Mission Critical Push-To-Talk (MCPTT) Implementation for Colorado

December 2017

Prepared by:
Signals Analytics, LLC

Disclaimer: This whitepaper was prepared for the State of Colorado - Governor's Office of Information Technology using funds under award 08-10-S13008 from the National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce (DOC). The statements, findings, conclusions, and recommendations are those of the author(s) and do not necessarily reflect the views of the NTIA, DOC or FirstNet.

Contents

Executive Overview

With the formal implementation of the Nationwide Public Safety Broadband Network (NPSBN) commencing in 2018, public safety jurisdictions throughout Colorado will begin the process of integrating Long Term Evolution (LTE) technology into their overall communications systems. Whether the state opts-in or out of the FirstNet/AT&T state plan, it must work to develop a comprehensive and proactive approach to ensure the fundamental goal of the NPSBN is met, communications interoperability. As the organization tasked with overseeing the planning and implementation of the NPSBN, the State of Colorado Governor's Office of Information Technology (OIT) has identified Push-To-Talk (PTT) and eventually Mission Critical Push-To-Talk (MCPTT) services as a foundational application that will determine how the NPSBN is adopted and the impact on statewide interoperability. This includes the successful integration of PTT/MCPTT with the existing Land Mobile Radio (LMR) networks within the state. Current LMR users in Colorado utilize the statewide Digital Trunked Radio System (DTRS), which is an Association of Public-Safety Communications Officials Project 25 (P25) system that is interconnected to other P25 networks via the Inter RF Sub-System Interface (ISSI). Additionally, agencies in the state also have deployed their own P25 and non-P25 LMR networks that are utilized on a daily basis. Due to the cost and technical limitations of these LMR radios, it has been difficult and sometimes impossible to provide interoperability across all LMR networks. The primary purpose of the NPSBN is to help alleviate the issue of interoperable communications.[1] ***MCPTT technology is accelerating at a rapid pace and Colorado has to make a decision on how to best implement this technology to allow for interoperable public safety communications between its existing LMR networks and its public safety wireless broadband partners.*** The purpose of this paper is to analyze the potential implementations of PTT/MCPTT and LMR integration in both an opt-in and opt-out scenario to assist state leaders in making an educated decision regarding the implementation of the NPSBN in Colorado.

The Problem

The ultimate implementation of PTT/MCPTT may take place via a variety of technologies, methods and forms. From Over-The-Top (OTT) app-based implementations to network level integration with devices, how PTT functionality is implemented will have significant impacts on the overall public safety communications system within Colorado. In addition to the technology, the recent announcement by Verizon that it will offer competing public safety grade services, greatly increases the complexity no matter what decision (opt-in or out) the state makes.

After technical review of the SPP as well as analyzing the likely adoption of the FirstNet network (either opt-in or out), it is our perception that Colorado will continue to see local jurisdictions use a variety of commercial carriers in addition to the FirstNet offering.[2] Given this assumption, we have focused our efforts on the necessary interoperability required for

[1] Page 15 of 9/11 Commission Report - https://www.npr.org/documents/2004/9-11/911reportexec.pdf
[2] Local jurisdictions utilize service from mobile operators such as: Verizon, AT&T, T-Mobile, Sprint, Commnet, Viaero and Union Wireless.

implementing MCPTT in a coordinated, statewide, interoperable way. If the proper architecture is implemented by the NPSBN, these concerns can be alleviated.

Unfortunately, the current offering for prioritized, network level PTT/MCPTT voice from AT&T/FirstNet (as currently understood) and implemented by Motorola Solutions Incorporated (MSI) by AT&T will *only work on AT&T devices, within AT&T's network and not support the necessary connections for cross-carrier interoperability.* This analysis is based on information from the FirstNet state plan portal (SPP) as well as public statements from AT&T/FirstNet.[3] For jurisdictions that are not FirstNet/AT&T subscribers, the only way to ensure interoperability is to utilize third-party OTT applications, which is problematic and does not solve the interoperability issue. Also, the use of MSI could limit multi-vendor LMR interoperability as we have historical evidence of interoperability and cost related issues surrounding MSI.[4] While options to implement an open, standards based interface between LTE and LMR are being developed, it is unclear, based on the information presented in the SPP and outside research what form the interface implementation will be in the AT&T/FirstNet offering. If the ultimate solution presented is not completely interoperable with Colorado's LMR systems, it will by definition create interoperability problems for users in the state. The implementation of the proposed MCPTT solution, with no network level interoperability with other networks (outside AT&T) would severely impact voice communications on roaming networks where coverage is poor or jurisdictions have chosen to use other vendors and will affect all users who are on competing mobile networks. Not having MCPTT work across mobile networks could have detrimental impacts to overall interoperability throughout the state.

Currently, very few public safety entities (PSE) are using PTT services from any of the Mobile Network Operators (MNO). The primary reasons are that the cost of these services for the subscription, maintenance and interconnection to P25 is simply too high to justify. However, the need for cross-carrier MCPTT with LTE broadband is incredibly high.[5] Based on research and testing, we believe the integration of MCPTT with LMR will be the critical factor for long-term adoption of LTE technology. Everyday, jurisdictions across the state perform mutual aid, not only working border-to-border but outside of the state. Using an interoperable, open MCPTT system would enable direct communications that are cost effective, with bordering states of Wyoming, Nebraska, Kansas, Oklahoma, New Mexico, Utah and Arizona. Getting a MCPTT system that could meet the needs of users would immediately be put to use by undercover agents, task forces, support staff and regular LMR users.

Update: This paper was commissioned and primarily completed prior to the Governor's decision to opt-in to the FirstNet state plan, announced on December 18th and was thus focused on analyzing the implementation of PTT/MCPTT and LMR integration in both (opt-in/out) scenarios. It was determined to keep the original work and analysis largely intact while updating key areas to reflect the now known environment in which the NPSBN will be

[3] http://urgentcomm.com/public-safety-broadbandfirstnet/att-exec-discusses-core-core-interoperability-verizon-proposal-first
[4] https://www.publicintegrity.org/2010/02/17/4389/homeland-security-s-billion-dollar-bet-better-communications
[5] https://twitter.com/breaking911/status/925899288399446016

implemented in Colorado. The primary impact of the opt-in decision is the assumption that multiple commercial cellular carriers will be offering public safety grade services in the state (specifically PTT/MCPTT and LMR integration) is now known to be correct. Additionally, multiple requests were made to FirstNet, AT&T and Motorola Solutions to discuss this paper and gather information, but were rejected by all organizations.

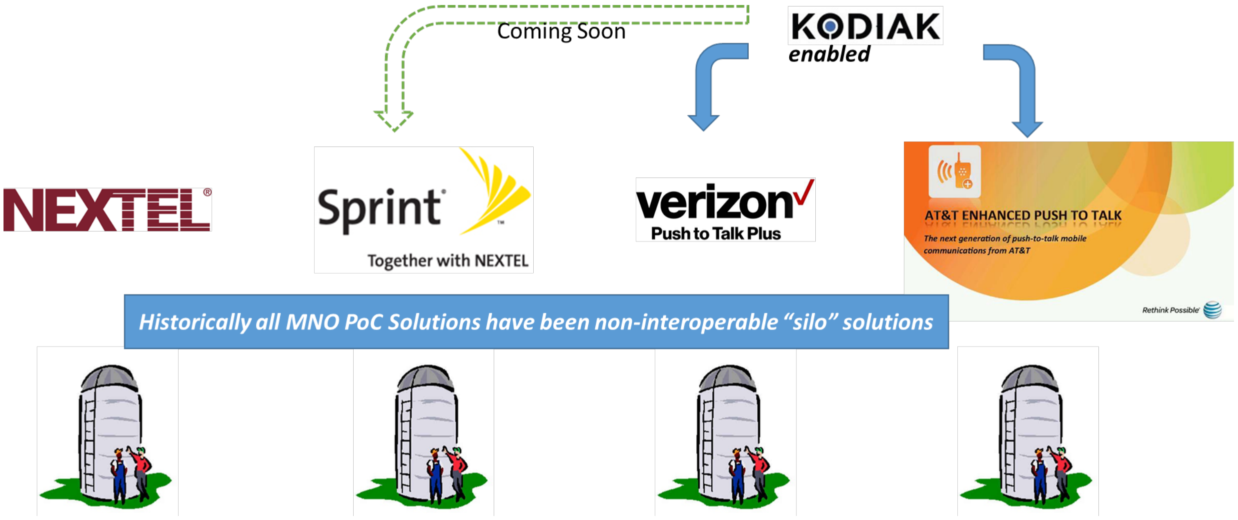
Overview of PTT & MCPTT

Public safety users have long identified the use of PTT services on broadband to be the most important application used on the network.[6] The primary means of communication is voice via LMR networks and the entire incident command structure (ICS) is currently based on voice commands from the incident commander. Situational awareness flows back to the incident commander in the same manner – this makes getting mission critical voice communications crucial to ensuring public safety operations.

The current P25 network standard used for LMR was created in 1988 and has not kept up with the pace of commercial wireless technology in offering broadband capability, which is now entering its fifth generation. Just as technology has changed, so have the threats and dangers that first responders must address. Ensuring they can communicate with voice, data and video requires the use of mobile broadband technology – which was one of the major tenets of allocating dedicated spectrum in the 700 MHz band and creating the First Responder Network Authority. The choice to use P25 as the new standard for LMR nearly 30 years ago was borne out of frustration from disparate, non-interoperable communications between public safety agencies. It provided a basic technology implementation but did not address fundamental interoperability for nearly 20 years. Having learned lessons from this, the decision to use commercial based 4G LTE technology has put public safety on a good path into the next 25 years. However, the same challenges of interoperability exist with the MCPTT implementation for the state and choosing poorly may result in similar, very costly changes in the future that will be required to enable interoperability on MCPTT and LMR.

PTT services over cellular (PoC) have been available for nearly 20 years with MNO solutions such as iDEN communications from Nextel. This concept of carrier deployed or MNO offered PTT was continued with Sprint in their QChat enabled service and Kodiak enabled services for Verizon and AT&T.

