June 2019

TCCA White Paper

Public Safety prioritisation on commercial networks

Important Note

The opinions and information given by TCCA in this white paper are provided in good faith. Whilst we make every attempt to ensure that the information contained in such documents is correct, TCCA is unable to guarantee the accuracy or completeness of any information contained herein. TCCA, its employees and agents will not be responsible for any loss, however arising, from the use of, or reliance on this information.

First issued by TCCA's Broadband Industry Group, June 2019.

The Grainger Suite, Dobson House, Regent Centre,
Gosforth, Newcastle NE3 3PF, UK
T +44 (0) 191 231 4328 E admin@tcca.info

Public Safety prioritisation on commercial networks

Contents

1 Executive summary

Many studies carried out in different countries show that Public Safety broadband services will most likely rely on both commercial Mobile Network Operator (MNO) infrastructure and dedicated infrastructure. This is commonly referred to as "Hybrid Infrastructure" as described in following TCCA white paper: A discussion on the use of commercial and dedicated networks for delivering Mission Critical Mobile Broadband Services. To ensure that first responders get the highest level of priority to the shared Radio Access Network when they are using an MNO infrastructure, there are already many prioritisation mechanisms (Access Class Barring, Pre-emption, Quality of Service Class Identifiers (QCIs), etc.) that have been standardised by 3GPP to provide mission critical services. Furthermore, implementing national roaming between MNOs is also a consideration as a cost-effective way of implementing enhanced network resilience.

However, implementing these priority mechanisms may require changes to legislation in order to be adopted in each country. Two examples are Finland and Belgium – both countries have enshrined in law such necessary changes through decrees.

There are already some major early adopters that are currently implementing Public Safety broadband services over MNO infrastructures: FirstNet (US), built on top of AT&T's network and ESN (UK) built on top of EE's network.

2 Introduction

More and more countries are considering implementing broadband Public Safety (PS) services over MNO networks. There are many benefits in this approach:

- MNOs have already widely rolled out LTE allowing a fast time to market of PS broadband services on top of their commercial network.
- MNOs have usually a large amount of spectrum whereas in many countries there is very little or no spectrum available for a PS dedicated network.
- Sharing the network with MNOs can reduce the total cost of ownership for the PS agencies.
- Hosting PS services can benefit the image and brand of the MNO.

However, running PS services over commercial networks places many constraints on the network architecture. PS users have the most stringent requirements for network and service accessibility and service quality. During a major event, the MNO network might suffer congestion preventing PS users gaining critical access. Therefore, different prioritisation mechanisms need to be implemented.

This white paper will review the different prioritisation mechanisms that already exist, and also the legal aspects to be considered to implement them. We will also provide some feedback from Public Safety end users and from early adopter ESN in the UK.

3 Public Safety constraints to be considered by MNOs

There are three main areas in which MNOs need to enhance their networks to fulfil mission critical requirements: network availability, network performance and network security.

3.1 Network Availability: Radio coverage, network resilience and PTT interworking

The radio coverage of the network needs usually to be extended to cover the widest geographical area. Typically, uplink video for a bodycam for example will require a reasonably good coverage/signal quality level to ensure the streaming is of sufficient quality. Special care needs to be taken when MNOs refarm 2G/3G frequencies to LTE to ensure coverage holes do not appear or Quality of Service (QoS) is degraded. Some new use cases might also be required such as Air-to-ground (A2G) and/or Ship-to-Shore communications that will impact the radio design.

Network resilience needs to be enhanced through different means:

- Enabling of local calls on each site even if backhaul transmission is lost, possibly realised by using Isolated Operation for Public Safety (IOPS) or by using a redundant backhaul.
- Reassessing the Core Network and Transmission design to check the required redundancies are implemented.

- Implementation of national roaming with all the MNOs to introduce Radio Access Network (RAN) redundancy.
- Site hardening: power supply needs to be secured through longer battery backup time and / or local generators and the site itself needs to be protected against vandalism and extreme weather conditions.
- Push To Talk (PTT) interworking: In most countries PTT still relies on the existing narrowband systems, referred to depending on the world region as either Land Mobile Radio (LMR) or Professional or Private Mobile Radio (PMR). It is therefore important that the broadband Mission Critical PTT (MCPTT as defined since 3GPP Releases 13) implemented on top of the MNO network will be able to interwork with the existing narrowband PTT service. However, some other countries believe that it is possible to replace an existing narrowband network with a new broadband network without such interworking, with the reasoning that it is better to concentrate on the new network instead of using resources to implement and operate interworking.

