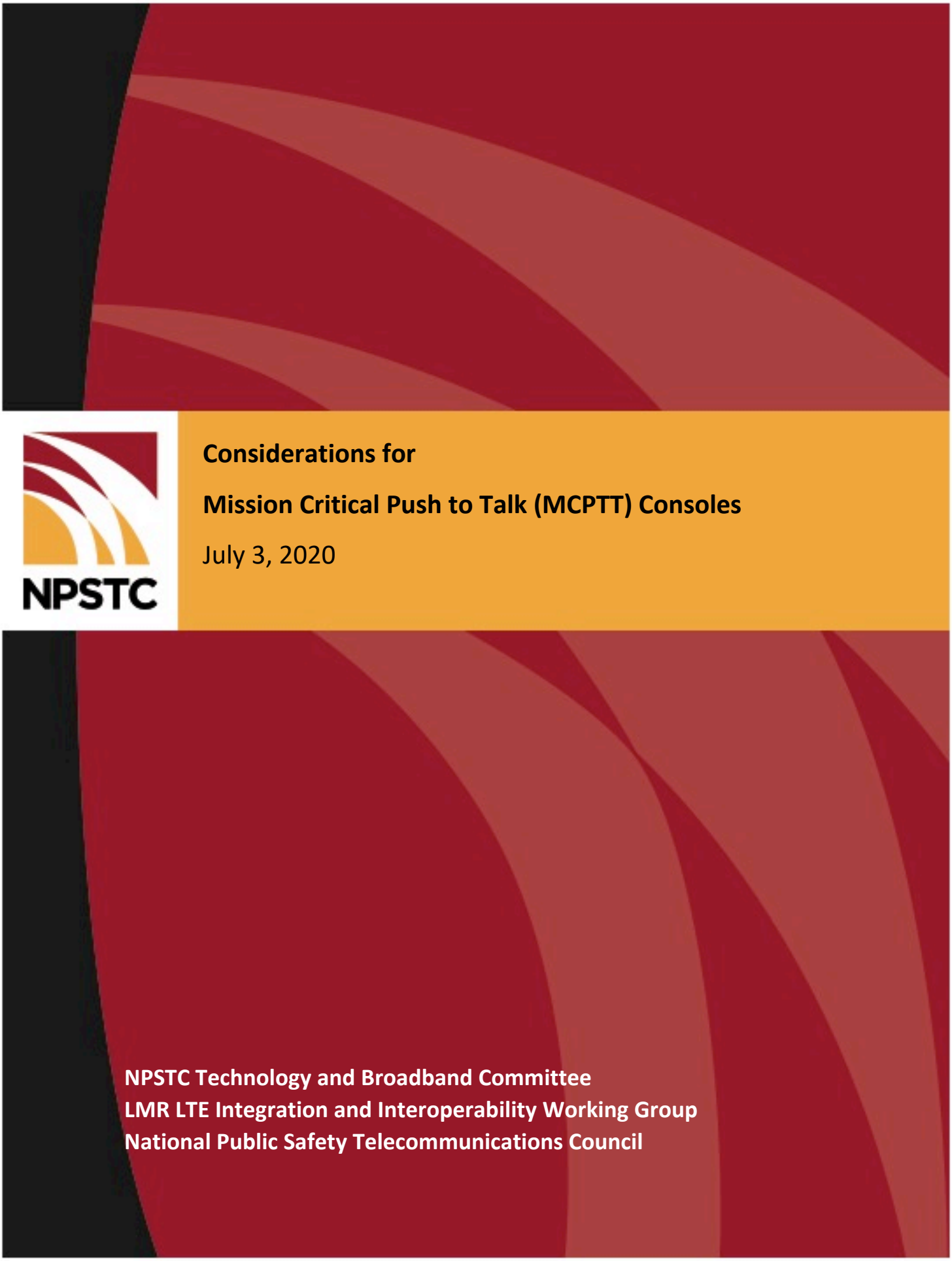

Considerations for

Mission Critical Push to Talk (MCPTT) Consoles

July 3, 2020

NPSTC Technology and Broadband Committee
LMR LTE Integration and Interoperability Working Group
National Public Safety Telecommunications Council

TABLE OF CONTENTS

Executive Summary

This report provides an overview of selected technical and operational issues associated with the implementation of Mission Critical Push-to-Talk (MCPTT) on the Nationwide Public Safety Broadband Network (NPSBN), also known as FirstNet. Specifically, this report focuses on MCPTT consoles used by public safety agencies. The information in this report captures the discussions of the LMR LTE Integration and Interoperability Working Group and represents the output of its deliberations. It is believed to be accurate as of the publication date.

Emergency Communications Centers (ECC) [also known as "control rooms" in Europe] provide daily command and control support for first responders. Today, virtually all public safety agencies use some type of Land Mobile Radio (LMR) console to manage their mission critical voice communications. Consoles supporting LMR have evolved over many years and include a large set of features and capabilities to support conventional and trunked radio systems. Cellular Push to Talk (PTT) services are currently available on most commercial cellular systems and some specialized PTT systems [1]are available on FirstNet. However, MCPTT solutions are different from these existing PTT applications in that they are built against a set of international standards and are designed to guarantee high availability together with extremely fast and reliable voice communications. MCPTT standards also provide for an array of expanded capabilities including transmission of data to support location, emergency alerting, creation of ad hoc talkgroups and integration with other Mission Critical Services including data and video devices.

A new type of console will be required to access and control MCPTT features and capabilities. MCPTT consoles may exist in different form factors that are suitable for use in an ECC or at other fixed locations, including Emergency Operations Centers (EOCs) and hospitals. Portable and transportable versions of MCPTT consoles will be needed to provide communications support at the scene of a large-scale tactical incident or during disaster operations when cellular infrastructure is unavailable.

It is important to note that the majority of public safety agencies are likely to use both LMR and MCPTT solutions at the same time. This dual use approach is necessary to give first responders sufficient time to test the MCPTT service in their respective areas to examine reliability and coverage. These early deployments should occur in non-mission critical environments until an agency decides that MCPTT is a suitable enhancement to their operations or a suitable replacement for some portions of the workforce.

This transitional state will require that the ECC have infrastructure in place to communicate with first responders operating on both systems. In the short term, console solutions must provide the ability for telecommunicators to manage radio traffic on both networks easily, with minimal disruption caused by the need to use multiple consoles and screens.

[1] These include PTT services designed for use by first responders, including Kodiak, Wave, and ES Chat.

In the longer term, a fully integrated console solution must allow for seamless access across all radio and cellular networks used by the agency, including access to interoperability channels and talkgroups as well as patching to alternate networks used by mutual aid agencies.

MCPTT consoles need to support a wide range of operational scenarios and some public safety responses inject complexity in the way MCPTT systems and MCPTT consoles are designed and interconnected. These include the need to share talkgroup access among multiple consoles, between consoles in different ECCs, and to directly communicate with, as well as patch, MCPTT talkgroups with LMR talkgroups and with talkgroups existing on a different vendor's MCPTT system[2].

