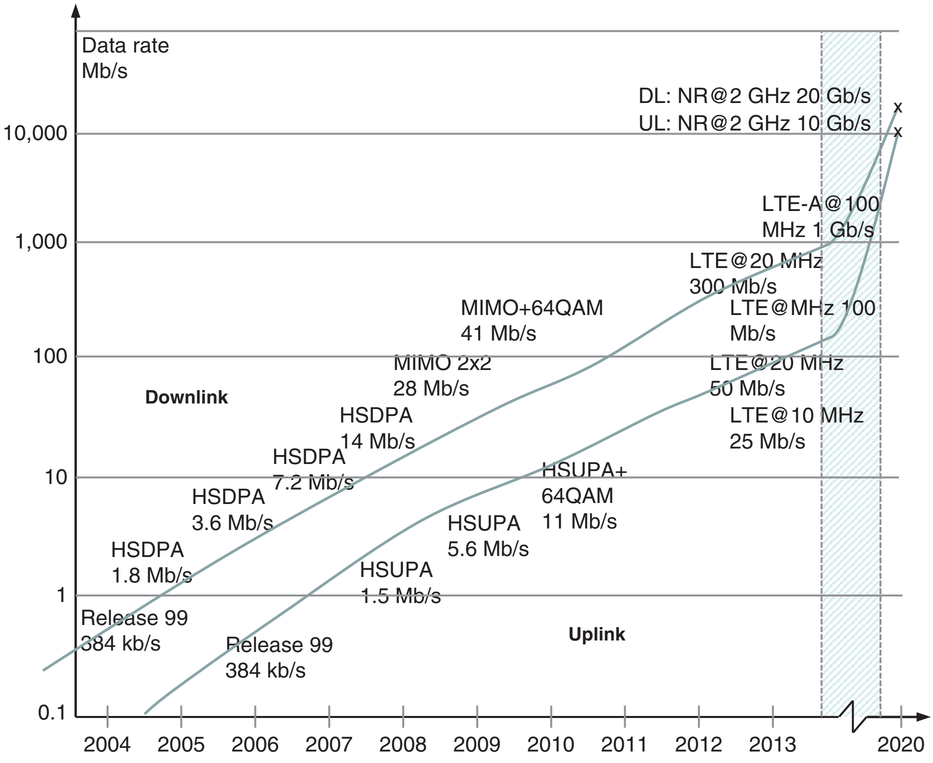

Figure 1.1 The development of mobile data rates.

Along with the new M2M and IoT applications and services, there will be role-changing technologies developed to support and complement the existing ones. The 5G is one of the most logical bases for managing this environment, together with the legacy systems in the markets.

Although the 5G is still in its infancy until the ITU officially dictates its requirements and selects the suitable technologies from the candidates, the 5G systems will be reality soon. During the deployment and operation of 5G networks, we can expect to see many novelty solutions such as highly integrated wearable devices, household appliances, industry solutions, robotics, self-driving cars, virtual reality, and other advanced, always-on technologies that benefit greatly from enabling 5G platforms.

In addition to the "traditional" type of IoT devices such as wearable devices with integrated mobile communications systems (smart watch), car communications systems and utility meters, there are also emerging technology areas such as self-driving cars that require high reliability as for the functionality as well as for the secure communications, which 5G can tackle.

As Next Generation Mobile Networks (NGMN) states in [8], the 5G will address the demands and business contexts as of 2020 by enabling a fully mobile and connected society. This facilitates the socioeconomic transformations contributing to productivity, sustainability, and overall well-being. This is achieved via a huge growth in connectivity and volume of data communications. This, in turn, is possible to provide via advanced, multilayer densification in the radio network planning and providing much faster data throughput, considerably lower latency, and higher reliability and density of simultaneously communicating devices.

In addition, to manage this new, highly complex environment, new means for managing and controlling the heterogeneous and highly energy-efficient environment is needed. One of the major needs is to ensure the proper security of the new 5G services and infrastructure, including protection of identity and privacy.

Another aspect in the advanced 5G system is the clearly better flexibility compared to any of the previous mobile communication generations. This refers to the optimal network resource utilization and providing new business models for variety of new stakeholders. This means that the 5G network functionality will be highly modular, which facilitates cost-efficient, on-demand scalability.

In practice, the above-mentioned goals are possible to achieve only via renewed radio interfaces, including totally new, higher frequencies and capacity enhancements for the accommodation of increasing the customer base in consumer markets as well as support for the expected huge amount of simultaneously communication IoT devices.

The 5G network infrastructure will be more heterogeneous than ever before, so there will be a variety of access technologies, end-user devices, and network types characterized by deeper multilayering. The challenge in this new environment is to provide to the end-users as seamless a user experience as possible.

To achieve the practical deployment schedule for the mature 5G initiating the commercial era by 2020, 3GPP as well as supporting entities such as NGMN are collaborating with the industry and relevant standardization organizations covering both "traditional" teams as well as new, open-source-based standardization bodies.

1.7 5G and Security

As for the security assurance of the new 5G era, there can be impacts expected in the “traditional” forms of SIM (Subscriber Identity Module), Universal Integrated Circuit Card (UICC), and subscription types, as the environment will be much more dynamic. The ongoing efforts in developing interoperable subscription management solutions that respond in near real time for changing devices and operators upon the need of the users are creating one of the building blocks for the always connected society. It is still to be seen what the consumer and M2M devices will look like physically in the 5G era, but we might see much more variety compared to any previous mobile network generations, including multiple wearable devices per user and highly advanced control and monitoring equipment.

Along with these completely new types of devices, the role of the removable subscription identity modules such as SIM/UICC can change; the much smaller personal devices require smaller form factors. At the same time, the techniques to tackle with the constantly changing subscriptions between devices need to be developed further, as do their security solutions. The cloud-based security such as tokenization and host card emulation (HCE), as well as the development of the device-based technologies like Trusted Execution Environment (TEE) may be in key positions in the 5G era, although the traditional SIM/UICC can still act as a base for the high security demands.

1.8 Motivations

One might wonder why yet another mobile communications generation is really needed. In fact, the fourth generation already provides quite impressive performance with low latency and high data rates.

The reasons are many-folded. Not only the increasing utilization of the mobile communications networks for ever-advancing applications including higher-definition video, virtual reality, and artificial intelligence require much more capacity even in remote areas, but – and one might argue if even primarily – the need is derived from the exponential increase of the IoT devices. The number of the intelligent sensors and other machines communicating with each other, service back-ends require support for much more simultaneously connected devices. The amount may be, as stated in one of the core requirements of the ITU, one million devices per km^2, which outnumbers clearly even the theoretically achievable capacity the advanced 4G can offer. The 5G would thus benefit especially massive IoT development, the increased data rates for consumers being another positive outcome of the new technology.

1.9 5G Standardization and Regulation

1.9.1 ITU

The ITU-R is the highest-level authority for defining the universal principles of 5G. The ITU is thus planning to produce a set of requirements for the official 5G-capable systems under the term IMT-2020. As the term indicates, the commercial systems are assumed to be ready for deployment as of 2020. This follows the logical path for ITU-defined 3G and 4G, as depicted in Figure 1.2.

The IMT-2020 is in practice a program to describe the 5G as a next-evolution step after the IMT-2000 and IMT-Advanced, and it also sets the stage for the international 5G research activities. The aim of the ITU-R is to finalize the vision of 5G mobile broadband society which, in turn, is an instrumental base for the ITU's frequency allocation discussions at the WRC events from which the WRC'15 was the most concrete session up today for discussing the 5G frequency strategies. The WRC decides the ways for reorganizing the frequency bands for the current and forthcoming networks, including the ones that will be assigned to the 5G.

Concretely, the Working Party 5D (WP5D) of ITU-R coordinates information sharing about the advances of 5G, including the vision and technical trends, requirements, RF sharing and compatibility, support for applications and deployments, and most importantly, the creation of the IMT-2020 requirement specifications.

ITU-R WP5D uses the same process for 5G as was applied to IMT-Advanced. Specifically for the 5G system evaluation process, the timeline of ITU is the following (Figure 1.3):

- *2016–2017*. Performance requirements, evaluation criteria, and assessment methodology of new radio;

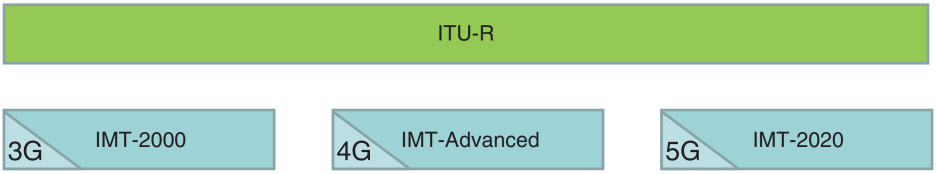

Figure 1.2 The 3G and 4G systems that comply with the ITU requirements for respective generations. The requirements for 5G are also produced by ITU. So far, 3GPP has made a concrete plan to submit the candidate proposal by 2019.

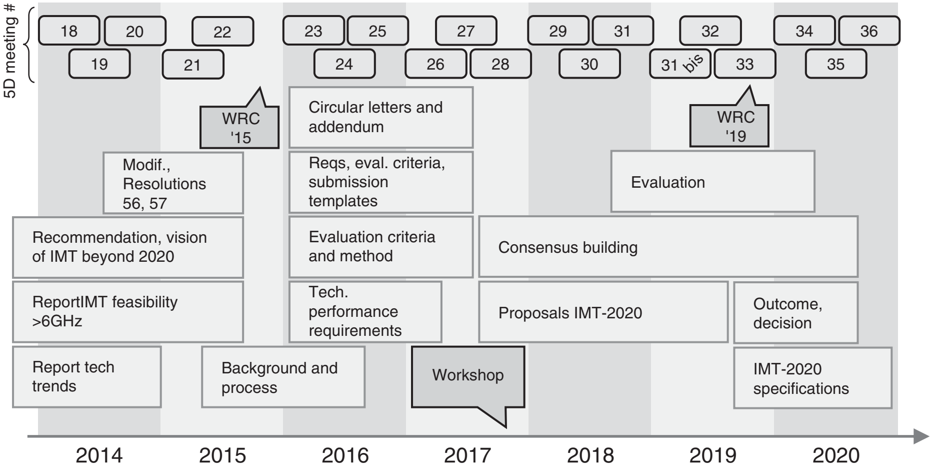

Figure 1.3 ITU time schedule for IMT-2020 as interpreted from [9].

- *2018*. Time frame for proposal;
- *2018–2020*. Definition of the new radio interfaces;
- *2020*. Process completed.

1.9.2 3GPP

While ITU-R is preparing for the evaluation of the 5G candidate technologies that would be compatible with the 5G framework as seen by ITU, one of the active standardization bodies driving the practical 5G solutions is the 3GPP, which is committed to submitting a candidate technology to the IMT-2020 process. The 3GPP is aiming to send the initial technical proposal to the ITU-R WP5D meeting #32 in June 2019 and plans to provide the detailed specification by meeting #36 in October 2020. To align the technical specification work accordingly, the 3GPP has decided to submit the final 5G candidate proposal based on the further evolved LTE-Advanced specifications, as will be their status by December 2019. In addition to the 3GPP, there may also be other candidate technologies seen, such as an enhanced variant of IEEE 802.11.

As for the 3GPP specifications, 5G will affect several technology areas of radio and core networks. The expected aim is to increase the theoretical 4G data rates perhaps 10–50 times higher whilst the response time of the data would be reduced drastically, close to zero. The 3GPP RAN TSG (Radio Access Network Technical Specification Group) is the responsible entity committed to identify more specifically these requirements, scope, and 3GPP requirements for the new radio interface. The RAN TSG works in parallel fashion for enhancing the ongoing LTE evolution that belongs to the LTE-Advanced phase of the 3GPP, aiming to comply with the future IMT-2020 requirements of the ITU. At the same time, the evolved core network technologies need to be revised by the system architecture teams so that they can support the increased data rates accordingly.

3GPP is committed to submitting a candidate technology to the IMT 2020 process based on the following time schedule, as described in the reference SP-150149 (5G timeline in 3GPP) (Figure 1.4):

- *June 2018*. Release 15, Stage 3 freeze;
- *June 2019*. Initial technology submission by ITU-R WP5D meeting #32;
- *October 2020*. Detailed specification submission by ITU-R WP5D meeting #36.

As for the development of the security aspects, 3GPP SA3 has produced the 5G security specification TS 33.501, V15.2.0. Some of the most important topics relevant to UICC follow:

- Tamper-resistant hardware is mandatory for key storage, key derivation, and running the authentication algorithm. Please note that it is not explicitly stated that this applies for both 3GPP and non-3GPP networks and for both primary and secondary authentication.
- Both Extensible Authentication Protocol (EAP) Authentication and Key Agreement (AKA’) and 5G AKA are mandatory to be supported for accessing 5G network using a primary authentication.
- 4G and 5G AKA are similar with enhancement on the Authentication Confirmation message.

