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

A discussion on the use of commercial and dedicated networks for delivering Mission Critical Mobile Broadband Services

Important Note

The opinions and information given by the 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, the TCCA is unable to guarantee the accuracy or completeness of any information contained herein. The 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 the TCCA February 2017

Executive Summary

General

Public Safety organisations in Europe and the rest of the world currently provide mission critical mobile radio communication services to police officers, ambulance crews, fire and rescue personnel and others using dedicated radio networks. These specialised networks are based on TETRA, Project 25 or Tetrapol radio communications standards. Such standards provide excellent voice communication but have limited data capabilities. However, there is an increasing need for high speed data communications for mobile staff to supplement these voice services. Typical applications include the transmission of incident details, images and video clips to staff, whether on the street or in vehicles. Internet access, email and social media are also becoming important as well as accessing back office databases as information sources and for report filing.

Commercial Mobile Network Operators (MNOs) already offer high speed data access to businesses and the public either direct to mobile phones or to personal computers. Commercial MNOs have the ability to deliver mobile broadband to Public Safety services as well. Indeed, many Public Safety organisations are already taking advantage of this capability but only for non mission critical applications. Such traffic will be carried by a 'best efforts' commercial service. However, for safety critical applications such as despatching ambulances, passing details of terrorist suspects and dealing with major incidents, it is essential that networks are employed that are suited to mission critical communication.

Until such time as 4G and 5G networks are proven to be truly Mission Critical, today's voice networks will be the only mission critical service available.

This paper has been written to assist Government organisations and those responsible for Public Safety mobile communications, to consider the most appropriate solution for delivering such capabilities. Issues addressed include spectrum, security, speed of roll out, political influences and cost.

One solution is a combination of dedicated network infrastructure combined with service from one or more commercial MNOs. The potential benefit of such an arrangement is that mobile broadband applications can be taken advantage of more quickly and with lower capital investment for public administrations than building a private nationwide dedicated broadband network. For the purposes of this paper the term Hybrid Infrastructure is used to describe a combination of dedicated infrastructure and service provided by commercial MNOs.

Key Issues

There are a number of key considerations when deciding to what extent the use of commercial MNO services is appropriate.

Spectrum

The availability of spectrum is key to enabling choice in the provision of broadband data services. For a Public Safety operator to build its own infrastructure anywhere in the country, it will be necessary to obtain suitable spectrum.

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. In many countries, there is an immediate opportunity to secure sufficient spectrum for Public Safety operations and such an opportunity may not occur again for a very long time.

Those responsible for public safety communications should urgently review the opportunities for obtaining spectrum and engage with the appropriate government ministries and the national regulator to establish how spectrum can be made available for those with responsibility for the health, welfare and security of our citizens.

Security

Police and security services require secure communications to enable confidential information to be passed safely over the network. The TETRA standard, used widely throughout the world, includes highly secure encryption mechanisms. 3GPP, which is the standards body responsible for LTE, is building security mechanisms into the LTE standard. However, these will be different from TETRA.

Broadband data services will likely carry a significant volume of confidential information; more than existing voice networks. A review of the security arrangements available in LTE systems, and in any commercial network that is used, should be undertaken by suitably qualified staff.

Ownership

Commercial networks are subject to being bought and sold, as is the case with any commercial business. Such transfers of ownership may be to companies in any region of the world. Some governments are cautious about critical national infrastructure being owned by foreign companies.

Those responsible for public safety communications should consider the national government policy with regard to foreign ownership and operation of telecommunications infrastructure.

Funding

Dedicated telecommunications infrastructure will require significant capital investment, especially if such networks are to be deployed over large areas. The use of commercial networks will significantly reduce the capital investment for public administrations and also the time required to implement Public Safety services. The use of commercial networks will, however, incur ongoing service charges.

An analysis of the total cost of ownership should be performed to establish the optimum balance between the costs of dedicated and commercial solutions.

From 4G to 5G

The term 5G is receiving a great deal of interest in both the technical and popular press and it would be tempting to conclude that 4G is soon to be superseded by 5G. However, 5G is in fact a basket of standards, some of which are aimed more at the future Internet of Things (IoT), automotive applications and other sectors with very high numbers of devices.

---

[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.

In the frequency bands likely to be utilised by Public Safety, 5G will be an evolution of 4G. It is planned that Public Safety functionality will be included in the 5G standards which should result in an easier transition from 4G to 5G in the future.

Public Safety users have less access to broadband technology than the criminals and terrorists that they pursue. It is vital that mobile broadband services are provided to Public Safety users as soon as possible. Solutions based on the currently available 4G LTE technology will provide staff with much needed applications and information in the short term. If, at a later point in time, a migration to 5G seems to be beneficial for critical users, a necessary migration path can be planned and undertaken, when respective 5G systems become available.

Will the MNOs take on the challenge?

Current experience shows that, in most cases, MNOs are attracted by the possibility of a significant group of additional users to add to their customer base. However, providing the necessary functionality, coverage and resilience is not a trivial or low cost exercise for the MNO. Similarly, the responsibility for providing safety of life services may not sit well with an MNO's business model.

It should not be assumed that MNOs will wish to take on the responsibility or costs associated with the provision of service to Public Safety users. Early engagement with potential MNOs is strongly advised.

Sharing

There are a number of options for sharing spectrum, sites and infrastructure with MNOs to mitigate the high cost of a dedicated network.

Suitably qualified staff should review these possibilities with the MNOs before any firm decisions are made.

Who should be involved in the decision

Providing a mobile broadband capability to Public Safety users, whether for voice, data or both, will be a significant and costly undertaking. There will be many organisations that will need to be involved in the process. In addition to the Ministry of Interior, who will probably be the lead organisation, the Ministry of Defence may also have common interests. With the enormous cost of creating digital network infrastructures it makes sense to engage with all government departments that could share some of the costs. Transport and Utilities, for example, are two significant users of Critical Communications. The Ministry of Finance will, of course, be heavily involved in all issues to do with the funding of such a project.

It is also important to engage with other relevant organisations including: The Regulator (over matters of spectrum), the national representatives in the international standards bodies (ETSI, 3GPP, etc.) and the Industry who, together with the standards bodies, have joint responsibility for ensuring that the necessary technology and equipment are available.

Those responsible for the provision of Public Safety communications capability are strongly urged to engage early with the relevant ministries, the regulator, the standards makers and with industry. These organisations need to be involved in the development of a project to update the existing Public Safety communications system. Maintaining such dialogue is essential.

Conclusion

A decision on why to make Broadband services available to Public Safety users will need to be taken in an environment of increasing threats from natural and man-made disasters. Terrorism, in particular, is an increasing problem and, with incidents in Brussels, Paris, Nice and elsewhere, the threat level for governments in mainland Europe is becoming a major concern. Despite the appalling nature of these incidents, they are good examples of why the investment in Public Safety communications is so important.

Clearly, the decision to use a combination of one or more dedicated, owned networks along with service provided by a commercial network operator is a complex matter with many issues to consider. Spectrum is critical to ensure that the options remain open and it is essential that sufficient spectrum at 700MHz is made available: either through allocation or regulation. If governments are not willing to dedicate spectrum for Public Safety purposes, or implement new regulation, then the natural consequence of this decision is that market forces will prevail and Commercial Operators will have a strong position in negotiations. That could be to the detriment of Public Safety.

Governments are urged to take due consideration of the needs of Public Safety organisations. This can be achieved by taking positive decisions that will ensure those that are tasked with the safety and security of our citizens have the appropriate tools to do their job.

Contents

Foreword

The Critical Communications market is heading for a major change in the delivery of information to and from Public Safety officers on the street. Whilst voice communication is well satisfied by digital technologies such as TETRA, Project 25 and Tetrapol, the demand for broadband services to mobile devices, both handheld and in-vehicle, is increasing rapidly.

It is clear that LTE is the preferred technology for enabling mobile broadband for Critical Communications users and the TCCA is driving the standards bodies to add Critical Communications functionality and use cases to the LTE standard. This will ensure that Public Safety users have the right tools to undertake their increasingly complex role and that resources are used in the most efficient manner possible.

The delivery of 4G LTE (and future 5G) services to Public Safety users can be undertaken in a variety of ways depending on local priorities, cost/performance balance and the willingness of, and business opportunities for, cellular Mobile Network Operators (MNOs) to engage with the current providers of critical communications services.

This document has been produced by the TCCA as a publicly available document aimed at Governments, Regulators, senior Public Safety officials and other professional users for whom mobile communications is a critical element in providing safety services and in protecting critical national infrastructure. Its purpose is to assist those faced with decisions in the provision of mobile broadband services by exploring some of the primary options for such delivery and laying out the advantages and disadvantages of these options. Whilst the document is primarily aimed at the European Public Safety community it is recognised that other user groups that rely on Critical Communications are facing similar challenges and may also find this document relevant.

This document can be read in isolation but forms the third in a series of documents looking at the provision of Mobile Broadband services. These additional documents are 1) 'The Strategic Case'[3] that offers reasons why investment in Mobile Broadband services is justifiable for Public Safety and other Critical Communications users and 2) 'Delivery Options'[4] which explores a variety of methodologies for making broadband services available. Both of the previous documents are available from the TCCA. Contact details can be found on the web site[5].