Any new technology brings a multitude of implementation issues that include policy, governance, training and interoperability considerations. Two significant concerns were identified that impact both MCPTT consoles and interoperability. First is the use of encryption and how it will be managed when users are communicating on a shared LMR and MCPTT talkgroup. The second issue involves the ability of the console to patch MCPTT talkgroups to LMR systems and/or other networks. Both of these concerns are also currently being examined by other groups and by the Standards organizations who are working on interoperability. There are also a variety of technical issues involving design of MCPTT consoles and how they will connect to the MCPTT systems. Chapter 7 of this report includes detailed discussions on different approaches.

<u>The following conclusions were reached by the Working Group:</u>

- **MCPTT represents a huge shift in thinking for public safety agencies,** in that operations and infrastructure are moving from a locally controlled LMR radio network to a nationwide, centralized communications network.
- **While the first version of MCPTT is being rolled out now,** public safety agencies should understand that fully functional consoles and interfaces to LMR will not be available in the short term.
- **MCPTT continues to evolve as 3GPP standards are refined and improved**, as industry develops first- and second-generation solutions, and as public safety agencies gain experience with MCPTT capabilities and features.
- **As with all standards, there can be ambiguity** in the interpretation of 3GPP MCPTT standards which may lead to a lack of interoperability between vendors. Conformance and interoperability testing are essential, and industry needs clarity on the testing process and requirements.
- The **requirements**[3] for connecting an MCPTT console (on an agency network) to a FirstNet MCPTT solution have not been fully defined, and modification or upgrades to internal agency networks may be required to meet performance requirements.
- Because MCPTT console development is in its early stages, **there is concern about the viability of a multi-vendor marketplace** for these services.

It is important that public safety agencies monitor the availability of MCPTT and MCPTT console solutions, as well as examine how this new technology may integrate into existing operations.

---

[2] FirstNet has announced that it is working with 2 vendors to provide MCPTT service.

[3] FirstNet/AT&T have provided guidance on public safety agency interconnection for other services, which allow use of an embedded VPN or a wireless data connection using an AT&T dedicated APN to access the FirstNet Core.

1. Introduction to the Report

This document is a follow up to a report published by NPSTC in 2014 "Console LTE Report"[4] which provided a high-level overview of public safety requirements for next generation dispatch center consoles. New features and functionality were envisioned to be available on consoles following the implementation of the Nationwide Public Safety Broadband Network (NPSBN). The 2014 report was written before the 3GPP international standards body completed the requirements for Mission Critical Push to Talk (MCPTT). This report provides additional insight into several issues that will impact public safety operations.

This document is designed to communicate important information to public safety executives on the status of MCPTT and to provide additional technical details to help inform standards groups and industry participants.

The term "*console*" may be used to describe a wide range of systems and software operating in a public safety Emergency Communications Center (ECC) which is also called a "control room" in Europe. Consoles may refer to the radio control systems for Land Mobile Radio (LMR) networks or Computer Aided Dispatch (CAD) systems that track unit activity and manage emergency calls. Consoles may also be used to manage public safety video and data, including Internet of Things (IoT) devices.

For this report, "***MCPTT* console**" refers to the hardware and software that manages MCPTT communications (and associated features documented in the 3GPP standards[5]) within the ECC. This definition would be analogous to that of an LMR console. ***MCPTT System*** refers to the software and hardware infrastructure, described in 3GPP standards, which enable MCPTT capabilities. This would be analogous to an LMR system. An MCPTT console connects to an MCPTT system and provides command and control functionality. The MCPTT console may be provided by the same manufacturer as the MCPTT system or it may be provided by another vendor.

MCPTT consoles may exist in different form factors, such as a fixed desktop computer, laptop with mobile internet access, or other types of User Equipment (UE) carried by first responders that support console functionality. MCPTT consoles may also be used to support public safety operations, including those inside the Emergency Communication Center, at other fixed locations (e.g. hospitals and Emergency Operations Centers), and at remote field command posts.

Public safety voice communications may include MCPTT, LMR, or a mixture of both. This mixture of MCPTT and LMR may be a temporary situation (during a cut over to full MCPTT operation) or may represent a more long-term configuration (i.e. greater than ten years) involving dual use of both systems. Public safety agencies likely will want to maximize their existing capital investments in LMR radios and consoles, which will impact their adoption timeline. To facilitate training and dual use with LMR systems, vendors building early versions of MCPTT consoles should consider aligning their user interface design with existing LMR console layouts. This is especially important in early phases of adoption where the MCPTT system is not being used for tactical operations. It must also be noted that ECC personnel cannot be required to navigate between two different

[4] Console LTE Report, Published September 30, 2014, available at this link: http://npstc.org/download.jsp?tableId=37&column=217&id=3205&file=Console_LTE_Report_FINAL_20140930.pdf

[5] https://www.3gpp.org/specifications-groups/sa-plenary/sa6-mission-critical-applications/home

console solutions simultaneously during an emergency, even if they have similar symbology and operational characteristics.

Early versions of MCPTT consoles are unlikely to offer a standard's based MCPTT console integration with LMR because the associated LMR interface standards are still being developed and time is needed for the MCPTT ecosystem to develop and implement solutions. The 3GPP international standards group has published documents on the design of MCPTT systems. The standards also support MCPTT consoles and the interconnection of MCPTT consoles which may be external to the MCPTT provider solution. 3GPP Standards also provide for the connection of MCPTT and LMR radio systems through an Interworking Function (IWF). The Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) have established a Joint Committee to create standards for connecting conventional and P25 radio systems into this framework. While this work is ongoing industry providers may offer non standards-based solutions in order to get early versions of their products to market.

It is important to note that the availability and usability of any console feature is very dependent on its technical design and implementation which can vary across the entire set of vendors needed to support a console solution.

As is the case with LMR, public safety agencies expect to be able to purchase MCPTT service and MCPTT consoles from different vendors and with different tiers of functionality and price point. Public safety agencies (and their budgets) come in different sizes and configurations and with unique operational requirements.

While the primary emphasis of this report will be on MCPTT-based consoles, the need for interoperability with LMR consoles is also noted. The mapping of existing LMR console functionality and emphasizing its inclusion into MCPTT console development, will help insure that needed capabilities are present moving forward. MCPTT also provides greatly enhanced services and capabilities that make it a unique solution. Finally, there is international interest in the area of next generation console development. Countries, including those in the European Union, are actively discussing this issue and are implementing solutions to support public safety operations[6].

2. Current Landscape: MCPTT

MCPTT continues to evolve as standards are being updated and as industry begins to deploy early generation solutions. Public safety agencies have been using non-mission critical Cellular Push to Talk (PTT) systems for many years, starting with the introduction of Nextel's push to talk service in 1996.

MCPTT solutions are different from cellular PTT applications[7] in that they are designed to guarantee high availability and extremely fast and reliable voice communications. MCPTT standards also provide for an array

[6] https://www.rrmediagroup.com/News/NewsDetails/newsID/19614

[7] Many of these solutions are also known as Over-The-Top or OTT applications based on how they interact with the carrier network.

of expanded capabilities involving transmission of data to support location, emergency alerting, and other Mission Critical Services including data and video integration.

There are several PTT solutions available on FirstNet, and AT&T recently announced the availability of its first MCPTT based solution[8] called "FirstNet PTT". Clarity in how MCPTT will eventually impact public safety is not possible at this time due to factors involving the complexity of the build-out and the need for fully functional console systems.