[6] http://www.npstc.org/download.jsp?tableId=37&column=217&id=1238&file=Interoperability%20-%20Olbrich%20-%20NPSTC%20700MHz%20Questionnaire%20Results%20IO-0061A.pdf



Historically all MNO PoC Solutions have been non-interoperable "silo" solutions

Figure 1: PoC Solutions *Source – Signals Analytics*

Each of these services provides integration into LMR networks and feature rich PTT services but they are currently offered as non-interoperable solutions. This means that a department using Sprint and another using Verizon that both have PoC services would not be able to communicate with each other directly on PoC.[7]

However, ***there is no technical reason*** why these networks cannot directly communication over PoC. Kodiak PTT services which is now wholly owned by MSI has offered hosted services to both Verizon, marketed as PTT+ and to AT&T, marketed as Enhanced PTT. This summer, Sprint announced that they would be transitioning off of their existing QChat system onto the Kodiak enabled solution that will be marketed as Direct Connect Plus. This means that 3 of the 4 largest MNOs in Colorado will be using the same hosted solution from MSI and all have the *capability* to communicate on the same talk groups, across carrier network boundaries. FirstNet has stated that their application network is a closed network and MCPTT services will currently only be offered on their network with no cross carrier network interoperability. Later in this paper we will discuss cross-carrier interoperability being offered by Verizon.

[7] NOTE: The first responders in the state that worked on putting this whitepaper together agree that agencies across the state must have the ability to cooperate and communicate with each other in response situations.

Over the Top PTT (OTT PTT)

Figure 2: OTT PTT Solutions Source - Alibaba

With the advent of carrier agnostic applications for both Android and Apple, the PTT application space is inundated with feature rich, cost effective (often times called “freemium”) systems that work across networks. These OTT PTT applications have had good success in both the commercial and public safety markets. On Google Play there are over 150 applications available for download that purport to offer PTT functionality; two years ago there were only 16 apps. Examples of public safety and enterprise grade applications are Wave, Zello and Voxer.[8] These are typically cloud-based solutions that can be implemented immediately, are cost competitive and scale from single user to massive enterprise grade with relative ease. An advantage of nearly all OTT PTT applications is the ability to work on multiple broadband access technologies such as Wi-Fi, LTE and even 3G data on multiple platforms like Chrome, iOS, Android and Windows. MCPTT development is primarily concerned with creating equivalent mission critical voice within the network. Innovation is really the other area of mass appeal for OTT applications. Without the constraints of the network or standards process, they can integrate in data sharing, video, photos, text and location awareness geo-fencing capabilities enabled from the device.

- Chat or text integration.
- File transfer.
- Nearly unlimited virtual talk group creation.
- Geo-fenced talk group creation.
- Geo-location tracking.
- Push-to-Video integration.
- Presence indicators (to see who’s in service or online).
- PTT to PC, smartphone, tablet, IP Phone and LMR.
- Advanced security at the application layer.

Integration into Digital Mobile Radio (DMR), LMR and P25 ISSI is available with many solutions. It should be noted that OTT apps have been very adept at implementing advanced features like immediate peril and man-down button functionality. Their ability to integrate ISSI, implement changes and adapt dynamically to the market demands makes their use very attractive. Overall these will make the incident scene for responders and the community safer and more secure. Two applications have made significant development for public safety – Mutualink and ESChat. These solutions have servers located on premise for access to the LMR networks and are connected to the MNO via a secure virtual private network (VPN) connection.

[8] No recommendations are to be inferred with any of these applications. It is merely a representation of some of the available choices.

Additionally, Colorado's North Central Region[9] users are evaluating two major vendors of LMR/LTE equipment in Harris BeOn and MSI Wave.

A major advantage these OTT applications have is that they can work on a variety of devices and across multiple carrier networks as these are application layer enabled systems. However, the drawback on these systems being evaluated is they use the P25 improved multiband excitation (IMBE)/advanced multiband excitation (AMBE) codec, which is implemented in both Android and iOS devices. This allows for the concept of end-to-end functionality with encryption. However, this functionality does not scale well economically as the IMBE/AMBE codec is a licensed piece of software. In most cases this makes the app cost over $300 per device – which could be more than the cost of a low-tier smartphone. The cost structure is essentially linear with very little discount for the volumes that Colorado would need and this makes enabling its use for all smartphone users potentially cost prohibitive.

The biggest issue though with OTT PTT is that once a vendor is selected for the application, you are locked into an ecosystem where everyone needs to have the same application. For instance, a Harris BeOn PTT system cannot directly communicate to a MSI Wave PTT system. This quickly destroys interoperability and becomes a large-scale management problem. For mutual aid users across state borders or from the NPSBN that may be using another app or MCPTT there would be no direct interoperability. This constraint will likely cause more confusion and has the potential to make the scene unstable. Also, any advanced features in LTE would need to be manually created for the OTT application or they may only be available for MCPTT use. Going forward, Colorado responders would want to use a globally recognized MCPTT implementation from Third Generation Partnership Project (3GPP) rather than an OTT application.

Other applications like FireChat have the ability to create ad-hoc mesh networks and allow peer-to-peer communications. However, this innovation comes at the cost of interoperability since each of these OTT applications is proprietary in design. It is because of this common need for voice communications that MCPTT development has been accelerated in 3GPP System Architecture Group six (SA6) for the past two years.

National Public Safety Telecommunications Council (NPSTC) Efforts

Some organizations such as NPSTC have worked to create requirements for MCPTT that can be adopted by 3GPP. These requirements are a high level view into the basics of what MCPTT needs to offer. The following is an excerpt from NPSTC on MCPTT related requirements.[10]

1. Direct or Talk Around: This mode of communications provides public safety with the ability to communicate unit-to-unit when out of range of a wireless network OR when working in a confined area where direct unit-to-unit communications is required.

[9] Harris BeOn, MSI Wave and other apps are being evaluated by multiple agencies in the NCR.

[10] http://www.npstc.org/download.jsp?tableId=37&column=217&id=2055&file=Mission%20Critical%20Voice%20Fu

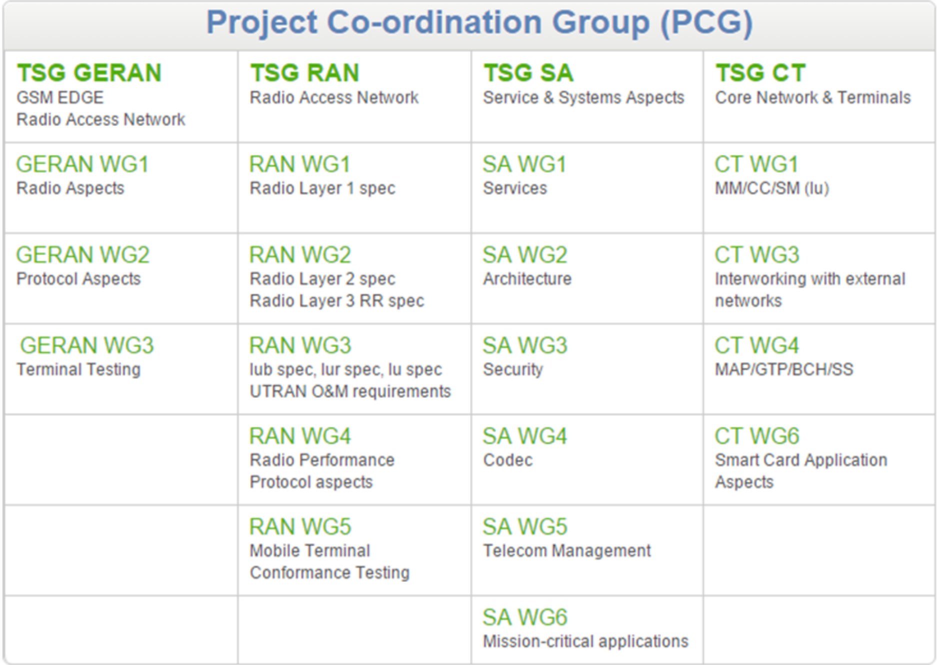
2. Push-to-Talk (PTT): This is the standard form of public safety voice communications today - the speaker pushes a button on the radio and transmits the voice message to other units. When they are done speaking they release the Push-to-Talk switch and return to the listen mode of operation.
3. Full Duplex Voice Systems: This form of voice communications mimics what is in use today on cellular or commercial wireless networks where the networks are interconnected to the Public Switched Telephone Network (PSTN).
4. Group Call: This method of voice communications provides communications from one-to-many members of a group and is of vital importance to the public safety community.
5. Talker Identification: This provides the ability for a user to identify who is speaking at any given time and could be equated to caller ID available on most commercial cellular systems today.
6. Emergency Alerting: This indicates that a user has encountered a life-threatening condition and requires access to the system immediately and is, therefore, given the highest level of priority.
7. Audio Quality: This is a vital ingredient for mission critical voice. The listener MUST be able to understand without repetition, and can identify the speaker, can detect stress in a speaker's voice, and be able to hear background sounds as well without interfering with the prime voice communications.

With exception to Direct/Talk Around mode, all of these requirements are now being addressed or have been standardized in MCPTT. For users in the state, the features and functionality available on LMR are similar and the response from the first responders interviewed was that LTE MCPTT should mimic existing LMR devices.

