TCCA
14 Blandford Square
Newcastle upon Tyne
NE1 4HZ UK
+44 191 231 4328
admin@tandcca.com

4G and 5G for Public Safety

Technology Options

Registered Office,
6, High Street,
Ely, Cambridgeshire, CB7 4JU, UK
Registration No.4155039 in UK
VAT Registration Number GB 755 4236 24
www.tandcca.com

Contents

1 Introduction 3
2 Evolution towards broadband 3
3 Technology selection 5
4 3GPP ecosystem 6
5 Public Safety standardisation 7
6 4G LTE 9
7 5G 10
8 Applying 4G LTE and looking forward to 5G for Public Safety 12
8.1 When is the correct time to start applying 3GPP technologies in Public Safety? 13
8.2 Is 4G LTE forming a good enough basis for Public Safety implementations? 13
8.3 Is it better to wait for 5G before starting Public Safety implementations? 13
8.4 Will 5G offering better service than 4G for Public Safety? 14
8.5 How can the 4G LTE defined Public Safety content also be included in 5G? 14
8.6 What is the linkage between 4G-5G evolution and spectrum for Public Safety? 14
8.7 What is the best way to connect 4G and future 5G solutions for Public Safety use? 14

1 Introduction

Public Safety users have traditionally operated with voice-based communication systems and narrowband data services. However it has become evident that these users also need high speed broadband data services and applications. With 4G LTE, this capability is starting to become a reality, and there are already some national procurement/implementation projects active in this area

This development of broadband is still quite new for the Public Safety community, including end-users, operators and governmental bodies, and there is still confusion and misunderstandings related to implementation of these broadband services. The purpose of this document is to clarify the basics of Public Safety 3GPP standardisation, the 3GPP ecosystem, 4G LTE applicability for Public Safety, and to look forward to the potential of 5G.

There is some confusion around the terms 4G and 5G. These are labels highlighting technology evolution and technology generations. It is easier to understand the technology evolution by putting the generation labels aside and regarding the evolution as a continuous stream of 3GPP defined releases.

This document has been prepared within the timeframe from November 2016 till March 2017, and the document content is based on information available during this time.

Intended readers of the document are Public Safety users and user organisations, operators of Public Safety networks, governmental bodies and the Public Safety industry in general – in short anyone who wants to get a basic understanding of applying 4G LTE technologies for Public Safety and to learn about the future potential of 5G.

2 Evolution towards broadband

Public Safety organisations have high-quality critical communication voice services in place as of today. These services are based on PMR standards which are specialised digital technologies, and dedicated network implementations. Business models have also been following a dedicated approach with many critical communications services provided by a specialised government controlled operator.

Public Safety operations are largely based on group voice and messaging communication, an efficient way to share information and manage field operations. Current critical communications voice and messaging services match well with the operational needs of public safety users - high availability, reliability, uncompromised security and special operational scenarios. Proper management of organisational structures, communication groups and user rights are also very important in Public Safety solutions.

All the above mentioned aspects have been carefully implemented in current critical communications solutions. This though is no longer enough and the current PMR standards are not able to evolve to offer the broadband services that users will need in future. The main drivers for this evolution are:

1. **Improved operational efficiency**: Public Safety operations and mission critical field services are expected to leapfrog to the next levels of efficiency by applying new applications utilising broadband data communications. There are two different efficiency improvement aspects: mobilising current office-bound applications and enabling completely new applications. Video transfer, remote database access, image transfer and mobile office are the most obvious examples of applications improving the efficiency of first responders.

2. **Demand for improved safety**: Terrorist attacks have placed security and safety questions high in governmental agendas. The question of safety is relevant, not only for citizens but also for first responders. Certain mission critical applications requiring broadband data connections, such as situational awareness applications, can significantly improve the safety of first responders and citizens.

3. **Reduction of costs**: Government budgets are under constant cost reduction pressure and critical communications services need to contribute to this cost control too. Cost related benefits are a combination of improved efficiency and productivity as well as new business models where, for instance, significant day-one CAPEX investments could be replaced by monthly OPEX fees.