[3] The Strategic Case for Mission Critical Mobile Broadband is available from the TCCA website.
See: http://www.tandcca.com/fm_file/mcmbb-strategic-case-v1_0-pdf

[4] The Delivery Options paper is available from the TCCA website.
See: http://www.tandcca.com/fm_file/mcmbb-delivery-options-v1-0-pdf

[5] TCCA web site can be found at www.tandcca.com

Introduction

Those operating in the world of Critical Mobile Communications will be aware of the growing demand for mobile broadband data services suitable for a Mission Critical communications environment. In the 21st century it is regrettable that citizens regularly use more advanced technology than our emergency responders. To ensure that Public Safety users are able to perform their duties in an efficient and effective manner, urgent steps are needed to bring broadband data services, new devices and Public Safety applications to those that are responsible for the health, safety and wellbeing of the citizens of this world. When the standardisation of Mission Critical voice functionality over LTE has been completed and is proven in the field, then it will make economic sense to transfer voice services from the existing mission critical voice networks as they become time expired. Until such time as 4G and 5G networks are proven to be truly Mission Critical, today's voice networks will be the only mission critical service available.

As will be discussed later, the primary urgency relates to securing sufficient access to spectrum. The opportunity to do so will be short lived.

The Critical Communications Broadband Group (CCBG) is a working group of the TCCA and is tasked with driving the development and adoption of common, mobile broadband standards and solutions for users who operate in a mission critical or business critical environment. These standards are part of the 4th generation of mobile communications (LTE Advanced) and future 5G standards. In so doing, the CCBG has formed relationships with a wide variety of user and operator groups that have common aims. It is working closely with the Standards Development Organisations relevant to this requirement, including ETSI[6], 3GPP[7], ATIS[8] and OMA[9].

The CCBG's goals are to enable all Critical Communications users to access their information systems and applications, reliably, and at broadband[10] speeds, on their professional mobile devices, wherever they are and whenever they have the need.

The creation of the necessary standards and technology is only part of the solution. Delivering services that take advantage of such capabilities in a timely, cost effective and affordable manner is also a significant task. This paper specifically addresses how coverage and capacity can be provided by a combination of commercial cellular networks along with networks owned and operated by a Public Safety operator. The balance between these two methods of service provision will depend on the specific requirements of each country. This "Hybrid" option is considered to be the most likely delivery option for the foreseeable future.

6 ETSI – European Telecommunications Institute. See www.etsi.org

7 3GPP – 3rd Generation Partnership Project. See: www.3gpp.org

8 ATIS - Alliance for Telecommunications Industry Solutions. See www.atis.org

9 OMA - Open Mobile Alliance. See: www.openmobilealliance.org

10 For the purposes of this document, mobile broadband is defined as data with a rate above 384kbit/s (based on UMTS being a broadband service)

Context

Since the introduction of text messaging services in the mid 1990s, society has transitioned from communicating solely by voice to using data services (email, text messaging, social media, etc.) for passing messages to others. Whilst this transition may have also impacted on Public Safety communications, in most emergency situations, voice continues to be the primary form of communication. That principle is likely to remain the case for many years to come due to the inherent speed that voice messages can be passed. However, the younger generation of police officers, paramedics and fire and rescue personnel are more comfortable than ever in communicating via portable laptops, tablets and smartphones. Sharing messages and images, uploading and exchanging video clips are now considered the norm. In time it is likely that such usage will become so fundamental to their daily operations that it will become 'Mission Critical'.

The premise of this document is that the demand for mobile broadband capability is already established. In fact, many user organisations are already using mobile data services in day to day operations, some with dedicated systems (e.g. MoI Qatar, UAE) but often also using commercial services (e.g. Belgium (ASTRID), UK, Finland and others). There is much anecdotal evidence of personnel using commercial networks unofficially – which can present many legal, privacy and procedural challenges for government entities.

It is assumed that the business case for the implementation of mission critical mobile broadband services has already been made. It is further assumed that the internationally agreed standard of LTE, or more specifically the LTE-Advanced Pro specification, (Release 13 onwards) is to be employed in providing mission critical mobile broadband services to mobile resources. Public Safety functionality is being incorporated into the core LTE standard[11]. It should be understood that the functionality for Public Safety users will be different than that which is currently available in TETRA networks. Those responsible for the provision of new broadband services need to take care that 4G and 5G technologies will meet the needs of Public Safety users as these standards and services become widely available.

Having made these fundamental decisions the responsible political institutions, Critical Communication network operators and end user representatives will need to consider the most appropriate and cost effective solution for delivering mobile broadband services. Such solutions will need to be provided whilst maintaining an effective mission critical mobile voice communications capability based on existing Public Safety systems in service, until both mission critical voice and data services are provided by the LTE broadband data network.

[11] See Appendix A for further details on LTE standards for Mission Critical users

Scope

The mobile communications industry is working towards the implementation of mission critical voice services using LTE as a bearer. However, many Public Safety organisations have concluded that transferring mission critical voice to LTE is a step too far[12] until such time as the following issues have been resolved:

- the definition of Mission Critical (MC) or Critical Communications features is completed within 3GPP. The current Rel13 provides the baseline for mission critical use, with additional Critical Communications services planned to be added in Release 14. As stated above, it should not be assumed that all functionality available in existing TETRA systems will be directly replicated in LTE. Some functionality may be provided in a different way
- the infrastructure and device vendors have implemented (or committed to implement) the above standards in commercially available equipment
- that the MC features such as group based calling (for voice, data or video) are proven, including demonstrations of interoperability between manufacturers
- Mobile Network Operators (MNOs) have deployed (or committed to deploy) the necessary hardware and /or software release to make the MC features required by Public Safety users
- MNOs have proven their ability and commitment to deliver Public Safety service levels, providing the reliability, coverage and resilience that is essential for these users

The more immediate need is to enable Public Ssafety's mobile users to make widespread use of broadband data services. Applications for this capability will include:

- Video from the scene of an incident back to command and control centres
- Video clips from CCTV to officers on the street
- Email, social media and other text based services to be used whilst on the move
- Form filling and report writing direct from the scene of an incident
- Access to central databases such as criminal person records, vehicle records, premises records, building key-holders, patient records, building plans etc.
- and many more

In the immediate future it is likely that the above functionality will be considered a highly beneficial addition to existing critical voice communication. As long as the use of mobile data is considered supplementary to mission critical voice services then it may be acceptable to use a 'best endeavours' service such as that currently offered by the MNOs. However, as these applications become used on a routine basis, officers and command staff will begin to rely on these capabilities. Operational procedures will be modified to fall in line with actual operations. These procedures will make use of the enhanced capability and richer information that mobile broadband applications can provide.

[12] "The VIRVE network must remain in operation longer than originally anticipated – until the 2030s." – Strategic Guidelines for Critical Communications (Virve).

Belgium and the Netherlands are upgrading their existing TETRA voice networks.

As a result, this capability will inevitably become classed as genuinely mission critical. At this point, mobile data services will need to be supplied as a mission critical service and appropriate resilience, reliability and coverage will need to be in place.

Whilst a dedicated government owned and operated nationwide network should be able to meet all the essential criteria for mission critical operation, it is generally considered too costly. In addition to the high CAPEX required, lack of spectrum and insufficient demand are also examples of inhibiting factors. Similarly, it is possible to rely solely on a commercial MNO for all critical mobile communications. Indeed, the UK and South Korean governments are both pursuing such a solution. However, at this time, many of the Public Safety operators, that are members of the TCCA, consider this to be a high-risk strategy. The UK Government's National Audit Office issued a report with similar views[13]. Therefore, neither fully dedicated, nor fully commercial solutions are addressed within this White Paper.

The purpose of this document is to explore how a dedicated mobile broadband service, owned and/or operated by an emergency service network operator, can be combined with that of a commercial cellular mobile network to provide an acceptable level of service at an affordable cost.

It is important to understand that previous analyses of the transition to LTE based networks have looked at 'Hybrid' networks that integrate TETRA Voice (or other Public Safety voice networks) combined with LTE Data into one solution. This paper uses a different definition of 'Hybrid' and concentrates solely on a combination of a dedicated, 'Public Safety owned and /or operated' network with a commercial MNO service to provide end users with a mobile broadband capability. Voice services are outside the scope of this paper, although it should be noted that these are being standardised in 4G (and 5G) along with data and video services. It is reasonable to assume, therefore, that 4G and 5G LTE networks will become capable of carrying mission critical voice services at some point in the future.

[13] See https://www.nao.org.uk/report/upgrading-emergency-service-communications-the-emergency-services-network/

Mission critical service – a quick reminder

Commercial mobile network operators clearly have a role to play in the future provision of Public Safety communications. However, it is important to be aware of the fundamental differences between Public Safety communications and standard commercial services when considering the use of commercial carriers for Public Safety traffic.

Public Safety staff have relied on mission critical mobile communications to carry out their work for several decades. They utilise such communication in a very different way to the users of mobile cellular services. Public Safety staff work in groups and therefore need to communicate in groups, especially if they are to operate in a safe and efficient manner. 'Push To Talk' (PTT) enables almost instant communication between individuals and with groups, without having to wait for dialling and calls to be set up. This is vital in fast moving emergency situations.

Group based voice communication is a fundamental requirement that must be provided in any future communication system, as is the ability of a despatcher to manage the communication flow and interrupt where necessary. It is evident that group working is also applicable to data communication. The ability to send a picture of a missing child or a wanted person to a large group of officers simultaneously would be an example.

The Police and other Public Safety users also rely on secure communications. They routinely use encryption to ensure radio traffic, including voice, personal data and signalling, (e.g. user identities) remains confidential. As sensitive information of a personal nature will be carried over future data communications, full end-to-end encryption will be equally important for many applications/communications, and it is essential that commercial carriers are able to handle such traffic on a routine basis.