MCPTT Standards

MCPTT is a global standard that is being led by the SA6 of the 3GPP. 3GPP manages the entire standards process for LTE but SA6 was created for the "definition, evolution and maintenance of technical specification(s) for application layer functional elements and interfaces supporting critical communications (e.g. Mission Critical Push To Talk)."[11]

[11] Source 3GPP SA6



Project Co-ordination Group (PCG)

TSG GERAN GSM EDGE Radio Access Network	TSG RAN Radio Access Network	TSG SA Service & Systems Aspects	TSG CT Core Network & Terminals
GERAN WG1 Radio Aspects	RAN WG1 Radio Layer 1 spec	SA WG1 Services	CT WG1 MM/CC/SM (lu)
GERAN WG2 Protocol Aspects	RAN WG2 Radio Layer 2 spec Radio Layer 3 RR spec	SA WG2 Architecture	CT WG3 Interworking with external networks
GERAN WG3 Terminal Testing	RAN WG3 lub spec, lur spec, lu spec UTRAN O&M requirements	SA WG3 Security	CT WG4 MAP/GTP/BCH/SS
	RAN WG4 Radio Performance Protocol aspects	SA WG4 Codec	CT WG6 Smart Card Application Aspects
	RAN WG5 Mobile Terminal Conformance Testing	SA WG5 Telecom Management	
		SA WG6 Mission-critical applications	

Figure 3: 3GPP & SA6 Organizational Structure

The seminal document for MCPTT is 3GPP TS 23.279 Functional Architecture and Information Flows to Support Mission Critical Push-To-Talk (MCPTT). This document was initially part of the 3GPP Release 13 specification and the latest version reflects Stage 2 requirements for 3GPP Release 15. This document specifies the functional architecture; features and data flows for MCPTT and it specifically addresses making MCPTT calls on multiple networks.

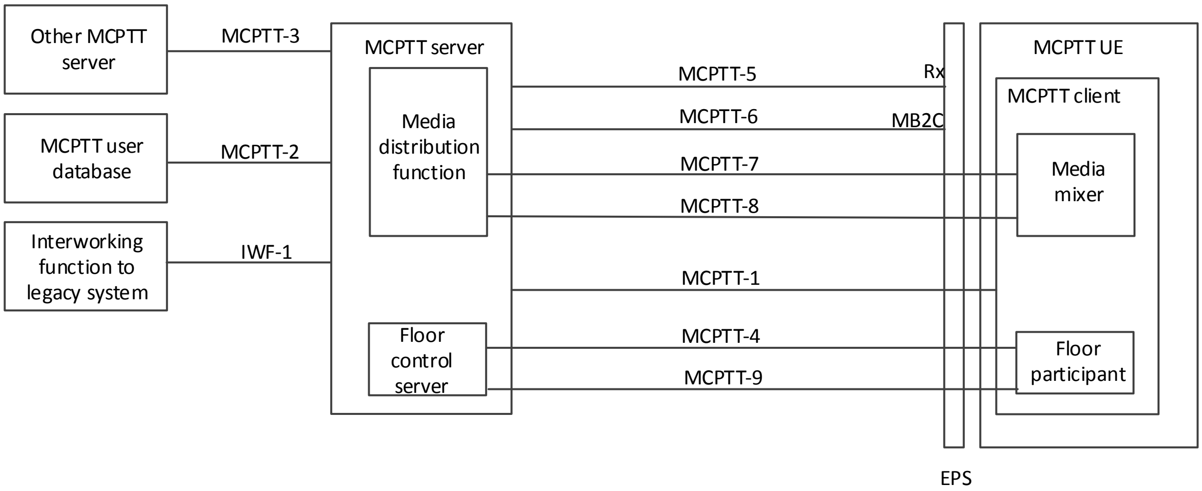


Figure 4: MCPTT Functional Model per TS23.379

Some things to note from Figure 4 are that MCPTT requires an integrated client application of the LTE device and a MCPTT server that connects to the LTE core network. The MCPTT server can also run the database functions, as this is all software implemented. The use of the IP Multimedia System (IMS) as optional for MCPTT is signficant. Without the need for an IMS function, this can simplify call processing, reduce cost and allow for unique deployments such as backpack deployable systems. Unlike voice over LTE (VoLTE), which mandates use of IMS, MCPTT offers some flexibility. It is very likely though that MCPTT delivered from a MNO will utilize the same IMS core as VoLTE.

The primary interface from the MCPTT application server to LMR will be accomplished via the IWF-1 interface. The Interworking Function (IWF) is defined in 3GPP TS 23.283 Mission Critical Communication Interworking with LMR Systems. Interworking in this context is a means of communication between MCPTT and LMR systems whereby users obtaining service from a MCPTT system can communicate with LMR users who are obtaining their service from a LMR network. The purpose of the IWF is to adapt LMR data and signaling to MCPTT data flows. This means that there will be no direct connection between a P25 ISSI, such as Colorado's Digital Trunked Radio System (DTRS), into the NPSBN LTE network without an IWF implemented. As of the latest version of the document for Release 15, there remains a tremendous amount of work to further define the IWF.

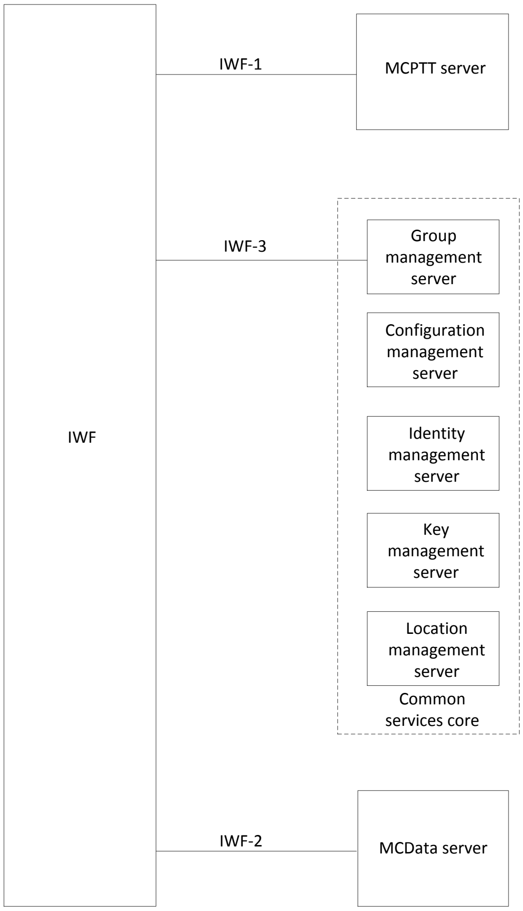


Figure 5: IWF Functional Model per 3GPP TS 23.283

Although work is being done in 3GPP to define the LMR IWF Gateway interface specifications, the actual specification from a LMR network to the LMR IWF Gateway is not being defined by any industry standards organizations.

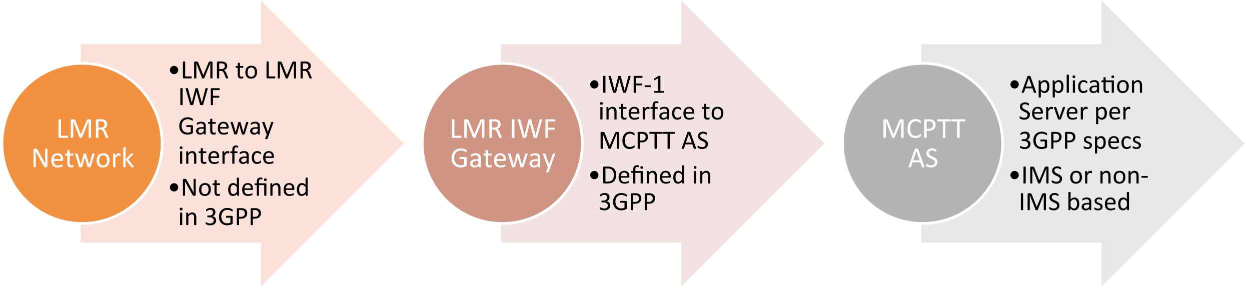

LMR Network
•LMR to LMR IWF Gateway interface
•Not defined in 3GPP
LMR IWF Gateway
•IWF-1 interface to MCPTT AS
•Defined in 3GPP
MCPTT AS
•Application Server per 3GPP specs
•IMS or non-IMS based

Figure 6: LMR to IWF Functions

From a basic standpoint there are two major LMR interfaces utilized in the state. The first is the P25 ISSI interface, which is standardized and does work in a multi-vendor implementation within the state. The limitations of this interface and interoperability are well known by the users. The second interface uses a donor radio and is generically called Radio over IP (RoIP). The Bridging Systems Interface (BSI) was created nearly a decade ago to help facilitate RoIP interoperability with essentially reference implementation of session initiation protocol (SIP) signaling However, the Department of Homeland Security (DHS) support has waned in recent years and the BSI was never developed to its fullest potential. Many RoIP gateways now emulate P25 ISSI and this is quickly becoming the de facto standard for LMR interoperability. Additionally, the CSSI interface used for PSAP interoperability is being considered as an interface for the IWF Gateway.

LMR user and signaling data flows from a P25 ISSI and a RoIP gateway vary differently between each other and MCPTT. Colorado's statewide LMR system, the DTRS[12], utilizes P25 technology for PTT voice services. The DTRS P25 network can and does connect to other P25 networks via ISSI. The use of ISSI allows disparate P25 systems like Front Range Communications Consortium (FRCC) and City of Westminster to be connected via a standardized SIP based interface or ISSI. P25 also utilizes a different voice codec called AMBE. MCPTT uses the AMR codec, which is used globally on billions of devices – license free, whereas the AMBE codec is licensed at great cost to public safety. This means that MCPTT to LMR communications will be required to transcode from AMBE to AMR.[13] Transcoding is not a problem in itself; however one of the issues with P25 implementation within the state is that each P25 network uses its own security and encryption protocols, thus making key sharing costly and complicated. Every single ISSI connection to the IWF would need to be separately and securely connected – making management and cost of this implementation unfeasible. Use of an ISSI hub as depicted in Figure 7 would be a more efficient way to interconnect MPCTT to state

[12] See http://www.oit.state.co.us/cto/dtrs for more information on DTRS.
[13] See ISSI whitepaper for extended details.

and local LMR networks. However, there is a cost for hardware, software and maintenance of such a solution.