3.2 Network Performance: High prioritisation for Public Safety communications

Network performance is mainly about making sure first responders get the right level of service and priority when hosted on a commercial network that might get congested in the event of a major incident.

Call prioritisation is implemented in critical narrowband networks. TETRA for example offers:

- Priority Calls: there are 16 levels of priority in TETRA providing different Grades of Service (GoS).
- Pre-emptive Priority Call: if there is congestion, lowest priority calls get pre-empted by highest priority calls
- Call Retention: Selected users will get protected from pre-emptive calls (emergency calls)
- Busy Queuing: if congestion occurs, calls are queued and handled once a traffic channel becomes free.

Likewise, in 4G there are a number of prioritisation mechanisms that have been standardised by 3GPP to allow mission critical services. Chapter 5 provides more details about these mechanisms.

First responders' calls will always be treated with higher priority than commercial calls. However, there must be some mechanisms implemented that, in the case of a major incident, enable commercial users to still make calls to some extent. In a crisis situation, MNOs can for instance free one frequency band from commercial traffic and assign it to PS usage by diverting all commercial calls to their 2G/3G layers or to some other 4G bands. MNOs have usually more than one frequency band that allows them to implement such mechanism. However, in some countries legislation may allow the full capacity to be assigned to PS.

To further improve the network performance for group communications, either MCPTT, MCData or MCVideo, MNOs might implement the evolved Multimedia Broadcast Multicast Service (eMBMS). By using a secured and standardised broadcast channel, eMBMS optimises the usage of radio resources while ensuring the best quality for voice and video group calls.

3.3 End to End (E2E) Network Security

Security needs to be ensured from an E2E perspective, from network (management/user/control planes) to devices. As 4G is a native IP technology, there are already many proven solutions available.

- 3GPP SA3 is determining the security and privacy requirements, specifying the security architectures and protocols at application level. Typically, all LTE networks from MNOs benefit already from the 3GPP security framework as they implement cyphering and integrity keys.
- A security gateway (SEG) is placed in front of the core network to stand as a guard to the network and only allows traffic into the core network after it has been authenticated.
- Thanks to IPSec on the transport network, the whole core network is hidden behind the SEG. The traffic is encrypted, no traffic injection can take place, ensuring data confidentiality and integrity.
- E2E Encryption between LTE and legacy LMR/PMR networks can be solved at application level or codec level:
  - Codec level E2EE can be made E2E interoperable with legacy LMR/PMR E2EE systems.
  - Concatenated access VPN does not offer the same level of security as E2EE.

- On the terminal side, there are ways to re-install very secure closed operating system (unlike regular Android OS) in order to control the applications that are installed on the device.
- In case of a National (or International) Roaming agreement (see §6.3), the E2E network security will also need to be considered with all the MNOs involved in that agreement.

E2E security is more than just pieces of security here and there. When the different types of security threats that are likely to lead to attacks and interference have been identified, the network needs to be engineered with a holistic approach knowing that there are security mechanisms at IP level (transport and routing) under the control of the MNOs and security mechanisms at application level under the control of the PS agencies.