The next question is about ways to implement Broadband services, and there are many options to consider.

Mission critical communication systems have traditionally been implemented with dedicated networks. Broadband solutions for Public Safety can also be implemented as dedicated systems, but in many countries this approach is limited by lack of dedicated spectrum and lack of government budgets. On the other hand, commercial mobile networks exist everywhere and those can be used also for Public Safety purposes. However, this approach is suffering from the fact that commercial networks are currently not able to deliver mission critical communication service; with lack of sufficient nationwide radio coverage and lack of standardised critical features being the most serious drawbacks. That being said, there are examples where commercial networks are used for some Public Safety services, but these are not mission critical.

Several models are possible for the implementation of broadband services for Public Safety. This enables each country to select a solution fitting their specific requirements and other local conditions. Some countries, such as South Korea, may select the dedicated approach and some countries, such as the United Kingdom, may select an approach based fully on commercial networks. Generally speaking, it looks like the vast majority of countries are inclined towards a hybrid network solution where both dedicated and commercial resources will be combined in order to construct a national broadband Public Safety solution. In addition to this, radio coverage can also be implemented in different ways: some countries will start from a traditional macro coverage solution, and others will start from local bubbles with transportable solutions and expand to macro coverage in the next step.

More information about Public Safety broadband implementation by combining both dedicated and commercial resources can be found from the TCCA document *Mobile Broadband for Critical*

Communications users - A review of options for delivering Mission Critical solutions, which is available in the Broadband zone of www.tandcca.com

In conclusion, there will not be a 'one size fits all' solution. And in order to see the full picture, it's important to understand that current PMR solutions will be still be required for the foreseeable future to deliver reliable mission critical voice and messaging services. The solution environment in the future will be more complex than the existing one of narrowband mission critical solutions.

3 Technology selection

When further discussing Public Safety broadband implementation, we hit the question of which technology will be used as the basis for Broadband implementations. Technology selection has been mainly driven by the Public Safety community, primarily FirstNet in the US and the UK's ESMCP project, and it has been mainly governed by the following key requirements related to solutions and technology.

1. Solutions need to be standards-based, and preferably one global standard enabling at least vendors interoperable terminal-infrastructure interface, avoiding market fragmentation across different technologies.
2. There needs to be a strong ecosystem in place, guaranteeing continuous development for the standard and related technology
3. There needs to be multi-vendor environment and competition, guaranteeing the lowering of equipment and device prices
4. There needs to be interoperability between equipment delivered by different vendors
5. The selected technology needs to have synergy with mainstream mobile network technologies
6. The selected standard/technology needs to provide governmental Public Safety procurement with flexibility i.e. it needs to be possible to implement the network procurement as a one single procurement entity, or to split it to different procurement lots.
7. It must be possible to apply existing smart phones and other smart devices also to Public Safety. Commercially available devices can be used by mission critical users with certified applications and security software. Some user groups will need specific devices with additional ruggedisation and hardening.

When looking at the above mentioned key requirements, it is clear that Public Safety Broadband solutions need to use the same technology as that used in the mainstream mobile network business. However, this is not straightforward from a solution implementation point of view, as Public Safety operational procedures trigger several requirements which are not provided in the current consumer-led standards, such as group communication and direct device-to-device communication. Additional standardisation work efforts to those used to fulfil the commercial needs are needed in order to match Public Safety requirements.

This technology selection has been articulated to explain why 4G LTE technology has been selected to be the basis for Public Safety implementations in the future. While 4G LTE is an existing technology, this is more about leveraging the dynamic 3GPP ecosystem.