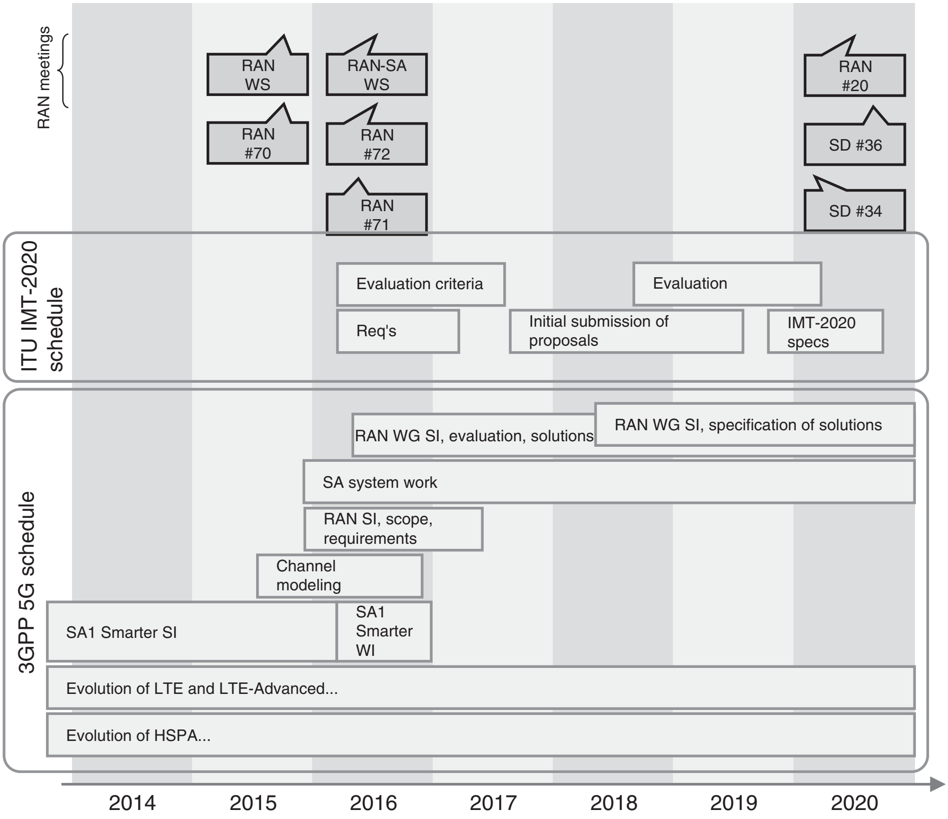

Figure 1.4 3GPP 5G time schedule for Release 15 is aligned with the ITU IMT-2020 progress [10].

- EAP AKA' will also be used to access non-3GPP networks.
- 256-bit algorithms are required in 5G.
- New 5G user identifiers are SUPI (Subscription Permanent Identifier), SUCI (Subscription Concealed Identifier) and 5G-GUTI (5G Globally Unique Temporary Identity).

As for the radio interface, the most remarkable news of 2017 was the decision to include the 3GPP's 5G Next Radio (NR) work item for the non-standalone mode, i.e. for the scenarios with 5G radio base station relying on 4G Evolved Packet Core (EPC). At the same time, there was agreement on:

- Stage 3 for non-standalone 5G-NR evolved Multimedia Broadband (eMBB) includes low-latency support.
- 4G LTE EPC network will be reused.
- The control plane on EPC-eNB-user equipment (UE) will be reused.
- An additional next-generation user plane is adapted on NR gNB–UE.

The 3GPP Release 15 was formally frozen on June 2018, meaning that no new work items were accepted into that release. Release 15 thus contains the first phase of 5G and provides the eMBB services for the early markets, either via non-standalone (NSA) or standalone (SA) modes.

The ASN.1 notation for the NSA was ready on March 2018, while the ASN.1 for the SA variant was ready September 2018. These notation documents are in practice the implementation guides for the equipment manufacturers, and based on these, the first standard-based lightweight 5G networks were deployed soon after.

The second phase of 5G as defined by 3GPP Release 16 with full functionality can be expected to be reality a few months after the freezing of the Release 16 ASN.1 notation set, meaning that the first IMT-2020-compatible 3GPP-based 5G networks will be deployed during 2020. These networks can support also the rest of the 5G pillars in addition to the eMBB, i.e. massive Internet of Things (mIoT) and critical communications referred to as ultrareliable low latency communications (URLLC).

1.10 Global Standardization in 5G Era

The following sections summarize some of the key standardization bodies and industry forums that influence 5G either directly or indirectly, as well as the ones dealing with IoT standardization paving the way for the IoT in the 5G era.

1.10.1 GlobalPlatform

GlobalPlatform is a standardization body with interest areas covering, e.g. UICC and embedded UICC (eUICC), Secure Element (SE), Secure Device, trusted service manager (TSM), certification authority (CA), and TEE. The key standards of the GlobalPlatform related to the IoT include the embedded UICC protection profile, and the body has established an IoT task force. The respective solutions are also valid in 5G, including all the form factors of UICCs (such as embedded and integrated) and their remote management. The organization is outlined in [11] and the respective task forces are listed in [12].

1.10.2 ITU

The International Telecommunications Union (ITU) is a standardization body with a variety of global telecommunications-related requirements and standards. ITU has a leading role in setting the expectations for the 5G era, and the IMT-2020 requirements are the reference for these performance expectations [9, 13, 14].

As for the development of IoT, the ITU has an IoT Global Standards Initiative (IoT-GSI) established in 2015, as well as a study group 20 on IoT, applications, smart cities, and communities. The aim of the ITU is to ensure a unified approach in ITU-T for development of standards enabling the IoT on a global scale. The key IoT-related standard is the Rec. ITU-T Y.2060 (06/2012). It can be expected that the massive IoT will be a major component of the 5G pillars, along with the eMBB and Critical Communications [15]. The ITU-T SG-20 deals with IoT and its applications, including smart cities and communities (SC&C). The resulting standard is designed for IoT and smart cities. There also is an international standard for the development of IoT including M2M communications and sensor networks [16].

The IoT-GSI concluded its activities in July 2015 following Telecommunication Standardization Advisory Group's (TSAG) decision to establish the new Study Group 20 on *IoT and its applications including smart cities and communities*. All activities ongoing in the IoT-GSI were transferred to the SG20. The IoT-GSI aimed to promote a unified approach in ITU-T for the development of technical standards enabling the IoT on a global scale. ITU-T recommendations developed under the IoT-GSI by the various ITU-T questions, in collaboration with other standards developing organizations (SDOs), will enable worldwide service providers to offer the wide range of services expected by this technology. The IoT-GSI also acts as an umbrella for IoT standards development worldwide [17].

1.10.3 IETF

The Internet Engineering Task Force (IETF) develops the Internet architecture. The IETF has dedicated IETF Security Area (https://tools.ietf.org/area/sec/trac/wiki). Some of the key standards include the Constrained Application Protocol (CoAP), and adaptation to the current communication security for use with CoAP. There also is the standard for IPv6 Low-power Wireless Personal Area Network (6LoWPAN) [18]. The IoT directory of IETF is found in [19].

1.10.4 3GPP/3GPP2

3GPP and its US counterparty 3GPP2 focus on cellular connectivity specifications that have been actively widened to cover also low-power wide area network (LPWAN) area. These include most concretely LTE-M and category 0 for low-bit rate M2M, and the further enhanced terminal categories that are optimized for IoT such as Cat-M1 and NB-IoT. The standardization body also develops security aspects, 2G/3G/4G/5G security principles and architectures, algorithms, lawful interception, key derivation, backhaul security, and SIM/UICC that can give added value for the cellular IoT compared to the competing proprietary variants [20].

1.10.5 ETSI

The European Telecommunications Standards Institute (ETSI) executes security standardization of, e.g. UICC and its evolution under the term SSP (smart secure platform). The latter is a continuum that opens room for new forms of UICCs such as embedded and integrated UICCs. The ETSI Technical Committee (TC) M2M is a relevant group for IoT development at ETSI. The organization's overall information can be found at Ref. [21] and IoT-related program in [22]. Furthermore, the ETSI portal of work documents for members is found at [23].

1.10.6 IEEE

The Institute of Electrical and Electronics Engineers (IEEE) 802 series includes aspects for IoT connectivity. There also exist many other related standards useful for IoT environment, like the IEEE Std 1363 series for public key cryptography. The IEEE 802.11 has many variants from which e.g. 802.11p is designed specifically for vehicle-to-vehicle

(V2V) communications. That can be considered as a competing technology for the 3GPP-based modes that will be optimized for vehicle communications, especially in the 5G era [24].

The IEEE Project P.2413 revises IEEE standards for better use within the IoT. The goal of the project is to build reference architecture covering the definition of basic architecture building blocks and integration into multitiered systems. The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals, including transportation and health care, as well as common architecture elements. It also provides means for data abstraction, protection, security, privacy, and safety. The reference architecture of the project covers the basic architectural building blocks and their ability to be integrated into multitiered systems [25].

1.10.7 SIMalliance

The task of SIMalliance is to simplify SE implementation, and it drives deployment and management of secure mobile services. It also promotes SE for secure mobile applications and services and promotes subscription management standardization, which is beneficial to provide a standardized means for the remote management of embedded universal integrated circuit card (eUICC) and integrated universal integrated circuit card (iUICC), which can be expected to be elemental components of 5G ecosystem [26].

1.10.8 Smart Card Alliance

Smart Card Alliance (SCA) has been a centralized industry interface for smart card technology, and it has followed the impact and value of smart cards in the United States and Latin America. As the 5G IoT can be based largely on the basic concept of the SIM card, and thus smart card technology, this task continues being relevant in the 5G era as well. From its inception as the SCA, its current form of Secure Technology Alliance (STA) facilitates the adoption of secure solutions in the United States. The Alliance's focus is set on securing a connected digital world by driving adoption of new secure solutions [27].

1.10.9 GSMA

The GSM Association (GSMA) represents interests of MNOs worldwide. It is involved in the Network 2020 paving the way for 5G. GSMA is involved in the standardization of subscription management and embedded Subscriber Identity Module (eSIM), and their development for M2M and consumer environment. It should be noted that the previous term of GSMA for indicating remote Subscriber Identity Module provisioning (RSP) is now generalized via the term eSIM, which has been approved by the GSMA as a global product label that can be used to indicate that a device is "RSP enabled" [28].

1.10.10 NIST

The US National Institute of Standards Technology (NIST) develops cybersecurity frameworks to address critical infrastructure including IoT/M2M space. The focus is on security and privacy for the evolution of IoT and M2M. It produces Federal

Information Processing Standards Publications (FIPS PUBS). FIPS are developed by the Computer Security Division within the NIST for protecting federal assets such as computer and telecom systems. FIPS 140 (1–3) contains security requirements. The topics on International Technical Working Group on IoT-Enabled Smart City Framework of NIST are found in [29] and FIPS PUBS are in [30].

1.10.11 NHTSA

The National Highway Transportation and Safety Administration (NHTSA) improves safety and mobility on US roadways. It also investigates connected vehicle technology and communications of safety and mobility information to one another. It has International Technical Working Group on IoT-Enabled Smart City Framework [31].

1.10.12 ISO/IEC

The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) is an elemental body for smart card technology standardization. ISO/IEC 7816 and 14400 are SIM/UICC standards for contact-oriented and contactless integrated circuit cards (ICCs). There are various solutions in the markets based on these standards, including transport cards, and IoT devices can be expected to be based largely on UICC. ISO/IEC 27000 is Information Security Management framework, which is valid also for IoT security.

Related to IoT security, the ISO/IEC Common Criteria (CC) is an international security evaluation framework that provides reliable IT product evaluation for the security capabilities based on an international standard (ISO/IEC 15408) for computer security certification, which refers to standards denoting EAL (evaluation assurance level) of 1–7. ISO/IEC 19794 produces biometrics standards [32].

1.10.13 ISO/IEC JTC1

Joint Technical Committee (JTC) 1 is the standards development environment to develop worldwide information and communication technology (ICT) standards for business and consumer applications. Additionally, JTC 1 provides the standards approval environment for integrating diverse and complex ICT technologies. ISO/IEC JTC 1/SC 27 deals with IT security techniques [33].

1.10.14 OMA

Open Mobile Alliance (OMA) has developed device management (DM). OMA LightweightM2M aims to optimize the secure communications between all, especially economic, devices. OMA DM is a subgroup under the OMA alliance. OMA DM is an initiative for automotive environment, and it includes over the air (OTA) updates for future investigations. The role of OMA is detailed in [34].

1.10.15 CEPT/ECC

Conférence Européenne des Postes et des Télécommunications (CEPT) and Electronic Communications Committee (ECC) are coordinated by European Communications Office (ECO). They produce requirements for approval for certification bodies and testing labs. They work in the ECC on smart grids, smart metering, and others under the ultra-high frequency (UHF) roadmap. Related to IoT environment, there is an ECC Report 153 on Numbering and Addressing in M2M Communications.