4 Market trend for Public Safety over MNO

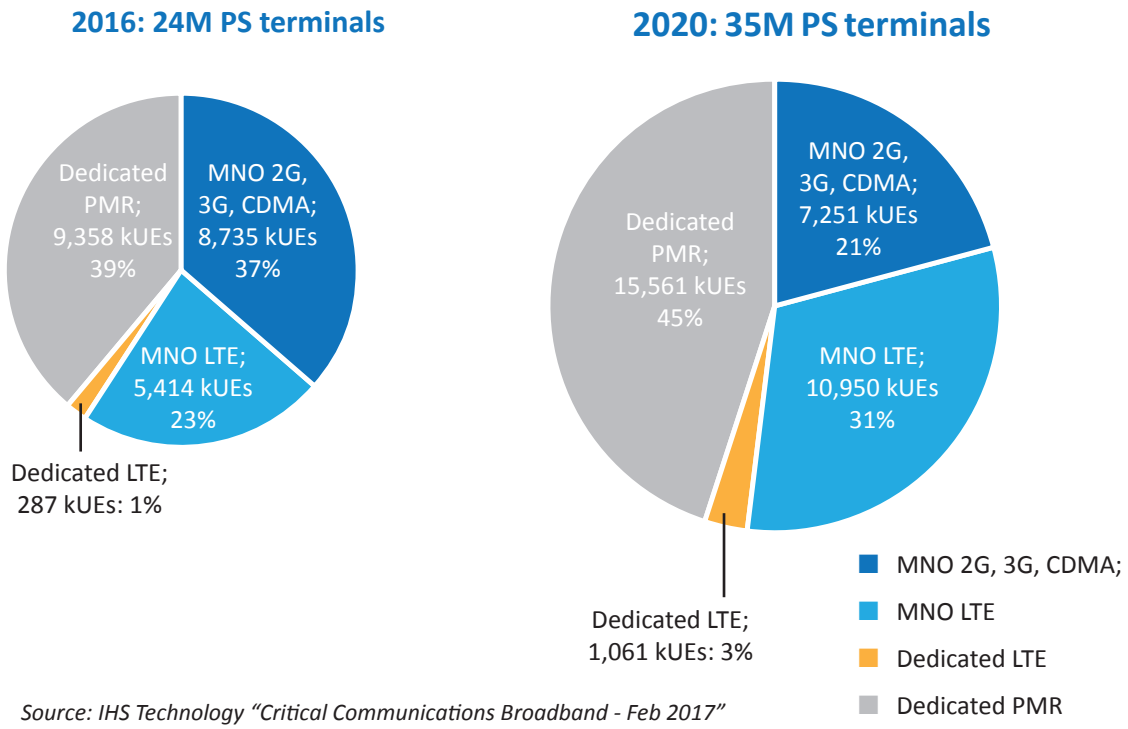
The need from Public Safety agencies to get broadband services is an opportunity for MNOs to leverage their network investments. The opportunity can be huge when addressing new promising vertical markets like eHealth, connected cars and critical communications users of all kinds of existing markets such as utilities, public safety, transportation, oil & gas, mining etc. Therefore, operators are encouraged to take time to build operational and commercial strategies considering all markets with different maturity levels.

Most of the vertical markets need network hardening and network resilience. It is important to encourage common resiliency investments. 5G will allow more services above the well-known IP architecture: higher throughputs, shorter latency, improved coverage thanks to 5G non-terrestrial networks (satellite, UAV, …) as explained in §10.2.2.

Professional and critical communications markets are the new revenue streams from which MNOs can benefit if they develop their networks, provided they can establish relevant business models and are not driven to develop non-profitable services under too many regulatory constraints.

The trend that shows more and more PS users will be utilising commercial networks is clearly captured by the IHS Markit report (Feb 2017). It shows a 102% expected growth for PS LTE terminals connected on MNO networks over the four years to 2020:

2016 to 2020 worldwide PS terminals forecasted



Source: IHS Technology "Critical Communications Broadband - Feb 2017"

Some major countries are already rolling out Public Safety networks over commercial networks:

FirstNet US is built on the AT&T network.

All federal states have opted in for FirstNet. The FirstNet Core network was launched in March 2018 and 72 Satellite Cell on Light Truck (SatCOLTs) are now deployed.

The following activities are in progress:

- Nationwide buildout of state Radio Access Networks / Band 14
- Applications and Devices Ecosystem development for Public Safety
- Testing network features in FirstNet Innovation and Test Lab
- Support local network operations and pilots

As of January 2019 5,250 agencies are on FirstNet with about 425,000 subscribers

ESN UK is built on the EE network:

EE's coverage in all 4G bands will be available to ESN as a base, with the network coverage being improved to meet ESN requirements, including extending coverage along major and minor roads, selected buildings, London Underground tunnels, road tunnels and railway facilities, as well as 12 miles out to sea and up to 500 feet above the ground, where coverage will rely on B3 (1.8 GHz) and B20 (800 MHz) bands from EE's network. It will be complemented with a new B40 A2G overlay network for traffic between 500 and 10,000 feet. EE has now completed construction of 354 of the new sites needed, with the remaining 111 masts due to be finished shortly.