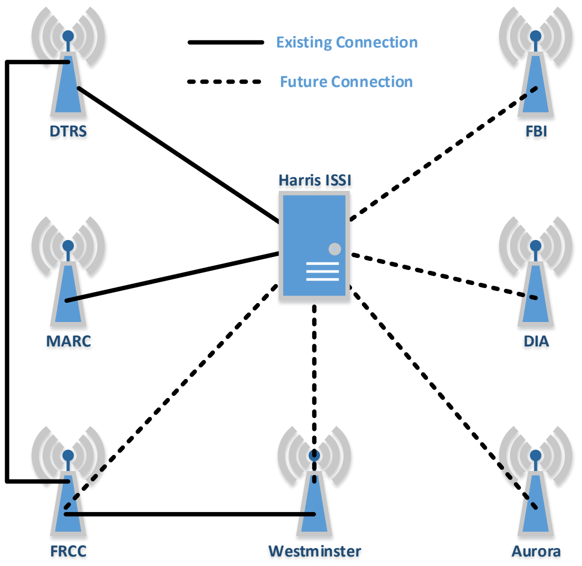


Figure 7: Proposed Front Range ISSI Interconnection *Source: Rendered from Harris Corp. Info*

QCI Updates

Besides coverage, the feature that best defines public safety grade LTE is the use of Quality of Service (QoS) for delivering voice and data to users when the network is loaded. For applications in a 3GPP LTE system, the use of QoS Class Identifiers (QCI) is the mechanism that defines the scheduling treatment of data throughout the network. The QCI is enforced at the air interface between the user equipment (UE) and eNodeB, on the backhaul from the eNodeB to the evolved packet core (EPC) and from there to the application server. This requires a significant amount of engineering to ensure that QoS performance metrics can be met. With the advent of VoLTE, the use of QCI was mandated to ensure end-to-end voice quality was preserved and as good as or better than circuit switched voice.

The creation of mission critical applications came after the development of the initial QCI values for LTE and therefore modifications to the standard were required to ensure that emergency communications took precedence over commercial traffic. The updates can be seen in Table 1: QCI Table per 3GPP TS 23.303 for MCPTT. This table defines whether a traffic or signaling bearer offers guaranteed or non-guaranteed bit rates of service within a specific window of latency and jitter. The traffic is then prioritized with the highest priority traffic being scheduled first. The highest priority traffic is now allocated to MCPTT. The signaling layer for MCPTT is given the highest priority to ensure that devices are alerted first before data is sent.

QCI	Resource Type	Priority Level	Packet Delay Budget	Packet Error Loss Rate (NOTE 2)	Example Services
1 (NOTE 3)	**GBR**	2	100 ms (NOTE 1, NOTE 11)	10^{-2}	Conversational Voice
2 (NOTE 3)		4	150 ms (NOTE 1, NOTE 11)	10^{-3}	Conversational Video (Live Streaming)
3 (NOTE 3)		3	50 ms (NOTE 1, NOTE 11)	10^{-3}	Real Time Gaming
4 (NOTE 3)		5	300 ms (NOTE 1, NOTE 11)	10^{-6}	Non-Conversational Video (Buffered Streaming)
65 **(NOTE 3, NOTE 9)**		**0.7**	**75 ms** **(NOTE 7, NOTE 8)**	10^{-2}	**Mission Critical user plane Push To Talk voice (e.g., MCPTT)**
66 **(NOTE 3)**		**2**	**100 ms** **(NOTE 1, NOTE 10)**	10^{-2}	**Non-Mission-Critical user plane Push To Talk voice**
5 (NOTE 3)	Non-GBR	1	100 ms (NOTE 1, NOTE 10)	10^{-6}	IMS Signalling
6 (NOTE 4)		6	300 ms (NOTE 1, NOTE 10)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7 (NOTE 3)		7	100 ms (NOTE 1, NOTE 10)	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8 (NOTE 5)		8	300 ms (NOTE 1)	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9 (NOTE 6)		9			
69 **(NOTE 3, NOTE 9)**		**0.5**	**60 ms** **(NOTE 7, NOTE 8)**	10^{-6}	**Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)**
70 **(NOTE 4)**		**5.5**	**200 ms** **(NOTE 7, NOTE 10)**	10^{-6}	**Mission Critical Data (e.g. example services are the same as QCI 6/8/9)**

Table 1: QCI Table per 3GPP TS 23.303

The initial QCIs 1-9 have been supported for several years in all LTE networks. The only large-scale deployment of the latest mission critical QCI implementation is with SKTelecom in South Korea. However, most MNOs in the United States will be undergoing significant software upgrades in 2018 for their respective networks, which will bring in 3GPP Release 13 features – including MC QCI values.

Currently both Verizon and AT&T have offered QoS for specific applications like Kodiak PTT, Mutualink and ESChat on their commercial network but these applications are using the standard commercial QCI values. Verizon provides their Private Network Traffic Management and AT&T has a similar service called Dynamic Traffic Manager. These provide QCI above commercial traffic but not at mission critical levels. It should be noted that the QoS offering to FirstNet will be initially based off of the AT&T DTM offering that is available commercially.

Enhanced Multimedia Multicast (eMBMS)

Typical communications in a LMR network are on a broadcast type of communications channel or one to many communications simultaneously. Users are assigned a talk group with which to communicate half-duplex with each other. It consumes few resources and allows large-scale group communications to happen with ease. However, in an LTE network the communication is unicast or one-to-one. This means that a data session needs to be established for each device that is being communicated to individually. The ability to communicate one-to-many in LTE is called eMBMS and was initially introduced into the 3GPP standards over 12 years ago.

The original intent of eMBMS was to deliver broadcast TV to devices over the network. However, the reservation of spectrum and complexity in the device and network design and most importantly changes in view habits (think YouTube and Netflix) have diminished the necessity for eMBMS. Currently only one network, Telstra in Australia, has deployed eMBMS in very limited areas. Nearly three years ago Verizon actually showcased eMBMS during the Bronco's superbowl in New York but never deployed it and AT&T showcased eMBMS during a college football national championship game. It is unknown and highly speculative whether any MNO will deploy eMBMS or wait until 5G to enable multicast services.

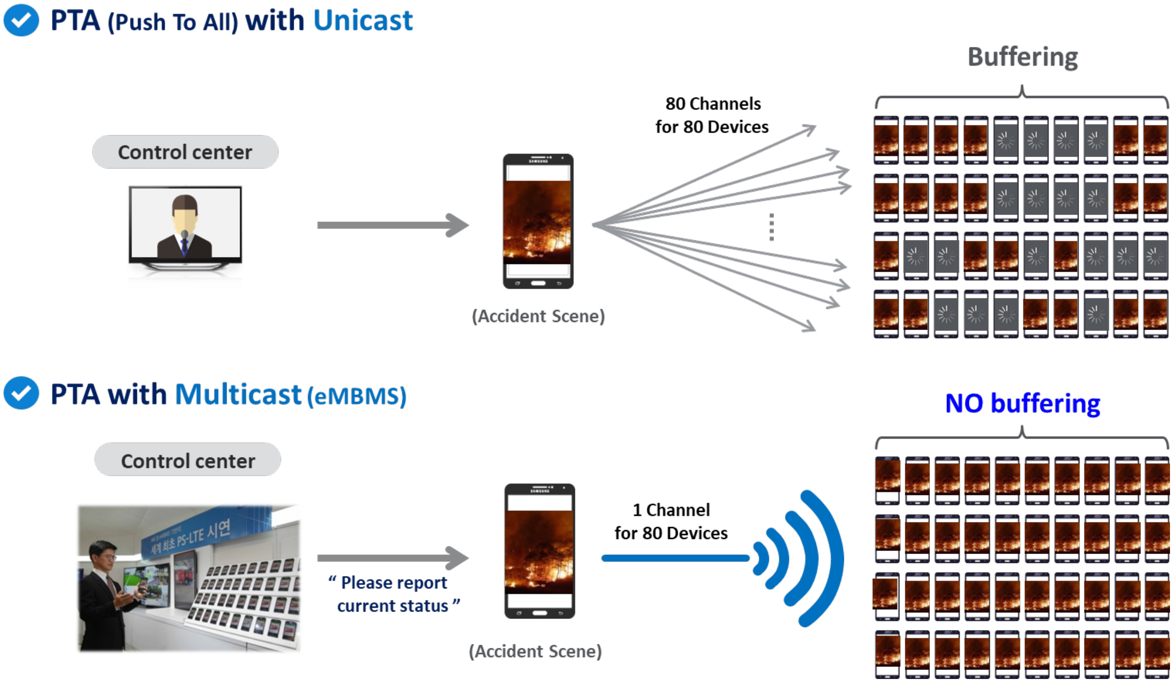


Figure 8: eMBMS Example   *Source - Samsung*

The use of eMBMS for public safety is crucial for large-scale events. The number of users that can be supported on MCPTT is directly coupled to the capacity of the site. If a data stream is 1

Mbps for each user, then a unicast system must support 80 Mbps for 80 users. In an eMBMS solution a single 1 Mbps stream would be allocated for all users simultaneously, thus allowing more capacity on the cell for other users. For MCPTT it is likely that supporting 300 users in a cell simultaneously, with no noticeable degradation is possible, given call modelling done by various vendors on VoLTE. However, the addition of live video calls, streaming video and augmented reality updates will likely consume a significant amount of bandwidth and necessitate the need for an efficient solution. The availability of eMBMS support in devices and in the network are less than likely from any MNO and for rural carriers like Commnet, Viaero and Union Wireless the use of eMBMS is not even a consideration. This is mainly due to the cost and complexity of deployment and management of the technology as a MBMS-GW, which has to be deployed in the core network and each eNodeB must have multi-cast coordination entity (MCE) capability added to it, which sometimes requires a hardware upgrade.

With QCI implementation and multiple bands available commercially on AT&T, the necessity for MCPTT enabled eMBMS is not an immediate need for Colorado users. However, Colorado does see the need for eMBMS due to the rapid growth of broadband and video as it reduces overall network capacity.