Public safety's expectation of MCPTT capabilities and features are impacted by a complex set of factors, including:

1. Which 3GPP standard is being used by FirstNet?
   There are multiple versions of the 3GPP international standard for MCPTT and each release includes new features and capabilities. MCPTT is initially designed in Release 13 and features are expanded in Release 14,15 and 16. There is a normal time lapse as new standards are finalized and implemented by industry. This means that newly developed features and functionality may not be available for public safety use immediately after they are codified in a standard and reported publicly.

2. How will MCPTT be implemented by the MCPTT provider?
   There are many features and options in the configuration of MCPTT systems that may, or may not, be enabled by the vendor. 3GPP standards provide carriers and hardware/software vendors with flexibility around which features to activate and how those features are used. Public safety agencies may find that a desired capability is not available.

3. How will vendors implement MCPTT UE/Client API?
   MCPTT vendors may use User Equipment (UE) Application Program Interface (API) to allow the exchange of data and commands between MCPTT and other components and systems, including consoles. There are several API providers supporting MCPTT[9] and these vendors may configure their API's differently which will impact how they support (or restrict) MCPTT functionality.

4. MCPTT enhancements that are added by the MCPTT vendor
   Industry providers of MCPTT will likely add additional features beyond those required in the 3GPP standards. While some of these features may enhance the overall user experience, they are likely to be vendor proprietary solutions that will not support full interoperability with other system components.

5. MCPTT network configuration requirements
   The LTE network operator (e.g. AT&T FirstNet) will mandate specific network and policy

[8] https://urgentcomm.com/2020/03/31/att-announces-mcptt-based-firstnet-ptt-certifications-for-hpue-products-from-assured-wireless/

[9] Current API providers, at the time of this report, included: Nemergent, Softil, Kodiak, Alea and MCOP

requirements to address security and operational efficiency. Some of these elements may enhance or restrict access to 3GPP functionality. There may also be hardware and network requirements for connection of specialty devices, such as consoles, including the ability to leverage cellular LTE, Wi-Fi and wired connections.

6. MCPTT User Interface
   MCPTT handset manufacturers will design the layout of the user display screen and configuration of hardware buttons and virtual (software) buttons. Some elements of the handset device will be configured by the manufacturer and other options may be configured by the public safety agency. Similarly, at the far end of the network from the handsets are MCPTT consoles, which will also have user interfaces tailored for the console's capabilities.

The various factors described above will result in a multitude of configurations used by public safety agencies (based on their selection of an MCPTT vendor, MCPTT handset, and MCPTT console).

Public safety agencies also need to interoperate with other emergency and non-emergency responders at the scene of an incident. Those assisting agencies may be using a different configuration of MCPTT carriers, solutions, and devices.

Compliance and interoperability testing will be critical to confirm that all pieces of the MCPTT ecosystem work together as described in 3GPP standards and as required by the public safety agency to meet its unique operational environment. It is very important that industry providers and public safety representatives agree on a minimum set of tests to define a baseline of interoperability and functionality. There is also a need for a testing and validation process to ensure successful implementation. While the European Telecommunications Standards Institute (ETSI) is managing Plugtests that allow industry providers to check interoperability of their MCPTT equipment with different vendor systems, there is no formal suite of tests and processes to measure this performance. The Department of Homeland Security (DHS) has a compliance testing process[10] designed to measure performance of LMR radio systems using the P25 standard, but this work does not include MCPTT systems. The federal Public Safety Communications Research (PSCR) program recently awarded six million dollars to three companies to accelerate development of MCPTT testing equipment and services[11]. However, additional details regarding how testing will be conducted, and by whom, remain unclear.

3. Current Landscape: MCPTT Consoles

As MCPTT continues to evolve, industry also continues to develop MCPTT dispatch console solutions.

A fully functional MCPTT console may not be available in the short term, nor is there likely to be a standards based MCPTT console integration with LMR in the early stages of the deployment. 3GPP international standards continue to refine the MCPTT interconnection with LMR as other regional standards groups define requirements for the specific LMR interconnection used in their area (e.g. P25, TETRA, etc.). This work is

[10] https://www.dhs.gov/science-and-technology/p25-cap

[11] https://www.rrmediagroup.com/News/NewsDetails/NewsID/19218

ongoing and industry providers may offer non standards-based solutions in order to get early versions of their products to market.

Just as a multitude of factors impact MCPTT service, MCPTT Consoles also have a layered set of industry participants, adding to the overall complexity. MCPTT console development and implementation involves the following entities:

1. Public Safety Network operator (FirstNet by AT&T)
2. MCPTT service provider (one of the 2 MCPTT vendors approved by AT&T/FirstNet)
3. MCPTT UE/Client API vendor (if used)
4. MCPTT Console manufacturer (if different from the MCPTT infrastructure vendor)

Each of the industry providers may implement MCPTT features in different ways. This creates downstream complexity for the other vendors who are working to provide a seamless integration of MCPTT capabilities.

Most public safety agencies that adopt MCPTT will be in a transition state for a period of time, in which first responders will be using both LMR and MCPTT. This requires that a single console solution be able to manage LMR and MCPTT network functions and the users on both networks. Personnel in the ECC should not, and cannot, be expected to shift between different consoles to manage mission critical communications during a law enforcement incident, fire or medical emergency.

At the time of this report, the Working Group is not aware of an MCPTT console offering that emulates all of the existing LMR functionality expected by public safety agencies. A public safety LMR console manages the agency's radio traffic while it also interconnects users from other radio networks. The LMR dispatch console is often the main "controller" of all agency mission critical traffic. MCPTT consoles will need to mirror the same type of functionality and also support the new features available in MCPTT. For example, there is an expectation that Talker-ID[12] and location data be exchanged between LMR and MCPTT networks[13] even though the information is stored and managed differently in each system.

LMR consoles today control other critical aspects of voice communications, including use of digital encryption, management of talkgroups, and control of radio channel/talkgroup patching. MCPTT solutions provide a number of enhancements and additional features to both of these processes.

4. MCPTT Console: Operational Scenarios

Much of the existing conversation nationally has been focused on how to leverage 3GPP standards to enable full console functionality on a single MCPTT system. There also have been interoperability discussions on how to connect first responders using an MCPTT system to first responders operating on a P25 LMR system.

[12] See NPSTC report on Talker-ID: http://npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_MCPTT_IO_TG_Naming_181214.pdf

[13] 3GPP standards currently provide for sharing of location data among MCPTT services and future enhancements in Rel-17 may ensure mutual location server access across LMR and MCPTT.

The Working Group identified a larger set of operational scenarios that are common to public safety operations. This list only includes law enforcement agencies to maintain consistency between the scenarios, but the text is applicable for fire and EMS agencies as well. Functionality will be needed to support these and other public safety communications center configurations, including:

1. A single public safety dispatch console may need to manage MCPTT users who are **on two different MCPTT systems.**

- The city police may be using FirstNet MCPTT Provider #1 and the county sheriff's office may be using FirstNet MCPTT Provider #2 – but both agencies are dispatched from the same communications center.

2. A public safety dispatch console in Agency #1 may need to access MCPTT talkgroups also appearing on a console used in Agency #2's communications center, where both are using the **same MCPTT provider**.

- The city police communications center may need to communicate on an interoperability talkgroup also used by the County Sheriff's Office communications center, where both agencies are using the same MCPTT vendor.