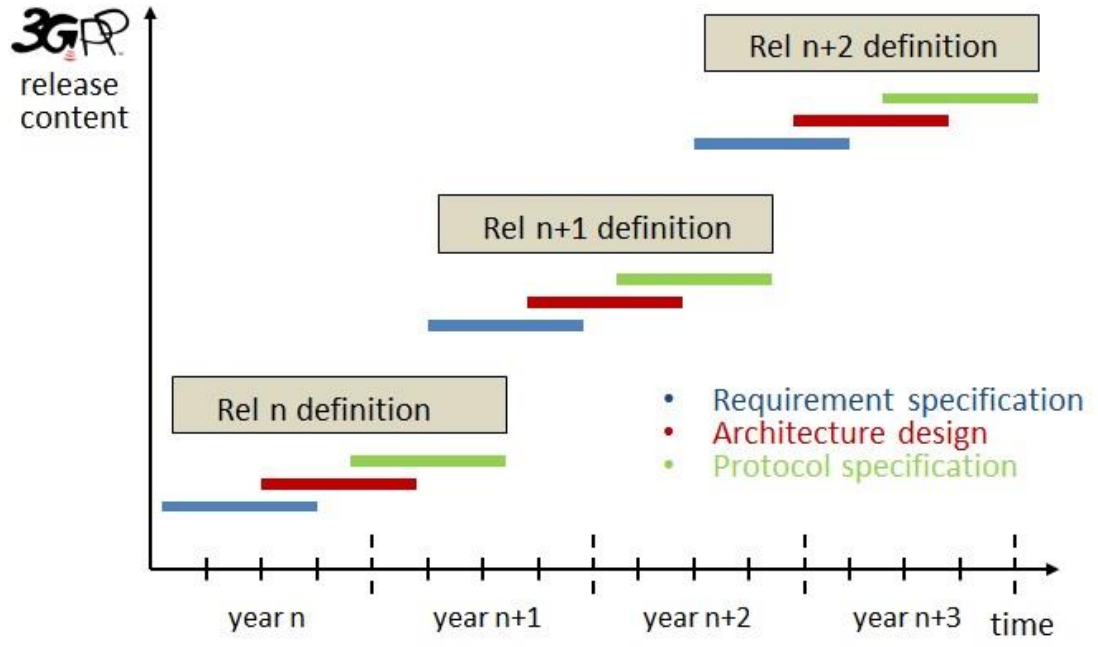
4 3GPP ecosystem

3GPP is the ecosystem which is driving the evolution of mobile networks globally. 3GPP is the glue which is uniting all different national/regional standard development organisations such as ETSI towards one global standard. Many different kinds of organisations are involved in the 3GPP ecosystem. Large mobile network operators and leading equipment providers are the most powerful due to scale, but Public Safety stakeholders are also included. Fierce competition between mobile network operators is actually the primary driver that keeps the 3GPP organisation running and ensures continuous evolution of standards and technology.

3GPP concentrates on defining and specifying new Releases; this work is carried out jointly by a large number of delegates from different involved parties. The practical work is organised into multiple different working groups which are each focusing on their own specific work areas. The SA6 working group is addressing the architecture for mission critical applications. Concrete deliverables are requirement specifications, architecture design documents and detailed protocol specifications – these deliverables are needed to define the content of new Releases at such level of detail that interoperable implementation is possible for equipment and device providers. However, as always with standards, equipment providers are not automatically implementing everything included in specifications – every provider will make these decisions separately on a business basis.

Obviously there is one significant challenge built in this machinery from a Public Safety point of view. Historically, 3GPP work has been based on a volume driven business logic and Public Safety business volume is very small compared to consumer business volume. This may lead to such prioritisation decisions where the definition of some Public Safety specific content could be delayed or even completely dropped if no market volume is seen. Therefore, it is important for successful standardisation of 3GPP Public Safety features that governments, regulators and industry engage fully with the 3GPP process and related areas.

Figure 1 : Principle of 3GPP Release definition cycle



The 3GPP Release cycle is that on average every 18 months there is a new 3GPP Release defined and published. The new Release always has more content than the previous one, but the new Release is also by default inheriting the content from the previous Release. Equipment providers implement new Releases in such a way that they are backwards compatible with previous Releases. Requirement for this backwards compatibility comes from the business of mobile network operators: upgrading the existing large nationwide network with millions of users with a new Release cannot trigger incompatibility at a technical or functional level – this would become too expensive either because of a too complicated network upgrade procedure or because of the disruption to customers and damage to the operator brand.