Proximity Service (ProSe) – LTE-Direct (LTE-D)

The use of simplex mode or device-to-device communications in LMR is a common occurrence especially for fire departments. Often times when arriving on scene the fire fighters use a vehicular repeater and tune their radios to a simplex radio channel. The simplex radio channel is connected to the repeater and then communicates to the LMR network. This is historically done to ensure coverage between users in a building where they may be in a basement or areas with poor external network coverage. Simplex communications are also done to cut down on voice traffic to dispatch that they do not need to hear and it releases LMR channels for other users. In theory, if coverage was good and there was sufficient capacity then the users would not have to utilize simplex mode.

LTE devices were never intended to directly communicate with each other, as it requires the use of the core network for communications. However, the ability to communication directly between devices is being developed for LTE commercially for commerce and vehicular device location.

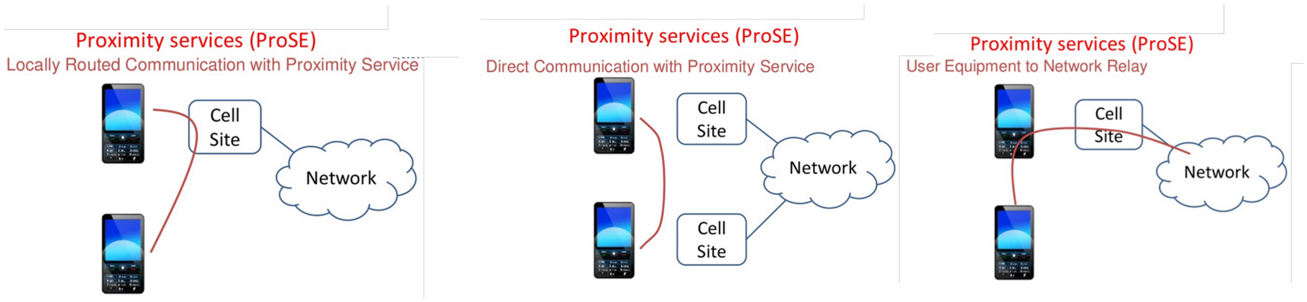

Proximity services (ProSE)
Locally Routed Communication with Proximity Service
Cell Site
Network
Proximity services (ProSE)
Direct Communication with Proximity Service
Cell Site
Network
Cell Site
Proximity services (ProSE)
User Equipment to Network Relay
Cell Site
Network

Figure 9: ProSe/LTE-D use case Source - 3GPP

LTE-D or ProSe is intended to provide direct device-to-device communications off network for operational support of public safety users that are out of LTE network coverage. The functionality is similar to operating in P25 simplex or direct mode. Operationally though, the performance of LTE-D devices may vary from P25 subscribers since LTE smartphone power will likely be limited to 23 dBm. This means that the ability to communicate long distances (e.g., over ½ mile) or through dense building materials (cinder block walls) will be limited compared to P25.

The development of LTE-D for public safety is conceptual at this time. There are currently no commercial devices, RF chipsets or system deployments anywhere in the world. The poor performance in non-line of sight conditions and the complexity of implementing MCPTT on the device are just some of the issues plaguing development. The main issue though is commercial interest in MCPTT LTE-D development. The frequency bands like Band 14 and commercial LTE bands used by AT&T (and other MNOs) require the use of the uplink or reverse link frequency band to transmit on for LTE-D mode. Implementation of this would require a change in the diplexer of the device and thus a layout change and increase in the bill of materials. With the increase in cost, low production volumes and performance issues, it is unlikely that LTE-D for public safety will be developed any further. The caveat to this though, is the development of LTE based vehicular communications or V2X (vehicle to everything). If breakthroughs and adoption of V2X happen with mass adoption commercially, public safety may be able to draft off of this success to enable public safety LTE-D.

Lastly, MCPTT is designed to work on an LTE network and it should be noted that in the current 3GPP specifications there is no additional functionality that will be supported for non-3GPP access.[14] This is potentially a very big issue in Colorado for several reasons. Current OTT applications i.e. Kodiak and ESChat do support calls over Wi-Fi and use of corporate Wi-Fi indoors. Current MCPTT implementations would lose this capability and require innovation beyond what is being proposed in 3GPP. One of the indoor coverage solutions provided by FirstNet is use of AT&Ts +40,000 Wi-Fi hotspots. If MCPTT is not available while in Wi-Fi coverage, this would need to be addressed from either a coverage, or functionality, perspective to ensure MCPTT works indoors.

[14] Per 3GPP TS23.303 Section 1 – "The present document is applicable primarily to MCPTT voice service using E-UTRAN access based on the EPC architecture …but no additional functionality is specified to support non-3GPP access."

Vendor Solutions

As mentioned before, the MCPTT system can be split into different parts to include the user device, client or user application and application server. MCPTT does require tight integration between the network and application to ensure performance. A few different implementations have been developed by vendors to address how large and small jurisdictions can cost effectively integrate in their LMR networks with MCPTT.

For research on this paper Samsung, Nokia, Bittium, Nemergent, Harris, Kodiak (pre-MSI) and Verizon were interviewed. It should be noted that MSI, AT&T and FirstNet were all contacted multiple times over a 4-week period and they chose not to discuss the topic of how to support interoperable MCPTT within the state. Other research information from 3GPP and previous meetings with ESChat and Mutualink were also used in developing this paper.

Samsung

In June, 2015 Samsung produced the first 3GPP based PTT demo using a full LTE network with IMS and eMBMS. Since then, they have created a 3GPP Release 13 MCPTT system. Samsung is not only one of the largest LTE handset developers, but they are a leading LTE infrastructure company too.

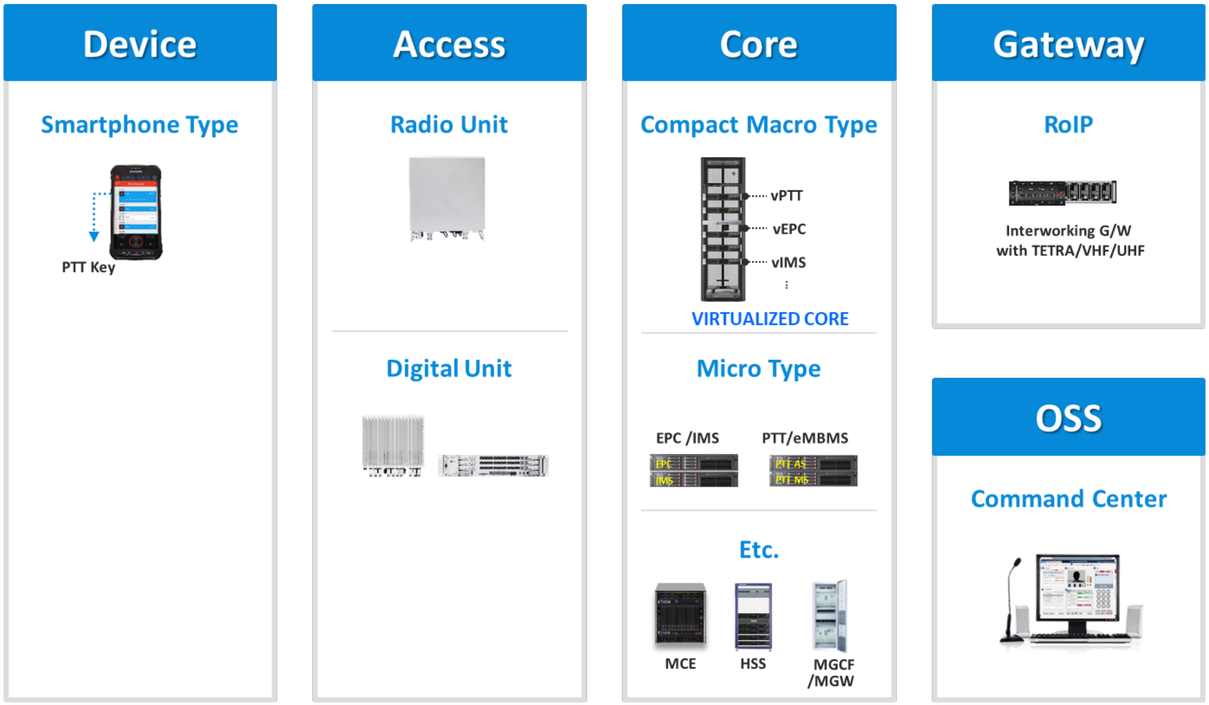


Figure 10: Samsung End-to-End MCPTT Source – Samsung

Samsung is the only vendor that is able to offer an end-to-end solution, which is impressive. However, this raises some interoperability concerns in that they have not had to work with any other vendors in their implementation nor have they chosen do so with any North American deployments. They are not one of the major infrastructure vendors for FirstNet but they are a major handset vendor with the Galaxy line of devices. Additionally, they are designing handsets that are geared towards public safety and these may be introduced into the US market pending demand from FirstNet. It is likely that Samsung will be a device-only player for Colorado users.

Nokia & SKTelecom

Nokia is one of the largest infrastructure vendors globally for LTE. In February, 2016 they debuted the first 3GPP compliant MCPTT system. It was based on Release 12 due to QCI support in devices but the infrastructure is Release 13 compliant. This system was a combined effort from Cybertel and Bittium on devices, SKTelecom with application development and Nokia on infrastructure.