M2M can be used in several licensed and unlicensed frequency bands. The aim of ECC is to understand better the spectrum as well as numbering and addressing harmonization needs of existing and future M2M applications since related initiatives are present in various for a within the ECC, aligning with industry. The Working Group for Frequency Management (WGFM) of the ECC had prepared information to the ECC on the regulatory framework for M2M communications on the basis of frequency bands already available for various M2M usages; see ECC(15)039 Annex 13 [35].

1.10.16 NERC

Indirectly related to IoT, North American Electric Reliability Corporation (NERC) is committed to protecting the bulk power system against cybersecurity compromises that could lead to faulty operation or instability. CIP refers to Critical Infrastructure Protection cybersecurity standards, the CIP V5 Transition Program being the most recent one in the United States [36].

1.10.17 OWASP

Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. OWASP IoT Project provides information on IoT attack surface areas and IoT testing guides and maintains a top-10 IoT vulnerabilities list [37].

1.10.18 OneM2M

OneM2M's architecture and standards for M2M communications are designed to be applied in many different industries and take account of input and requirements from any sector. It works on eHealth and Telemedicine, Industrial, and Home Automation [38].

1.10.19 Global Standards Collaboration

Global Standards Collaboration (GSC) is an unincorporated voluntary organization dedicated to enhancing global cooperation and collaboration regarding communications standards and the related standards development environment. GSC is not a standards development organization and therefore will not develop standards. The members of GSC include ARIB (Association of Radio Industries and Businesses in Japan), ATIS (Alliance for Telecommunications Industry Solutions in the United States), CCSA (China Communications Standards Association), ETSI, IEC, IEEE-SA (IEEE

Standards Association), ISO, ITU, TIA (Telecommunications Industry Association in the United States), TSDSI (Telecommunications Standards Development Society in India), TTA (Telecommunications Technology Association in Korea), and TTC (Telecommunication Technology Committee in Japan) [39].

1.10.20 CSA

Cloud Security Alliance (CSA) is a nonprofit organization to promote the use of practices for providing security assurance within cloud computing and provide education on the uses of cloud computing to help secure all other forms of computing. CSA operates the cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self-assessment, third-party audit, and continuous monitoring [40]. Cloud computing and data centers form an integral part of the 5G infrastructure.

1.10.21 NGMN

Next Generation Mobile Networks (NGMN) is relevant for overall advanced network technologies as well as for the IoT [41]. As an example, NGMN has launched a projects "Spectrum and deployment efficiencies," "URLLC requirements for vertical industries," "RAN convergence," and "Extreme long-range communications for deep rural coverage." These activities are aimed to optimize and guide the telecoms industry toward the successful deployment of 5G beyond 2018.

1.10.22 Car-to-Car Communication Consortium

Car-to-Car Communication Consortium (C2C-CC) is industry forum for the V2V technology development. It is a nonprofit, industry driven organization initiated by European vehicle manufacturers and supported by equipment suppliers, research organizations, and other partners. The C2C-CC is dedicated to the objective of further increasing road traffic safety and efficiency by means of cooperative intelligent transport systems (C-ITS) with V2V communication supported by vehicle-to-infrastructure communication (V2I). It supports the creation of European standards for communicating vehicles spanning all brands. As a key contributor, the C2C-CC works in close cooperation with European and international standardization organizations [42].

1.10.23 5GAA

The mission of the 5G Automotive Association (5GAA) is to develop, test, and promote communications solutions, initiate their standardization, and accelerate their commercial availability and global market penetration to address society's connected mobility and road safety needs with applications such as autonomous driving, ubiquitous access to services, and integration into smart city and intelligent transportation. 5GAA offers several levels of membership for corporations, industry organizations, and academic institutions [43].

1.10.24 Trusted Computing Group

Through open standards and specifications, Trusted Computing Group (TCG) enables secure computing. Some benefits of TCG technologies include protection of business-critical data and systems, secure authentication and protection of user identities, and the establishment of machine identity and network integrity. The work groups are cloud; embedded systems; infrastructure; IoT; mobile; PC client; regional forums; server; software stack; storage; trusted network communications; trusted platform module (TPM); and virtualized platform [44].

1.10.25 InterDigital

InterDigital, Inc. designs and develops advanced technologies that enable and enhance mobile communications and capabilities for concept of the Living Network basing on intelligent networks, which self-optimize to deliver services tailored to the content, context and connectivity of the user, device, or need. Ecosystem partners providing devices, platforms, and data services, and affiliations include OneM2M, Industrial Internet Consortium, and Convida [45].

1.11 Introduction to the Book

This book is designed for the technical personnel of operators, equipment manufacturers, and telecom students. Previous knowledge about mobile communications would help in capturing the most detailed messages of the book, but the modular structure of the chapters – including the introductory part for the technology – is aimed to ensure that the book is useful also for the readers who are not yet familiar with the subject.

The readers in mobile equipment engineering, security, network planning, and optimization, as well as application development teams, benefit from the contents, as it details highly novelty aspects of the field, helping in updating the essential information in a compact way. The book is meant primarily for specialists of the field with a need to quickly capture the new key aspects of 5G, important differences compared to previous generations, and the possibilities and challenges in the 5G network deployment.

This contents thus demystifies the idea of fifth-generation mobile communications basing on the latest 5G standards and summarizes available information into a compact book form. The book focuses especially on the security aspects as well as on the network planning and deployment of the forthcoming 5G. It summarizes the 5G functionality with a special emphasis on the new security requirements. It discusses the security techniques and gives common-sense guidelines for planning, optimizing, and deploying the networks.

Chapters 1–3 of this book form the introductory module that will be useful for both technical and nontechnical readers with or without preliminary knowledge about existing mobile communications systems. Chapters 4–7 form the technical description and are directed to the advanced readers with some knowledge on mobile communications, while Chapters 8–10 represent the planning module and are meant for seasonal subject matter experts.

Figure 1.5 presents the main-level contents of this book to ease navigation between the modules. The modules and chapters are independent from each other, so they can be

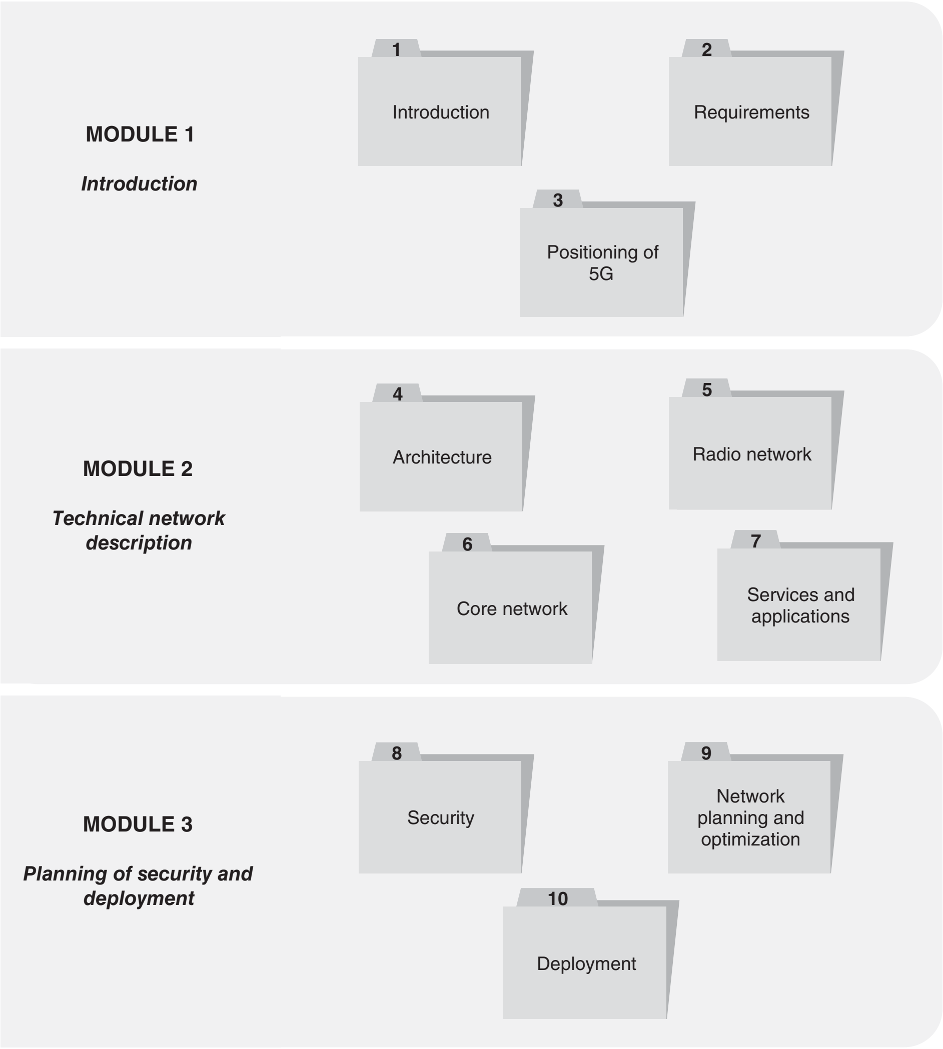

Figure 1.5 The contents of this LTE-A Deployment Handbook.

read through in any preferred order. Nevertheless, if you are starting from scratch (i.e. your knowledge of the subject area is less advanced), it is recommended that chapters be read in chronological order.

References

1 Penttinen, J. (2016). *The LTE-Advanced Deployment Handbook*. London: Wiley.
2 Penttinen, J. (2016). *The Wireless Communications Security*. London: Wiley.
3 Penttinen, J. (2015). *The Telecommunications Handbook*. London: Wiley.

4 Verizon, “Verizon 5G Technical Forum,” Verizon, http://5gtf.net. [Accessed 3 July 2018].

5 Qualcomm, “Making 5G NR mmWave a commercial reality,” Qualcomm, 2018.

6 European Commission, “Towards 5G,” 16 August 2017. http://ec.europa.eu/digital-agenda/en/towards-5g. [Accessed 26 September 2017].

7 European Union, “EU and Brazil to work together on 5G mobile technology,” 23 February 2016. http://europa.eu/rapid/press-release_IP-16-382_en.htm. [Accessed 26 September 2017].

8 NGMN, “NGMN 5G White Paper,” NGMN, 2015.

9 ITU, “ITU towards “IMT for 2020 and beyond”,” ITU, http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx. Accessed 3 July 2018.

10 3GPP, “Tentative 3GPP timeline for 5G,” 3GPP, 17 March 2015. http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g. [Accessed 3 July 2018].

11 GlobalPlatform, “GlobalPlatform,” GlobalPlatform, https://www.globalplatform.org. Accessed 3 July 2018.

12 GlobalPlatform, “GlobalPlatform,” GlobalPlatform, https://www.globalplatform.org/aboutustaskforcesIPconnect.asp. [Accessed 3 July 2018].

13 E. Mohyeldin, “Minimum Technical Performance Requirements for IMT-2020 radio interface(s),” ITU, 2016.

14 M. Carugi, “Key features and requirements of 5G/IMT-2020 networks,” ITU, Algeria, 2018.

15 ITU, “ITU,” ITU, www.itu.int. Accessed 3 July 2018.

16 ITU, “ITU IoT,” ITU, http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx. [Accessed 3 July 2018].

17 ITU, “Internet of Things Global Standards Initiative,” ITU, http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. [Accessed 4 July 2018].

18 IETF, “IETF,” IETF, https://www.ietf.org. [Accessed 4 July 2018].

19 IETF, “Internet-of-Things Directorate,” IETF, https://trac.ietf.org/trac/int/wiki/IOTDirWiki. Accessed 4 July 2018.

20 3GPP, “3GPP,” 3GPP, www.3gpp.org. Accessed 4 July 2018.

21 ETSI, “ETSI,” ETSI, www.etsi.org. Accessed 3 July 2018.

22 ETSI, “Connecting Things,” ETSI, http://www.etsi.org/technologies-clusters/clusters/connecting-things. [Accessed 3 July 2018].

23 ETSI, “ETSI work documents,” ETSI, https://portal.etsi.org/tb.aspx?tbid=726&SubTB=726. Accessed 3 July 2018.

24 IEEE, “Internet of Things,” IEEE, http://iot.ieee.org. Accessed 03 07 2018.

25 IEEE, “IEEE Project 2413 – Standard for an Architectural Framework for the Internet of Things (IoT),” IEEE, https://standards.ieee.org/develop/project/2413.html. [Accessed 03 07 2018].

26 SIMalliance, “Identity, security, mobility,” SIMalliance, http://simalliance.org. [Accessed 3 July 2018].

27 Secure Technology Alliance, “Digital security industry’s premier association,” Secure Technology Alliance, http://www.smartcardalliance.org. [Accessed 3 July 2018].