This ecosystem is now also defining future solutions for Public Safety (mission critical communications). Catalysed by the TCCA, this work has been ongoing since 2012. Leading 4G LTE network equipment providers including Ericsson, Huawei and Nokia are addressing Public Safety business, and are involved in the standardisation process.

5 Public Safety standardisation

There were a lot of discussions and differing opinions during 2013-2014 with regard to the best standardisation setup needed for future Public Safety systems. Finally, late in 2014 it was decided that the required standardisation work will be done within 3GPP in such a way that the required Public Safety functionalities will be incorporated in generic 3GPP Releases which are primarily targeted at the consumer business.

There have been two main waves of evolution after 3G. LTE was defined within 3GPP Releases 8 and 9, LTE-Advanced (4G) in Releases 10 and 11. This was a major piece of work, followed by a stable period without new major standardisation efforts. 3GPP Releases 12 and13 were the first to addressing Public Safety specific requirements, and this work is on-going with Release 14. Further functionalities and enhancements are planned for Release 15, and it is expected that new refinements and enhancements will be needed in future Releases.

The next programme of 3GPP standardisation effort focusing on 5G and the Internet of Things (IoT) has already started.Releases 15 and 16 will begin to define 5G and IoT. Part of Public Safety functionality initially included in Release 14 has been shifted to these later Releases. Public Safety lacks priority when compared to 5G, but providing there is continued support, the expectation is that 3GPP will be able to complete the required functionality for Public Safety solutions.

The reason for the Public Safety standardisation work is simple: Public Safety users have communications needs that are not addressed by standards defined for consumer use. Group calls and direct device-to-device communication are the main Public Safety functionalities that are not included in 3GPP Releases 10 & 11 (LTE), and this triggered the need for additional standardisation on top of those Releases.

This is not just adding some new features in 3GPP Releases, but also creating some basic mechanisms which are needed to support Public Safety functionalities, like creating agile multicast and broadcast

mechanisms needed for group calls or multimedia sessions. Fortunately, these mechanisms, called eMBMS, are already addressed by major LTE network equipment providers.

Listed here one-by-one are the Public Safety related standardisation items:

GCSE - Group Call System Enablers (Rel12): This standardisation item is a collection of different mechanisms to provide both unicast transmissions and multicast transmissions for group communication, including mechanisms for floor control and pre-emption. These mechanisms are enablers which are needed by Public Safety functionalities to be standardised with later 3GPP Releases.

ProSe - Proximity Services (Rel12-Rel14,…): This standardisation item defines the architecture and radio interface for direct device-to-device communication. Equivalent functionality within narrowband PMR systems has been called Direct Mode communication. Some basic mechanisms like good in-building penetration are still being explored.

IOPS - Isolated E-UTRAN Operations for Public Safety (Rel13-Rel14): The high service availability requirements of Public Safety need base stations to deliver service autonomously during a break in connection between the base station and the core network. This functionality has been called Base Station Fallback in narrowband PMR systems. IOPS is targeting to define equivalent functionality for LTE based networks. IOPS is currently an architecture recommendation while no stage 3 (interfaces and protocols) work has been identified.

MCS – Mission Critical Services (Rel13-Rel14,…): Mission-critical applications required to deliver mission critical services for Public Safety users (MCPTT, MCData, MCVideo) need a generic common set of system capabilities in order to deliver the service to end users. This standardisation item is a collection of those generic system capabilities.

MCPTT – Mission Critical Push To Talk (Rel13-Rel14,…): This standardisation item defines the application needed for delivering voice services for Public Safety users.

MCData – Mission Critical Data (Rel14-Rel15): This standardisation item defines the application that delivers non real time data services for Public Safety users. This includes also text and multimedia messaging.

MCVideo – Mission Critical Video (Rel14-Rel15): This standardisation item defines the application that delivers real time video service for Public Safety users.

Interconnection of MC systems (Rel15,…): This facility will allow different MC systems to be connected together to assist communication for mutual aid situations.

Interworking with Legacy PMR Systems (Rel15,…): Existing narrowband Public Safety implementations will be used for the foreseeable future in parallel with new broadband based implementations, so Public Safety users require interworking between narrowband and broadband systems. This standardisation item defines the required interworking functionality.