ESN users will get priority use of the EE 4G network via a dedicated network code and utilise priority radio and core network bearers to access ESN Public Safety services. See:

https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network#programme-review

From early 2019 the police, fire and rescue services, ambulance services and other users have been able to use the ESN data services, with voice capabilities following. This incremental approach will allow the emergency services to test and choose which ESN products they want as and when they become available, rather than having to wait for the network to be fully implemented.

The ESN network has prioritisation mechanisms implemented as described in §9.1. They have successfully been field tested. Before the MCPTT app is released for users, further field testing will take place.

5 Available Prioritisation Mechanisms in 4G on shared network

In 4G, 3GPP standardisation foresaw four types of mechanisms to handle prioritisation of Public Safety users on a shared network:

5.1 Access Class Barring (ACB):

ACB prevents congestion at signalling level (random access procedure) when too many UEs try simultaneously to get a radio resource assigned (RRC connection). To set the priorities between the different UEs, 3GPP has defined 16 access classes:

- Class 0 to 9: for regular MNO subscribers. The access class is randomly assigned between 0 - 9
- Class 10: for Emergency calls
- Class 11: for PLMN Use.
- Class 12: for Security Services
- Class 13: for Public Utilities (e.g. water/gas suppliers)
- Class 14: for Emergency Services;
- Class 15: for PLMN Staff;

The network can automatically activate access class barring based on certain overload thresholds at a cell level. The access class is stored on the USIM.

5.2 Admission control through Allocation and Retention Priority (ARP)

Admission control prevents congestion at Evolved Packet switched System (EPS) bearer level, once Radio Resource Control (RRC)) is established. 3GPP has defined different levels of Allocation and Retention Priority (ARP) that are assigned to the EPS bearers. The range of the ARP priority level is 1 to 15 with 1 as the highest level of priority. An existing lower priority bearer can be pre-empted by a higher priority bearer, if the lower priority bearer has pre-emption vulnerability set and the higher priority bearer has pre-emption capability set.

ARP value is valid for both GBR (Guaranteed Bit Rate) bearers and non-GBR bearers. A typical Public Safety example could be prioritisation of GBR bearer for MCPTT service over regular Voice over LTE (VoLTE) call or any other bearer. The dedicated GBR bearer for MCPTT call could have ARP priority 3 and dedicated GBR bearer for VoLTE could have ARP priority 10. If all GBR resources were consumed in a cell and pre-emption enabled, then a new MCPTT call could pre-empt general internet traffic or video streaming.

ARP is part of QoS parameters. For default bearers the ARP priority is included in subscription data in the Home Subscriber Server (HSS) for each allowed Access Point Name (APN). Pre-emption capability and vulnerability for default bearers is set by the Mobility Management Entity (MME) according to operator policy. ARP priority and pre-emption settings can be also modified by the Packet Data Network Gateway (P-GW) based on interaction with the Policy and Charging Rules Function (PCRF). ARP for dedicated bearers is set by P-GW based on subscription or based on interaction with PCRF. [3GPP TS 23.401]

5.3 Traffic scheduling

Every default and dedicated EPS bearer has a QoS class identifier (QCI), which defines the resource type (GBR or non-GBR), latency target, packet loss rate and priority level for scheduling. The original 3GPP Release 8 specified standard GBR QCIs 1-4 and non-GBR QCIs 5-9.

3GPP Release 12 added additional QCIs for Public Safety applications. GBR QCIs 65 and 66 are respectively for mission critical PTT and non-mission critical PTT. Non-GBR QCI 69 is for mission critical signaling and non-GBR QCI 70 is for mission critical data. [3GPP TS 23.203]

MCPTT service will use QCI 69 bearer for signalling and QCI 65 for voice media. This is similar to VoLTE service, which uses QCI 5 for Session Initiation Protocol (SIP) signalling and QCI 1 for voice media. With these new QCIs PS users get priority scheduling for MCPTT even over the VoLTE service.

3GPP Release 15 added QCI 67 for MCVideo.