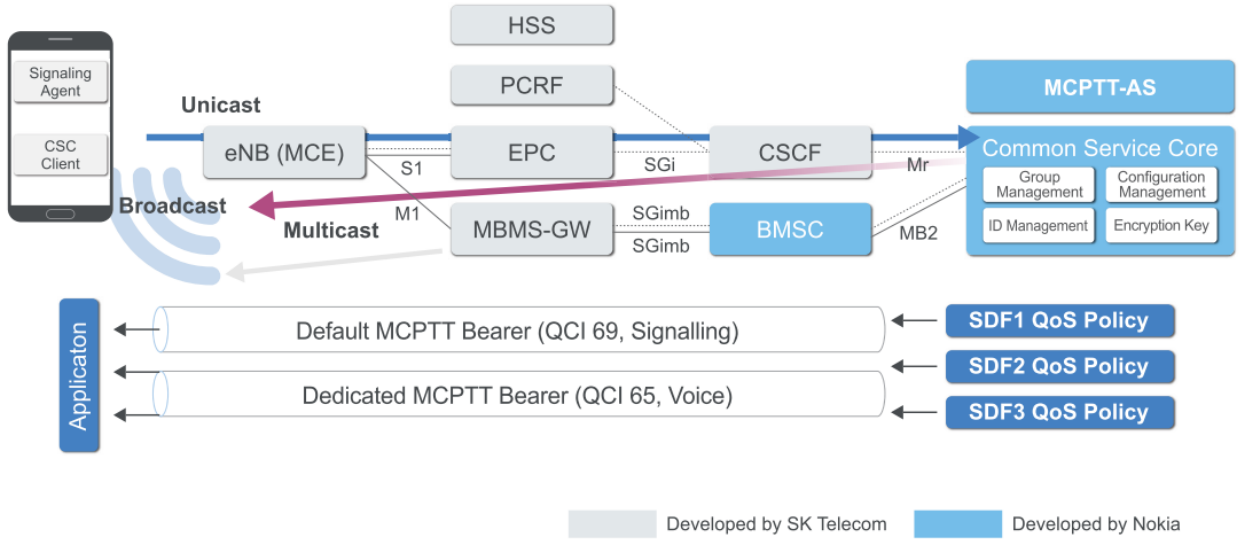


Figure 11: Nokia & SKTelcom MCPTT Deployment   Source - SKTelecom

The Nokia Group Communications solution offers advanced features beyond MCPTT with integrated instant messaging and push-to-video offerings. Support for one-to-one, one-to-many and priority calls is supported across the network with all QCIs support enabled.

- The system can be implemented in a deployable system such as a backpack LTE system or on a dedicated LTE network.
- Currently only the Android OS is supported and the client application is tied directly to the application server – not interoperable with any other Application Server.
- Full eMBMS integration for one-to-many support.
- If no QoS required, can be run as an OTT application.
- AES encryption supported with private call functionality and emergency button integration.
- RoIP connection available now, direct gateway being considered for ISSI in +12 months.
- Dispatch console support.
- Fully redundant solution.

Nemergent

Nemergent is a start-up company that is backed by academic R&D efforts in Spain regarding MCPTT on LTE. Their aim is to address the interoperability issues surrounding MCPTT and develop an open platform based on 3GPP MCPTT in an effort to reduce barriers to entry in the market. Their concept is so innovative that they were one of the winners of the NIST Public Safety Innovation Acceleration Program grant. With this grant they founded the Mission Critical Open Platform[15] (MCOP) project.

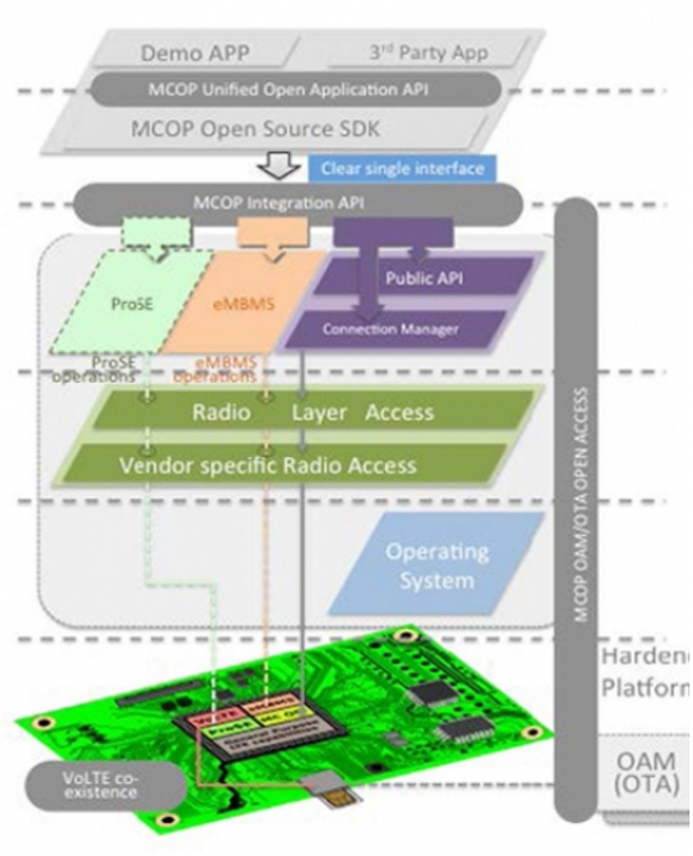
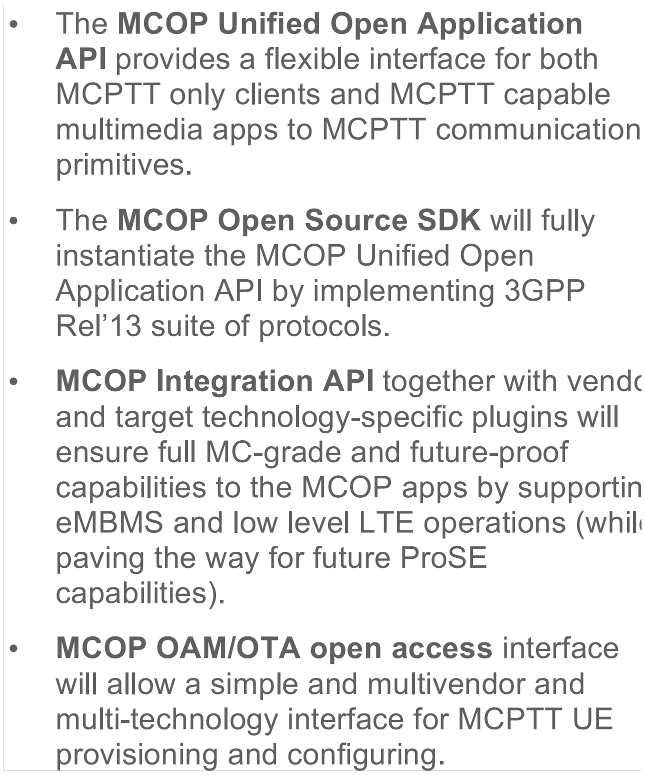


Figure 12: MCOP Platform Description Source - MCOP



- The **MCOP Unified Open Application API** provides a flexible interface for both MCPTT only clients and MCPTT capable multimedia apps to MCPTT communication primitives.
- The **MCOP Open Source SDK** will fully instantiate the MCOP Unified Open Application API by implementing 3GPP Rel'13 suite of protocols.
- **MCOP Integration API** together with vendc and target technology-specific plugins will ensure full MC-grade and future-proof capabilities to the MCOP apps by supportin eMBMS and low level LTE operations (whil paving the way for future ProSE capabilities).
- **MCOP OAM/OTA open access** interface will allow a simple and multivendor and multi-technology interface for MCPTT UE provisioning and configuring.

Nemergent is creating a unified open Software Developers Kit (SDK), application and integration Application Programming Interface (API) for all developers to use. In theory this would allow multiple vendors to communicate with each other's MCPTT implementations. The ETSI Plugtest[16] demonstrated this multi-vendor interoperability with an 85% success rate on the

[15] https://www.mcopenplatform.org/

[16] https://www.mcopenplatform.org/wp-content/uploads/2017/11/TCCA-Webinar_MCPTT-Interoperability_Results-and-Future-Projects_v2.pdf

first try. The solutions provided by Nokia and Samsung are MCPTT compliant but they cannot work with each other. For instance a Samsung MCPTT device application cannot work with a Nokia MCPTT Application Server – even though they are both 3GPP developed. This is because the APIs specific to how the device interacts with the application and application server are not defined. It should be noted that Samsung, Kodiak, MSI and Nokia did not participate in the plugtest and all have stated that their MCPTT applications only work within their infrastructure.

Initial results look good and the aspirational goal would be for all vendors to implement this open platform but MCOP is not an official liaison with 3GPP or Group Speciale Mobile Association (GSMA). Current participants in this open effort are limited to smaller partners and this may end up in the graveyard of well-intentioned but poorly supported efforts. The requirement to ensure interoperability with multiple MCPTT vendors should be mandated by FirstNet and the state.

Bittium

Bittium is a small device manufacturer that has developed several LTE smartphone devices, tablets and USB models for the public safety market. They have supported the SKTelecom and Nokia trial in addition to the ETSI MCPTT Plugtest. After seeing the amount of effort necessary for MCPTT integration into a single vendor solution they realized they needed a more flexible application platform to work with different MCPTT vendors. Bittium is opening up their device to developers via SDK and API to help ensure MCPTT interoperability via the MCOP project.

Currently they have a proof of concept API that integrates in Expway middleware to enable eMBMS for multi-user support. The ability to support both VoLTE and MCPTT on the same device brings up several issues they're working on. Both these applications use the same network authentication credentials on the user services identity module (USIM) and SIP pre-conditions for access to the IMS. 3GPP standards do not address this and it is likely that MCPTT and VoLTE client software will come from different vendors. Ensuring there are not device interoperability sharing issues between applications on the device that either prohibit use or diminish security are all being addressed in this process.

Commercial grade trials won't be available until mid-2018.