3. A public safety dispatch console in Agency #1 may need to access MCPTT talkgroups which also appear on a console used in Agency #2's communications center, where each agency is using a **different MCPTT provider**.

- The city police communications center (using consoles supporting MCPTT Provider #1) may need to communicate on an interoperability talkgroup also used by the County Sheriff's Office communications center (using consoles supporting MCPTT Provider #2).

4. A public safety dispatch console may need to connect talkgroups **from different networks** to facilitate response to a local incident for interoperability purposes**.**

- The city police communications center may need to "patch" three separate talk paths to provide interoperability among first responders from different agencies who are responding to a building fire. This may include an MCPTT talkgroup, a P25 trunked talkgroup and a conventional 800 MHz repeater.

5. A public safety dispatch console may need to connect first responders using a FirstNet approved MCPTT service with responding agencies who are using a different **(non-FirstNet) MCPTT network**.

- The city police communications center may need to "patch" different MCPTT systems to provide interoperability among first responders from different agencies. This may include users on a private MCPTT system operated by a regional utility company or mutual aid EMS units operating on a different carrier's network.

- The city police communications center may need to "patch" different MCPTT systems to provide interoperability among first responders from the same agency using multiple networks. This may be for cellular network redundancy purposes or to achieve the best coverage possible.

6. A public safety dispatch console may need to **share control** jointly of one or more MCPTT talkgroups with another console**.**

- A city police department telecommunicator normally monitors other police talkgroups (beyond their assigned primary talkgroup) to support administrative users and to coordinate mutual aid and needs rapid access to communicate on any of these talkgroups. (or)
- A telecommunicator starts his/her shift and takes over a dispatch console position from another dispatcher who is ending their tour of duty. The oncoming dispatcher is taking over responsibility for the management of field units on talkgroups assigned to that console position, including uninterrupted continuation of talkgroup accessibility, activated patches, etc. (or)
- A telecommunicator is taking over responsibility for other city police talkgroups to cover for another employee who is leaving their console for a break.

7. An **out-of-area first responder**, using MCPTT, arrives in the area to provide mutual aid for a major incident (in which no prior mutual-aid coordination exists) and needs to communicate with local first responders.

- Personnel in the ECC are alerted by their console to the presence of the arriving first responder and can see first responder's identity (e.g. agency affiliation, badge # and other data contained in their MCPTT ID).
- Personnel in the ECC are able to add the mutual aid unit to the appropriate incident talkgroup, including ad hoc talkgroups created for the emergency.
- The ability to receive notification and interact with a mutual aid first responder, must exist even if the agency and the first responder are using different MCPTT systems (e.g., FirstNet approved MCPTT provider 1 or MCPTT provider 2).
- This ability is also needed to support mutual aid users operating on different networks[14] (including other private networks and other carrier networks). This includes the requirement for effective voice and data communications to support cross border operations (as highlighted in a joint NPSTC Report on Cross Border Emergency Communications with Canada[15])

8. An incident commander needs to use a **transportable MCPTT console** to manage an emergency incident in which the primary MCPTT infrastructure is not available (i.e. ProSe and IOPS)

[14] This may require that first responders have certain mutual aid interoperability talkgroups installed in a device that supports multi-carrier access.

[15] http://npstc.org/download.jsp?tableId=37&column=217&id=3360&file=CrossBorder_Communications_FINAL_20150311.pdf

- Public safety agencies need to extend the command and control capabilities provided by the ECC to the scene of an incident during complex emergencies. In other situations, contact with the ECC may be lost, requiring the incident commander to establish the dispatch function locally.
- Example 1: Multiple public safety units are on the scene of a collapsed apartment building following a tornado strike which also destroyed nearby cellular towers. One nearby cell tower is operational and is functioning in "Isolated Operations for Public Safety (IOPS) mode. The incident commander needs to coordinate with multiple agencies and multiple teams that are using different talkgroups, using a console type device with a wireless or hardwire connection.
- Example 2: Using the same scenario above, but no cell tower is operational (there is no contact with the ECC or with other first responders through the LTE tower infrastructure). The incident commander needs to communicate with first responders who are using MCPTT direct mode service (ProSe) and/or UE Relay, to leverage as many console functions as may be available.
- Example 3: Tactical situations, including wildland fires, may occur in areas that do not have adequate cellular coverage. Incident commanders may be communicating through a portable MCPTT system deployed on a drone or terrestrial vehicular platform and will need console functionality to manage multiple first responders on multiple talkgroups.
- The MCPTT console in each of these examples may also need to interface with local LMR resources, such as transportable LMR repeaters.

5. 3GPP Standards and MCPTT Consoles:

Based on all of the operational scenarios described in Section 4, it is important that MCPTT consoles be standards-based and that public safety agencies be able to select a console among competing vendors that best meets their budget and operational requirements.

3GPP standards provide for a variety of ways in which MCPTT systems can be interconnected to other MCPTT systems (as well as other "non 3GPP" systems). These building blocks include the IWF, Security Gateway (SeGy), Mission Critical Service (MCS) to Mission Critical Service (MCS) interconnection with different trust domains, etc. The standards also support MCPTT consoles and the interconnection of MCPTT consoles which may be external to the MCPTT provider solution.

3GPP Standards also provide for the connection of MCPTT and LMR radio systems via the use of an Inter-Working-Function (IWF) which is documented in 3GPP Release 16. The Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) have established a Joint Committee to create standards for connecting P25 radio systems into the IWF framework. The European Telecommunications Standards Institute (ETSI) has a Technical Committee (TC TCCE) working on a similar interworking function for connecting TETRA systems to MCPTT.

MCPTT console functionality is envisioned by 3GPP to be an extension of the User Equipment (UE) client capabilities and features. Many basic console functions are provided in existing 3GPP standards, even though the word "console" is rarely used. In essence, a "user" with appropriate permissions and authority may function as an MCPTT console accessing more features and functionality than are available to a regular first responder UE device. This is, in some ways, similar to the "super user" functionality in P25 trunked LMR systems.

In 3GPP Release 13, 14 & 15, all open-standard MCX (Mission Critical Services) interfaces exposed outside the carrier network are designed to accept a User Equipment (UE) "Client" interface[16]. These external connections may be implemented in a variety of ways (e.g., wireline and RF) and must meet carrier requirements. Section 7 provides an overview of the various connections between an MCPTT system and an MCPTT console.

Enhancements to 3GPP standards are ongoing to support both MCPTT systems and MCPTT consoles. For example, Multimedia Broadcast and Multicast Service (MBMS), a feature that was refined in 3GPP Release 15 to manage bandwidth better, also allows for multiple talkgroup users at the same site to listen to a single audio stream of radio traffic (as opposed to having individual audio streams transmitted to each first responder device). This capability will also benefit MCPTT wireless console design.

3GPP uses a methodical process to create and finalize a standard which involves multiple steps (also known as "stages") supporting design and technical implementation. There is an additional time delay before a new standard is adopted by a vendor and enters their production system, eventually resulting in a new feature or capability. Typically, this may be a 3-year process from the time the standard is started until it is finalized and commercialized by industry.

The 3GPP standards development process in an international collaboration and the various participants (carriers, industry and government entities) may have competing or conflicting priorities regarding MCPTT and MCPTT consoles. Consensus is typically achieved following lengthy discussions. It is important for console vendors to participate with other industry stakeholders in the 3GPP process to ensure that console issues are addressed early in the standards development cycle. Public safety input into this process is also essential.