Standardisation of Public Safety functionalities will constantly evolve in order to enhance the service and include new mechanisms that will be beneficial to Public Safety operations - it is expected that a

number of additional Public Safety standardisation requirements will be identified in the future, and these need to be placed within forthcoming 3GPP Releases.

6 4G LTE

4G (LTE-Advanced, or shorter LTE-A) is a mobile network technology standardised by 3GPP Releases 10 and 11 and meeting the 4G requirements defined by ITU. This technology includes a large number of improvements and new content when compared to 3G and early LTE, some essential ones being

- significantly improved bandwidth, with data transfer bit rates up to 1 Gb/s
- shorter round trip delays (RTT) giving more responsive systems
- carrier aggregation enabling frequency band combining to make more bandwidth available for users
- improved quality of service (QoS) control mechanisms
- simplified network architecture, leading to lower implementation costs for mobile network operators

In order to give the full picture, it is worth of mentioning that 4G(LTE-A) also includes features addressing security, availability and prioritisation – these features are naturally important for Public Safety. However, these are not explored within this document.

4G (LTE-A) is the baseline technology level for Public Safety. However, 'LTE' may mean two different things when discussed in relation to Public Safety:

- commercial LTE-A (Release 10-11) without any Public Safety specific standardisation items
- LTE-A that includes currently identified Public Safety specific standardisation items of Releases 12/13/14/15

Commercial LTE-A (Release 10-11) is applicable also to Public Safety. However, this offers only consumer-level service without specific Public Safety features. The service level of this solution could be improved by having a Public Safety-specific MVNO (Mobile Virtual Network Operator) on top of the basic LTE solution operated by a commercial mobile network operator. This kind of solution can be a first reasonable step to provide Public Safety users with broadband data service. Public Safety users can also have a dedicated LTE-A network depending on spectrum availability.

LTE-A up to Release 14 offers all the same things as commercial LTE-A, and on top of those it also supports several functionalities needed for Public Safety, most important one being the Mission Critical Push-to-Talk (MCPTT) voice service. Mature specifications for MCData and MCVideo are expected to be included in Release 15. So, the Release 14 based solution offers both broadband data and voice services to Public Safety users, as well as basic functionality for mission critical data and video services. Release 14 is the first 3GPP Release which may be used as a platform to start the operational use for mission critical users. This is of course finally depends on user requirements, and the Public Safety community within each country needs to consider whether Release 14 is good enough, or whether they need to wait for Release 15.

3GPP Releases up to Release 13 are defined and published. Release 14 specifications are expected to be frozen mid-2017.

As already discussed, commercial networks are already used widely to provide Public Safety users with non-critical broadband data services. Public Safety specific functionalities of Releases 13/14/15 will widen and improve services which can be offered for Public Safety users. However, it is important to understand that new functionalities will not by themselves change the overall status of offered services. LTE networks will need to meet the stringent requirements of mission critical communication for coverage, availability and security in order to be applied for operational use in Public Safety organisations.

7 5G

The next technology level after 4G is named, not so surprisingly, as 5G, and this technology will be standardised by 3GPP Releases 15-16.

One of the key requirements of 5G is to address vertical and professional markets. Examples of market verticals are the automobile industry, IoT, industrial solutions and mission critical communications. Practical implementations are either MNO network based or private systems. The standardisation process for 5G is currently in the early stages and confirmed detailed plans do not yet exist – the content of and timing for the forthcoming 3GPP Releases evolve during the standardisation process. Releases 15 and 16 are expected to be finalised across 2018 and 2019, and trials as well as deployments are expected to start 2019-2020. However, key content for 5G is already outlined, and at least the following things are relevant for Public Safety:

Reliability and security

High availability and reliability are key requirements of public safety. When a police officer is in a dangerous situation, he/she must be able to rely on the radio device. Radio coverage needs to be widespread and communication immediately activated when the officer pushes the button on the device. Uncompromised security is also a must for Public Safety users.