28 GSMA, “Representing the worldwide mobile communications industry,” GSMA, http://www.gsma.com. [Accessed 3 July 2018].

29 NIST, “International Technical Working Group on IoT-Enabled Smart City Framework,” NIST, https://pages.nist.gov/smartcitiesarchitecture. [Accessed 3 July 2018].

30 NIST, "Federal Information Processing Standards Publications (FIPS PUBS)," NIST, https://www.nist.gov/itl/popular-links/federal-information-processing-standards-fips. [Accessed 3 July 2018].

31 NHTSA, "Main page," NHTSA, http://www.nhtsa.gov. [Accessed 3 July 2018].

32 ISO, "International Organization for Standardization," ISO, www.iso.org. [Accessed 3 July 2018].

33 ISO, "ISO/IEC JTC 1 – Information Technology," ISO, http://www.iso.org/iso/jtc1_home.html. Accessed 3 July 2018.

34 OMA, "OMA SpecWorks," OMA, http://openmobilealliance.org. [Accessed 3 July 2018].

35 CEPT, "Electronic Communications Committee," CEPT, http://www.cept.org/ecc. [Accessed 3 July 2018].

36 NERC, "CIP V5 Transition Program," NERC, http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx. Accessed 3 July 2018.

37 OWASP, "The OWASP Foundation," OWASP, https://www.owasp.org/index.php/Main_Page. [Accessed 3 July 2018].

38 OneM2M, "Standards for M2M and the Internet of Things," OneM2M, http://www.onem2m.org. [Accessed 4 July 2018].

39 Global Standards Collaboration, "Global Standards Collaboration," ITU, 04 07 2018. [Online]. Available: http://www.itu.int/en/ITU-T/gsc/Pages/default.aspx. Accessed 4 July 2018.

40 Cloud Security Alliance, "Cloud Security Alliance," Cloud Security Alliance, https://cloudsecurityalliance.org. Accessed 4 July 2018.

41 NGMN, "NGMN," NGMN, www.ngmn.org. Accessed 4 July 2018.

42 CAR 2 CAR Communication Consortium, "CAR 2 CAR Communication Consortium," CAR 2 CAR Communication Consortium, https://www.car-2-car.org. Accessed 4 July 2018.

43 5GAA, "5GAA," 5GAA, http://5gaa.org. Accessed 4 July 2018.

44 Trusted Computing Group, "Trusted Computing Group," Trusted Computing Group, https://trustedcomputinggroup.org. Accessed 4 July 2018.

45 InterDigital, "Creating the living network," InterDigital, http://www.interdigital.com/page/about. Accessed 4 July 2018.

2

Requirements

2.1 Overview

This chapter summarizes the technical requirements for fifth-generation (5G) systems. It should be noted that this book assumes ITU (International Telecommunications Union) to be the highest authority dictating the minimum 5G requirements. This book thus walks the reader through the explanation of the latest ITU statements for their 5G candidate selection. Furthermore, this chapter summarizes the statements the other relevant standardization body has presented, the Third Generation Partnership Project (3GPP) being one of the most active stakeholders in the standardization of the 5G.

The time schedule for the key aspects of the 5G development and deployment, by the writing of this publication, includes the ITU-R's (the radio section of ITU) high-level requirements presented in the document [1], and its finalized version [2]. The concrete requirement set for the candidate evaluation have been presented by the end of 2017 as stated in [3].

The 3GPP, on the other hand, is one of the most relevant standardization bodies to present a candidate 5G technology for ITU's 5G selection process. The 3GPP has sent the first draft technical specifications as defined in the Release 15 for the preliminary ITU-R review, and the final submission will be based on the frozen technical standard set by Release 16.

Other candidate technologies might also be presented to the ITU evaluation, according to the ITU time schedule, although as an example, the Institute of Electrical and Electronics Engineers (IEEE) has not planned to send a complete 5G system proposal to the ITU evaluation; instead, there will be many IEEE sub-solutions that are relevant in building up 5G networks.

This chapter thus introduces new requirements for 5G as far they can be interpreted from various relevant sources. These key sources of information are presented as available now, and based on this information, the requirements are interpreted for the already known and foreseen statements, e.g. via ITU-R, 3GPP, and other entities involved with the standardization of 5G.

This chapter also presents the aspects of the interworking of 5G services with legacy systems, presenting general considerations of cooperative functioning of 5G and other relevant systems. Also, the performance aspects of the 5G in fixed and wireless environment are discussed, along with the possibilities and constraints, including the performance in practice now and via expected standardized features. Finally,

5G Explained: Security and Deployment of Advanced Mobile Communications, First Edition.
Jyrki T. J. Penttinen.

there is discussion on the impacts of requirements, including impact analysis for the technologies and businesses.

2.2 Background

With such a variety of 5G announcements for the trial phase as well as the expected 5G deployments, and each press release indicating only limited functionalities and early, preliminary (i.e. not yet International Mobile Telecommunications [IMT]-2020 – compliant) approaches, one might ask who will dictate how 5G should look? There is obviously great interest in the industry to maintain the competitive edge compared to other stakeholders whilst the global standardization and jointly approved and agreed principles of 5G are still under work.

As is customary, ITU has taken the role of defining the mobile communications generations. This was the situation for the third generation (3G) and fourth generation (4G), after the success of the first, analogue generation, and second, digital generations. ITU defines 3G as a set of radio access and core technologies forming systems capable of complying with the IMT-2000 (3G) and International Mobile Telecommunications Advanced (IMT-Advanced) (4G) requirements. Based on the number of end users, Universal Mobile Telecommunications System (UMTS) and its evolution up to advanced HSPA (high-speed packet access) is the most popular 3G system while Long-Term Evolution (LTE)-Advanced, as of 3GPP Release 10, is the most utilized 4G technology.

As for the industry, the Next Generation Mobile Network (NGMN) Alliance represents the interests of mobile operators, device vendors, manufacturers, and research institutes. The NGMN is an open forum for participants to facilitate the evaluation of candidate technologies suitable for the evolved versions of wireless networks. One of the main aims of the forum is to pave the way for the commercial launch of new mobile broadband networks. Some practical methods to do this are the production of commonly agreed technology roadmap as well as user trials [4].

So, ITU is still acting as a highest authority to define the global and interoperable 5G requirements for the mobile communications systems in such a way that the requirements are agreed by all the stakeholders. This is to avoid different interpretations by the industry when deploying and marketing the networks.

ITU setting the scenery, the practical standardization work results in the ITU-5G-compliant technical specifications created by mobile communications industry. One of the most active standardization bodies for the mobile communications technologies is 3GPP, which has created standards for Global System for Mobile communications (GSM), UMTS/HSPA, and LTE/LTE-Advanced. At present, 3GPP is actively creating advanced standards that are aimed to comply with ITU's 5G requirements.

In addition to the 3GPP, many other standardization bodies and industry forums contribute to the 5G technologies. Maybe not complete end-to-end 5G systems are under construction in such a large scale, as is done by 3GPP, but, e.g. many recommendations by IEEE are used as a base for 5G (as well as any other existing mobile communication technology). The new IEEE recommendations are formalizing the 5G, as one part of the complete picture.

2.3 5G Requirements Based on ITU

2.3.1 Process

The ITU Recommendation ITU-R M.2083 describes the IMT-2020 overall aspects. It will provide enhanced capabilities, which are much more advanced compared to the ones found in the ITU Recommendation ITU-R M.1645. The IMT-2020 has a variety of aspects from different points of view, which greatly extends the requirements compared to previous mobile communication generations.

The ecosystem and respective performance are related to users, manufacturers, application developers, network operators, as well as service and content providers. This means that there are many deployment scenarios supported by the IMT-2020 with a multitude of environments, service capabilities, and technological solutions [1].

The ITU represents the highest authority in the field of defining the mobile system generations.

The overall vision of 5G, according to the ITU, is presented in [5]. In short, the ITU foresees the 5G to function as an enabler for a seamlessly connected society in the 2020 time frame and beyond. The high-level idea of the 5G is to bring together people via a set of "things," data, applications, transport systems, and cities in a smart networked communications environment. The ITU and the respective, interested partners believe that the relationship between IMT and 5G are elements that make it possible to deploy the vision in practice by relying on mobile broadband communications.

The idea of 5G was presented as early as 2012 when ITU-R initiated a program to develop IMT for the year 2020 and beyond. As a result, there were research activities established in global environment.

The ITU Working Party 5D (WP5D) has been working on the ITU's expected time frame paving the way for the IMT-2020, including the investigation of the key elements of 5G in cooperation with the mobile broadband industry and other stakeholders interested in the 5G.

One of the elemental parts of this development has been the 5G vision of the ITU-R for the mobile broadband connected society, which was agreed in 2015. This vision is considered as instrumental and serves as a solid foundation for the World Radiocommunication Conference 2019. That will be a major event for the decisions of the 5G frequency bands, including the additional spectrum that will be required in different regions for the massively increasing mobile communications traffic.

ITU has played an essential role in the development of mobile radio interface standards. The previous requirements of the ITU ensuring the internationally recognized systems for 3G (IMT-2000) and 4G (IMT-Advanced) is now extending to cover 5G via the IMT-2020 requirements. Figure 2.1 depicts the time schedule of the ITU for the development of the 5G, and for paving the way for the very first deployments as of 2020.

From various teams considering 5G evolution, one of the most significant is the ITU-R WP5D. It has a role of investigating study areas and deliverables toward IMT for 2020 and beyond via multitude of activities, such as workshops and seminars for the information sharing within the industry and standardization entities. Some of the more specific work item categories include the following:

- *Vision and technology trends.* These aspects include also market, traffic, and spectrum requirements for the forthcoming 5G era.

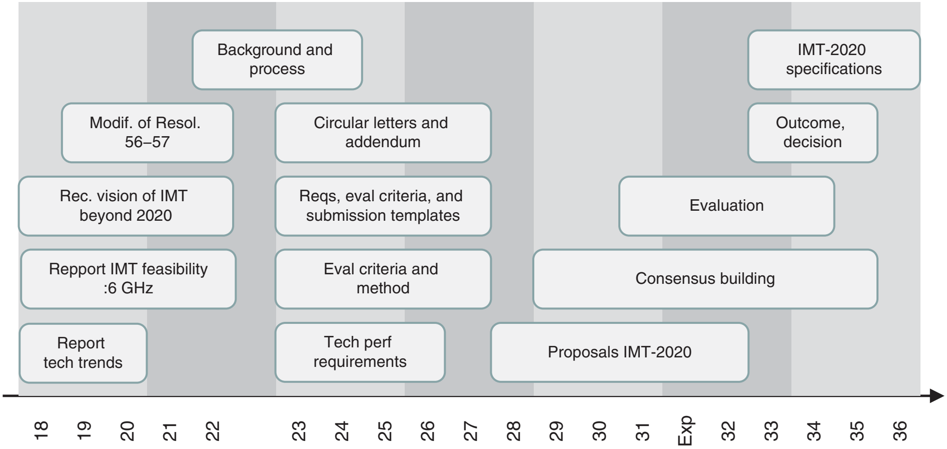

Figure 2.1 The main phases of the IMT-2020 development by the ITU. Within this process, World Radio Conferences 2015 and 2019 play an essential role for extending the 5G frequency band utilization.

- *Frequency band.* Investigations focus on frequency band channeling arrangements and spectrum sharing and compatibility.
- *IMT specifications.* This item also contains related technical works.
- *Support for IMT applications and deployments.* This item addresses the current and future use of International Mobile Telecommunications, such as the LTE to support broadband public protection and disaster relief (PPDR) communications.

The ITU IMT-2020 requirements form the foundation of the internationally recognized 5G systems. The respective ITU Radiocommunications Bureau Circular Letters work for announcing the invitation for standardization bodies to submit their formal 5G technical proposals for the ITU Working Party 5D evaluation of their compliance with the IMT-2020 requirements. This process follows the principles applied in the previous IMT-Advanced for selecting the 4G systems. Prior to the candidate evaluation, the WP5D finalized the performance requirements 2017 and formed the evaluation criteria and methodology for the assessment of the IMT-2020 radio interface.

After the candidate submission, the WP5D evaluates the proposals during the time of 2018–2020. The work is based on independent, external evaluation groups, and the process is estimated to be completed during 2020, along with draft ITU-R Recommendation that contains detailed specifications for the new radio (NR) interfaces.

2.3.2 Documents

The key sources of information for the ITU 5G development can be found in ITU-R M.2083 [6], which collects the documents for forming the 5G:

- *M.2083-0 (09/2015). IMT vision.* "Framework and overall objectives of the future development of IMT for 2020 and beyond." This document contains the recommendations for the future development of IMT for 2020 and beyond, and it defines the framework and overall objectives of the future development considering the roles that IMT could play to better serve the needs of the networked societies. It also includes a variety of detailed capabilities related to foreseen usage scenarios, as well as objectives of the future development of IMT-2020 and existing IMT-Advanced. It is based on Recommendation ITU-R M.1645.