There are many additional services that are utilised by Public Safety users that are unique to their operations. Such services include –

- emergency pre-emption where existing traffic is interrupted in order for emergency communication to get through immediately
- mutual authentication to ensure that only legitimate users are allowed access to the network (and crucially to prevent "spoof" networks from disrupting communications)
- multiple priority levels that are used to ensure senior staff can manage resources, especially at a major incident
- Dynamic groups that enable special groups to be created temporarily to deal with a particular event or incident
- and many others

Such features need to be available on any future communications network.

3GPP, the technical body that is responsible for the 4G LTE and future 5G standards, is incorporating Mission Critical (Public Safety) functionality into current and future releases of the LTE standard. This is very important for any future transition to the use of 4G and 5G technologies by Public Safety staff. However, the inclusion of such functionality does not, by itself, make commercial cellular networks suitable for mission critical operation.

It is a fundamental requirement that networks used by Public Safety personnel have a very high availability. Loss of service for even short periods of time can put lives at risk, especially when the service is used for despatching ambulances and fire crews.

Public Safety networks are mostly designed with built in resilience using techniques such as overlapping coverage, redundant radio equipment, dual routing of backhaul and battery backup power supplies. For high traffic sites, the latter are often supplemented with additional forms of electricity supply such as diesel generators, solar charging and fuel cells. These techniques ensure that the service remains available even when system failures occur.

Today, commercial networks are not designed to such a high standard of resilience - often due to the high costs of providing these capabilities. Therefore, where commercial networks are used to provide Public Safety services, upgrading or 'hardening' of the network will almost certainly be necessary. Alternatively, emergency plans have to be in place for a quick setup of deployable network elements, wherever and whenever critical communications services are not available, but urgently needed in specific geographic regions.

Finally, there is the issue of radio coverage. Incidents can occur anywhere in a geographical region, including in tunnels, underground car parks, and deep inside large buildings. Often, commercial cellular services are already present inside large buildings such as airport and rail terminals, sporting stadia, etc. which is beneficial.

Small towns and villages, as well as open rural areas, tend not to receive the radio coverage from commercial networks that urban areas receive. In-building coverage is becoming increasingly important in many countries and the lower frequencies typically employed by Public Safety network operators make in-building coverage easier to achieve. It is unfortunate that the coverage quoted by cellular operators does not follow the same rigorous definition as is typical of public safety networks[14]. Where commercial carriers are being considered, then an agreement needs to be reached on the definition of coverage, how it is to be specified and how it is to be measured.

It is essential for Public Safety staff to have a highly reliable communication service with an auditable coverage over the operational area. Group working and despatcher control are also fundamental. It should not be assumed that mobile commercial cellular networks are capable of meeting those needs. Where commercial networks are used for carrying mission critical traffic, guaranteed coverage, capacity, resilience and reliability service levels are paramount.

[14] In an article in the Financial Times (23/11/16 - Ofcom pushes boundaries on UK mobile coverage), the Chief Executive of the UK EE network admitted that the industry, including his own company, had been "misleading" customers with claims about how far each network reaches.

What are the implications of Hybrid?

Let us assume that the Public Safety operator has some spectrum – but not enough for the capacity necessary to cover the busy hour, major incidents or special events. The Public Safety operator can build a service with a dedicated network in addition to taking service from a commercial network operator. This may be supplemented by utilising deployable systems[15] in areas of low traffic demand. Such an arrangement requires that the Public Safety operator controls the system at both Service and Network levels[16]. The Public Safety operator also needs to have the skills necessary to interact with MNOs. This includes requesting enhancements to the network, advising the MNO of problems, negotiating and managing Service Level Agreements (SLAs), etc. The overall solution is likely to differ significantly from country to country.

Hybrid solutions can be seen as the most flexible route, with most options to choose from - options that can fit whatever spectrum and funding scheme a country finds itself in. However, it will not be an easy way out. The dedicated network component will need to be designed, procured, built and operated, whilst commercial services will need to be carefully specified and procured as well as building the necessary relationships with one or more MNOs. In addition, the Public Safety network operator will need to make the services and applications seamless to all users.

There will be issues involved with network management, fleet maps and roaming between dedicated and commercial networks. Subscriber management may be more complex than is experienced in a single dedicated network. Threats to security will be different with a hybrid network solution. Operators and users should be aware that LTE security will be split between the network level and the MCPTT / MCDATA / MCVIDEO application level which is very different from the way security is achieved in TETRA and will therefore need to be assessed carefully in order to avoid additional security clearances of MNO staff.

Whilst dedicated networks provide a Public Safety operator with greater certainty over capacity and resilience, commercial networks potentially offer a faster route to the provision of broadband data services and a less capital intensive start-up cost. A combination of these two alternatives (i.e. a Hybrid Solution) may well be a good compromise and could be an early step on the way to a fully dedicated network, if that is the ultimate goal. For smaller countries, a dedicated network may still be the most cost effective option as small nationwide networks may be more economic than the complexity of hybrid networks.

Benefits

In most European countries, and many other parts of the world, 4G LTE commercial networks are already in existence or being rolled out. In many cases, they are being used to provide some non mission critical services to Public Safety organisations. Typically, these networks are being deployed in urban and sub-urban areas. Such areas tend to be where public safety traffic is at its highest and where data services are routinely used.

[15] Deployable Systems refers to mobile infrastructure equipment that can be transported to the scene of an incident and made operational quickly to provide temporary radio coverage

[16] A full solution consist of applications, network switching (Core), backbone transmission and base stations (RAN)

As a result, Public Safety network operators can implement broadband data where the need is greatest and in the shortest time by utilising commercial services.

Interoperability with one or more commercial networks will also greatly improve the availability of Public Safety communications which, assuming the commercial networks have been hardened, may result in higher availability levels than could be achieved by dedicated networks alone.

Where coverage is not currently provided by the commercial MNOs, a Public Safety operator can either deploy its own dedicated network or negotiate additional coverage with one or more MNOs. It may be possible to negotiate a mutually beneficial arrangement with the commercial MNOs such that spare capacity from the dedicated network can be offered to the commercial operator, thereby enhancing the commercial service. Where simple coverage extension to an existing commercial network is being considered, this will be for non mission critical service only, as Mission Critical functionality and resilience will not be included.

Where a Public Safety Operator wishes to take advantage of commercial services, a formal tendering process will be required to find the most suitable MNO against a defined service level including coverage, capacity reliability, functionality etc.

As an alternative to installing permanent dedicated capacity, a Public Safety operator may choose to hold deployable mobile infrastructure equipment that can be taken to the location of incidents as and when necessary. This avoids the cost of expanding the ground based network; but the cost of deployable networks will include having personnel and equipment on standby and also the cost of providing backhaul which may require satellite licences or other transmission costs. The delay in moving deployable infrastructure to an incident also needs to be considered.

For capacity reasons, commercial mobile networks utilise small cells in urban areas to ensure that a large number of subscribers can be served even during busy hours. The additional traffic generated by Public Safety users for normal, ‘business as usual’ operations can usually be accommodated without the need for the Mobile Network Operator to provide additional capacity. As a result, Public Safety users can negotiate competitive prices for the data traffic used.

During major incidents or events, the capacity of commercial mobile phone networks can be put under strain. Under these circumstances, the additional capacity of a dedicated network can ensure that Public Safety users are still able to maintain required critical communications, despite the high traffic encountered on the commercial network.

Whilst every situation will have different economics, it is highly likely that a hybrid solution will initially incur lower costs than implementing a fully dedicated network. Operational costs, however, are likely to be higher in the long term as service charges will be incurred for the life of the contract.

Disadvantages

Any solution that employs one or more commercial networks will result in the users being reliant on a commercial entity for mobile communications. There are risks associated with the use of commercial providers including:

- Loss of service should the MNO become insolvent
- MNO could be subject of a takeover from an unfriendly investor
- If the MNO decides that the provision of Public Safety services is no longer financially attractive, or that the capacity would be better utilised for commercial customers, then the service could be withdrawn. Contract penalties for this may be less than the financial gain for the MNO

The special features needed by Public Safety users will need to be tested thoroughly and introduced to dedicated and commercial networks. Such features cannot be fully utilised until available in both networks.

The standards body (3GPP) is developing standards for Public Safety security within LTE networks. However, with traffic being carried across Hybrid networks, security will be an important issue and needs to be understood. A review of security mechanisms will be required.

The commercial networks that are supplying services for Public Safety must be hardened to be more resilient and reliable than normal commercial services typically demand. This may be a significant cost to the commercial operator which would almost certainly be passed on to the Public Safety users.

Whether or not a Public Safety Operator uses a dedicated network or a commercial MNO to provide mobile communication services, management of that network and its subscribers will be required. By using a combination of dedicated and commercial networks, the management task will be greater as two independent and diverse networks will need to be managed and coordinated.

The performance of any commercial MNOs involved in the provision of Public Safety services will need to be monitored and managed against a rigorous Service Level Agreement. Such monitoring and associated penalty calculation may themselves require significant administrative resources.

A hybrid network that provides service using a combination of separate networks will be more complex than using a single network, either dedicated or commercial. In order for users to have a seamless experience, roaming between the two networks will be necessary. This may require additional processes to ensure that the subscriber unit correctly chooses the optimum network. Such processes are included in LTE. Similarly, organising fleet maps (groups of radio identities that enable user groups to be managed) will be more complex with multiple networks.

Where deployable systems are utilised to provide temporary coverage for an incident, it will be necessary to have equipment distributed at suitable locations, along with trained personnel ready to deploy them. This will be a management and financial overhead. Note - this will also apply to future dedicated networks if coverage is insufficient to meet the needs of Public Safety users.