Finally, carriers need to clearly define which 3GPP version they are implementing, along with proposed timelines (and advanced notice) for upgrades. This includes transparency in the adoption of any optional standards, confirmation of the standards that are implemented, and notification of any deviations from the standard.

6. MCPTT Console: Operational Issues

Today, virtually all public safety agencies use some type of LMR console to manage their mission critical voice communications. Consoles supporting LMR have evolved over the years and include a large number of features and capabilities to support P25 conventional and trunked systems. While MCPTT provides push to talk service that is similar to LMR, MCPTT provides a new set of advanced features for the use of mission critical voice and data via MCX or MCS (Mission Critical Services) standards. While LMR systems are implemented on a local, regional or statewide basis, MCPTT will be implemented on a nationwide basis. This will dramatically change the way in which local public safety agencies manage and interact with the network. It will also require added console functionality to integrate these new features.

[16] 3GPP Technical Specification (TS) 23.379 describes how MCPTT UE's may use non-3GPP access to support a subset of functionality.

The new capabilities available in MCPTT also require increasing collaboration among public safety agencies in order to develop policy, procedure and governance frameworks to insure a standardized user experience.

As noted earlier in this report, there is a long list of features and functions that public safety agencies will expect in an MCPTT console solution. **Appendix A** contains a list of considerations for MCPTT console functionality and provides information to help agencies understand the extent of the implementation process.

Many of these implementation issues involve technical, operational and procedural solutions which revolve around MCPTT console use. It is important that public safety agency executives understand the complexity of these issues and start the planning and collaboration process now.

For example, first responders using MCPTT will be able to communicate with any other public safety agency that is also using MCPTT[17]. This may occur from any location in the U.S. First responders may be directed to select designated MCPTT talkgroup as they respond to an incident or their device may automatically switch to the appropriate talkgroup. This includes ad hoc talkgroups, created specifically for the incident, and which do not appear in any first responder's device. Management of these capabilities have significant technical and operational implications, including use of Group Management[18] functionality. How does the ECC translate a mutual aid responder's Talker-ID and Alias data when it appears on their console? If each agency creates their own scheme for assigning ID's there may be little standardization across a county or region. Additionally, how does a first responder find the correct MCPTT talkgroup in their radio if each agency creates talkgroup names without any regional guidance to avoid duplication or ambiguous assignments[19]?

How is interoperability managed when different networks and devices are connected? What features and functionality are preserved (or lost) when LMR and MCPTT talkgroups are patched? Encryption, emergency button activation, and other data centric features may not be shared with users (and consoles) operating on the other network and some features may not work at all.

How are MCPTT interoperability talkgroups created and which agency owns or manages them? Who approves giving other agencies access to these specialized talkgroups? Can an agency that does not manage the talkgroup add first responders to the group during an emergency?

---

[17] This communications capability is supported on an "as needed" and "as authorized" basis, as long as both users have access to a common talkgroup.

[18] Group Management functionality refers to the ability to access and control public safety user devices, including detection of the device, identification of the user, and the ability to push (and redirect) the user to a new talkgroup. This impacts system administrators and personnel in the Emergency Communications Center who will be interacting with first responder devices during emergencies.

[19] See NPSTC Report:
http://npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_MCPTT_IO_TG_Naming_181214.pdf

3GPP standards support the use of encryption within MCPTT, as well as other types of Mission Critical Service (MCX) offerings. Console solutions will need to integrate with the encryption system, as they do today with LMR.

There are also additional complexities when managing encrypted communications on a shared talkgroup that includes both LMR and MCPTT users (see next section).

7. MCPTT Consoles: Technical Issues

In the standards community, it is generally felt that the 3GPP MCX standards accommodate the requirements necessary to support consoles and provide for communications center integration via the use of UE/Client interfaces. However, it is also recognized that availability and usability of any console feature is very dependent on its technical design and implementation which can vary across the entire set of vendors needed to support a console solution.

The TETRA Critical Communications Association (TCCA) is developing a console implementation guide[20] that is designed to assist all stakeholders in maximizing system capabilities to meet the needs of public safety agencies. An important element will be educating vendors about the differences in approach to MCPTT systems and interfaces and the resulting impact on console functionality.

MCPTT consoles may connect to MCPTT systems in several ways including those supported by 3GPP MCX UE open standard interfaces[21] or APIs:

a) Consoles can be connected to MCPTT in the same way a first responder's UE connects. MCPTT views the console as a UE with additional permissions and authority. The connection to MCPTT can use any 3GPP supported access (e.g. 4G/5G) or non-3GPP access (e.g. wireline, Wi-Fi)

b) Consoles can be connected to an MCPTT server dedicated to the console subsystem. This server is part of the same MCPTT system as other MCPTT servers and connects to these systems using the 3GPP standardized MCPTT-3 interface.

c) Consoles may also be connected to a partner MCPTT system that interfaces to other MCPTT systems using the 3GPP standardized MCPTT-3 interface. Note that in this case the console resides in a different trust domain which has implications for permissions and authorizations within the interconnected MCPTT systems.

Each of these approaches has technical advantages and disadvantages as well as business case, console capability, and performance tradeoffs.

[20] NSPTC plans to support this effort with the TCCA.

[21] These include interfaces designated by 3GPP as: MCPTT 1,4, and 7 and CSC 1,2,4,8, and 14.

1. The use of MCX UE/Client interfaces likely will be universally available as a console interface, but they may pose limitations, especially those created using earlier versions of the 3GPP standard. A third-party API solution can simplify efforts to implement complex UE/Client interfaces and may increase the pool of potential console vendors. These API's may be very expensive to license for console use, which could increase the eventual cost of an MCPTT Console. Depending on their design, APIs may have limitations on which elements of console functionality are available and they may inject an additional point of failure or latency.

2. A console solution that is fully integrated with the MCPTT Application Server should provide maximum functionality, but this solution may only be available from selected vendors operating within the carrier's MCPTT ecosystem. This approach may reduce competition and negatively impact a public safety agency's choice of console vendors. An MCPTT vendor could also offer an API solution to third party console developers, but such an API might be proprietary and subject to licensing fees and restrictions.

3. A server-to-server interface, such as MCPTT-3, can offer high functionality, but the interfaces reside inside the carrier's network and may not be available externally due to security concerns and the inherent difficulty in vetting and supporting such solutions.

There are also other ways to connect consoles to MCPTT. These include the use of a proprietary infrastructure-integrated design in which the MCPTT console uses non-3GPP standardized connectivity (e.g. built into the MCPTT Application Server without using any 3GPP designated interface). The 3GPP defined Inter-Working Function (IWF) could also be leveraged to integrate the P25 Console Sub-System Interface (CSSI[22]) in order to provide basic control of MCPTT[23]. The IWF was not designed to support MCPTT console operation but does provide access to certain features and functionality. However, neither of these two approaches have been endorsed or recommended by 3GPP.