- *Report ITU-R M.2320.* Future technology trends of terrestrial IMT systems addresses the terrestrial IMT technology aspects and enablers during 2015–2020. It also includes aspects of terrestrial IMT systems related to WRC-15 studies.
- *Report ITU-R M.2376.* Technical feasibility of IMT in bands above 6 GHz summarizes the information obtained from the investigations related to the technical feasibility of IMT in the bands above 6 GHz as described in ITU-R Rec. 23.76 [7].
- *Recommendation ITU-R M.1645.* Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000.
- *Recommendation ITU-R M.2012.* Detailed specifications of the terrestrial radio interfaces of IMT-Advanced.
- *Report ITU-R M.2370.* IMT Traffic estimates for the years 2020–2030.
- *Report ITU-R M.2134.* Requirements related to technical performance for IMT-Advanced radio interface(s).

As summarized in the press release [8], ITU agreed the first 5G requirement set on 23 February 2017. The ITU's IMT-2020 standardization process follows the schedule plan presented in Figure 2.2.

ITU has published the minimum 5G requirements in the document IMT-2020 Technical Performance Requirements, available at [1]. The most important minimum set of technical performance requirements defined by ITU provide means for consistent definition, specification and evaluation of the candidate IMT-2020 radio interface technologies (RITs), or a set of radio interface technologies (SRITs).

There is a parallel, ongoing development for the ITU-R recommendations and reports related to 5G, including the detailed specifications of IMT-2020. As a highest-level global authority of such requirements for a new mobile communications generation,

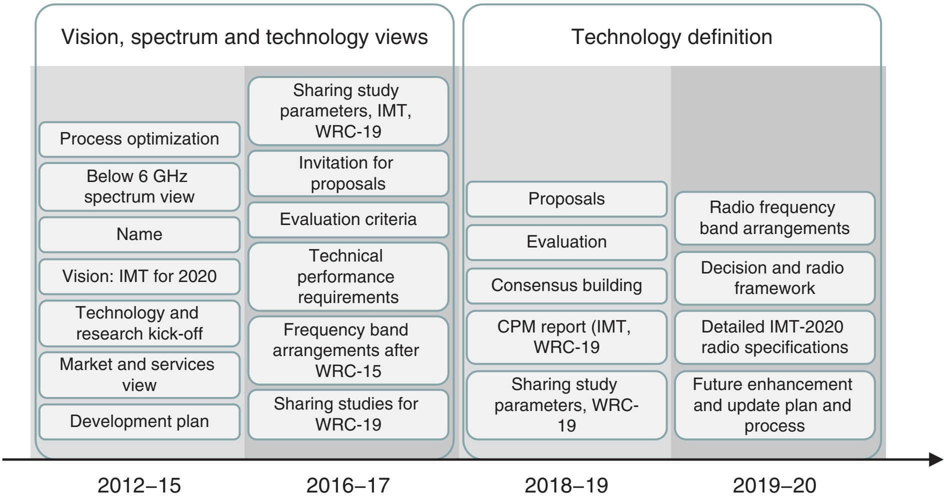
Vision, spectrum and technology views
Technology definition
Process optimization
Below 6 GHz spectrum view
Name
Vision: IMT for 2020
Technology and research kick-off
Market and services view
Development plan
Sharing study parameters, IMT, WRC-19
Invitation for proposals
Evaluation criteria
Technical performance requirements
Frequency band arrangements after WRC-15
Sharing studies for WRC-19
Proposals
Evaluation
Consensus building
CPM report (IMT, WRC-19
Sharing study parameters, WRC-19
Radio frequency band arrangements
Decision and radio framework
Detailed IMT-2020 radio specifications
Future enhancement and update plan and process
2012–15
2016–17
2018–19
2019–20

Figure 2.2 The high-level IMT-2020 process schedule as presented by ITU.

ITU aims, with the production of these requirements, to ensure that IMT-2020 technologies can comply with the objectives of the IMT-2020. Furthermore, the requirements set the goal for the technical performance that the proposed set of RITs must achieve for being called ITU-R's IMT-2020 compliant 5G technologies.

ITU will evaluate the IMT-2020-compliant 5G candidate technologies based on the following documents and for the development of IMT-2020:

- Report ITU-R IMT 2020 M-Recommendation for Evaluation
- Report ITU-R IMT-2020 M-Recommendation for Submission

The Recommendation ITU-R M.2083 contains eight *key capabilities* for IMT-2020, and functions as a basis for the technical performance requirements of 5G. It should be noted that the key capabilities have varying relevance and applicability as a function of different use cases within the IMT-2020.

In summary, the ITU's minimum radio interface requirements include the 5G performance requirements is presented in the next section. More specific test evaluation is described in the IMT-2020 Evaluation report of ITU-R [9].

2.3.3 Peak Data Rate

The peak data rate (b/s) refers to the maximum possible data rate assuming ideal, error-free radio conditions that are assigned to a single mobile station with all the available radio resources, excluding the resources for physical layer synchronization, reference signals, pilots, guard bands, and guard times. The term W representing bandwidth, E_{sp} referring to a peak spectral efficiency, the user's peak data rate $Rp = WE_{\mathrm{sp}}$. The total peak spectral efficiency is obtained by summing the value per each applicable component frequency bandwidth. This requirement is meant to evaluate the evolved Multimedia Broadband (eMBB) use case, for which the minimum downlink peak data rate is 20 Gb/s whereas the value for uplink is 10 Gb/s.

2.3.4 Peak Spectral Efficiency

The peak spectral efficiency (b/s/Hz) normalizes the peak data rate of a single mobile station under the same ideal conditions over the utilized channel bandwidth. The peak spectral efficiency for the downlink is set to 30 b/s/Hz, whereas the value for the uplink is 15 b/s/Hz.

2.3.5 User Experienced Data Rate

The user experienced (UX) data rate is obtained from the 5% point of the CDF (cumulative distribution function) of the overall user throughput, i.e. correctly received service data units (SDUs) of the whole data set in layer 3 during the active data transfer. If the data transfer takes place over multiple frequency bands, each component bandwidth is summed up over the relevant bands, and the UX data rate $\mathrm{R}_{\mathrm{user}} = WE_{\text{s-user}}$. This equation refers to the channel bandwidth multiplied by the fifth percentile user spectral efficiency. The ITU requirements for the UX data rate in downlink is 100 Mb/s, whereas it is 50 Mb/s for uplink.

2.3.6 Fifth Percentile User Spectral Efficiency

The fifth percentile user spectral efficiency refers to the 5% point of the CDF of the normalized user data throughput. The normalized user throughput (b/s/Hz) is the ratio of correctly received SDUs in layer 3 during selected time divided by the channel bandwidth. This requirement is applicable to eMBB use case, and the requirement values are, for downlink and uplink, respectively, the following:

- *Indoor hotspot*. 0.3 b/s/Hz (DL) and 0.21 b/s/Hz (UL).
- *Dense urban*. 0.225 b/s/Hz (DL) and 0.15 b/s/Hz (UL), applicable to the Macro TRxP (Transmission Reception Point) layer of Dense Urban eMBB test environment.
- *Rural*. 0.12 b/s/Hz (DL) and 0.045 b/s/Hz (UL), excluding the LMLC (low mobility large cell) scenario.

2.3.7 Average Spectral Efficiency

Average spectral efficiency can also be called spectrum efficiency, as has been stated in ITU Recommendation ITU-R M.2083. It refers to the aggregated throughput, taking into account the data streams of all the users. More specifically, the spectrum efficiency is calculated via the correctly received SDU bits on layer 3 during a measurement time window compared to the channel bandwidth of a specific frequency band divided further by the number of TRxPs, resulting in the value that is expressed in b/s/Hz/TRxP. The ITU requirement values are, for downlink and uplink for eMBB use case, respectively, the following:

- *Indoor hotspot*. 9 b/s/Hz/TRxP (DL) and 6.75 b/s/Hz/TRxP (UL).
- *Dense urban for macro TRxP layer*. 7.8 b/s/Hz/TRxP (DL) and 5.4 b/s/Hz/TRxP (UL).
- *Rural (including LMLC)*. 3.3 (DL) and 1.6 (UL).

2.3.8 Area Traffic Capacity

The area traffic capacity refers to the total traffic throughput within a certain geographic area, and is expressed in Mb/s/m^2. More specifically, the throughput refers to the correctly received bits in layer 3 SDUs during a selected time window. If the bandwidth is aggregated over more than one frequency band, the area traffic capacity is a sum of individual bands. The target value for the area traffic capacity is set to 10 Mb/s/m^2.

2.3.9 Latency

The user plane latency refers to the time it takes for the source sending a packet in radio protocol layer 2/3 to reach its destination on the respective layer. The latency is expressed in milliseconds. The requirement for the user plane latency is 4 ms for eMBB use case, whilst it is 1 ms for ultra-reliable low latency communications (URLLCs). The assumption here is an unloaded condition in both downlink and uplink without other users than the observed one whilst the packet size is small (zero payload and only internet protocol [IP] header).

The control plane latency, in turn, refers to the transition time it takes to change from the idle stage to the active stage in URLLC use case. The requirement for the control plane latency is maximum of 20 ms, and preferably 10 ms or less.

2.3.10 Connection Density

Connection density refers to the total number of 5G devices that can still comply with the target QoS (quality of service) level within a geographical area which is set to 1 km^2, with a limited frequency bandwidth and the number of the TRxPs, the variables being the message size, time and probability for successful reception of the messages. This requirement applies to the massive machine-type communications (mMTCs) use case, and the minimum requirement for the connection density is set to 1 000 000 devices per km^2.

2.3.11 Energy Efficiency

The high-level definition of the 5G energy efficiency indicates the capability of the radio interface technology (RIT) and set of RITs (SRIT) to minimize the radio access network (RAN) energy consumption for the provided area traffic capacity. Furthermore, the device energy efficiency is specifically the capability of the RIT and SRIT to optimize the consumed device modem power down to a minimum that still suffices for the adequate quality of the connection. For the energy efficiency of the network as well as the device, the support of efficient data transmission is needed for the loaded case, and the energy consumption should be the lowest possible for the cases when data transmission is not present. For the latter, the sleep ratio indicates the efficiency of the power consumption. Energy efficiency is relevant for the eMBB use case, and the RIT and SRIT must have the capability to support a high sleep ratio and long sleep duration.

2.3.12 Reliability

The reliability of 5G in general refers to the ability of the system to deliver the desired amount of packet data on layers 2 and 3 within expected time window with high success probability, which is dictated by a channel quality. This requirement is applicable to the URLLC use cases.

More specifically, the reliability requirement in 5G has been set to comply with the successful reception of a 32-bit packet data unit (PDU) on layer 2 within 1 ms period with a 1×10^{-5} success probability. This requirement is applicable to the edge of the cell in urban macro-URLLC, assuming 20 bytes of application data and relevant protocol overhead.

2.3.13 Mobility

The 5G mobility requirement refers to the maximum mobile station speed in such a way that the minimum QoS requirement is still fulfilled. There is a total of four mobility classes defined in 5G: (i) stationary with 0 km/h speed; (ii) pedestrian with 0–10 km/h; (iii) Vehicular with 10–120 km/h; (iv) high-speed vehicular with speeds of 120–500 km/h. The applicable test environments for the mobility requirement are indoor hotspot eMBB (stationary, pedestrian), dense urban eMBB (stationary, pedestrian, and vehicular 0–30 km/h), and rural eMBB (pedestrian, vehicular, high-speed vehicular).

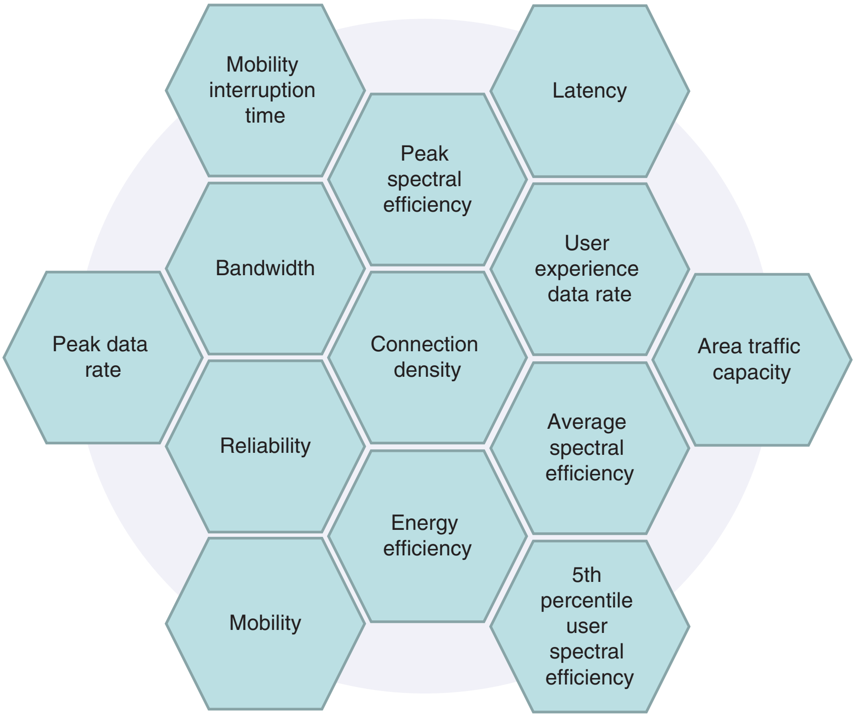

Figure 2.3 As summary of ITU's IMT-2020 requirement categories for 5G.

