MOTOROLA

Motorola Solutions Australia Pty Ltd
ABN 16 004 742 312 ACN 004 742 312
10 Wesley Court, Tally Ho Business Park, East Burwood Victoria 3151
Postal address: Locked Bag 27, Mt Waverley Victoria 3149

Telephone +61 3 9847 7500
Fax +61 3 9847 7501

Response to Australian Productivity Commission questions from Motorola Solutions – September 2015

Prioritisation and access

1. **Does technology exist for prioritising or pre-empting PSA access to LTE networks (pre-emption) when networks are already congested? Has such technology been deployed anywhere? Are 3GPP LTE standards for this likely to be developed and, if so, when could they be expected?**

The need for prioritised access and traffic for PSAs to ensure they can get their information through at times of congestion above all other forms of network traffic is a key requirement in any mission critical communication system used by public safety agencies. Furthermore, during an incident where there is limited capacity on the network or its is congested, it is the agencies themselves that need the ability to control who has access to the network and which information takes priority.

3GPP LTE standards define the following prioritisation concepts:

1. Access Priority
Access Priority allows an LTE network to control UE access attempts to communicate with the network. This capability is implemented by enablement of Access Class Barring to protect congestion on the Random Access Channel.

2. Admission Priority
Admission Priority allows the LTE network to determine that a device is allowed to be allocated system resources. Previously allocated system resources may also be pre-empted from UEs and reassigned to other UEs according to Allocation and Retention Priority (ARP) parameters.

3. Scheduling Priority
Scheduling Priority allows the LTE network to regulate over the air transmission (which and how frequently user packets are sent over-the-air) in order to satisfy differentiated service performance requirements for radio bearers. The scheduling priority is governed by the QoS Class Indicator (QCI) parameter.

These concepts have been widely implemented and deployed in LTE commercial deployments.

However, the following limitations should be considered for PSA access:

- *LTE prioritisation concepts are designed to provide static differentiation between subscription types. They are not designed to consider dynamic situational differences required for PSA access.*

- *LTE prioritisation concepts are designed with the assumption of one to one mapping between a user and an LTE UE device subscription. Public Safety use cases introduce different user-device relationships, where a device can be shared (e.g. across shifts) or a user may be associated with multiple devices.*

- *Lack of ability to classify encrypted user traffic: In order to apply different admission and scheduling priority to different applications, the LTE network must be able to differentiate user traffic, which may not be possible when a Virtual Private Network (VPN) is used for PSA Access.*

3GPP does not address these limitations, however, the need to overcome them has led to the development of solutions designed to provide dynamic, agency controlled prioritisation and access capability at a user, and application basis. These solutions are in the early stages of deployment, on purpose built or hybrid PSA LTE networks.

2. **How costly, complex and/or time consuming would it be to implement prioritisation and preferential access solutions? What changes would be required to existing commercial networks to deliver this? — could solutions be implemented only in the network core, or would changes need to be made to radio sites, backhaul, handsets or other equipment/infrastructure?**

   There are a number of factors that will determine the cost and complexity of implementing a PSA prioritisation and preferential access solution. These include the architecture (private, carrier, hybrid), release version, features supported by the respective network, and the commercial principles around what level of prioritisation is enabled, by whom and when.

3. **As far as you are aware, have any commercial networks implemented preferential access features to date?**

   Carriers are best placed to answer this question.

Roaming

4. **If public safety users were to be given the ability to roam from a dedicated network on to existing commercial networks (e.g. to boost coverage or capacity), what technical changes would be required on each network (e.g. hardware/software)? What are the associated challenges, complexities and costs?**

   Carriers are best placed to answer this question.

Security

5. **What new network core equipment (if any) or other equipment would be needed to deliver end to end security to PSA users? How would existing equipment or infrastructure need to be modified? Do 3GPP LTE standards incorporate security/encryption measures?**

Security requirements and the impact they may have on the network, devices and applications environments are directly related to the requirements of individual agencies. The 3GPP LTE standards currently support device authentication, signaling protection, and media protection with respect to the LTE portion of the network services.
Many PSA’s (especially police) have specified the need for mission critical applications (for both voice and data) to achieve a higher level of security compared to commercial sectors.

The following provides some general considerations;

Access control, configuration and provisioning
Data relating to the configuration of users such as provisioning, access and configuration data, may be required by PSAs to be separated or isolated and as such may dictate the need for separate database system components depending on the model implemented.