Several differences in the technical approach were discussed which revolved around implementation of the UE Client design envisioned by 3GPP. It is the intent of this report to highlight that different approaches to the console gateway architecture may be needed to leverage the full capabilities of both MCPTT systems and MCPTT consoles. The diagrams below represent two approaches on how to manage the gateway using either individual connections ("instances") to the MCPTT system (Diagram 7.1) or using a local server to manage multiple connections ("instances") to the MCPTT system (Diagram 7.2). These are presented for discussion purposes only and do not seek to imply a preferred architecture.

[22] The 3GPP defined Inter-Working Function (IWF) and ISSI interface could also be leveraged to integrate the P25 Console Sub-System Interface (CSSI).

[23] The use of the IWF would introduce complications regarding access to the group database, key management, authorizations/privileges, etc.

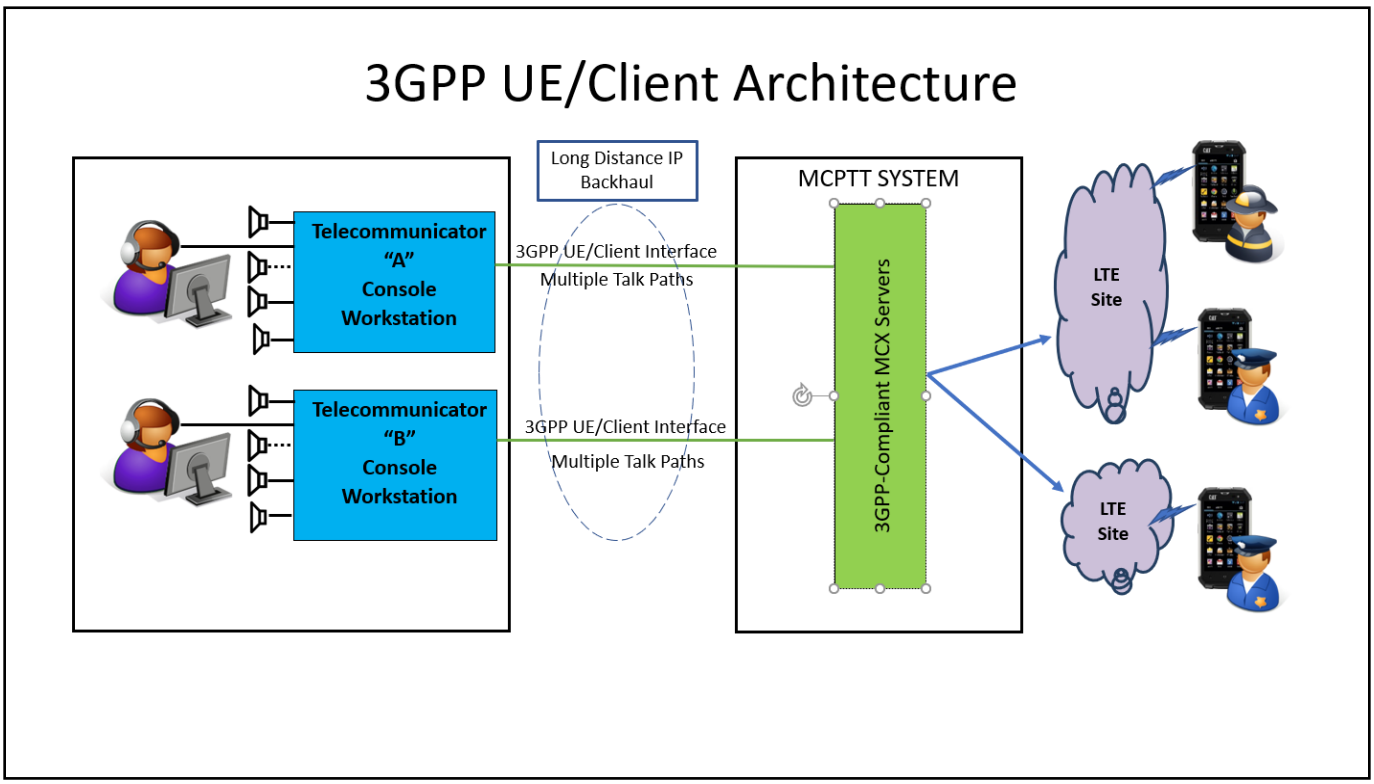

Diagram 7.1 Example of 3GPP Console Implementation (UE/Client Architecture)

Diagram 7.1 illustrates a console connection as envisioned by 3GPP standards leveraging the UE client interface. In this configuration each MCPTT console is running sufficient sessions (e.g. instances of the UE/Client interface) to manage all of the talkgroups that they are managing or monitoring[24].

[24] A single session or "instance" of a UE/Client interface can typically monitor multiple talkgroups simultaneously, although the console may only be able to transmit on one of the talkgroups at a time).

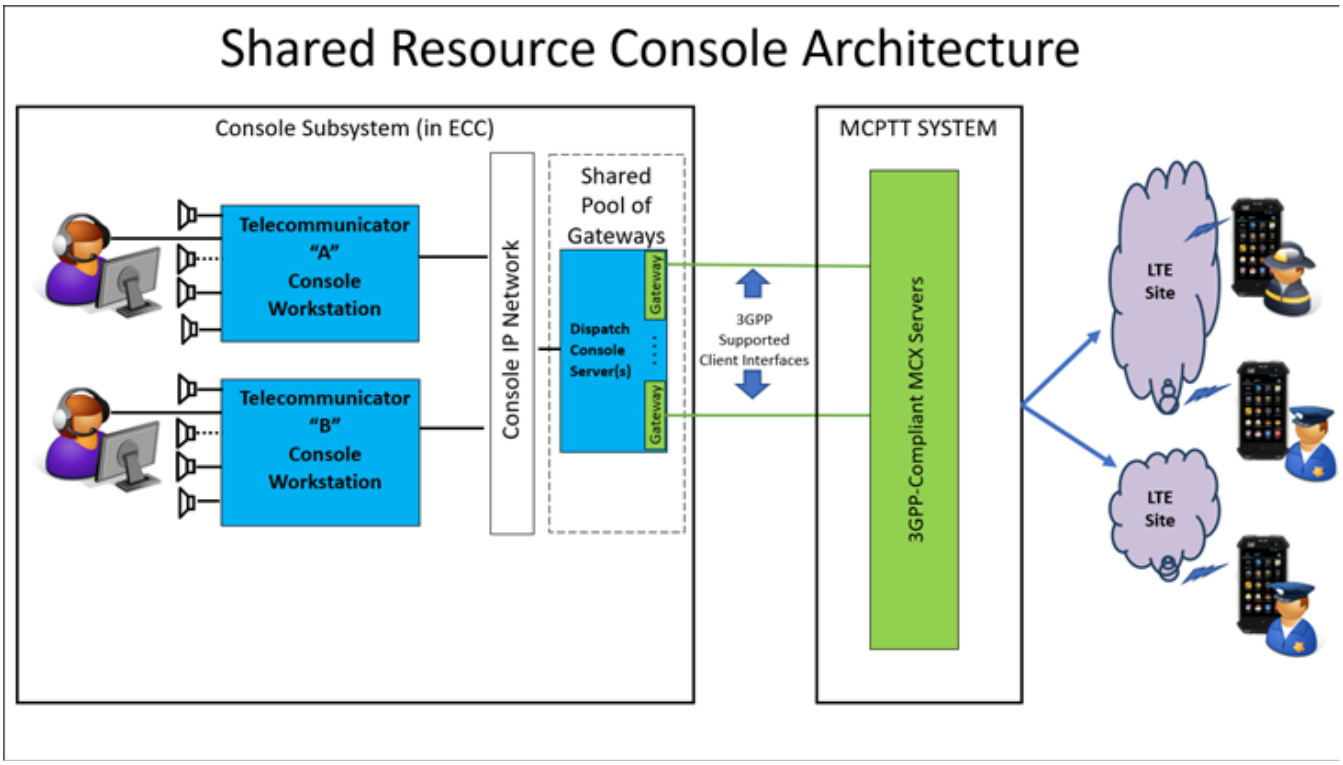

Diagram 7.2 Example of 3GPP Console Implementation (Shared Resource Architecture)

Diagram 7.2 illustrates another way of connection while still using 3GPP standards. This configuration allows the MCPTT console to share access and control with a group of UE/Client sessions ("instances") and the associated talkgroups that are established and maintained within the MCPTT console architecture. This approach mimics the way that some console systems connect to LMR networks. This approach may reduce bandwidth requirements.