2.3.14 Mobility Interruption Time

The mobility interruption time refers to the duration of the interruption in the reception between the user equipment (UE) and base station, including RAN procedure execution, radio resource control (RRC) signaling or any other messaging. This requirement is valid for eMBB and URLLC use cases and is set to 0 ms.

2.3.15 Bandwidth

The bandwidth in 5G refers to the maximum aggregated system bandwidth and can consist of one or more radio frequency (RF) carriers. The minimum supported bandwidth requirement is set to 100 MHz, and the RIT/SRIT shall support bandwidths up to 1 GHz for high-frequency bands such as 6 GHz. Furthermore, the ray tracing (RT)/SRIT shall support scalable bandwidth (Figure 2.3).

2.4 The Technical Specifications of 3GPP

2.4.1 Releases

There are two paths within the Release 15 of the 3GPP, one defining the ITU-R – compliant 5G whilst the other route continues developing the LTE under further stage of the LTE-Advanced Pro. The overall 5G as defined via the Release 15 of the 3GPP is described in [10].

Remarkably, the development of the 5G radio interface divides NR into two phases. The first phase is an intermediate step relying on the 4G infrastructure, referred to as non-standalone scenario, while the final, native, and fully 5G-based core and radio system is referred to as standalone. The respective features can be found in 3GPP Release summary [11].

In the path toward 3GPP Release area 15, which is the first set of technical specifications defining 5G, the 3GPP has studied plenty of items to comply with the high-level 5G requirements of the ITU-R. The items are related to the enhancement of the LTE, as well as the completely new topics related to 5G. Some of these study items are as follows:

- *Uplink data compression* (*UDC*). This is a feature that would be implemented between evolved NodeB (eNB) and UE. The benefit of the UDC is the compression gain especially for web browsing and text uploading, and the benefits cover also the online video performance and instant messaging. The result is thus the capacity enhancement and better latency in the uplink direction especially in the challenging radio conditions [12].
- *Enhanced LTE bandwidth flexibility*. This item aims to further optimize the spectral efficiency within the bandwidths of 1.4–20 MHz.
- *Enhanced Voice over Long-Term Evolution (VoLTE) performance*. This item refers to the maintenance of the voice call quality sufficiently high to delay the Single Radio Voice Call Continuity (SRVCC), thus optimizing the signaling and network resource utilization.
- *Virtual reality*. This item refers to the innovation of potential use cases and their respective technical requirements on virtual reality.
- *NR-based access to unlicensed spectrum*. This item is related to the advanced phase of the Release 15 by investigating further the feasibility of license assisted access (LAA) both below and above 6 GHz frequency band, such as 5, 37, and 60 GHz.
- *NR support on nonterrestrial networks*. This item refers to the channel models and system parameters respective to the nonterrestrial networks, to support satellite systems as one part of the 5G ecosystem.
- *Enablers for network automation for 5G*. This item relates to the automatic slicing network analysis, based on network data analytics (NWDA).
- *System and functional aspects of energy efficiency in 5G networks*. This item refers to the overall topic of energy efficiency (EE). The subtopics include EE key performance indicators (KPIs) relevant to the 5G system, including the ones identified by European Telecommunications Standards Institute (ETSI) TC EE, ITU-T (Telecommunication Standardization Sector of ITU) SG5, and ETSI Network Functions Virtualization (NFV) ISG (Industry Specification Group), as well as the feasibility of the operation and maintenance to support the 5G EE and innovation in general for better optimizing the energy optimization.

2.4.2 Security Requirements for 5G

The 3GPP has defined a set of security requirements for 5G in technical specification TS 33.501. Figure 2.4 summarizes the key elements and functionalities, and the following sections detail the respective key requirements.

The respective security requirements are summarized in the following sections.

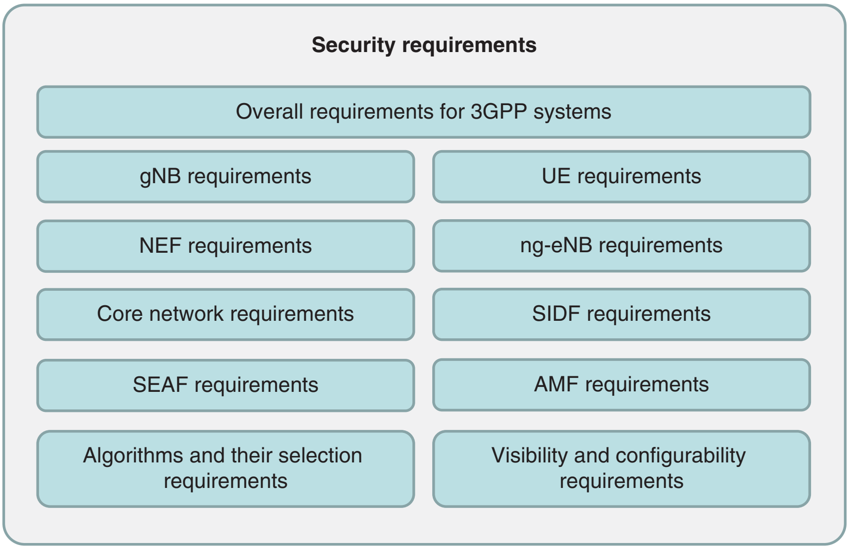
Security requirements
Overall requirements for 3GPP systems
gNB requirements
UE requirements
NEF requirements
ng-eNB requirements
Core network requirements
SIDF requirements
SEAF requirements
AMF requirements
Algorithms and their selection requirements
Visibility and configurability requirements

Figure 2.4 The 3GPP security requirement categories.

2.4.2.1 Overall Security Requirements

The generic security requirements of the 3GPP TS 33.501 cover the following cases:

- UE must include protection against bidding-down attack.
- Network must support the subscription authentication and key agreement (AKA).

The bidding-down attack refers to the intentions to modify the functionality of the UE and/or network to make it believe that the networks and/or UE would not support security features. This may lead to security breaches by forcing reduction of the security measures between the UE and network.

The subscription AKA is based on a 5G-specific identifier SUPI (Subscription Permanent Identifier). There is also a protected network identifier for the mutual authentication procedure so that the UE can reliably authenticate the network. The serving network authentication refers to the procedure where the UE authenticates the serving network identifier based on successful key use as a result of the AKA.

Furthermore, the requirement for the UE authorization refers to the procedure where the serving network authorizes the UE through authenticated SUPI and the subsequent subscription profile, which is provided by the home network.

The serving network authorization, on the other hand, refers to the procedure where the home network authorizes the serving network and the UE can rely on the authenticity of the connected serving network.

Lastly, the access network authorization refers to the procedure where UE can rely on all the access networks after they are authorized by the serving network.

Each mobile equipment (ME) must support unauthenticated emergency services, which refers to the possibility to make an emergency call even without the subscription credentials of the Universal Integrated Circuit Card (UICC). In other words, the ME must be able to execute emergency calls without the Universal Subscriber Identity Module (USIM). This requirement applies only to serving networks that are dictated by local regulation to support such service. Where regulation does not allow this service, the serving networks must not provide with the unauthenticated emergency services.

2.4.2.2 UE

As dictated by the 3GPP TS 33.501 [13], the 5G UE must comply with the requirements summarized in Table 2.1.

Table 2.1 The 5G UE requirements as interpreted from 3GPP TS 33.501.

Requirement	Description of the requirement
Ciphering and *integrity protection*	Must be equal for the ciphering and integrity protection between the UE and the ng-eNB, as well as between the UE and the eNB as dictated in 3GPP TS 33.401.
User data and signaling data *confidentiality*	UE must be able to activate used data ciphering as indicated by gNB. In addition, UE needs to support the following: 1. User data, and RRC and NAS signaling ciphering in UE–gNB. 2. NEA0, 128-NEA1, and 128-NEA2 ciphering algorithms, and optionally 128-NEA3. 3. Ciphering algorithms detailed in the 3GPP 33.401 if the UE can provide E-UTRA connectivity to 5GC. UE should use confidentiality protection when regulations so permit, although the confidentiality protection of user data between the UE and the gNB, and confidentiality protection of RRC-signaling and NAS-signaling, are left optional.
User data and signaling data *integrity*	The UE supports the following: 1. Integrity protection and replay protection of user data in UE–gNB. 2. Integrity protection and replay protection of RRC and NAS-signaling, and integrity protection of user data as dictated by the gNB. 3. NIA0, 128-NIA1, 128-NIA2 integrity protection algorithms. The UE may implement optionally also the 128-NIA3. 4. Integrity algorithms as detailed in 3GPP TS 33.401 if the UE supports E-UTRA connectivity to 5G core network. Nevertheless, the actual use of user data integrity protection in UE–gNB interface is left optional, as it adds overhead and processing load. 5. Integrity protection of the RRC and NAS signaling with some exceptions indicated in 3GPP TS 24.501 and TS 38.331.
Secure *storage* and *processing* of subscription credentials	For the storage and processing of the subscription credentials to access the 5G network, the following applies: 1. The subscription credentials are integrity-protected within the UE using a tamper-resistant secure hardware component. 2. The long-term K keys of the subscription credentials are confidentiality-protected within the UE using a tamper-resistant secure hardware component. 3. The long-term keys of the subscription credentials are never presented in the clear format outside of the tamper-resistant secure hardware component. 4. The authentication algorithms for the subscription credentials are executed within the tamper-resistant secure hardware component. 5. A security evaluation and assessment must be possible to assess the compliance of security requirements of the tamper-resistant secure hardware component.

Table 2.1 (Continued)

Requirement	Description of the requirement
Subscriber *privacy*	As for the subscriber privacy, the following applies: 1. The UE supports 5G-GUTI. 2. The SUPI is not transferred in clear text format via 5G RAN. The exception of this rule is the routing information (Mobile Country Code, MCC and Mobile Network Code, MNC), which can be exposed. Please note that SUPI privacy protection is not required for unauthenticated emergency call. 3. USIM houses the home network public key. 4. ME supports the null-scheme. This applies in the scenario when the home network has not provisioned the public key within USIM, and there is thus no SUPI protection in initial registration procedure, and the ME uses null-scheme. 5. Either USIM or ME can calculate the SUCI upon MNO rules, which USIM indicates. 6. Home network operator controls the provisioning and updating of the home network public key within the tamper-resistant hardware, as well as the subscriber privacy enablement. For the user and signaling data integrity, the following applies: 1. The UE supports integrity protection and replays protection of user data and RRC/NAS signaling in UE–gNB interface. 2. gNB indicates the use and UE activates accordingly integrity protection of user data. 3. Support of NIA0, 128-NIA1, and 128-NIA2 integrity protection algorithms, and optionally 128-NIA3. Nevertheless, the actual use of integrity protection of the user data in UE–gNB is optional. 4. The UE houses the integrity algorithms as defined in 3GPP TS 33.401, if the UE supports E-UTRA connectivity to 5GC. 5. Integrity protection of the RRC and NAS-signaling is mandatory to use, except in cases summarized in 3GPP TS 24.501 and TS 38.331.

2.4.2.3 gNB

As dictated by the 3GPP TS 33.501 [13], the 5G based station, i.e. fifth-generation NodeB (gNB), must comply with the requirements summarized in Table 2.2.

2.4.2.4 ng-eNB

For the detailed security requirements of ng-eNB, please refer to the security requirements as specified for gNB above and in the 3GPP TS 33.401.

2.4.2.5 AMF

The 3GPP TS 33.501 includes requirements for the AMF as for signaling data confidentiality and integrity, and subscriber privacy.

The AMF supports ciphering of non-access stratum (NAS)-signaling by applying one of the New Radio Encryption Algorithms (NEA) from the set of NEA0, 128-NEA1, and 128-NEA2. The AMF may also support the optional 128-NEA3. Also, the confidentiality protection of the NAS-signaling is optional to use, although it is encouraged to be applied when regulations so permit.

Table 2.2 Key requirements for gNB.