End-to-end encryption
Depending on the agencies requirements, software and hardware end-to-end encrypted solutions should be supported.
In line with current digital LMR networks’ hardware based encryption, via a module that is FIPS 140-2 level 3 compliant, should also be offered. This means that the keys stored on the encryption module are protected from tampering. For stolen device or any unauthorised attempts to access these keys in the device, the crypto module will be “zerorised” thus rendering the device unusable to protect the confidentiality of further communications and information.

Security management tools

PSAs need the ability to control the encryption of devices and workgroups in a dynamic manner, with the ability to regularly and remotely change the encryption key (especially for specific operational groups handling sensitive information), Hence the addition of some form of Key Management Facility will be required if not already available or reusable from the LMR network.
The ability to control access is dependent on having up-to-date authentication credentials which are mainly based on certificate assurance. Having a PKI (Public Key Infrastructure) and the ability to centrally manage the certificates as well as update them over the air will provide a higher level security and integrity for PSAs.

Interoperability with LMR
Public Safety Push to Talk (called Mission Critical PTT in 3GPP) is currently under development in 3GPP Release 13. For some PSA's involved in critical operational

situations, end-to-end encrypted interoperability will provide a higher level of communications security that will be offered by 3GPP. To achieve this PSAs can leverage existing LMR security management tools for common management of security credentials in LMR radios and LTE devices. Both LMR and LTE devices should support this common encryption to achieve true end to end encryption.

Device Platform Security

PSAs need to consider the security provided by the device platform and be able to offer different device tiers based on the mission need. For high assurance users, the device platform should offer defence in-depth security layers including integrity services to minimise threats to the kernel and hardware encryption module to protect credentials and keys.

Security is one of the key design considerations in any PS LTE solution architecture. The security solution needs to provide an extensive, security solution, with multiple layers of protection to ensure information confidentiality, integrity and user privacy. The end-to-end security solution should include the following standards as an absolute minimum:

- *LTE Core Security*
- *In-transit Data Security*
- *Authentication*
- *Over-The-Air Security management*
- *Device platform assurance*
- *Data at rest security*

Mission critical voice

6. Have the proprietary solutions that exist for delivering push to talk voice services over LTE networks been trialed or deployed by PSAs anywhere in the world? Is there any information on these trials that you could point us to?

While there are trials and deployments of commercial over the top push-to-talk services on carrier LTE networks, these do not meet Mission Critical PSA push-to-talk requirements. These are targeted to complement the existing LMR networks for specific non mission-critical use cases, where a ‘best efforts’ delivery service will suffice.

Interoperability

7. **Would current technology allow PSA staff to operate simultaneously across LTE and Land Mobile Radio (narrowband) networks? Has such interoperability been incorporated into 3GPP LTE standards yet? Are commercial solutions available?**

The impact of simultaneously using multiple networks for PSA's needs to consider the level of capabilities, features and suitability of the respective networks to ensure that the overall service delivered meets the needs of the respective PSA's.

Current narrowband LMR PPDR technologies such as APCO P25 and TETRA comply with 'mission critical' requirements for narrowband mission critical voice and data.

Although the LTE standard is currently being enhanced to support mission critical communication, it will be some time before mission-critical features are developed, standardised and implemented by the LTE equipment manufacturers. Beyond these steps, it will take more time for operators to upgrade their networks to meet mission-critical standards.

Current (non mission-critical) technology allows PSA staff to utilise either a Land Mobile Radio (LMR) network or an LTE network for voice and limited data transfer opportunities.
Over the top push-to-talk solutions are currently available that enable PSA users on an LMR network to communicate with PSA users on an LTE network via IP connectivity between these networks.

LMR networks are not designed to handle broadband data traffic. Standards-based LMR networks such as APCO P25 and Tetra do support narrowband IP data, allowing functions such as location, duress, text, and limited imaging to be shared between LMR and LTE networks.

While interoperability between LMR networks has been defined by the P25 and Tetra standards bodies, 3GPP has not standardised interoperability between LTE and LMR networks.

8. **What infrastructure or equipment is needed to provide interoperability between LTE and LMR? Would it be sufficient to link network cores or would changes need to be made to radio sites? Are dual mode handsets currently available?**

It is sufficient to link network cores to provide interoperability. No changes need to be made to radio sites. A commercial over the top PTT and/or narrowband data application server that supports interoperability must be connected to the LMR and LTE network. IP connectivity must be established between the LMR and LTE *network cores. Additional equipment such as a site router, ethernet switch and a firewall are required.*

Dual mode handsets are in development and early implementations are now available. However it is still challenging to overcome the requirements for simultaneous operation including high-powered, narrowband LMR and low powered broadband LTE. PSA LTE features and standards are still in development.