In order to ensure a seamless experience for end users, those responsible for Public Safety communications will need to ensure that user functionality is fully compatible between commercial, dedicated and deployable infrastructure.

Hybrid networks can offer significant cost advantages and are likely to enable Public Safety users to take advantage of mobile broadband services more quickly than by building dedicated networks. Interoperability with one or more commercial networks will also improve the availability of PPDR communications. However, it should be recognised that many commercial MNOs do not have the experience or understanding of the needs of Public Safety users. It is strongly recommended that early engagement with MNOs in your country be undertaken so that both parties understand the issues described here. A formal 'Request For Information' (RFI) may be a suitable mechanism to achieve this.

Spectrum

All radio systems require spectrum in which to operate. Spectrum is a finite resource and, with the increasing demands of a mobile society, the available airwaves are under real pressure. Governments will need to balance the revenue potential from auctioning spectrum against the importance of ensuring the Public Safety and Rescue community (PPDR[17]) has excellent mobile communications, especially in the increasingly turbulent society in which we all live.

Why is control over spectrum so important?

There are only three parameters available when discussing mission critical service:

- having control over spectrum
- having funding available to buy the service you need from the market
- exercising government regulation

If commercial operators are not willing to provide the required service, and regulation in a much liberalized sector is not an option, then Government must retain control of specific spectrum or accept the consequences of inadequate control over the service provided by commercial operators.

The choice of spectrum needs to be coordinated internationally to allow interoperability and to build an ecosystem of industry support based on an expanded market for compatible products.

According to the international and European regulators such as ITU[18], ECC and the EC, spectrum serving Public Safety operations has to be found in the 700 MHz band, but it is up to each country to determine how and how much. In many countries, there is an immediate opportunity to secure sufficient spectrum for Public Safety operations and such an opportunity may not occur again for a very long time – 10-15 years.

Public Safety agencies need to be in control of their mobile communications. By exercising control over traditional narrowband voice services, public safety organisations have benefited from the best voice and data services they have ever had. This has drastically reduced communication problems in all areas of operation and increased overall efficiency and effectiveness. This is particularly true in dealing with major incidents and public order situations.

Public Safety organisations are mandated by law to deliver an extremely high standard of service to society, and Public Safety staff are employees of the state who need a safe work environment. The view of much of the Public Safety community is, that it is essential for government organisations to control enough radio spectrum in order for them to deliver critical services to society.

What are the spectrum options?

Following the recent decision in CEPT/ECC and the EU, there are two options where spectrum can be allocated: The safe decision - which is also the most controversial - or the un-certain decision.

[17] Public Protection and Disaster Relief is a term favoured by the European Regulators. It includes Public Safety but also covers those specialising in major disasters.

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

Spectrum administrations are typically concerned with the commercial use of available spectrum and competition between commercial operators. The belief is that those who are willing to pay the most for spectrum will use it most effectively.

The safe decision is to allocate spectrum within the spectrum range 703–736MHz paired with 758–791MHz known as Band 28. A few countries have already auctioned, or have solid plans to auction, the whole of band 28 to commercial use without considering the needs of Public Safety services. As a result, all that they will have left will be that which is known as Band 68[19] and potentially 2x3 MHz which is part of band 28 but hasn't been auctioned off. The problem with band 68 is the un-certainty with respect to availability of devices. The very stringent technical conditions applied, coupled with a small market that moves slowly, do not make this market opportunity appealing to chip vendors. Furthermore, the same stringent technical conditions will mean that a government business case for use of this band is almost non-existent. The safe decision is clearly band 28, but requires a political instruction to the spectrum administration.

As mentioned above, a spectrum administration has a few options - either allocate spectrum to Public Safety in band 28 or use regulation to mandate Public Safety service from commercial operators. If the auction of band 28 has not yet taken place, specific conditions should be included in the auction process. If an auction has taken place, future regulation will, in theory, still be possible but in practice this is usually not the case. Under these circumstances, the allocation of band 68 together with the 2x3 MHz above band 28 is the only option left.[20]

It is possible that Mobile Network Operators will agree to meet the needs of Public Safety users including additional coverage and Public Safety functionality. However, the responsibility for ensuring system availability during major natural or man-made incidents and the effect on company image if there is a failure to do so, may discourage MNOs from providing Public Safety services at an affordable cost and in a stiff penalty regime.

Having agreements with MNOs might also include a guarantee for capacity under certain situations, where an MNO promises to temporarily vacate a certain band by moving all normal users to other bands - i.e. from 700MHz to 800MHz or 1800MHz. That would leave capacity free for Public Safety users in the 700MHz band. Such agreement would still require the core switching to remain fully operational even when the Radio Access Network (RAN) becomes overloaded. It will also require the MNO to be able to perform such moving or switching of commercial users in a matter of minutes if not seconds - even if the subscriber equipment (handheld radios) is not registered on the network.

It was relatively clear, until mid-2016, that 4G LTE would be implemented in the 700 MHz band. Some European operators and telecom suppliers now have firm plans to use the 700 MHz band as a "pioneer band" for 5G and this is supported by the European Commission. It is, however, important to note that 5G in the 700 MHz band will carry Public Safety requirements over from 4G. Implementing 4G - LTE networks now should result in an easier transition to 5G.

[19] Public Safety Band 68 is a small section below band 28: 698-703MHz paired with 753-758MHz. There are restrictions proposed to avoid interference with TV channels and these may limit the usefulness of the band.

[20] For further information on spectrum for Public Safety see: http://www.tandcca.com/fm_file/a-review-of-the-spectrum-status-for-broadband-ppdr_july2016-pdf

Public Safety operators should engage with their national MNOs at the earliest possible opportunity and present them with the required Public Safety Service Level Agreements and associated legal frameworks. The discussions should also cover the functionality that is required in the 700MHz implementations. The outcome of such discussions should determine if spectrum allocation or regulation is required.

If governments are not willing to dedicate spectrum for Public Safety purposes, or implement new regulation, then the natural consequence of this decision is that market forces will prevail and Commercial Operators will have a strong position in negotiations. That could be to the detriment of Public Safety.

Commercial MNOs may have access to significant bands of spectrum. Of course, these have differing characteristics in turns of coverage and capacity, and these serve the entire user population, consisting of large numbers of citizens as well as Public Safety users. How a network manages congestion, and the competing priorities between the different users of the network, will be crucially important in meeting the SLAs demanded by Public Safety users. At least one MNO[21] has agreed to prioritise use of the 800 MHz band for the Emergency Services if operational circumstances require it. Other ways and means of achieving the required SLAs should also be considered.

Recommendation for auctions in band 28:
The Regulator should only auction 703-713 and 723-733 MHz (paired). Keep the 713-723 paired under government control. When the winners of the two slots are known - run a second auction where the government will offer to share its spectrum with one of the two winners on conditions supporting PPDR (Public Safety) services, resilience, availability and coverage. The benefit for the winners is that they will then be able to run a 2 x 20 MHz service with double speed and be in a better competitive situation. If one of the winners is willing to do so then the Public Safety requirements will be satisfied. If not, the government still has an option open to build a network that meets the requirements of Public Safety.

Where are you now?

Experience shows that planning future networks typically takes many years. Public Safety networks in Europe are at many different stages. For the purposes of this document we have considered the two extremes for the lifetime of existing Public Safety voice networks. We can classify them in two main categories as follows:

A. Today's network has a limited lifespan left – either due to age of equipment / lack of continued support or end of contract period. A decision on the way forward needs to be taken as soon as possible.
B. Today's network is either relatively new or has recently been upgraded and has more than 10 years left.

[21] EE (owned by BT)

In the latter case it would not make sense to replace the voice network but it is likely that additional mobile broadband capability will still be needed, either now, or in the medium term.

This capability would typically be provided by commercial services along with dedicated networks for high population areas and facilities that are at high risk; such as airports and critical national infrastructure.

It is easy to fall into the trap of delaying a spectrum allocation to Public Safety, as an existing mission critical service is available (TETRA, P25 etc.) and mobile broadband data is being used from commercial networks – but that is not at mission critical level. A spectrum opportunity is here and now and will not be on the ITU agenda again until 2023 at the earliest, with availability around 2030.

Where the existing voice network is reaching the end of life then decisions will need to be taken about how ongoing voice services will be provided alongside mobile broadband capability. The only option is to replace today's voice networks if sufficient spectrum for broadband is not allocated or if the MNOs are not willing to provide mission critical service.

What are the key factors influencing a decision?

Implementing a Broadband data communications network for Public Safety personnel is not an easy decision. As already noted, there are many factors affecting the decision including costs, political issues, technical considerations and the availability of spectrum in which to operate such a network. The decision will be different for each administration and is likely to require a considerable amount of time and resource to achieve an acceptable result.

This paper cannot offer a simple formula that will be relevant across different countries and different regions. However, below are some key issues that should be considered in the decision making process.

Spectrum

Probably the most significant influencing factor affecting the balance between "owned and operated" vs "taking commercial service" is the availability of suitable spectrum and this has been covered in detail above. Without access to LTE spectrum there is little opportunity for a Public Safety network operator to build their own infrastructure regardless of the need, the politics, or the funding issues. However, where spectrum access is available then the following elements of the decision making process can be addressed.

Political considerations

Security

Security is covered in more detail later, however, for many Governments, security is a significant concern and may outweigh many other considerations. The political situation may justify the increased capital outlay that dedicated networks typically incur.

Ownership

Public Safety communications are essential for the health, safety and security of our citizens. Cellular operators are generally fully commercial businesses that are subject to normal commercial pressures and practices.