Requirement	Description of the requirement
User data and signaling data *confidentiality*	For the user data and signaling data confidentiality, the following applies: 1. The gNB supports ciphering of user data and RRC-signaling in UE–gNB. 2. Session management function (SMF) dictates the use, and the gNB activates ciphering of user data. 3. The gNB supports NEA0, 128-NEA1, and 128-NEA2 ciphering algorithms, and optionally, the 128-NEA3. 4. It is optional to support confidentiality protection of user data and RRC-signaling in UE–gNB. It should be noted that confidentiality protection is encouraged to be applied when regulations so permit.
User data and signaling data *integrity*	For the user and signaling data integrity, the following applies: 1. The gNB supports integrity protection and replays protection of user data and RRC signaling in UE–gNB. 2. SMF dictates and gNB activates integrity protection of user data. 3. The gNB supports NIA0, 128-NIA1, and 128-NIA2 integrity protection algorithms, and optionally 128-NIA3. Nevertheless, the actual use of integrity protection of the user data in UE–gNB is left as optional. 4. RRC signaling messages excluding the cases detailed in the 3GPP TS 38.331 are integrity-protected. The enablement of NIA0 in gNB depends on the regulatory requirements for the support of unauthenticated emergency session.
gNB setup and configuration	For the gNB setup and configuration, the following applies: 1. When O&M sets up and configures gNBs, if MNO so dictates, the gNB authenticates and authorizes the procedure according to the certification scenario detailed in 3GPP TS 33.310. This is to prevent external parties to modify gNB settings and configuration by using local or remote access. 2. The communication in O&M–gNB is confidentiality, integrity and replay protected. The security associations between O&M, gNB, and the 5G core network are detailed in the 3GPP TS 33.210 and TS 33.310. 3. The gNB can authorize the intentions for (authorized) software and data changes. 4. Secure environment is applied for execution of sensitive parts of the boot-up. 5. Confidentiality and integrity of software, which is transferred to gNB, needs to be ensured, and the software update of gNB must be verified upon installation as dictated in 3GPP TS 33.117.
gNB key management	For the key management in the gNB, the following applies: 1. The key protection is of utmost importance when 5G core network provides the keying material for the gNBs. 2. The parts of gNB deployment storing or processing keys in clear format must be protected from physical attacks, possibly applying secure physical environment. Keys in such secure environment must be stored only there, excluding cases allowed by 3GPP specifications.
Handling of user and control data for the gNB	For handling gNB user and control plane data, the following applies: 1. Parts of gNB storing or processing user or control plane data in clear format must be protected against physical attacks. Otherwise, the entity needs to be placed in a physically secure location for storing and processing the user and control plane data in clear format.

Table 2.2 (Continued)

Requirement	Description of the requirement
Secure environment of the gNB	The secure environment protects sensitive information and operations from unauthorized access or exposure. For the secure environment logically defined within gNB, the following applies: 1. It supports secure storage for sensitive data and execution of sensitive functions such as encryption and decryption of user data. 2. It also supports the execution of sensitive parts of the boot-process. 3. The integrity of the secure environment must be assured. 4. The access to the secure environment must be authorized.
gNB *F1* interfaces	The set of NBs with split DU-CU (distributed unit, centralized unit) implementations based on *F1* interface is defined in 3GPP TS 38.470. For the gNB *F1* interface, the following applies: 1. Signaling traffic F1-C as defined in 3GPP TS 38.470, F1-C signaling bearer as defined in TS 38.472, and user plane data can use *F1* interface in DU–CU. 2. gNB supports confidentiality, integrity, and replay protection for F1-C signaling bearer, and the management traffic on F1-C interface (as per 3GPP TS 38.470) must be integrity, confidentiality, and replay protected. 3. The gNB supports confidentiality, integrity, and replay protection on the gNB DU–CU F1-U interface for user plane.
gNB E1 interfaces	The 3GPP TR 38.806 describes the *E1* interface. For the gNB *E1* interface, the following applies: 1. The 3GPP TS 38.460 defines the principles for the gNBs with split DU–CU implementation, including open interface between CU–CP and CU–UP using the *E1* interface. 2. The E1 interface between CU–CP and CU–UP is confidentiality, integrity, and replay protected.

The AMF supports integrity protection and replay protection of NAS-signaling via one of the following New Radio Integrity protection Algorithms (NIA): NIA-0, 128-NIA1, and 128-NIA2, or via optional 128-NIA3. It should be noted that AMF must disable the NIA-0 in those deployments where support of unauthenticated emergency session is not a regulatory requirement. The NAS signaling messages must be integrity-protected with exceptions summarized in the 3GPP TS 24.501.

The AMF supports the triggering of the primary authentication based on the Subscriber Concealed Identifier (SUCI). The AMF also supports the procedures to assign and reallocate 5G-GUTI to the UE. The AMF can confirm SUPI derived from UE and home network and may only proceed with the service to the UE if the confirmation is successful.

2.4.2.6 SEAF

The key security requirement for the SEAF is to support primary authentication using SUCI.

2.4.2.7 NEF

The Network Exposure Function (NEF) provides external exposure of network function (NF) capabilities to the application function (AF). AFs thus interact with the selected

NFs via the NEF of the 5G network. To do so, the NEF must be able to determine if the AF is authorized to interact with the NFs. The communication in NEF–AF supports integrity protection, replay protection, and confidentiality protection. The interface also supports mutual authentication.

There are restrictions for the handled data. Thus, internal 5G core information, e.g. Data Network Name (DNN) and single network slice selection assistance information (S-NSSAI), must not be sent outside the 3GPP mobile network operator (MNO) network. Furthermore, NEF must not send SUPI outside of the 3GPP operator domain.

2.4.2.8 SIDF

The task of Subscription Identifier Deconcealing Function (SIDF) is to resolve the SUPI from the SUCI. This happens based on the protection scheme meant for generating the SUCI. The SIDF is in the home network, and in practice, unified data management (UDM) offers the SIDF services.

2.4.2.9 Core Network

The 3GPP TS 33.501 collects security requirements for the 5G core network. These include trust boundaries, service-based architecture, and end-to-end interconnectivity. The following summarizes the respective key statements.

Trust Zones The 5G systems provide the possibility for MNO to divide the network into trust boundaries, or zones. The default assumption is that two different MNOs are not sharing a single trust zone. The data transferred between the trust zones is handled by the principles of the service-based architecture of the 5G, although it also can be protected by applying end-to-end security based on Network Domain Security (NDS) and IP, as described in 3GPP TS 33.210.

Service-Based Architecture The 5G system allows the service-based architectural model, which is novel concept compared to the previous generations. The respective security requirements for service registration, discovery, and authorization include the following:

- NF service-based discovery and registration supports confidentiality, integrity, and replay protection, and there must be assurance that the NF discovery and registration requests are authorized.
- NF service-based discovery and registration can hide the topology of the NFs between trust domains, e.g. between home and visited networks.
- NF service request and response procedure supports mutual authentication between NFs.
- There must be a mutual authentication between Network Repository Function (NRF) and the set of NFs requesting service from it.

End-to-End Core Network Interconnection Security The end-to-end security solution supports application-layer mechanisms for addition, deletion, and modification of message elements handled by intermediate nodes, excluding special message elements such as those related to routing in Internet Protocol Packet eXchange (IPX) environment. These exceptions are detailed in 3GPP TS 33.501. By default, the solution provides end-to-end confidentiality, integrity, and authenticity between source and destination network by utilizing the Security Edge Protection Proxy (SEPP) concept. It is required that the solution would have only minimal impact on functionality, performance, interfaces, and equipment compared to 3GPP network elements, relying on standard security protocols.

The role of the SEPP is to function as a nontransparent proxy node. Its tasks include the protection of application layer control plane *N32* interface-based messages between two NFs of separate Public Land Mobile Networks (PLMNs), mutual authentication, and ciphering procedures with the counterparty SEPP, key management for securing messages on the *N32* interface between two SEPPs, and topology hiding. Furthermore, the SEPP functions as a reverse proxy providing a single point of access and control to internal NFs.

In the *N32* interface, the integrity protection applies to all of the transferred attributes. *N32* also applies confidentiality protection for the authentication vectors, cryptographic material, location data including Cell ID and SUPI.

2.4.2.10 5G Algorithms

The initial authentication procedure of the 5G is still based on the same AKA concept as in previous generation. Thus, the same respective algorithms, i.e. MILENAGE and TUAK, are still valid. Nevertheless, the rest of the security as for the key derivation is renewed in 5G. 5G brings thus along with new algorithms for the integrity, confidentiality, and ciphering.

Table 2.3 summarizes the 5G encryption (ciphering) algorithms and Table 2.4 summarizes the integrity protection algorithms [13].

The UE and serving network will negotiate the utilized algorithm based on the MNO policies and equipment security capabilities. This applies to the ciphering and integrity protection of RRC signaling and user plane for UE–gNB, and ciphering and integrity protection of RRC signaling and ciphering of user plane for UE–ng-NB. The algorithms also take place in NAS ciphering and NAS integrity protection for UE–AMF.

Table 2.3 5G ciphering algorithms.

Algorithm	Description
NEA0	Null ciphering algorithm
128-NEA1	128-bit SNOW 3G-based algorithm as referenced in 3GPP TS 35.215
128-NEA2	128-bit AES-based algorithm in CTR mode
128-NEA3	128-bit ZUC-based algorithm as referenced in 3GPP TS 35.221

Table 2.4 5G integrity protection algorithms.

Algorithm	Description
NIA0	Null integrity protection algorithm
128-NIA1	Null integrity protection algorithm-based on SNOW 3G (3GPP TS 35.215)
128-NIA2	128-bit AES-based algorithm in CMAC mode
128-NIA3	128-bit ZUC-based algorithm as referenced in 3GPP TS 35.221

The security capabilities of a multiple Radio Access Technology (RAT) UE-supporting Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and NR connected to the 5G core network include the LTE and NR algorithms. The UE security capabilities are protected against so-called bidding-down attacks referring to an attacker forcing the connectivity to be directed via older and less protected mobile generation networks.

2.5 NGMN

The NGMNs is an initiative that also contributes, among many other technology areas, to the 5G development.

The 5G vision of NGMN is as follows:

> 5G is an end-to-end ecosystem to enable a fully mobile and connected society. It empowers value creation toward customers and partners, through existing and emerging use cases, delivered with consistent experience, and enabled by sustainable business models.

To comply with these aspects, Ref. [14] lists the following items that the NGMN Alliance considers priorities:

- UX
- System performance
- Device
- Enhanced services
- New business models
- Network deployment, operation, and management

2.5.1 User Experience

UX refers to the end-UX while consuming a single or multiple simultaneous service. In the ever-increasing competitor environment, this is one of the key aspects that differentiates the stakeholders and can either fortify or break the customer relationship.

Especially for the 5G era, the enhanced networks need to deliver smooth and consistent UX independent of the time or location. The KPIs contributing to the UX include the minimum needed data rate and maximum allowed latency within the service area, among a set of various other parameters that are configurable, including their allowed ranges of variations, by each MNO. These service-dependent KPIs and their respective values are investigated by many stakeholders at present, including ITU-R, which has designed the minimum requirements for the 5G systems, so they may be called ITU-compliant 5G (IMT-2020) systems.

The UX data rate is dictated by the vision of providing broadband mobile access everywhere. In terms of use cases of NGMN, the practical requirement is to provide at least 50 Mb/s peak data rate for a single user over the whole service area of the 5G. The NGMN emphasizes that this value must be provided constantly over the planned area, including the cell edge regions.

The UX mobility requirements of the NGMN are use cases. They include the following:

- *High-speed train.* The train's velocity could be over 500 km/s. The 5G must support the data transmission during the train trips, including HD video streaming and video conferencing.
- *Remote computing.* This category includes both stationary (e.g. home office) and mobile environments (e.g. public transportation).
- *Moving hot spots.* This category refers to the extension of the static hot-spot concept to better tackle with the high mobility demands in 5G era. As dictated by the NGMN, 5G shall complement the stationary mode of planning of capacity by adding the nonstationary, dynamic and real-time provision of capacity.
- *3D connectivity.* This is important for, e.g. aircrafts, for providing advanced passenger services during the flight comparable with the UX on the ground.

Other important 5G requirements, per NGMN Alliance, that are related to the UX are the system performance in general, connection density, traffic density, spectrum efficiency, radio coverage area, resource and signaling efficiency, and system performance.

In addition to these requirements for the broadband access everywhere and high-user mobility, the NGMN has formed an extensive list of other cases and their requirements for 5G. These include the following aspects:

- *Massive Internet of Things* (*IoT*). The vision beyond 2020 includes remarkably the need to support of a considerably higher number of all types of devices compared to current markets, such as smart wearables and clothes equipped with multitude of sensors, sensor networks, and mobile video surveillance applications.
- *Extreme real-time communications.* These cases represent the environment for the most demanding real-time interactions, and for the full compliance may require more than one attributes amongst extremely high data throughput, high mobility, and critical reliability. A real-world example in this category includes the tactile Internet, which requires tactile controlling and audiovisual feedback. Robotic control falls into this category.
- *Lifeline communication, such as disaster relief and emergency prediction.* Along with the 5G, there will be increasing expectations to rely on the mobile communications in the role of a lifeline in all the situations and in wide areas. Remarkably, 5G would need to be optimized for robust communications in case of natural disasters such as earthquakes, tsunamis, floods, and hurricanes.
- *Ultrareliable communications.* This category includes critical cases such as automated traffic control and driving, i.e. self-driving vehicles, collaborative robots and their respective networking, life-critical health care, and people's emergency services such as remote surgery, 3D-connectivity for drones (large coverage for ensuring packet transport), and public safety (real-time video from emergency areas).
- *Broadcast-like services.* This category extends the traditional model of information broadcast such as TV networks by adding means for more advanced interaction.