5.4 Dynamic QoS modification

Default EPS bearers have QoS defined in HSS (QCI, ARP priority, Maximum Bit Rate (MBR) + Aggregated MBR (AMBR)). It is possible to dynamically modify the QoS of EPS bearers including default bearers. This can be achieved by having a PS application (e.g. a dispatcher application in a PS control room) that triggers policy change via PCRF. A less sophisticated option is also possible where predefined rules per traffic type are defined for example. So, the scenario for dynamic priority level for PS users is possible with bearer QoS modification. PS users could for example have QCI 6 with ARP priority 8 for generic data connection normally and in the case of an emergency mission the data connection QoS could be modified to QCI 70 and ARP priority 6.

6 Regulation and Legal aspects:

Implementing Public Safety use on an MNO network might have some impact on commercial users. Typically, in the case of an incident, the network capacity might get partly pre-empted (through ACB, ARP) by the authorities responsible for PS users. Efficient network tuning will allow sufficient capacity for commercial users. Nevertheless, depending on the local legislation, resource pre-emption on the commercial network can be a legal issue. Also, the fact that first responders get first priority on the mobile network might be in contradiction with net neutrality.

6.1 ACB: Access Class Barring:

- is used in many countries as a “defence” mechanism against overload that could lead to a total outage of the telecom equipment

- is forbidden in some countries such as Austria, as commercial users cannot be discriminated from PS users

6.2 Net Neutrality:

Net neutrality means that the internet service provider must handle all traffic carried by the network in equal manner. Net neutrality principle can be seen somewhat in contradiction with the need to offer prioritised services for critical communication users.

The European Union is in favour of net neutrality, and this is backed up by regulation. See the BEREC report: https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

In the US, the Federal Communications Commission (FCC) adopted network neutrality principles in 2005 but repealed this decision in 2018.

PS operators need to consider net neutrality depending on the specificities of the regulation and laws in each country. They should plan these legal aspects at a very early stage of their PS broadband implementation schedule.

6.3 National Roaming

National roaming is a very efficient way to implement RAN redundancy and therefore to improve the resilience of a PPDR network. It can also be a way to improve the coverage. However, in many countries, national roaming is not allowed as it could harm competition between the different MNOs. Some countries like Belgium and Finland have already taken legal action to enable national roaming between all their MNOs limited to first responders. Norway has already national roaming for qualified users with a role or function of vital interest to the society.

Now some PS agencies are even requesting international roaming.

6.4 Legislative status in some countries:

- Belgium: A royal decree has been issued by the Minister of Telecommunication and the Minister of Interior that means MNOs must implement network availability and prioritisation for first responders.

  https://www.bipt.be/public/files/fr/22572/Communication_projet_reglementation__encheres_multibande.pdf

  https://www.bipt.be/public/files/nl/22572/Mededeling_ontwerpregelgeving_multibandveiling.pdf

- Finland: Finland has adopted the “Virve 2.0” law that ensures the legal base for future broadband mission critical communications. It is now legal to prioritise Public Safety users over consumers. It will also be mandatory for the MNOs to give national roaming to Public Safety users.

  http://www.criticalcomms.com/news/finland-law-passed-virve-2-0-critical-communications

- Norway: Qualified users with a role or function of vital interest to the society already have the ability to pre-empt 3G and 2G voice traffic.

7 Public Safety Service Providers implementation aspects:

7.1 Feedback from French MoI:

Using MNO services means using a shared network without a full control of the radio resources. The fear of congestion has long been the main issue hindering the use of commercial networks for PPDR. With the introduction of 3GPP Release 13 mission critical features for PPDR and the possibility to use Release 12 and newer features for quality of service, congestion issues can be dealt with. The fear of congestion comes with the massive rollout of broadband video, such as police body worn cameras. Today we have no clear mechanisms in place to perform the prioritisation between different video streams (content based prioritisation). This issue needs still to be tackled.

Dealing with MNOs means negotiating an SLA about service availability rate. Using priority and pre-emption, national multi-MNO roaming can lead to a real 99,99xxx availability rate under coverage of more than 98% of the territory and population.