Harris

Harris is a supplier of LMR networks within Colorado, devices and applications like the Harris BeOn PTT system which has been operational for a couple of years in Colorado. Looking towards the future of MCPTT, Harris has taken a leadership role in 3GPP as the official rapporteur for the IWF-1 interface and gateway. Having the second largest LMR vendor lead this standardization effort for interworking between LMR and LTE is encouraging for the state. Harris was also one of the 19 companies that completed the ETSI MCPTT Plugtest successfully with their client application, application server and devices. (NOTE: They achieved 90% compliance whereas the average was 85%)

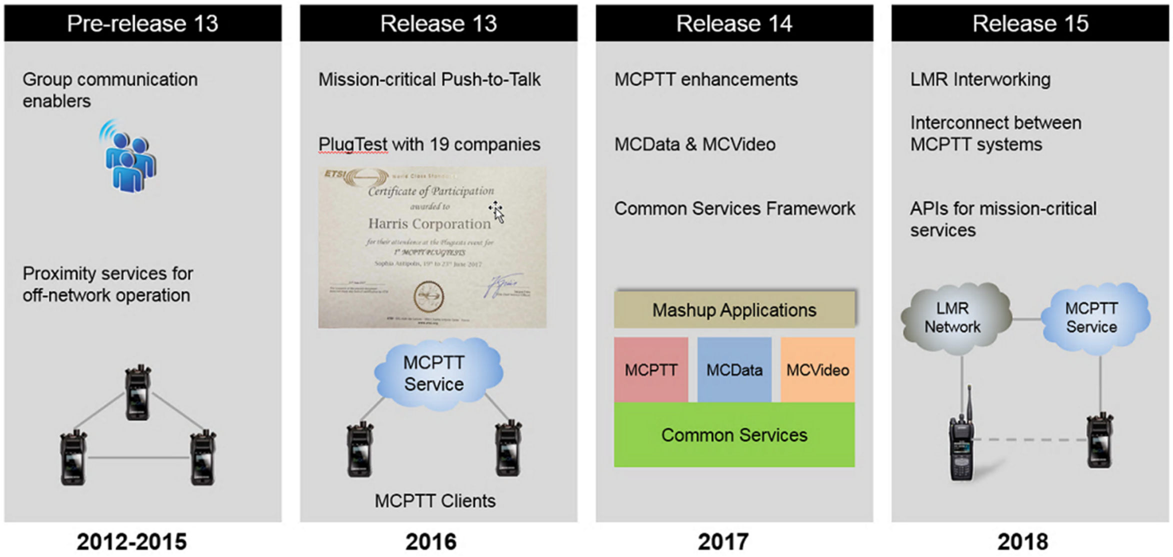

Pre-release 13
Group communication enablers
Proximity services for off-network operation
2012-2015
Release 13
Mission-critical Push-to-Talk
PlugTest with 19 companies
ETSI World Class Standards
Certificate of Participation
awarded to
Harris Corporation
for their attendance at the Plugtests event for
1st MCPTT PLUGTESTS
Sophia Antipolis, 19th to 23rd June 2017
MCPTT Service
MCPTT Clients
2016
Release 14
MCPTT enhancements
MCData & MCVideo
Common Services Framework
Mashup Applications
MCPTT
MCData
MCVideo
Common Services
2017
Release 15
LMR Interworking
Interconnect between MCPTT systems
APIs for mission-critical services
LMR Network
MCPTT Service
2018

Figure 13: Harris 3GPP Feature Schedule   Source - Harris

Basic MCPTT functionality was accomplished this year on their VIDA infrastructure and devices with Release 13 and 14 functions. Like Nemergent and Bittium, Harris is developing an API for their MCPTT application server to allow 3rd party development of MCPTT client software. The ability to interconnect multi-vendor MCPTT with LMR interworking is scheduled for late 2018 but trial networks are likely 18 months away in the mid-2019 timeframe.

One of the major issues with BeOn was subscriber scaling and the associated cost for PTT client licenses. The main source of this cost was the use of the AMBE vocoder in the software that was loaded onto each device. Harris has committed to MCPTT and will be using the AMR codec in their commercial release. This move will drastically reduce the cost for MCPTT per device and should decrease the cost of entry.

Harris has also worked on addressing the implementation of MCPTT from a business case perspective. Their solution can be implemented in three different variants:

1. On Premise – the MCPTT application server (AS), IWF Gateway and P25 interfaces are all located or hosted within the PSE network.
2. Cloud Hosted – A VPN connection from the P25 network connects to a cloud hosted MCPTT AS and IWF Gateway, these are then connected to the MNO LTE network.
3. Carrier Centric – The P25 to 3GPP IWF is hosted by the PSE and connected via VPN to the MNO which hosts the MCPTT AS and LTE network services.

With the first two options, the proposed Harris solutions offer connectivity to multiple mobile networks and full interoperability between the LMR and LTE networks regardless of who is providing service.

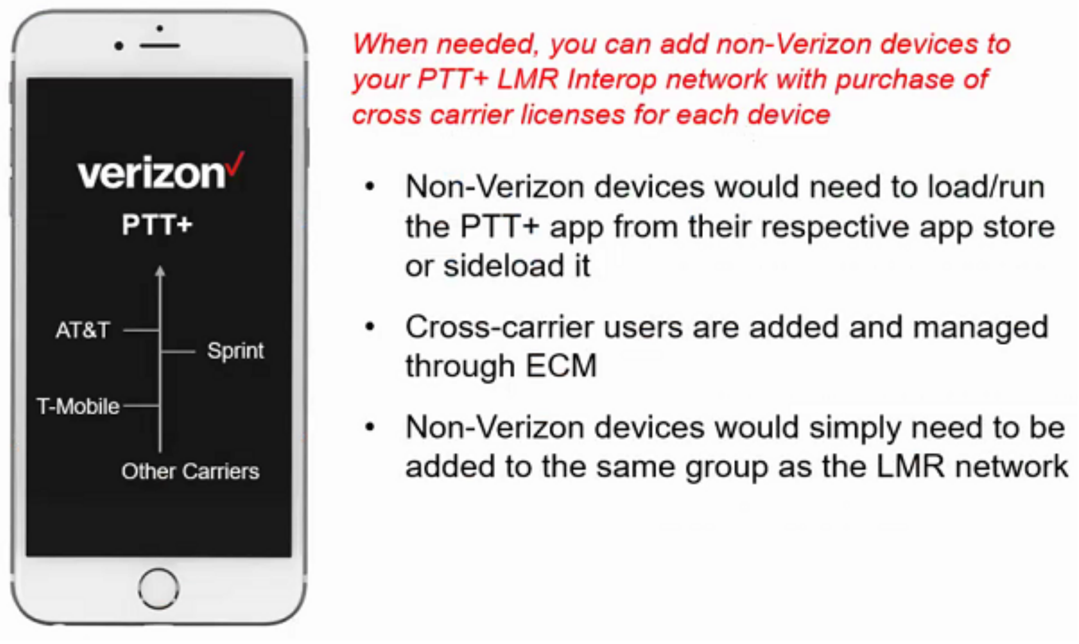
Additionally, Harris is looking to provide PSEs a mobile virtual network operator (MVNO) service for common billing of MCPTT, which could be provided in any of the three Harris deployments and a common bill for services would be provided (i.e. flat rate) to the PSE billing departments. This could help make procurements and capturing of costs much more efficient for agencies.

Harris agrees that ProSe/LTE-D development and deployment is not happening now and it is unknown when it will be available. They have also seen major performance issues, which caused them to update the XL250 combination P25/LTE device. This radio will support all Verizon, AT&T and FirstNet bands with MCPTT integration.

Verizon

Verizon currently offers PTT service on their network called PTT+. This service is provided via a hosted solution from Kodiak Networks. With this solution, the PTT+ system offers RoIP and ISSI LMR interworking via a VPN connection from the agency interface to the Verizon/Kodiak hosted solution. Verizon does offer some QoS differentiation with their Private Network Traffic Management solution. However, moving forward when serving public safety, Verizon has committed to providing upgrades to MCPTT that will have priority and preemption capabilities with no additional cost to users.

Verizon is also offering cross carrier support for PTT+ with the Kodiak solution. To our knowledge, they are the only MNO to offer this. Since the Kodiak solution is hosted in the cloud, it provides service from the same system to Verizon, AT&T and Sprint. In theory this service could be used on LTE networks such as Viaero, Commnet and Union Wireless using an Internet connection.



When needed, you can add non-Verizon devices to your PTT+ LMR Interop network with purchase of cross carrier licenses for each device

- Non-Verizon devices would need to load/run the PTT+ app from their respective app store or sideload it
- Cross-carrier users are added and managed through ECM
- Non-Verizon devices would simply need to be added to the same group as the LMR network

Figure 14: Verizon Cross Carrier Support *Source: Verizon*

The availability of Verizon supported cross carrier interoperability is industry leading and game changing in several aspects. However there are some requirements for this service:

- The PSE must have at least one device with service on Verizon. All other non-VZW devices would link to this account for PTT+ management.
- Accounts and talk groups are managed from the VZW Enterprise Contact Management (ECM) tool.
- The VZW PTT+ application from Google or Apple would need to be installed on the device.
- The serving MNO would be best effort data as any QCI parameters would not be available in the other network.

Verizon stated this is currently in use by a few agencies and they will begin to market it publically. AT&T has declined to interoperate with their talk groups on their solution, thus a new VZW talk group definition would need to be added to manage these users. Their current system supports AES 256 bit encryption and they are looking at FIPS 140-2 compliant devices, but the cost seems prohibitive at the time.

Verizon is also committed to providing ISSI and PSAP CSSI console interfaces into a 3GPP MCPTT solution. They are currently pushing their vendor Kodiak/Motorola to provide them with a 3GPP MCPTT compliant solution by mid-2018. They are creating an Excel template that can be provided to agencies to define talk groups in a common schema. This spreadsheet can then be automatically uploaded to the MCPTT AS with all the proper talk groups defined.

From a QoS perspective the major issue for MCPTT support is from the device. The Kyocera Duraforce Pro and Sonim XP5 are the only devices that support PTT+ and QCI. VZW is working to provide this capability to a majority of their device portfolio in the future for MCPTT.