The willingness to become reliant on commercial providers is highly variable, with some, like the UK, being comfortable with placing their trust in fully commercial, third party operators, despite the need to carry communications involving highly sensitive information. One could argue that the decision to pursue this philosophy has proven to be correct, with the UK nationwide Public Safety voice network, now known as Airwave, having been bought and sold on several occasions. From 2007 until 2015 ownership of the network was with Macquarie in Australia and it is now owned by Motorola Solutions of the USA.

However, others are more cautious in following this route, with many countries preferring to keep ownership of their mission critical communications infrastructure, either through close ownership, such as C2000 in the Netherlands, or via a pseudo independent company such as the Government owned Astrid company in Belgium.

Hybrid solutions, as defined above, are based partly on government owned infrastructure and partly by taking service from commercial network operators. As mission critical data communications become more heavily relied upon to carry Public Safety traffic and, as that traffic becomes more significant and more sensitive, governments will need to make a conscious decision as to whether they are comfortable with independent network operators being responsible for data communications; some of which may have issues of national security.

As in the case of the UK, it is increasingly likely that such networks may be owned by companies based anywhere in the world. It is common for ownership of commercial cellular businesses to be the subject of takeover from companies of different nationality. It is possible that the carrier of Public Safety services could become owned by organisations in countries with which relations are not considered friendly. This may cause concern to Governments.

In addition to the ownership of the network there have also been concerns about infrastructure equipment being supplied by countries that are not considered to be acceptable. The US, in particular, has expressed serious concerns about the influence of suppliers from certain Far Eastern countries. In particular there are concerns that the complex nature of modern telecommunications infrastructure equipment may have software embedded that allows 'back door' access for non-friendly governments to intercept communications. Whilst such concerns appear to be less prevalent in some parts of Europe, the threat should at least receive consideration.

Governments will need to give careful consideration as to whether they are prepared to relinquish ownership of Public Safety communications and pass that to a commercial, possibly foreign owned, company.

UK ESN

Despite the above considerations, it is worthy of note that the UK Government has decided to place its entire mission critical mobile voice and data communications with one Mobile Network Operator supported by a 'User Services' supplier and a 'Delivery Partner'. The issues listed above have therefore not dissuaded the UK Government from pursuing such an arrangement. Other countries may take a different view.

It is also noteworthy that the UK Governmental audit and review body, the National Audit Office, has recently (September 2016) released a review of the ESN project which expresses serious concern about the programme which they believe "remains inherently high risk"[22].

Security

Public Safety communications carry a variety of traffic classes thus requiring different security levels. Much of the traffic will be of a day to day operational nature. However, some of the traffic will be sensitive information that is personal to members of the public such as name and address, previous convictions, history of abuse etc. Some communications will be confidential to the initiating organisation. i.e. details of upcoming operations, despatch of officers to a 112 call etc. Finally, some of the information may have national security status such as details of terrorist activities, serious crime information etc.

[22] See: https://www.nao.org.uk/report/upgrading-emergency-service-communications-the-emergency-services-network

With such sensitive information to be carried across a network, some Governments may prefer to keep control over some, or all, of its voice and data networks. However, it is important to note that the standards body that is responsible for LTE (3GPP) has included a number of security mechanisms into current releases and will continue to add further security mechanisms into future releases of the LTE standard.

Whilst there are many security mechanisms specified in 3GPP for a LTE network, additional mechanisms are being standardised in the MCPTT application layer to better support critical communication users. However, the split between Network level and MCPTT application level is different from the way security is achieved in TETRA and will therefore need to be assessed and understood in order to avoid having to provide security clearances of MNO staff.

Telecommunications security deals with four criteria: availability, confidentiality, integrity and traceability. In order to design a secure telecommunications system, these four criteria are taken into account early in architecture work. For each criterion there are different means and techniques to secure a telecommunication network or service. Owning the entire network and controlling all of the subscriber equipment is one solution but this can be unmanageable and lead to unaffordable costs. This is particularly true when considering mobile networks with thousands of pieces of equipment which need to be spread over wide areas.

3GPP has developed different solutions to meet these requirements. For instance, application identities are not seen by commercial operators when their networks are used and it can be ensured that Public Safety officers cannot be tracked. The interoperability between deployable networks fixed or mobile will provide a way for Public Safety practitioners to be fully independent of any commercial company if necessary.

Each government organisation will have to study what is provided by the standard, what the additional needs are likely to be, bearing in mind new threats, and how the standard can be implemented.

Funding

Infrastructure Costs

By definition, a hybrid solution will require the purchase, installation and ongoing running costs for any part of the network that is owned and operated by the Public Safety operator. Obtaining funds for major infrastructure projects in the current economic climate is likely to be difficult. Using commercial cellular services reduces the need for major capital investment, although some initial investment will be required to set up the management equipment and processes for any future communications network.

Capex vs Opex

Although Public Safety will form a relatively small part of the overall subscriber base for a Mobile Network Operator it is still likely to be a significant potential revenue stream for the MNO. The provision of hardened sites, additional coverage and Public Safety specific functionality will result in additional costs for the MNO. However, it should still be possible to negotiate preferential terms bearing in mind the opportunity to offer the MNO a significant number of additional users, and, in some cases, access to additional assets such as radio sites and backhaul.

A balance will need to be struck between the capital outlay required for Public Safety owned infrastructure and the ongoing costs of using a commercial service. Regardless of the balance between owned infrastructure and commercial service there will be ongoing costs associated with the management of the network and mobile devices, permitted applications etc.

Will the MNOs take on the challenge?

For a commercial Mobile Network Operator to provide Public Safety services it will be necessary for the MNO to make substantial investment in their network in order to provide the essential coverage, resilience and functionality that is typically required by Public Safety agencies. The LTE standards body (3GPP) is in the process of adding some essential functionality to the standard (See Appendix A). Whilst there is no obligation for any MNO to incorporate such additional functionality into its network, the additional demand from Public Safety may encourage MNOs to further invest in their network.

Whilst the evidence so far suggests that there is an appetite for MNOs to pursue Public Safety business[23], it should not be assumed that the MNOs in a particular country are willing to make the necessary modifications and investments or that they would be prepared to take the additional responsibilities of providing a safety of life service. Public Safety operators should approach the local MNOs to discuss their requirements and ascertain the willingness of the MNOs to make the necessary investments.

In the longer term there is an expectation that mobile networks will become a significant carrier of traffic from “The Internet of Things” (IoT). Such traffic may well be critical for "well paying" customers, such as the car industry, smart cities, healthcare and others. The overall subscriber base for "critical network services" is expected to increase massively and having a Public Safety user as a customer could be a useful marketing tool for the MNO to demonstrate its capabilities. However, in this scenario, Public Safety users may remain a relatively small "critical user" base.

What are the options to share commercial LTE networks for Public Safety?

A dedicated network can offer guaranteed spectrum and optimised security and resilience to all its Critical Communications users. This type of deployment model applies to most current narrowband public safety networks and is a viable option for LTE based Public Safety networks as well, with some countries continuing to prefer this solution.

However, such solutions depend on the availability of dedicated spectrum and are likely to be difficult to achieve in the current economic climate. One alternative to reduce the cost for Public Safety organisations is to select one or more commercial mobile operators to supply mission critical voice and data services for Critical Communications users. This approach may be based upon shared spectrum and the use of one common LTE infrastructure, or parts thereof, for consumers, enterprise customers and Critical Communications users. Sharing is typically considered to be based on sharing with a commercial cellular mobile operator but can include sharing with other entities, including Military, Transportation, Utilities and other organisations who also require mission critical communications.

[23] UK ESN, Belgium’s Astrid MVNO arrangements, Finland’s Virve network, U.S. FirstNet project

The drawback of this solution is that a Public Safety organisation may lose control of the Critical Communications services provided to their "customers". As the main cost in any mobile network is the radio access network for both commercial services and Public Safety services, a major saving can be derived from sharing the radio access network and available spectrum between consumers and Critical Communications users. This can be achieved by using traditional and standardised sharing techniques, i.e. with infrastructure sharing models, such as RAN sharing or with a "Mobile Virtual Network Operator" (MVNO) model.

Where necessary, shared networks may be supplemented by temporary deployable infrastructure to cover major incidents, planned events or other situations where additional radio coverage and/or capacity is needed (provided the time to deploy such temporary infrastructure is acceptable)..

When network sharing is used, LTE network features, planning and configuration must all take into account the additional requirements of Public Safety organisations. Public Safety services provided via a commercial network are likely to require tighter security and resilience solutions than are commonly implemented in such networks. Furthermore, prioritisation of Public Safety subscribers and services is critical in emergency situations, and may be at odds with the service model of commercial network operators. Technical standards for these have been developed but may not be acceptable to the MNO's business model.

A comprehensive study on the possibilities for sharing should be undertaken in your country taking account of the capabilities and the willingness of local MNOs to participate in a sharing arrangement. This study should include the issues of subscriber management across multiple networks (fleet maps etc.) See section "What are the implications of Hybrid?".

From 4G to 5G

The term 5G is receiving a great deal of interest in both the technical and popular press and it would be tempting to conclude that 4G is soon to be superseded by 5G. However, 5G is in fact a basket of standards, some of which are aimed more at the future Internet of Things (IoT), automotive applications and other sectors with very high numbers of devices. For the purpose of Public Safety, and its use in the 700 MHz band in Europe, the distinction between 4G and 5G becomes somewhat blurred.

5G is the name given to the 3GPP system from Release 15 onwards. The precise definition of 5G is not yet clear. However, it will comprise of at least a new radio interface (NR) and an evolution of LTE Advanced Pro as well as a new Core Network (NextGEN) and an evolution of the existing core (EPC). Critical Communications requirements are a fundamental part of 3GPP activities and it is certain that these will be carried over to future 5G standards.[24] Critical Communications functionality may not be included in the early phases. In the meantime, LTE Advanced Pro should satisfy the needs of Public Safety users for many years to come.