But it's not enough: for PPDR issues we also need resilience. That means that, in some cases, we have to remain fully independent and to be able to quickly deploy our own network, for instance, in cases of a hurricane or wildfire destroying infrastructures, or terrorists taking hostages. Those events happen rarely and concern generally a small area (a few square km). That's why we need tactical networks of relevant sizes to complete the solution. For industrial plants, harbours, airports, etc… that usually have their own private (or semi-private) LTE network, the resilience can be improved cost efficiently by allowing seamless roaming between these private LTE networks and the main PPDR network for first responders.

A last issue is the direct mode. In legacy networks, you can use some dedicated frequencies to communicate between devices without using the network infrastructure. That does not yet exist in commercial networks with different radio resources management (and billing…).

This is the very last solution, when nothing else works, to be able to communicate between close users, and it's always a user requirement. Small tactical networks (backpack type) could be a solution or small tactical networks carried by patrol vehicle (as BYOD in business, you can use the BYOC concept: bring your own coverage). Those deployable solutions could use an opportunistic backhaul based either on enhanced antenna systems for land coverage or on satellite links.

7.2 Feedback from ASTRID Belgium:

The Belgium federal authority made a comprehensive study of the future of their PPDR network and made the following statements during the ASTRID Days beginning October 2018:

- The future of PPDR is LTE that will replace TETRA technology to enable broadband services.
- Building a nationwide LTE network dedicated to PPDR is too expensive for Belgium.
- Instead, collaboration with MNOs is needed as they have already rolled out LTE countrywide.
- Stringent Service Level Agreements (SLAs) will need to be signed with the different MNOs to ensure the same guarantees as with today's TETRA network. The following three main KPIs will need to be guaranteed: coverage, prioritisation and network availability.
- Coverage will be needed in places that are not necessarily attractive businesswise for MNOs but needed for safety reasons like for instance "Seveso classified" areas - http://ec.europa.eu/environment/seveso/. Additional sites will need to be rolled out.
- Network availability and prioritisation for first responders have been the subject of a royal decree issued in August 2018.

7.3 Feedback from Virve Finland:

Erillisverkot is in the process of moving mission critical communications from the TETRA-network called Virve to a commercial LTE service. End users of the Virve-service have set a goal that the availability of the new service must meet that of the current TETRA based system. From one side, availability comes from hardening the system with power resilience and doubling base station connections but prioritising the traffic over consumer traffic is even more important. To begin with, we need 4G or newer radio access network -technology, in order to have functional priority mechanisms. These are called QPP functionalities (Quality, Priority, Pre-emption). Quality means that when mission critical service requires it, good enough quality is guaranteed to that service, even if it means poorer quality of service for consumers. Priority ensures prioritised access to mission critical services when there is congestion in the network. Pre-emption allows resources to be transferred from consumers to Public Safety users in similar conditions. For all MNOs it will also be mandatory to offer national roaming to Public Safety. These measures can only be used for users and purposes defined in the law. Also, issuing priority and controlling these features shall be a proprietary task for one party, since priority is only as good as it is compared to that of others.

8 MNOs implementation aspects

8.1 Orange Business Service (France)

Orange Business Services have been awarded a contract by the French Ministry of Interior, the purpose of this contract being to deliver nationwide mobile critical communications for the security forces.

To achieve that Orange Business Services will provide the security forces with network solutions relying on the LTE connectivity.

Specific features are being tested and implemented by Orange Business Services. These comprise Mission Critical Push to X services (MCX is the combination of MCPTT, MCData and MCVideo) meaning that these services will encompass the traditional MCPTT services and in addition push to data services allowing the transmission and sharing of texts, pictures and videos inside a group.

Furthermore, the Security Forces will be provided with a high Quality of Service and they will be guaranteed access to the network in all situations including crisis situations.

This will be made possible by the use of 3GPP functions, e.g. use of the QCIs.