5G will provide several new technologies which improve the reliability, availability and security of communications. These include Device-to-Device (D2D) communication, user- and control plane separation by using Software Defined Networking (SDN) and Mobile-Edge Computing (MEC). Flexible use of radio resources with the Multi-Connectivity technology also contributes to improved reliability.

Connected and automated cars are one of the major use cases for 5G. This use case sets demanding real time requirements related to ultra-high reliability, security and very low latencies, and these same aspects of 5G performance will also serve Public Safety users.

Traffic prioritisation

Critical communications networks need to be designed for the very worst cases. The dimensioning of the network capacity should be based on situations where large numbers of people are in a small area and the network load is peaking simultaneously. Typically, when first responders need to have the most capacity, for example at big events or major accidents, people around them also want to communicate. If using the same network, priorities must allow the necessary capacity and performance for first responders. This includes the ability to ruthlessly pre-empt some users' services in order to provide immediate services for first responders in emergency or perilous situations.

5G will add new technologies to the existing ones, which enable different use cases with different requirements in one physical network. With Network Slicing technology, a single network can be divided into several virtual networks with different use cases and priorities. This opens new business opportunities for infrastructure sharing for different niche operators, including Public Safety. Separating user- and control plane traffic with SDN and NFV (Network Function Virtualisation) technologies are key for managing dynamically changing capacity needs in the network. These technologies offer new capabilities to manage a portfolio of different use cases with different priority requirements by using a single physical network. This will add more possibilities to the already available 4G solutions.

Sensors and Internet of Things

The IoT is one of the key drivers of 5G. The target is to support very large number of machines that can communicate with each other, exchange data and automate processes. New requirements include ultra-low cost devices, a long battery life and properly managed network capacity, even with a very large number of devices. Sensors and machines can also be very critical, for example industrial solutions or autonomous cars. This calls for very low latency and highly reliable communication.

In the future, sensors, cameras and other automated devices will be a significant source of information for the Public Safety community, complementing conventional sources such as police officers in the field. Information from citizens about incidents will also become increasingly important for building a full picture.

By integrating all this information into Public Safety operations, first responders can be less reactive and more proactive – for example moving from the investigation of crimes towards the prevention of crimes.

Radio performance

Air interface performance is always high on the 3GPP agenda, and new Releases are constantly defining improvement for this critical aspect. And so it is also with 5G (Releases 15-16), which will significantly improve air interface data transfer speed and capacity with so called enhanced Mobile Broadband (eMBB) functionality.

In 4G the old concept that more power is needed for more users is complemented with the possibility to add more cells that cooperate in the same spectrum to make coverage better, e.g. large and small cells together. 5G expands on the existing 4G radio interface, but in addition to that there will be also a new radio interface designed to be used with extremely high millimetre wave frequencies (20 .. 60

GHz). Cell size remains moderate with these frequencies, and these cells are more Wi-Fi like small spots than wide area mobile network cells. Using other frequency bands will add more options when planning a Public Safety network. Regarding the new radio interface, as with similar 3GPP features, it is expected to inherit all Public Safety specific functionality defined for 4G.

It is expected that Public Safety community will find practical use cases also for new ultra-high frequency cells.