Industry providers of MCPTT systems and MCPTT consoles should assess how any given architecture may support (or hinder) various capabilities that are needed by public safety and which are present in LMR consoles today[25]. Industry providers are encouraged to review the list of operational scenarios in Section 4, which illustrate the potential complexity of the architecture.

A small set of console functions was identified to help better focus the discussion of the two diagrams. Each function listed below would be performed by Telecommunicator "A" in Diagram 7.1 or 7.2.

1. Select a primary talkgroup to communicate with assigned units
2. Monitor the audio of several other talkgroups with the ability to individually control the volume level of each monitored talkgroup.
3. Communicate with units and telecommunicators who are connected in a patch that was set up by Telecommunicator "B".

[25] MCPTT consoles must also support a wide range of additional features and capabilities beyond those in LMR consoles.

4. Select and manage a second primary talkgroup (in order to cover for Telecommunicator "B" who is going on break and leaving their console). This involves monitoring and transmitting on the second talkgroup as well as using other functionality, including patching (see #5 below).
5. Disconnect the patch created by Telecommunicator "B" at the completion of the incident for which it was created.
6. Monitor the audio of some talkgroups that may also be monitored by Telecommunicator "B", including the transmissions of Telecommunicator "B" on those shared talkgroups.
7. Transmit to multiple talkgroups on a momentary basis, without previously creating a supergroup containing those talkgroups.

The discussion of the two approaches described in Diagram 7.1 and 7.2 revealed a number of issues, many of which require additional review by the affected industry providers.

Console MCX Client Instances

In Diagram 7.1, each console has dedicated instances of MCX Clients in order to manage and monitor a set of talkgroups. That approach may cause unintentional negative consequences when operationalized. In Diagram 7.2 the MCPTT console ecosystem aggregates multiple instances of MCX Clients to be shared with a set of console users. In that model, each MCX Client (e.g. talkgroup) may be shared by multiple console users. Both approaches should be examined to determine how they scale to support consoles that need to share management of 100 (or more) talkgroups.

Cost and Bandwidth Considerations

Public safety agencies need cost effective solutions and there is an expense associated with each instance of an MCPTT interface connected to their console system. The architecture in Diagram 7.1 may better support agencies with a small number of dispatch positions and/or a small number of talkgroups due to the limited number of interfaces that would be required and avoiding the cost of server infrastructure. The architecture in Diagram 7.2 consolidates the interfaces and allows them to be shared by multiple consoles. This solution may be advantageous to larger agencies due to a lower cost based on the reduction of interfaces that are needed (as compared to Diagram 7.1). Additionally, in situations where multiple telecommunicators are monitoring the same talk groups, the architecture of Diagram 7.2 may reduce the total bandwidth needed to support backhaul from the MCPTT carrier.

Console MCX Gateway Registration

In Diagram 7.1, the telecommunicator may log into the MCPTT UE client to perform registration with the MCPTT system. In Diagram 7.2, the Console Subsystem is managing the gateway on behalf of multiple dispatchers. That architecture may require a different registration process since the instance is being created for shared use and not on behalf of a single user.

Console MCX Gateway User Talker-ID

In Diagram 7.1, the Talker-ID displayed when the telecommunicator transmits may be based on their sign-on credentials which initiated registration. This supports the agency preferred display of the ID, whether it be the

individual telecommunicator (e.g., “Sue Smith”) or the functional name of the console that they are using (e.g., “Dispatch North”). In Diagram 7.2, it is unclear what Talker-ID would be displayed when more than one console position may be transmitting on that talkgroup through the shared UE instance. NPSTC published a report that was devoted to Talkgroup and User ID recommendations[26].

Receive and Transmit Echo

In the communications center, there are often multiple telecommunicators in close proximity and those adjacent personnel may be monitoring the same talk groups. Telecommunicator “A” and Telecommunicator “B” may be monitoring the same incoming transmission. If the audio arrives at the two consoles at different times, it can produce an echo which can hinder both telecommunicator’s ability to clearly understand the message. Also, when Telecommunicator “A” transmits on a talkgroup monitored by Telecommunicator “B”, both may be hindered by the resulting echo. Management of parallel audio arrival and smart cross-console muting may be required. The architecture in Diagram 7.2 may better support those capabilities.

Receive Audio Stream Distribution

3GPP standards allow a UE/Client interface to simultaneously receive the audio of multiple talkgroups. This capability takes on greater importance inside the ECC and distribution of multiple audio streams to console users must be carefully managed. It is important to know that audio from a single talkgroup may be monitored by multiple console users, and each user may be monitoring a dozen or more talk groups. LMR Console workstations typically have a multitude of audio destinations (e.g. talkgroup audio may be going to a headset as well as to selected and unselected speakers). While legacy LMR consoles typically sum the audio of all non-primary (selected) talkgroups to a common speaker, newer designs may provide an enhanced capability with individual speakers spaced around the telecommunicator so as to better perceive aural separation. Audio destinations may be assigned for the traffic of one fixed talk group while others may be flexibly assigned by the user as needed. This capability would require that each provided audio stream contain the audio of a single talkgroup. While 3GPP standards do not call for summing of audio streams, some MCPTT implementations create summed audio streams in which individual talkgroup audio cannot be extracted.

Multiple Transmissions from One Dispatcher

Telecommunicator “A” may need to transmit to multiple MCPTT talk groups simultaneously without using a previously creating supergroup. The solution in Diagram 7.1 would require an interface capable of supporting multiple simultaneous outgoing transmissions.

Talkgroup Visualization & Access

MCPTT consoles will allow personnel in the ECC to access a large number of talkgroups across multiple agencies, including those which are outside of traditional radio coverage. Some of these talkgroups may only be used for specialty purposes, including interoperability and tactical operations. If bandwidth becomes a

[26] NPSTC Report on MCPTT User-ID/Talker-ID:
http://npstc.org/download.jsp?tableId=37&column=217&id=4169&file=NPSTC_MCPTT_UserID_181109.pdf
[26]NPSTC Report on MCPTT Talkgroup Naming:
http://npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_MCPTT_IO_TG_Naming_181214.pdf

limiting factor, public safety agencies may desire a console feature[27] that would allow designated talkgroups to be "display only" (e.g., not receiving audio streams unless the talkgroup was selected, but still seeing data associated with talkgroup users). The audio stream may automatically start if an emergency condition occurred (e.g., a field unit activates their Emergency Button). First responders may also be able to mute their user devices (or specific talkgroups). The MCPTT console should have a way to visualize this status along with alternate methods of reaching the first responder.