Until such time as 4G and 5G networks are proven to be truly Mission Critical, today's voice networks will be the only mission critical service available.

[24] As advised by Adrian Scrase (CTO and 3GPP Coordinator, ETSI) November 2016 in an email to the chair of CCBG

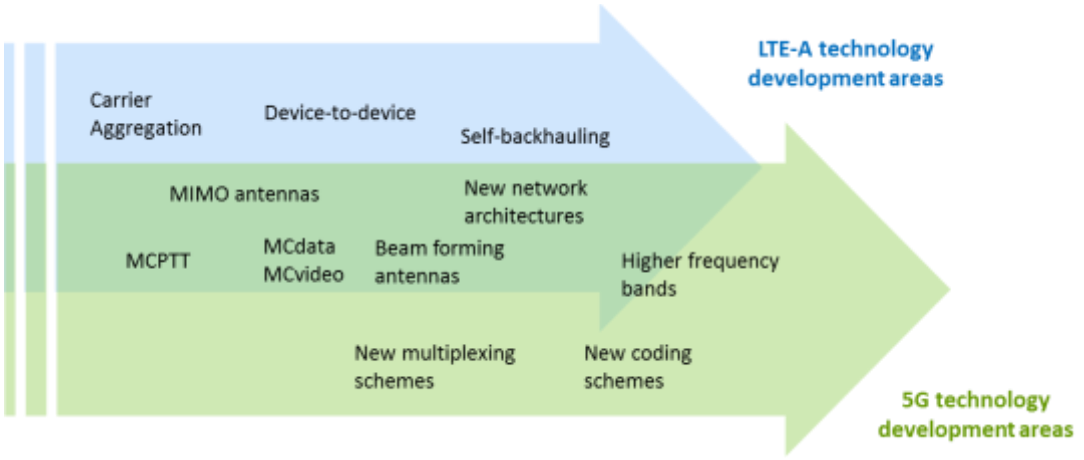

Figure 3: Research and development areas for future wireless networks (Source GSA)

As shown in Figure 3, the evolution of 4G LTE is a vital part of 5G. However, 5G will include the evolution of all parts of the network to accommodate the higher frequency band needed. The evolution includes such items as core and management systems, as well as all protocol layers ranging from radio to enhanced applications.

Much of the promise of 5G rests on making networks denser, and using new spectrum bands with high throughput but very short ranges. That means deploying more cells that are smaller and cheaper, using more antennas to increase capacity through a technology called massive MIMO (multiple-input, multiple output), and using untapped, unlicensed, or under-used spectrum bands between 3 and 300 GHz. The situation regarding large cells for rural areas is still under discussion.

In an effort to drive a coordinated release of 700 MHz spectrum for mobile services, the European Commission has proposed to use the 700 MHz as a "pioneer band" for 5G (see “What are the spectrum options” above). The 700 MHz band is the only real opportunity for operators to provide national coverage of "5G".

Resilience and high availability will be essential to ensure communications services are available to critical infrastructures or service providers even in case of disaster. Network sharing business models involve a relationship between the service provider and the operator, and between operators, in which their respectively owned physical network infrastructures are tightly coupled.

The evolution of current 4G and upcoming 5G network architectures are being designed to share significant levels of commonality. These are expected to provide a smooth evolution from 4G based Critical Communication networks towards tomorrows 5G network architecture and services. As there is still much uncertainty over 5G’s capabilities and deployments, particularly in 700 MHz, it would be unwise to delay implementation of Critical Mobile Broadband for Public Safety users.[25]

[25] See the 3GPP website at www.3gpp.org

Who needs to be involved in the decision?

In most countries the Ministry of the Interior (MoI), or a comparable institution, has the responsibility for Public Safety services to the public. This will include the supervision of police forces, fire and rescue workers and others. It may also include responsibility for the operation of current Public Safety radio networks; or at least the political responsibility for their operators. Depending on a central or, rather, a federal structure of the respective government and administration, the Ministry might be relatively autonomous in taking decisions on internal security matters or it might have to coordinate its activities with regional administrations. The last scenario will, most likely, result in a time consuming process.

Irrespective of the governmental structure of a country, the Ministry of the Interior, or equivalent, will be the central institution as far as the systematic collection of user requirements is concerned. It will also possess the relevant information about current and future threats to society and its institutions. Thus, it is essential to talk to the Ministry, or, in a federal state, to the Ministries of the Interior, when considering the set-up of a new network infrastructure. The MoI has to be the main actor pushing forward any initiative towards the establishment of a Critical Communication network. In the end, the Ministry and its partners will also be responsible for creating an adequate budget and spectrum resources, which implies that the Ministry has to represent the internal security sector toward the spectrum regulator. It will also be responsible for introducing the legal base for the new infrastructure.

On the other hand, the Ministry and its partners may also be asked to deliver consistent overviews of end user requirements in relation to existing security threats, since it is, by obligation, in constant contact with the internal security forces. (This should not prevent Public Safety Network Operators from cultivating appropriate contacts with end user organisations.)

Recommendation I: As an operator, end user organisation, industry representative, manufacturer or law maker; when talking about critical communications digital radio, it is essential to address the Ministry (or the Ministries) of the Interior. When presenting the scenario, it may be useful to take into account the Ministry's current attitude towards in-sourcing versus out-sourcing of services.

It should be recognised that the scope of Critical Communications is increasing. Two factors lead to this development:

- Information and Communications Technology (ICT) has become increasingly critical for the functioning of different sectors of society (utilities, transport, banking, health etc.), and continues to do so. That means the requirement for Critical Communications reaches far beyond a strictly defined public safety sector
- The increasing possibilities of ICT, and the challenges of globalisation, lead to far more complex security scenarios. Other than in conventional warfare, the division of responsibilities between the Ministries of Defence and Interior are becoming increasingly blurred as they share more common interests

Recommendation II: Considering the enormous costs of digital radio infrastructures, it makes sense to form coalitions between the different sectors and eventually share network infrastructures. A Ministry of the Interior has to seek alignment with the Ministry of Defence; it might also address the Ministry of Transport and others. The same applies to agencies in these sectors which have to strive for more cooperation. Other actors might want to provide support to forge a coalition.

Although political support among the actors in internal and external security, as well as in critical infrastructures, might be very strong, assembling an adequate budget for Public Safety radio communications is crucial. A strong business case is needed together with solid calculations of the project's costs for set-up and permanent maintenance of the network infrastructure. Depending on existing assets, available budget, topology, population distribution and other factors, the scenarios will vary greatly across different countries. However, the Ministry of Finance will be the decisive factor in all countries.

Recommendation III: It will be important to monitor the current policies of the Ministry of Finance. Is the budget for Public Safety generally increasing? Might the Ministry be inclined to put more resources into the sector in response to new threats that have recently arisen? In addition, those responsible for implementing new broadband capability for Critical Communications users will have to start talking to the financial administrator early, since, for its annual or bi-annual cycles, budgeting needs a long preparatory phase.

Recommendation IV: Since, at the end of the day, it is the Parliament who will decide about the budget, it will be necessary to talk to the responsible committees, chairmen and party representatives (budget, interior, defence etc.) very early in the process.

As outlined in a separate chapter of this document, spectrum is crucial when defining the business case for a Public Safety network. Obtaining a substantial and usable bandwidth of spectrum is, for an operator, like securing the necessary budget, and will provide additional leverage when talking to potential providers.

Unfortunately, from the perspective of Public Safety representatives, the Telecom Regulators in most countries are looking at the spectrum question from an overwhelmingly economic angle. By default, they are part of, or belong to, the Ministry of Commerce or other Ministries that take care of the development of commercial telecom infrastructures. They tend to auction off their available bands for the highest price possible in order to fund the development of public infrastructure projects including, in some cases, telecommunications infrastructure. Public Safety requirements are often not amongst their considerations.

Recommendation V: Talk to the regulators. They have to be aware of the requirements of the Public Safety sector and, under certain historic conditions, a wider critical communications coalition of user groups might make a difference here.

Last but not least: Manufacturers and providers are indispensable partners when planning for a new network infrastructure. Network operators have to build their infrastructure on a technology that delivers state-of-the-art services for the end-users and, at the same time, provides long-term sustainability. They have to take informed decisions.

The Standards makers too are critical to the successful implementation of Broadband services. Without additional Mission Critical functionality becoming embedded in the LTE standard, the 4G and 5G technologies will not provide the tools needed by Public Safety users. The standards makers are under enormous pressure to deliver new functionality and it is essential to maintain pressure on the them to ensure that the necessary functionality is delivered.

Commercial providers follow their own agenda and will have their own ideas about reasonable business cases for running a Public Safety broadband network. These might, or might not be, in line with the requirements of Public Safety, or might be unaffordable in the light of those requirements. And most likely, before entering into discussion with the Public Safety organisations, they were not even aware of these requirements.

Recommendation VI: Get into a dialogue the standards makers and with potential providers, in order to explore to what extent Public Safety requirements can be covered by contracting with a commercial provider. Try to define a business model that is realistic for both sides. It is also important to establish which requirements cannot be provided at a reasonable cost

Recommendation VII: Undertake a continuous review of the market. Talk to the manufacturers, but also talk to colleagues in other countries who are in a similar situation.

Recommendation VIII: Start talking early: Legislation for critical communication network services will take years, and this needs to take place before the implementation can even start.