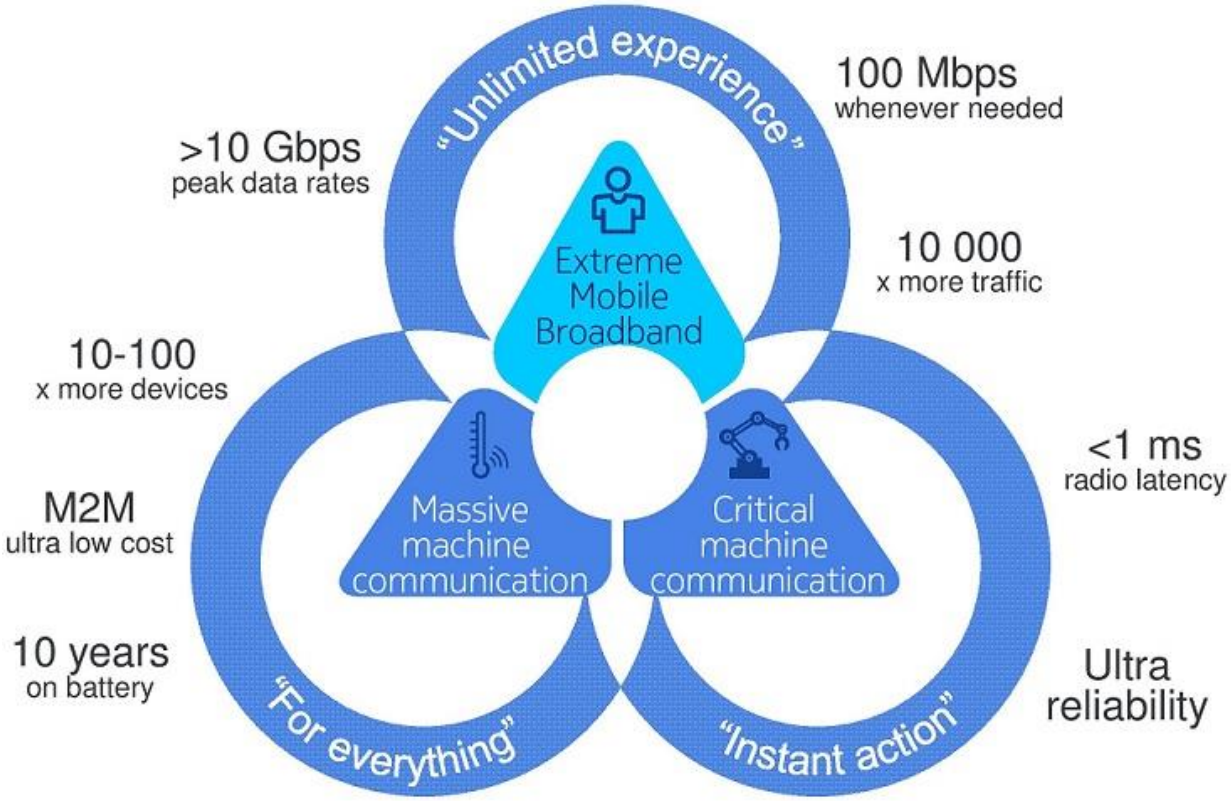


Figure 2 : 5G key content outlined

8 Applying 4G and 5G for Public Safety

Every country has its own requirements and plans in relation to the implementation of a next generation Public Safety communication solution. These plans depend on multiple national drivers including national security policy, financial situation, life-cycle phase of the current deployed narrowband solution and mobile network operators' interest/capability to offer mission critical service.

Rather than trying to provide some generic recommendations for implementation models of a next generation Public Safety solution, it's more useful to address basic questions related to standardisation, 3GPP Releases and Public Safety solutions. Some of these basic questions, with brief answers, are listed below.

8.1 When is the correct time to start applying 3GPP technologies in Public Safety?

First of all, it's important to realise that Public Safety users are already today using 3GPP technologies widely and these mainstream technologies have been used already for years. According to IHS Markit, there are 1.5 million Public Safety users within Europe who are using mainstream commercial technologies (i.e. consumer networks) as of today. This usage is providing Public Safety users with broadband data services which are used to complement the existing mission critical voice service i.e. to compensate for the lack of broadband capability in PMR technologies.

However, typically this question doesn't include the above mentioned usage of existing consumer networks. It's more about when and how to start applying 4G and those Public Safety specific functionalities which are defined on top of 4G within 3GPP Releases 12-13-14.

Generally speaking the time to start is determined by user needs. In case of urgent needs, 4G usage can be started quickly, but will probably not support all the capabilities and features of current PMR systems. One easy way to start would be to use broadband data services with an MVNO arrangement which is improving service availability and security. Adding national roaming with all operators will increase the coverage and availability further. Standard compliant 4G based PTT voice service could be started as soon as implementations from equipment providers are proven, trialled properly by Public Safety users and mature enough for operational use.