9 Feedback from early adopter ESN UK:

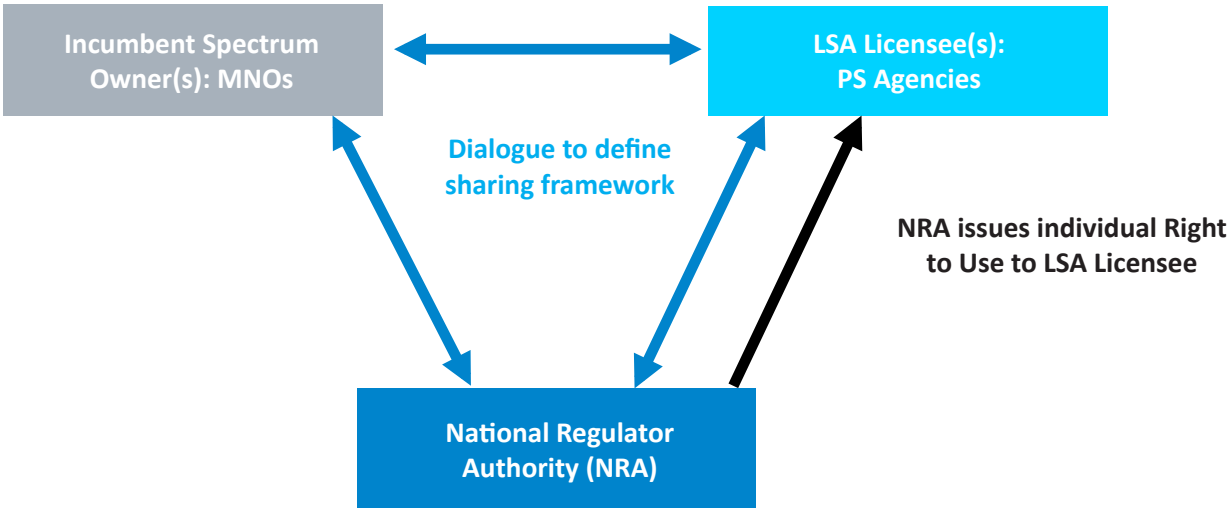
- Allocation and Retention Priority (ARP) has been implemented. As non-GBR bearers are not guaranteed any service rate after admission they are given relatively little consideration in the admission control procedures, e.g., they may be accepted as long as no non-scheduling limits are hit, and then passed to scheduling domain. Similarly, admission of a GBR bearer does not generally consider its impact to ongoing non-GBR bearers, i.e., as non-GBR services utilise resources left over after GBR traffic has been scheduled the non-GBR bearers can validly be retained but data limited by scheduling to have little throughput in periods of congestion (i.e., not requiring pre-emption). If control/overhead resources cannot be allocated, then non-GBR bearers may be pre-empted. In comparison, admission of GBR services must consider whether the requested attributes of the new GBR request can be met given the ongoing guaranteed load on the cell. In terms of air interface resource, the existing guaranteed load is a continuously varying load due to changing radio conditions, mobility, and the variation of the actual traffic on GBR bearers – which is not normally a constant rate. Due to these variations it would neither be possible nor efficient to hard-reserve air interface resource for GBR bearers. Rather, the eNB assesses whether a new GBR bearer can be admitted based on its requested QoS rates compared to the amount of resource unused by ongoing GBR bearers. Exact algorithms are vendor-proprietary, but naturally are designed to maximize admission control success with minimum pre-emption and with maximum radio resource efficiency. It should be noted that good practice for maximizing good admission/congestion control is that GBR bearers be used for relatively low-throughput services (e.g., voice calls) rather than high bit rate services (e.g., Video); as a single GBR service demanding a high guaranteed bit rate can cause disproportionately high resource impacts and multiple pre-emptions
- Pre-emption is applied where a request cannot be satisfied with the available resources, but only when the bearer has a higher ARP priority and pre-emption rights vs other bearers with lower ARP priorities and are pre-emption vulnerability – in accordance with 3GPP. The eNB will pre-empt in order of ARP priority, targeting the lowest vulnerable priority bearer first. Where multiple target UEs have the same priority then the pre-emption selection will first be targeted towards those using the most resources. E.g., if two pre-emptible users have the same ARP priority in a VoLTE call when a higher priority PTT call comes in, the VoLTE user at the cell edge will be pre-empted in preference as more resource-intensive. Note that it may be necessary to pre-empt multiple UEs to admit one UE's new request and if pre-emption is unsuccessful the new admission attempt will be rejected. Admission control for GBR bearers is based on the eNB current utilisation not reservation or previously admitted bearers. It must be noted that the pre-emption behaviour describer may differ depending on the vendor implementation and could be adapted for the specific use case, i.e. small cell deployments.
- Congestion Control is not normally necessary due to there being a mix of non-GBR and GBR traffic such that non-GBR traffic is scheduled less when necessary. However, high GBR-traffic, changing radio conditions, mobility and varying bit rates could cause congestion of ongoing GBR bearers to occur (i.e. as opposed congestion that would be caused by a new admission request). If congested and in need of releasing an ongoing GBR service because not all existing GBR services can continue to be adequately be serviced, then the eNB would target for release low-priority ARP GBR services first. If multiple bearers with equal priorities are potential targets, then the bearer