Conclusions

There is no simple answer to how mobile broadband should be provided to Public Safety users. Every nation will be in a different part of the lifecycle of their current communications networks and each will have a different set of local circumstances. The key issues raised in this document are:

- Spectrum: this is the single most significant influence on the decision. Without spectrum there is no opportunity for dedicated or hybrid networks to be deployed for Public Safety users. Operators must seek access to the bands described above in order to have some control over their future communications capabilities.
- Ownership: If a Government is concerned about controlling Public Safety communications, and the network over which it is carried, then some dedicated network capability is essential. Commercial networks are subject to changes in ownership and this may be of concern to the Government. Ensuring the necessary coverage, reliability and resilience is more difficult with commercial networks than with dedicated and, as a minimum, needs well defined and enforceable Service Level Agreements outlining expected network performance, availability and reporting methods.
- Security: As with ownership, security of commercial networks is a potential risk compared to dedicated networks. At this time, LTE does not have the same level of security embedded into the standard as is currently available in TETRA networks. The standards makers are addressing LTE security for the future[26].
- Funding: Assuming that spectrum has been secured, the degree to which dedicated infrastructure can be built will be dependent on funding. Nationwide infrastructure will be relatively costly in many countries and an optimal balance between dedicated and commercial networks will need to be found. It is likely that the reuse of existing base station sites and sharing infrastructure can mitigate some of these costs.
- Capex vs Opex: Dedicated networks are capital intensive at the early stage of deployment but total cost of ownership over 10 – 15 years could be less. However, the marginal cost of the increased traffic from Public Safety should make the ongoing costs relatively low. Bear in mind that the additional costs of providing the increased coverage and resilience required by Public Safety users will also need to be recovered. Public Safety operators will need to review the total costs of ownership/operation during the decision-making process.
- Interest from MNOs: Although current experience shows that there is good interest from MNOs, it should not be assumed that all MNOs will be willing to take on the responsibility for providing sufficient coverage, reliability and functionality for Public Safety users. This may become apparent later in negotiations when a service level agreement is being negotiated and penalty arrangements become apparent. Early engagement with MNOs is strongly recommended.
- Involvement in the decision process: Every country will have a different political backdrop and it is vital to establish who, within Government, will be involved in the process. This may include Ministry of Interior, Ministry of Finance, Ministry of Defence, Ministry of Transport and others. Early engagement with the appropriate parties is strongly advised.

[26] See Appendix B for information supporting this statement

- Competent Resources: Creating Hybrid networks will require personnel with appropriate and up to date knowledge of LTE network design. Negotiating integration of dedicated networks and subscribers with a commercial operator will be a complex task, as will the development, oversight and management of any required SLA's.
  Public Safety operators will need to ensure that sufficient competent personnel are available to ensure a successful result.
- 5G: Whilst there is much discussion about future 5G services, the reality is that the technology is still in development and it will likely be mid 2020s before the wide scale deployment of networks has taken place. Due to the wide area coverage requirements of Public Safety services, it is likely that equipment in the 700MHz band will be the primary solution. 5G in 700MHz will be based closely on 4G's LTE Advanced Pro and will therefore be a migration rather than a replacement. The need for mission critical mobile broadband exists today and 4G LTE can satisfy that need. There would be little benefit in waiting for Public Safety 5G especially as its capability and availability is still under discussion.

Decisions on how best to make Broadband services available to Public Safety users will need to be taken in an environment of increasing threats from natural and man-made disasters. Terrorism, in particular, is an increasing problem and, with incidents in Brussels, Paris, Nice and elsewhere, the threat level for governments in mainland Europe is becoming a major concern. Despite the appalling nature of these incidents they are good examples of why the investment in Public Safety communications is so important.

There is no doubt that Mobile Broadband services are likely to bring significant benefits for many users of Critical Communications, enabling faster and more targeted responses to incidents as well as efficiency savings for many Public Safety organisations. Commercial broadband networks are already operational in many countries and roll out is accelerating as new spectrum is made available.

Commercial networks undoubtedly have a role to play in many Critical Communications solutions and will enable Public Safety users to experience the benefits of mobile broadband in a relatively short time. Dedicated networks may be justified where traffic levels are high and where continuity of service is essential. It is hoped that this paper will assist Public Safety Network Operators and End Users in their decision making for the provision of such services.

For further information please see www.tandcca.com

Appendix A

What are the Critical Communications services provided by today's 3GPP Standards

The International Standards bodies that are responsible for developing and maintaining the standards for Mobile Networks are coordinated under the umbrella of 3GPP. 3GPP are therefore responsible for the development of the LTE standards and are already looking at 5G as well.

3GPP's objective is to preserve the considerable strengths of LTE while also adding features for Public Safety. One of their goals is to maximise the technical commonalties between commercial and Public Safety aspects to provide cost effective solutions for both communities.

Based on already defined LTE functions in earlier 3GPP releases and features implemented for commercial LTE networks some strongly required Critical Communications functions are part of 3GPP release 13, finalised and agreed upon in March 2016. A few are listed below:

- Proximity Services (ProSe) enhancements to enable direct communication between terminals
- Group Call System Enablers (GCSE) to support efficient group communications operations such as one-to-many calling and dispatcher services[27]
- Mission critical Push-to-Talk services
- Requirements for a further service, Isolated E-UTRAN Operation for Public Safety (IOPS) have been identified, but no solutions have yet been produced (other than to replicate a network core at the base station)

Besides the above mentioned functions, 3GPP is working on mission critical video and data services in Release 14. In future releases we can expect further enhancements regarding prioritisation of mission critical service flows (QoS), as well as improvements in network security and resilience.

Proximity Services (ProSE) for Critical Communications users

Direct connection among devices (Direct Mode Operation - DMO) is a mandatory feature in present-day PMR systems. It allows Critical Communications users to communicate without the involvement of the network infrastructure (e.g. in case the network is not available due to a system failure or lack of coverage). Current PMR systems provide the use of DMO not only for direct connections between user terminals but also between users and special terminals that operate as Relay and/or Gateway towards the network operating in Trunked Mode (TMO) mode, thus extending the coverage of the existing radio network.

Proximity Services (ProSe) were introduced in 3GPP release 12 for consumers and included a number of Public Safety features. It was amended in 3GPP release 13 with specific functions for Critical

[27] GCSE functionality was first included in Release 12 with further work on building applications and services in Release 13

Communications users. ProSe allow two devices to communicate directly, i.e. without the data path being routed via the network infrastructure.

The proximity range varies depending on the power level used for transmitting the radio signal and other radio conditions such as interference.

The currently defined high-level ProSe feature set for public safety consists of:

- ProSe discovery: allows a device to find other devices in its vicinity by using direct radio links or via the operator network
- ProSe Communication: allows a device to establish communication between one or more ProSe enabled devices that are in direct communication range (no control plane involved)
- Additionally, a device to network relay has been specified that allows a device to act as a relay between the radio network and a device out of radio network coverage Further enhancements to replicate the repeater and gateway functions used in traditional PMR networks may be standardised in future releases

Group Call System Enablers (GCSE) for Critical Communications users

Group Calls represents one of the most significant and indispensable service of PMR networks that involve both mobile users and fixed users, such as dispatchers in a control room.

To enable group communications services 3GPP has introduced the concept of a Group Communication Service application server (GCS AS). It provides a means to achieve one-to-many communications services. Public Safety devices use the GCS AS to initiate, modify or terminate group communication sessions. The GCS AS is the entity which makes the decision to use either unicast or broadcast mode for sending voice, video or data to the Public Safety devices.

In unicast mode, the GCS-AS uses information available to it to derive appropriate application level priority levels, which are further communicated together with other relevant data to a Policy and Charging Rule Function (PRCF), to create, or update, individual bearer channels with desired quality-of-service (QoS) values to each of the addressed Critical Communications users.

In multicast mode, the GCS AS uses information available to it to derive an appropriate priority level, which is communicated together with other relevant data to a Broadcast Multicast Service Center (BM-SC), to create or update an MBMS bearer channel with the specified quality-of-service (QoS) values for all Critical Communications users using multicast in the specified area of service. The evolved Multimedia Broadcast Multicast Service (eMBMS) can send information on a single bearer channel to multiple Critical Communications devices within the same cell or Single Frequency Network area. The eMBMS bearer can either be pre-established, for example for mass events, or it can be established dynamically, for example when the number of users within a certain area exceed a pre-defined threshold. The concept of eMBMS was first defined in 3GPP release 9 to deliver mobile TV to LTE devices and extended in 3GPP release 11 to provide service continuity.

Receiving Critical Communications users will not recognise, whether unicast or broadcast mode was used to setup a call. However, using eMBMS broadcast mode enhances network efficiency significantly, when a large number of Critical Communications users within a certain area needs to be addressed at the same time.

Mission critical Push-to-Talk (MCPTT for Critical Communications users

Mission Critical Push to Talk (MCPTT) provides one-to-one and one-to many voice communication services. The idea is simple. To start an individual MCPTT communication session, a Critical Communications user simply selects the individual they wish to talk to and then presses the 'talk key' on the terminal to start talking. For group calls, the group is selected in advance (using a process called 'affiliation') and so to start the call, the user merely presses the 'talk key'. The call is connected in real time. Push-to-talk calls use one-way communication channels (also known as 'half-duplex'): while one person speaks, the others only listen. Requests to speak are granted on a call prioritisation basis, for example a dispatcher has a higher priority level than other Critical Communications users.

The push to talk service for group communication is based either on multiple unicast bearers or in broadcasting mode. Each sending device sends speech contained in data packets to a dedicated MCPTT server. The MCPTT server in turn then copies the traffic to all of the recipients, either in unicast or broadcast mode. The same call may have recipients with some using unicast, and some receiving the broadcast transmission.