Recommendations and Deployment Options

MCPTT can be deployed in a variety of ways. This flexibility has caused some vendors like Harris and Nokia to explore these various options. ***There are some functional and operational differences in each deployment, but the majority of the MCPTT deployment options are business case driven.***

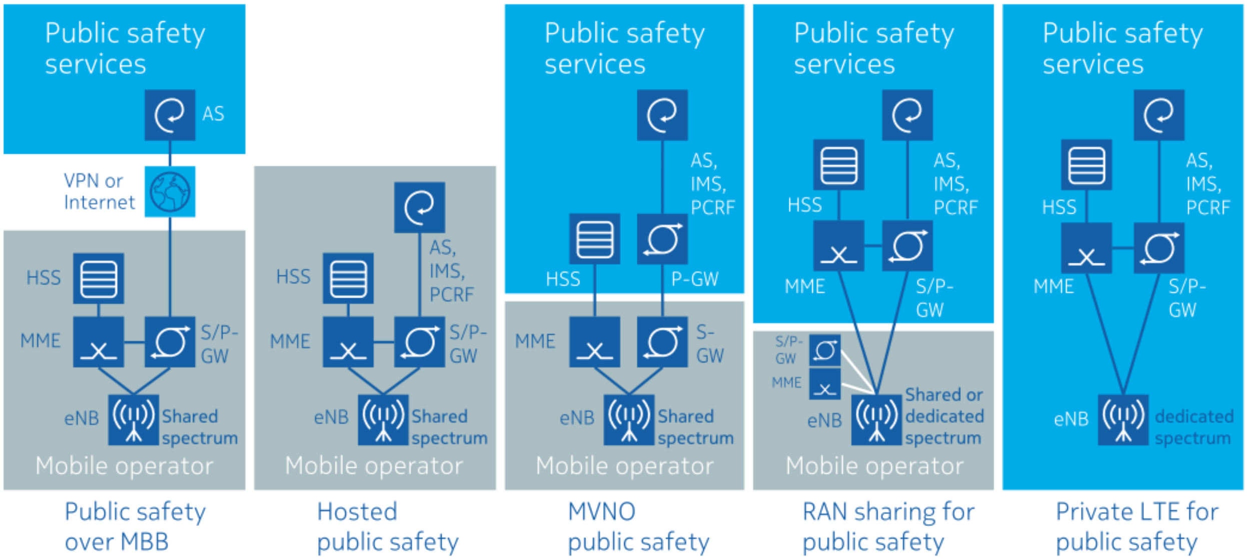


Figure 15: MCPTT Deployment Options   Source - Nokia

Figure 15 shows the range of deployment options from a private LTE network solution, which would be similar to a full opt-out scenario envisioned by Rivada Networks, to a hosted public safety network envisioned by FirstNet. The main emphasis of any of these proposed deployments is that interoperability between multiple, disparate LMR networks and LTE networks is a requirement. The aforementioned deployment options in their default state are not interoperable for users in the state.

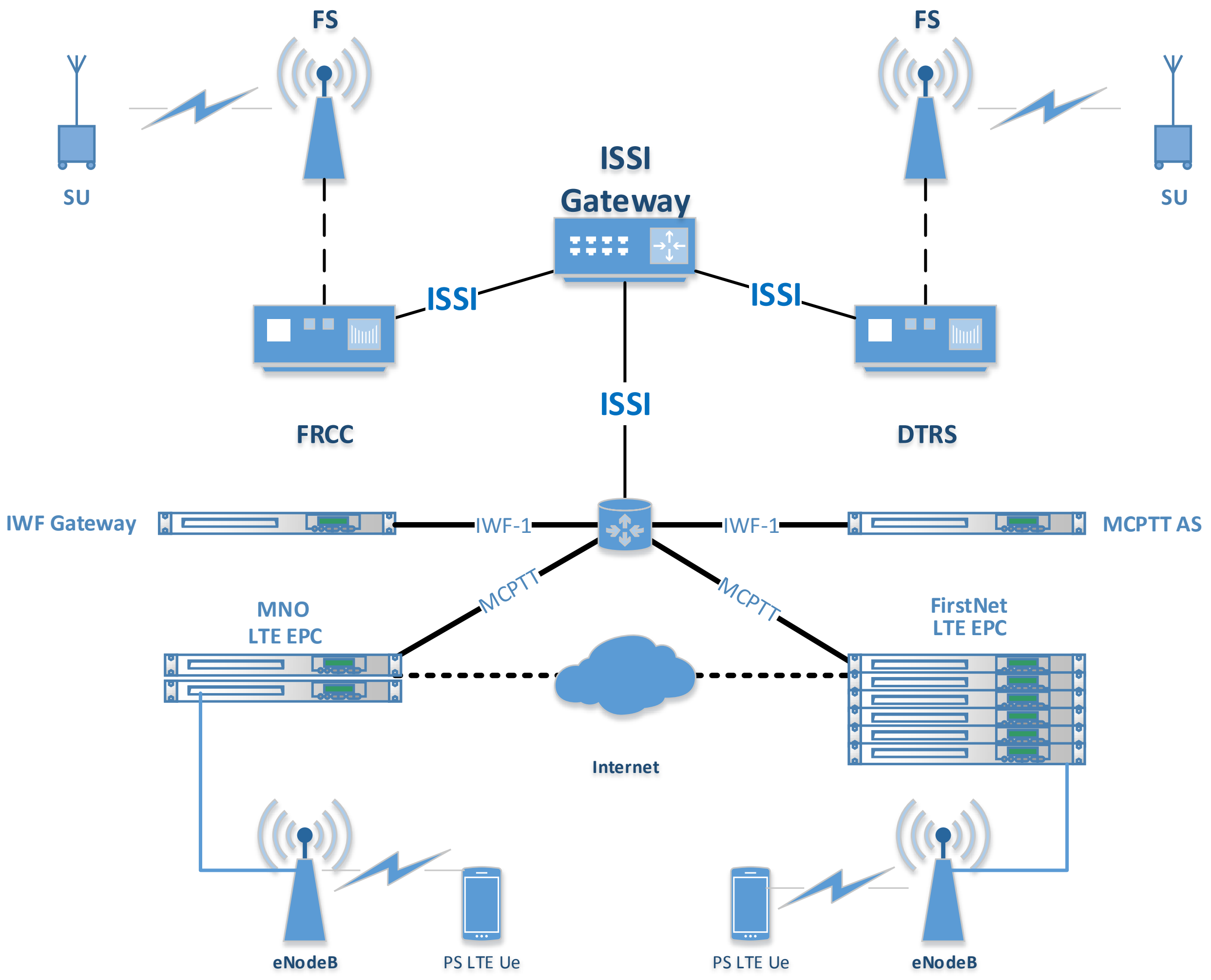


Figure 16: Example MCPTT & ISSI Deployment Diagram

Figure 16 depicts a proposed MCPTT deployment option that would provide a redundant VPN connection to a future statewide P25 ISSI hub (depicted in the first option – Public Safety over mobile broadband (MBB)). This would be a cost effective and easier to secure single point of entry into the P25 LMR networks in the state. It would also allow support for multiple LTE MNOs that are utilized across the state. This would require agencies to provide ISSI VPN access to their networks, establish interoperable talk groups and provide maintenance support for these interfaces.

MCPTT Recommendations

Luckily, there are technology solutions that are cost effective and commercially available to the state. Several solutions are presented in detail in this whitepaper that offer interoperability between the various LMR networks in use by agencies and the cellular service they are using. The following are suggested requirements that Colorado should adopt in a MCPTT solution:

1. Use of 3GPP standards based MCPTT solution that can be software upgradeable with each systems release in both the device client and application server.
2. The application server and client application should have open APIs for SDKs to allow maximum vendor interoperability and competition for best in class implementation.
3. The system should allow for both hosted and local implementations for integration into existing P25 ISSI, CSSI and non-ISSI based LMR systems. This includes the ability to relay simplex LMR communications on MCPTT.
4. The MCPTT service should work across **all mobile operator networks utilized by PSEs in the state**, including nationally, roaming internationally and over Wi-Fi.
5. The MCPTT solution should be able to implement all of the talk groups already defined across the state, with proper authentication and security – allowing only those authorized access to specific talk groups.
6. Support for a both Android and iOS devices is required.
7. The MCPTT solution must be cost effective to implement for all agency sizes with minimal if any impact to the user on cost and complexity.

One of the most important capabilities for public safety is to operate across MNOs. This capability can be achieved with hosted MCPTT solutions offered by several MCPTT vendors and by Verizon Wireless. Based on what is currently known, the AT&T/FirstNet PTT/MCPTT solution will not be interoperable with any other users who are not on their network, which could be a major setback to the nationwide interoperability envisioned in the Spectrum Act of 2012. However, the AT&T/FirstNet network is fully capable of meeting most of the aforementioned MCPTT requirements for the state either now or in the near future with coming MCPTT releases. The intent of this whitepaper is the draw attention to the importance of MCPTT and to push the vendor community and FirstNet to ensure MCPTT interoperability across all the agencies in Colorado and across the nation.

Glossary

Acronym	Definition
3GPP	Third Generation Partnership Project
AMBE	Advanced Multiband Excitation
API	Application Programming Interface
AS	MCPTT Application Server
CSSI	Console Subsystem Interface
DHS	Department of Homeland Security
DMR	Digital Mobile Radio
DTRS	Digital Trunked Radio System
eMBMS	Enhanced Multimedia Broadcast Multicast System
FRCC	Front Range Communications Consortium
iDEN	Integrated Digital Enhanced Network
IMBE	Improved Multiband Excitation
IMS	IP Multimedia System
IP	Internet Protocol
ISSI	Inter RF Subsystem Interface
IWF	Interworking Function
LMR	Land Mobile Radio
LTE	Long Term Evolution
LTE-D	LTE Direct
MCPTT	Mission Critical Push To Talk
MNO	Mobile Network Operator
MSI	Motorola Solutions Incorporated
MVNO	Mobile Virtual Network Operator
NPSBN	National Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
OIT	Governor's Office of Information Technology
OTT	Over The Top
P25	Project 25
PoC	Push To Talk Over Cellular
ProSe	Proximity Services
PSE	Public Safety Entity
PTT	Push To Talk
QCI	Quality of Service Class Identifier
QoS	Quality of Service
RoIP	Radio Over IP

SA6	Systems Architecture Group 6
SDK	Software Developers Kit
SPP	State Plan Portal
V2X	Vehicle to Everything
VPN	Virtual Private Network