8.2 Is 4G (LTE) forming good enough basis for Public Safety implementations?

4G forms a good basis for Public Safety implementations. However, this naturally requires that Public Safety fit for purpose functionalities are implemented by network equipment vendors, tested across multiple vendors' solutions and trialled properly with Public Safety users.

8.3 Is it better to wait for 5G before starting Public Safety implementations?

Once again this is dependent on user needs, related urgency and also the life-cycle of existing Public Safety networks. A 5G implementation will also include all 4G functionality and all required Public Safety services will be available. However, the idea of waiting for the next technology level or 3GPP Release because it is offering better service for Public Safety can easily trigger an everlasting waiting loop while the next technology level is always offering something more and better than the previous one. Deploying 4G will also give additional experiences for the use cases that are most needed and can improve 3GPP standards more quickly. In addition to this, deploying 4G would also enable users to start learning characteristics of the new solution.

Improved air interface performance (extreme Mobile Broadband and new radio interface) is completely new content within 5G but the improvements in 4G (on which 5G is based) is ongoing. However, new radio interface aimed at supporting very high frequencies i.e. very small cells, and all related Public Safety use cases have not yet been identified.

The ecosystem change from the narrowband PMR ecosystem to 3GPP ecosystem is a big step and it is a challenge for the Public Safety community to operate properly within this environment. This is time consuming, and learning the new environment can be done only with efforts related to Public Safety service implementation and operational use of implemented solutions.

It is best to start this learning period proactively, and to apply new technology and solutions sooner rather than later. This is simplified by the fact that narrowband and broadband systems can work in parallel and supplement each other.

8.4 Is 5G offering better service than 4G for Public Safety?

New 3GPP Releases are always offering new services, improvements and enhancements when compared to previous Release levels, and the same applies for those Releases also which are implementing the 5G, i.e. 3GPP Releases 15-16. In the same way, Releases defined in the future on top of 5G will also offer more than the 5G Releases.

5G content is outlined to include such kind of elements which can be used to improve the service offered for Public Safety. This will finally also depend on implementations by equipment providers, but the expectation is that 5G will be able to offer improved service to different user groups, including the Public Safety community.

8.5 How can the 4G defined Public Safety content also be included in 5G ?

3GPP standardisation machinery defines new Releases in such a way that the next Release will by default inherit content from the previous one. Furthermore, product implementations from network equipment vendors are in practice backwards compatible because of reasons of scale, economy and preventing disruption to the customer base. This means that Public Safety specific content defined on top of 4G (i.e. 3GPP Releases 12-13-14) will be included in 5G (i.e. 3GPP Releases 15-16), and there is a smooth evolution path.

8.6 What is the linkage between 4G-5G evolution and spectrum for Public Safety?

According to the international and European regulators such as ITU[1], ECC and the EC, spectrum serving Public Safety (PPDR)[2] operations has to be found in the 700 MHz band, but it is up to each country to determine how, and how much. So, for the purpose of Public Safety in 700 MHz band it is worth noting that deployments will use the 4G radio technology with additional services standardised in 3GPP Release 15 – and will be called 5G.

Release 15 is expected to be finalised in 3GPP 2018-2019 with products on the markets 18 months later. An upgrade from 4G to 5G within the 700 MHz band will be implemented as a software update without triggering changes to the radio network planning'.

8.7 What is the best way to connect 4G and 5G solutions for Public Safety use?

A 4G solution means a network implementation with 3GPP up to Release 14, and 5G solutions are network implementations with 3GPP Release 15 onwards. 5G solutions include both 4G defined content

[1] ITU Resolution 646 - PPDR spectrum should be found in 700 & 800 MHz bands.

[2] European regulators use the term PPDR, defined as Public Protection and Disaster Relief. This includes Public Safety.

and new 5G defined content. A network which has been upgraded to 5G level will offer both 4G services and new 5G services and there is no need for any specific connectivity solution between 4G and 5G.

Confusion, in relation to this question, comes mainly from the terms 4G and 5G, which are labels highlighting technology evolution and technology generations. It is easier to understand the technology evolution by putting the generation labels aside and regarding this evolution as a continuous stream of 3GPP defined Releases.