9. **Would current technology allow PSA staff to operate simultaneously across LTE and Wi-Fi networks? Has such interoperability been incorporated into 3GPP LTE standards yet? Are commercial solutions available?**

In the same way as described in response to question number 7, current technology allows PSA staff to use either a LMR network or a Wi-Fi network (but only for non mission-critical communications). 3GPP has not standardised interoperability between LMR and Wi-Fi networks. Multi-mode device availability and suitability also needs to be considered.

10. **What challenges would interoperability pose, and can these be addressed at present?**

Interoperability can be broken into three general methods:

1. ***Connected LMR and LTE networks***
   Interoperability between connected LMR and LTE networks, which has been discussed in the previous three questions. This allows devices on different networks (LMR, LTE) to communicate with each other when using applications such as PTT. Ensuring that each of the interconnected networks, applications and devices meet mission-critical requirements, such as resiliency, Grade of Service (GoS), access and traffic priority, redundancy, capacity, security, etc. to avoid compromising the overall PSA service is critical.

2. ***Dual Mode Handsets***
   Dual mode devices operating simultaneously on a PSA LTE network and an LMR network that are not connected for interoperability. Currently, PSA devices are typically designed to support either LMR or LTE, but not both. There are several dual mode PSA LTE/LMR handsets that have either been announced or are currently available. Most of these devices are designed to use PSA LMR capabilities while adding broadband data on an LTE network. Device configuration determines which applications a dual mode device uses on each network. Simultaneous operation, however, can be

limited by interference between the specific RF bands that are used by the LMR and LTE networks. For example, transmitting on one network could interfere with the device's reception on the other network. RF design is a challenge on these dual mode devices, but it can be addressed. Ensuring that each of the interconnected networks, applications and devices meet mission critical requirements to avoid compromising the overall PSA service is critical. Standards are still being developed to define device features and capabilities for mission critical PSA LTE use.

3. ***Connected networks and future dual mode devices***

The most ideal interoperability method combines the options described in points one and two. The LMR and LTE networks are connected for interoperability and the dual mode devices support simultaneous operation on both networks with PSA LTE features and capability. This capability is not currently available. A challenge will be ensuring that the standards are adequately defined to meet PSA mission-critical requirements and are supported by both network and device manufacturers.

Note - Interoperability Policy and Process: *It should be noted that one of the greatest barriers to achieving interoperability on a national scale in Australia are the policy and processes around the exchange of information for both voice and data messages. Motorola Solutions fully supports any policy changes which help PSAs to benefit from interoperability across jurisdictions and State borders.*

In addition, if a national, central forum were established to set the standards, policy frameworks, and user requirements for the nation's emergency services, then agencies would have the ability to coordinate their budget and procurement cycles to take advantage of collective purchasing power for broadband equipment and services.

11. For example, would users of dual mode handsets be able to receive messages from one network while transmitting/receiving on another? (E.g., would a police officer be able to receive urgent 'push to talk' messages when they are already on a call?)

Please see our response in question 10 above.

12. Could data transmitted over an LTE network be converted to the LMR format when a user is outside of the LTE range (but within the range of the narrowband network)

LMR networks are not designed to handle broadband data traffic. Standards-based LMR networks such as Project 25 and Tetra do support narrowband IP data, allowing functions such as location, duress, text and limited imaging. Data interoperability between LMR and LTE can be achieved that allows appropriate data to be transmitted from an LTE device to an LMR capable device, which will require either companion (separate LMR and LTE devices wirelessly connected) or dual mode devices.

General

13. **Are there any relevant 3GPP LTE standards that have been formalised but not yet incorporated into equipment on the market?**

    3GPP has previously specified two capabilities targeted for PSA users. They are higher power LTE devices (only specified for Band 14 use) and group communication service enablers (GCSE). Enhanced Multimedia Broadcast/Multicast (eMBMS) is also an available 3GPP capability that is useful to public safety for optimal group communication. Future releases will include additional PSA features.

    Release-compatible LTE infrastructure is typically available two years after 3GPP specifications are finalised for any release and product availability is determined by specific demands in individual markets.