using the most resources would be targeted first. As mentioned previously the pre-emption behaviour describer may differ depending on the vendor implementation.

10 Innovative prioritisation mechanisms and evolution towards 5G

10.1 Licensed Shared Access (LSA):

LSA allows a dynamic use of spectrum, whenever and wherever it is unused by incumbent users thanks to a three-party partnership. The LSA principle is frequency and technology agnostic.



Regulatory process for spectrum sharing as stated in ECC Report 205

Within Europe, many LSA trials have already been conducted to test the dynamic reallocation of the 2.3GHz spectrum from an MNO usage (LTE) to a Program Making and Special Events (PMSE) usage and the way back: Spain (Oct 2015), Finland (March 2016), France (October 2016), Italy (November 2016), The Netherlands (January 2017). Reports of all these trials can be found here: https://www.cept.org/ecc/topics/lsa-implementation

Such a dynamic spectrum allocation mechanism could be considered to reassign MNO spectrum to a PPDR exclusive usage at a given time, for a given duration, on a given location when Public Safety requires it. However, LSA necessitates that it is approved by the owner of the spectrum. Furthermore, the advantage and drawbacks of such a procedure are still to be assessed.

10.2 Evolution towards 5G:

10.2.1 5G prioritisation mechanisms, concept of Network Slicing.

Network slicing allows multiple logical networks to be created on top of a common shared physical infrastructure. Customised connectivity is provided for each network slice, with all slices running on the same shared infrastructure. This is achievable in 5G networks due to the availability of advanced virtualisation and orchestration capability, including Virtual Networking Functions (VNF) and Software Defined Networking (SDN) architectures.

Current and future critical communication applications are driving the need for a wide variety of network performance service characteristics. These required characteristics will vary in terms of priority, data rates, error rates, latency, security, availability, coverage, etc. Resources for these network slices can therefore be set up for various applications without one competing with the other, e.g.: Augmented Reality, MCPTT, Massive IoT, etc.

In summary, network slicing enables a customisable level of connectivity and priority for a plethora of critical applications, each with widely differing service characteristics, yet carried over the same physical network.

10.2.2 5G non-terrestrial networks.

3GPP has finished work on a Technical Report "TR 38.811: Study on New Radio (NR) to support non-terrestrial networks" as companies and organisations recognise the added value that satellite coverage brings, as part of the mix of access technologies for 5G, especially for mission critical and industrial applications where ubiquitous coverage is crucial.

Beyond satellites, Non-terrestrial networks (NTN) refer to networks, or segments of networks, using an airborne or spaceborne vehicle for transmission. Airborne vehicles refer to High Altitude Platforms (HAPs) encompassing Unmanned Aerial Systems (UAS).

Such 5G Non-terrestrial networks will:

- Reinforce service reliability by providing service continuity for user equipment or for moving platforms (e.g. passenger vehicles, aircraft, ships, high speed trains, buses)
- Increase service availability everywhere; especially for critical communications, future railway/maritime/aeronautical communications
- Enable 5G network scalability through the provision of efficient multicast/broadcast resources for data delivery towards the network edges or even directly to the user equipment

Public Safety in 5G is a large topic that TCCA will address more in detail in a dedicated white paper.

11 Conclusion

Today, major countries like the US and UK are rolling out Public Safety over MNO networks. Prioritisation and pre-emption features have been successfully field tested there. Technology-wise we can say that prioritisation of first responders connected to a shared commercial radio access network is no longer a challenge as there are already many mechanisms available to handle it and suitable hardening is applied. That said, some legal topics need to be addressed country by country to allow pre-emption and national roaming. Technology and the eco-system are now ready to allow Public Safety networks to leverage MNOs' radio access network.