Isolated E-UTRAN Operation for Public Safety (IOPS)

It is highly desirable to provide a 'fall-back' mode similar to that of today's PMR systems, so that a base station (eNodeB) can provide local communications in the event of a network failure. To this end, the Isolated E-UTRAN Operation for Public Safety (IOPS) work was initiated. However, the only solution possible to date has been to locate a complete evolved Packet Core (EPC) at the eNodeB, and, to enable push to talk communications, it would also be necessary to consider locating an MCPTT server in the same place. Because this is impractical and would have severe security concerns, fallback operation has to rely on fill-in coverage from other sites, or other alternatives such as off-network communications.

Appendix B

Security in hybrid LTE networks

3GPP have been implementing additional functionality to the LTE standard to improve security of LTE networks. Further work is ongoing in this regard. However, it should be recognised that technologies such as TETRA, that have been widely adopted for Public Safety communications, were designed from the outset with security in mind.

Understandably, LTE and TETRA have a different approach to security and a summary of the differences can be outlined as follows.

At the basic network level:

- LTE does not have the mutual authentication capability of TETRA. The closest it can be described is an 'implicit mutual' authentication, but that is not as strong as a terminal initiated challenge where the terminal contributes its own random material to the exchange.
- LTE does not have the same level of identity protection as TETRA. There is an identity exchange procedure which is more comprehensive than in early GSM but is not a complete identity encryption system.
- The network does not protect user traffic – that is up to the application. If air interface encryption is enabled, it is removed at the eNodeB.
- There is no inherent security in ProSe.
- There is no fallback mechanism (equivalent of local site trunking [in TETRA]) – IOPS would require a complete network core at every eNodeB, which is impractical and insecure.

At the MCPTT level:

MCPTT adds end-to-end encryption, which protects information from end user terminal to end user terminal. This is designed to overcome any protection issues in the network, and thus maintains confidentiality of user traffic even in the hybrid network case, where the security of the network is under the control of an MNO. The mechanism allows any MCPTT user to call any other MCPTT user with only knowledge of the target user's identity, using an Identity Based Encryption system. The encryption mechanism uses the well respected AES128 algorithm, however the effective key length achievable with the Identity Based Encryption mechanism is limited to 112 bit. Any user organisation that traditionally prefers longer key lengths may need to add their own additional mechanisms. Some TETRA users prefer the AES256 algorithm due to the longer key length.

This end-to-end encryption protects the message content from the MNO. This means that the MNO is not able to provide Lawful Interception facilities on the end user traffic. If Lawful Interception is needed, it must be provided by the MCPTT system to avoid having to remove encryption when used with the MNO network.

The signalling security mechanism in MCPTT allows application signalling to be encrypted between client and system (so MCPTT identities can be hidden for example), but the type of information being passed is still visible to the network operator.

So, specific fields can be identified which carry certain types of information allowing signalling analysis and the potential for targeted attacks. The authentication mechanisms act on the user – which is good – but there is no equivalent application level device authentication.

In conclusion, it is important that users understand the overall security solution and the differences between hybrid networks using LTE and their existing TETRA systems. This will allow users to make informed decisions relating to risk management, and to evolve a suitable security policy for their needs.

Glossary

3GPP	3rd Generation Partnership Project – the organisation responsible for the LTE standard
4G	4th Generation cellular radio technology covers 3GPP standards from Release 8 through Release 14
5G	5th Generation cellular radio technology. 5G is really a basket of technologies including the evolution of LTE along with new Radio Access technologies in ultra High Frequency bands (6GHz upwards)
ATIS	ATIS - Alliance for Telecommunications Industry Solutions. ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP). ATIS is accredited by the American National Standards Institute (ANSI). See: http://www.atis.org
CAPEX	Capital Expenditure
CCBG	Critical Communications Broadband Group. A working group of the TCCA
CEPT	European Conference of Postal and Telecommunications Administrations – a coordinating body for European state telecommunications
CGC	A Complementary Ground Component is a terrestrial infill system for a mobile satellite system that uses terrestrial base stations to provide connectivity in weak signal areas such as urban areas
CNI	Critical National Infrastructure typically includes the Utilities (Gas, Electricity and Water), Transportation (Rail and Metro, Buses and Trams, Ports and Airports) and other critical industries without whom society would quickly break down
DMO	Direct Mode Operation. A means of establishing communications between two radios without the intervention of a radio infrastructure
EC	European Commission
e-nodeB	e-nodeB (or ENB) is the radio base station and controller in an LTE network
ETSI	European Telecommunications Standards Institute
EUTC	European Utilities Telecom Council – an Association of Utility organisations in Europe similar to the UTC in the USA
e-UTRAN	e-UTRA is the air interface of 3GPP's Long Term Evolution (LTE) upgrade path for mobile networks. E-UTRAN is the radio access network based on that standard
EPC	Evolved Packet Core is the overall packet data handling system of a LTE network.
FCC	Federal Communications Commission – the US regulator
FirstNet	First Responder Network Authority (FirstNet)is an independent authority whose task is to provide emergency responders with the first high-speed, nationwide network dedicated to Public Safety in the USA
Group Call	A means of setting up a radio call to a large number of users simultaneously
HSPA	High Speed Packet Access is a 3G technology for delivering high speed data over a cellular telephone network
HSPA+	Evolved High-Speed Packet Access, is a technical standard for wireless, broadband telecommunication that provides increased data rates over HSPA
ITU	International Telecommunications Union – coordinates the shared global use of the radio spectrum
LMR	Land Mobile Radio is the US equivalent of PMR and also provides group based radio communications
LTE	Long Term Evolution – the latest standard for cellular communications. LTE provides higher data rates than 3G UMTS but is not quite a 4G technology LTE is classified as 3GPP standard Releases 8 and 9

LTE-A	LTE Advanced – A further development of the LTE standard defining additional functionality including aggregation of separate frequency bands and the addition of voice services. LTE Advanced is considered a true 4G technology LTE- Advanced is covered by 3GPP standards Releases 10, 11 & 12
LTE Advanced Pro	Building on LTE Advanced, 3GPP standards Releases 13 & 14 are the first standards to include Public Safety specific functionality
M2M	Machine to Machine communications
MCMBB	Mission Critical Mobile Broadband
MCDATA	Mission Critical Data – additional functionality being added to the LTE standard to carry prioritised group data communication over an LTE network
MCPTT	Mission Critical Push to Talk – a mechanism to allow group voice calls to be added to a LTE network
MCVIDEO	Mission Critical Video – additional functionality being added to the LTE standard to carry prioritised group video communication over an LTE network
MNO	Mobile Network Operator – A commercial cellular network Operator
MSS	Mobile Satellite Service
MVNO	Mobile Virtual Network Operator
NIST	The US National Institute of Standards and Technology is a measurement standards laboratory, and is a non-regulatory agency of the United States Department of Commerce. NIST is currently leading the US input to 3GPP LTE standards making on behalf of the National Public Safety agencies.
NoC	Satellite Network Operations Centre
NPSTC	National Public Safety Telecommunications Council is a Federation of associations representing Public Safety telecommunications
NTIA	National Telecommunications and Information Administration (NTIA) is an agency of the United States Department of Commerce that serves as the President's principal adviser on telecommunications policies pertaining to the United States' economic and technological advancement and to regulation of the telecommunications industry
OMA	Open Mobile Alliance. OMA develops mobile service enabler specifications, which support the creation of interoperable end-to-end mobile services See: http://openmobilealliance.org
OPEX	Operational Expenditure
PMR	Private Mobile Radio technology provides group based radio communications for business and professional users
Project 25	Project 25 is a digital mobile radio standard developed for Public Safety organisations in the USA
Public Safety	Public Protection and Disaster Relief is a term that encompasses the traditional Public Safety organisations and also major incident rescue services
ProSe	Proximity Services - the 3GPP descriptor for Direct Mode (DMO) in LTE
PSS/PS	Public Safety Services or Public Safety - describes the emergency services and includes Police, Fire, Ambulance, Border Guards, Security Services etc.
RAN	Radio Access Network
RSPP	The Radio Spectrum Policy Programme (RSPP) defines the roadmap for how Europe can translate political priorities into strategic policy objectives for radio spectrum use
S-Band	Frequencies that range from 2 to 4 GHz
SDO	Standards Development Organisation

SIM	Subscriber Identity Module - is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices
SLA	Service Level Agreement
TCCA	TETRA and Critical Communications Association (see www.tandcca.com)
TETRA	TErrestrial Trunked Radio - a digital trunked mobile radio technology
Tetrapol	A technology developed for the French Gendarmerie and in use by a number of Public Safety agencies in various parts of the world
UIC	Union Internationale des Chemins de fer' - the French-language acronym for the International Union of Railways
US	United States of America
UTC	Utilities Telecom Council – an Association of Utility organisations(in the USA)
VoLTE	Voice over LTE
VSAT	A very small aperture terminal (VSAT), is a two-way satellite ground station or a stabilised maritime VSAT antenna with a dish antenna that is smaller than 3 meters
Wi-Fi	A popular technology that allows an electronic device to exchange data or connect to the internet wirelessly using radio waves

Version Control

Version No.	Date	Changes/additions made
Final draft v1	25/11/2016	This document represents a consolidation of all inputs into a draft for consideration by TCCA Board
Final draft v2	18/12/2016	Final draft for approval
Issue 1.0	12/01/2017	First Issue
Issue 1.01	06/02/2017	Changed image on front page