2.5.2 Device Requirements

The role of the ever-evolving and increasingly complex devices is important in the 5G era. The HW, SW, and operating system (OS) continue to evolve, and the assurance of the correct and fluent functioning of those is of utmost importance. Not only do the devices such as isolated and individual elements need to perform correctly, but they

Table 2.5 NGMN Alliance's device requirements.

Requirement	Description
MNO controllability	Ability for NW or UE to choose desired profile depending on the QoS need, element capabilities and radio conditions; Ability for MNO to manage the HW and SW diagnostics, fixes, and updates; Ability to retrieve performance data from the UE as a basis for further optimization and customer care.
Multi-band and multi-mode	A sufficiently wide support of RF bands and modes (Time Division Duplex [TDD], Frequency Division Duplex [FDD], and mixed) is needed for efficient roaming scenarios. Ability to take advantage of simultaneous support of multiple bands optimizes the performance. Aggregation of data from different RATs and carriers is required.
Power efficiency	Whether the issue is support for a vast amount of IoT devices or devices that are in remote areas, enhanced battery efficiency is important. For the consumer devices (i.e. smart devices), the minimum battery life requirement is 3 days, while autonomously working IoT devices need to function up to 15 years.
Resource and signal efficiency	The 5G devices require optimized signaling as one of the ways to provide long battery life.

also are used increasingly as relay elements with the other 5G devices, especially in the IoT environment, as well as in various consumer use cases.

Table 2.5 summarizes the high-level device requirements as informed by NGMN Alliance.

2.5.3 Enhanced Services

There are various special requirements for enhanced functionality of 5G, related to connectivity, location, security, resilience, high availability, and reliability. The connectivity is related to the transparency, which is a key for delivering consistent experience in such a heterogeneous environment 5G will represent.

It is estimated that 5G combines both the native 5G networks as well as legacy Radio Access Technologies, especially as the 3GPP LTE system is evolving in a parallel fashion with the 5G system. Furthermore, 5G allows UE to connect simultaneously to more than one RAT at the time, including carrier aggregated connections. It should be noted that this type of connectivity may also involve other systems such as IEEE 802.11ax, which is state-of-the-art, high-efficiency Wi-Fi.

The 5G systems automatically optimize the respective combinations based on the most adequate achievable UX, which requires a fluent and seamless transition between the RATs. Detailing further, both the Inter-RAT and Intra-RAT mobility interruption time for all the RAT types and technologies need to be unnoticeable. Also, the inter-system authentication needs to be seamless, including the set of both internal 3GPP as well as non-3GPP RATs.

Another enhanced service requirement is the location, which is a key for contextual attributes. More concretely, the network-based positioning in 5G should be able to achieve accuracy of 1–10 m at least 80% of the occasions, and it should be better than 1 m indoors. Driven by high-speed devices, this accuracy must be provided in real time.

Furthermore, the network-based location of 5G should be able to cooperate with other location technologies. One example of such cooperation is the data delivery between partner sources so that the set of complete information enhances the final accuracy of the location. The NGMN also puts requirement on the cost of the 5G location-based solution, which should not exceed the currently available partner options based on, e.g. satellite systems or 4G solutions.

The NGMN also has requirements for the security of the 5G. It will support a variety of diverse applications and environments, including both human and machine-based communications. This means that there will be a greatly increased amount of sensitive data transferred over 5G networks, and it will need enhanced protection mechanisms beyond the traditional models of protecting the communications between nodes and end-to-end chain. This enhancement aims to better protect user data, to create new business models, and protect the users and systems against cybersecurity attacks.

5G will support a wide range of applications and environments, from human-based to machine-based communication, and it will deal with a huge amount of sensitive data that need to be protected against unauthorized access, use, disruption, modification, inspection, attack, etc. Since 5G offers services for critical sectors such as public safety and eHealth, the importance of providing a comprehensive set of features guaranteeing a high level of security is a core requirement for 5G systems.

2.5.4 The 5G Security

It can be generalized that the trust of the 5G system is a concept consisting of security, identity, and privacy:

- Specifically, for the security aspects, the NGMN states that the operator is the partner for state-of-the-art data security, running systems that are hardened according to recognized security practices, to provide security levels for all communication, connectivity, and cloud storage purposes.
- The identity refers to the operators' special role in the security, which is the trusted partner for master identity. The MNO provides secure, easy-to-use single sign-on and user profile management to fit all communication and interaction demand.
- The privacy refers to the operators' special role in partnering to safeguard sensitive data, while ensuring its transparency.

The traditional role of MNOs has been to provide subscriber authentication. As has been the case with the 4G stage, the 5G authentication is based on a robust platform that can be used as a base for MNOs to deploy single-sign-on services. A logical role for the 5G MNO is to act as an identity provider for the networks' own services as well as for external entities dealing with the MNOs' customers. MNO can thus provide transparent identification and seamless authentication to application services on behalf of the user.

What is then the role of the traditional subscriber identity module (SIM)/UICC that has been used for the subscriber identity vault since the very first commercial deployment of the 2G networks? There have been intensive discussions on the subject in standardization of the security of the mobile communications, including ETSI smart card platform (SCP). The consensus has been recently reached, and the outcome is that the secure element (SE) for storing the subscriber data does not need to rely any more on standalone SIM/UICC element. Instead, if the secure storing of this subscriber data combined with the secret data that allows the access to the mobile networks can be ensured in such a way that no external parties can intercept nor modify it, any secured physical entity is allowed for such storing.

The UICC is still valid for such storing, but equally, the storage can be, e.g. external nonvolatile memory of the mobile device while the handling of the cryptographic functions and execution of the plain data can happen, e.g. within a SoC (system on chip). There may be several technical terms for this concept, some being iUICC (Integrated Universal Integrated Circuit Card) and soft-SIM. In any case, the data used to access operator network remain solely owned by the operator running this network.

Interpreting further the security needs and requirements, the NGMN states that the system shall offer the capability to protect 5G customers from common security threats. These threats may include impersonation and traffic eavesdropping. This means that there is a need to increase the level of trust that is associated with the network subscribers' identity. In addition, the spirit of the 5G security requirements is that the planning of the security solutions for the operational phase of the networks, e.g. when the handover takes place between different RANs, must be better that in previous mobile communication generations, though in such a way that the efficiency to perform such protection mechanisms is higher.

Another trend is that 5G needs to enhance the current solutions for the privacy of the users as well as the equipment in the machine-type communications. In addition to the identity itself, the aspects requiring special attention include the information revealing the set of subscribed services, location and presence, mobility patterns, network usage behavior, and utilization of applications.

The adequate protection of the radio interface continues to be crucial, but also the higher-level protection needs to be reviewed in 5G. In fact, 5G is designed in a bearer-independent way in such a manner that the additional security and protection mechanisms may create additional value for advanced business, e.g. for extending the network protection into the Internet and end-to-end chain of the machine communications. This could better tackle the increasing threat of interoperator fraud and illegal use of international signaling networks. The 5G can handle this threat in 5G roaming, as the respective signaling protocols can enable the home network to verify that a user is attached to a serving network that claims it is. This aspect is thus the same as in domestic cases; one of the principals and priority tasks of the involved parties is to ensure that the one (consumer or machine) communication in the network is the one it/he/she claims to be.

The potential network vulnerabilities can be estimated to increase along with the huge increase of the number of the simultaneously communication parties in 5G, as the number of respective IP protocols for both control and user planes over such an overwhelming NFs increases. One of the very special new aspects is the introduction of extremely low-cost machines and open-OS smartphones, which by default open very easily the ports for mobile malware. These dangers can extend, not only between the devices and services, but also within the infrastructure of the 5G radio and core networks. As the NGMN states, there is thus an urgent need to fortify the following aspects of the networks to prepare MNOs to better tackle the new threats (intentional as well as accidental ones) by improving:

- Resilience against signaling-based threats, including direct attacks and overloading of the signaling channels;

- Security design for very low latency use cases for initial signaling and during the communications;
- Security requirements originated in the 4G technical specifications.

The NGMN mentions also the special needs for the public safety and mission-critical communications. The aim of the development is to reduce costs for these modes. As 5G supports the emergency communications in the same or better fashion as before, it also provides basic security functions in emergency situations, even if part of the network infrastructure and its security functions should be destroyed. Under these special conditions, 5G needs to continue providing protection against malicious attacks, including the ability to resist advanced radio jamming attacks over the 5G service area and attempts to compromise small-cell nodes distributed over wide geographical areas.

2.6 Mobile Network Operators

In a parallel fashion with the standardization work of 5G, several MNOs have been testing and developing concepts for 5G. These activities help in better understanding the performance of the NR and core network concepts and assist in the evaluation work of the standardization bodies.

As an example, the US-based MNO Verizon is active in evaluating the 5G concepts and has established a dedicated Verizon 5G Technology Forum, V5GTF, to study the item thoroughly [15]. The Forum is established in cooperation with Cisco, Ericsson, Intel, LG, Nokia, Qualcomm, and Samsung, with the focus on creating a common and extendable platform for Verizon's 28/39 GHz fixed wireless access trials and deployments.

As informed by the V5GTF, the participating partners have collaborated to create the 5G technical specifications for the 5G radio interface of OSI (Open Systems Interconnection model) layers 1, 2, and 3. The specifications also define the interfaces between the UE and the network for ensuring interoperability among network, UE, and chipset manufacturers.

The initial release, which has been ready since 2017, includes the V5G.200 series for the physical layer 1. The V5G.300 series describes layers 2 and 3 for Medium Access Control, Radio Link Control, Packet Data Convergence Protocol, and Radio Resource Control.

Many other MNOs are actively driving 5G development. Prior to the commercial Release-15-based deployments, some of the most active stakeholders were AT&T, Sprint, and DoCoMo.

2.7 Mobile Device Manufacturers

As an example, from the mobile network equipment manufacturing domain, Ericsson has identified the following aspects for the requirements [16]:

- *Massive system capacity*. The remarkable aspect in this category is that to support the augmented capacity, 5G networks must transfer data with lower cost per bit compared to today's networks. Also, a relevant aspect is the energy consumption, as increased

data consumption also increases the energy footprint of the networks; thus, 5G needs to optimize the energy better than is done today.
- *High data rates.* This aspect refers to considerably increasing sustainable, real-life data rates in much wider areas compared to previous generations, whereas the focus has traditionally been on the dimensioning of the networks based on the peak data rates. Concretely, 5G needs to support data rates of 10 Gb/s in limited environments such as indoors, whereas several hundreds of Mb/s must be offered in urban and suburban environments. Finally, the idea of 5G is to provide 10 Mb/s data rates almost everywhere.

As a comparison, Nokia, in alignment with merged Alcatel Lucent, summarizes expected 5G use cases and requirements in [17].

5G presents totally new solutions in many domains while it also is largely an evolution path from the previous mobile generations. One of the new aspects is related to IoT, including the M2M (machine-to-machine) communications. This results in a vast, new business, and new stakeholders produce products and services for IoT markets and relying increasingly on 5G infrastructure.

It is worth noting that 5G does not represent IoT as such, but it suits well the related communications, e.g. between machines. As in some examples, it will support a much higher number of simultaneously connected devices, which can be thousands under a single radio cell.

References

1 ITU, “Minimum requirements related to technical performance for IMT-2020 radio interface(s)”, ITU, 23 February 2017. https://www.itu.int/md/R15-SG05-C-0040/en. Accessed 1 March 2017.

2 ITU-R, “Rep. ITU-R M.2410-0, Minimum requirements related to technical performance for IMT-2020 radio interface(s)”, ITU, 2017 November.

3 ITU, “ITU agrees on key 5G performance requirements for IMT-2020,” 23 February 2017. http://www.itu.int/en/mediacentre/Pages/2017-PR04.aspx. Accessed 1 March 2017.

4 NGMN, “NGMN”, 04 July 2018 https://www.ngmn.org/home.html. Accessed 4 July 2018.

5 ITU, “ITU towards "IMT for 2020 and beyond,” 2016. http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx. Accessed 7 September 2016.

6 ITU-R, “ITU-R Recommendation M.2083”, ITU-R, 04 07 2018. http://www.itu.int/rec/R-REC-M.2083. Accessed 04 July 2018.

7 ITU-R, “Itu-R Recommendation M.2376, Technical feasibility of IMT in bands above 6 GHz”, ITU, July 2015. https://www.itu.int/pub/R-REP-M.2376. Accessed 4 July 2018.

8 ITU, “Press Release: ITU agrees on key 5G performance requirements for IMT-2020”, ITU, 27 February 2017. http://www.itu.int/en/mediacentre/Pages/2017-PR04.aspx. Accessed 4 July 2018.

9 ITU, “ITU-R M.[IMT-2020.EVAL]”, ITU, 2017.