It is hoped that later generations of MCPTT consoles will incorporate an enhanced feature set based on evolving standards and changing public safety expectations driven by field experience.

8. Interoperability Considerations: MCPTT and LMR Consoles

In order to facilitate interoperability between MCPTT and LMR consoles, a certain minimum set of features are required. Encryption and Patching were two of the most significant issues identified by the Working Group during this discussion.

Encryption[28]

There are significant differences in the way LMR and MCPTT manage encryption and there are several ways in which cross network encryption can be implemented. In general, there are transcoded solutions and End-To-End (E2E) solutions. Transcoded solutions maintain the individual LMR and MCPTT encryption protocols and perform a decode/recode at the border of the two networks. E2E encryption solutions maintain the same encryption protocol between all users.

Distribution of a new P25 encryption key (rekeying) remains a significant challenge for radio systems and consoles, both in manual processes and proprietary automatic processes. This issue will also impact encrypted communications occurring on shared talkgroups that include LMR and MCPTT users.

Standards work is ongoing to examine the best way to implement cross network encryption and there are many operational and technical considerations to be addressed. The impact on console functionality should remain a key area of focus in these deliberations.

[27] This feature was discussed by the U.K. Home Office regarding implementation of their Emergency Services Network (ESN).
[28] Encryption is discussed more thoroughly in the NPSTC LMR LTE Report: http://npstc.org/download.jsp?tableId=37&column=217&id=4031&file=NPSTC_Public_Safety_LMR_LTE_IO_Report_20180108.pdf

Patching

Next Generation consoles must support the ability to interconnect talkgroups and channels from different networks, commonly called "patching". There are many differences between LMR and MCPTT in the way talkgroups are established and managed which will impact patching. The ability (or inability) to interconnect users of different systems will be dependent on the type of solution(s) implemented by the local public safety agency. There are several ways to patch systems, including basic solutions that only pass audio and do not support the exchange of Unit ID/Talker-ID, Emergency Button activation, location data, etc. Shared (interworked) LMR-MCPTT talkgroups can be created as a part of a standardized local or regional interoperability approach. In other circumstances, the ECC may create an ad hoc patch to merge LMR and MCPTT talkgroups during response to an incident.

ECC personnel will need the ability to create, manage and cancel patches. At a minimum, the patching capabilities should mirror those available today on LMR consoles. For example, a telecommunicator at Console A should be able to create a patch that can be accessed, modified and canceled by a telecommunicator at Console B.

9. Summary

Several themes were identified during the Working Group deliberations that are noted below.

MCPTT represents a huge shift in thinking for public safety agencies, in that operations and infrastructure are moving from a locally controlled LMR radio network to a nationwide, centralized communications network. This will impact how public safety agencies approach policy, procedure, and implementation while also giving first responders new capabilities and improving interoperability.

While the first version of MCPTT is being rolled out now, public safety agencies should understand that fully functional consoles and interfaces to LMR will not be available early on. Fully developed consoles and LMR inter-working with MCPTT are essential elements before a public safety agency can "operationalize" MCPTT. There are also competing approaches to console design that involve either modification to existing LMR console system to support MCPTT and LMR simultaneously or the creation of an entirely brand-new console system and architecture for MCPTT.

MCPTT continues to evolve as 3GPP standards are refined and improved, as industry develops first- and second-generation solutions, and as public safety gains experience with MCPTT capabilities and features. This includes the introduction of data and video into the MCPTT solution. Public safety agencies should have patience and expect MCPTT to get better with time. MCPTT console development will likely follow this same course. It is important that all stakeholders participate in the 3GPP standards setting process. In addition, changes occurring in 3GPP need to ripple into the appropriate P25 standards, including needed revisions to ISSI and CSSI interfaces.

As with all standards, there can be ambiguity in the interpretation of 3GPP MCPTT standards which may lead to a lack of interoperability between vendors, which can be problematic for MCPTT console providers and

public safety agencies. The FirstNet Authority and FirstNet AT&T each have existing processes for review and approval of devices and applications operating on the network, but the **specific testing requirements for console solutions are unknown at this time.**

There is a need for fully functional interoperability solutions that will allow MCPTT consoles to communicate with any entity involved in an emergency response. Section 4 of this report highlights a number of different operational scenarios in which public safety consoles must connect to disparate networks. Ideally, all carriers, vendors and stakeholders would support MCPTT interoperability, as described in 3GPP standards, to promote the needs of public safety communications regardless of the network, device, or application used.

Console and API vendors should use open standards to implement their solutions, which will allow for easier cross vendor implementation while ensuring maximum flexibility. All stakeholders should participate in the European Telecommunications Standards Institute (ETSI) plug-tests which seek to validate interoperability and standards compliance.

Because MCPTT console development is in its early stages, **there is concern about the viability of a multi-vendor marketplace** for these services. While single vendor environments were common in radio system acquisition prior to adoption of the P25 LMR digital radio standard, public safety agencies today typically avoid single vendor environments. Solutions which are fully standards-based will allow agencies to mix and match the various components of their MCPTT ecosystem. 3GPP standards were specifically designed to support a mixed vendor environment.

End users should mandate open standards to promote both interoperability and the health of the MCPTT ecosystem. Public safety agencies are encouraged to advocate for their needs at the time of standards development as well as during the procurement process.

Finally, public safety agencies have had limited exposure to MCPTT and no experience with MCPTT console implementation. This creates an environment where first responders have more questions than there are available answers. The issues noted in this report are not meant to represent deficiencies in how MCPTT consoles will operate but are instead designed to highlight important features and functionality.

NPSTC has published three reports which provide expanded context regarding the implementation and operationalization of MCPTT and MCPTT consoles:

1. NPSTC Report[29] on MCPTT User ID's and implications for display at the Console.

2. NPSTC Report[30] on MCPTT Talkgroup naming and interoperability

[29] http://npstc.org/download.jsp?tableId=37&column=217&id=4169&file=NPSTC_MCPTT_UserID_181109.pdf
[30] http://npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_MCPTT_IO_TG_Naming_181214.pdf

3. NPSTC Report on Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk[31]

DHS has also published two reports[32] on MCPTT and interworking between LTE and LMR. Those reports examined the feasibility of developing a standards-based interworking solution that would enable communications between Land Mobile Radio (LMR) and Long Term Evolution (LTE) systems; and communications between different LMR systems.

Public Safety agencies should continue to monitor the implementation of MCPTT to gather best practices while also watching the development of MCPTT console solutions. Public Safety associations and organizations should continue to advocate for the inclusion of required features and capabilities to support mission critical operations.

NPSTC wishes to thank all the members of the LMR LTE Integration and Interoperability Working Group for their hard work in the development of this report. Members of the public safety community contributed extensively to this report including first responders and representatives of industry and academia.

[31] http://npstc.org/download.jsp?tableId=37&column=217&id=4031&file=NPSTC_Public_Safety_LMR_LTE_IO_Report_20180108.pdf
[32] https://www.dhs.gov/publication/st-interworking-mission-critical-push-talk-between-lte-and-lmr-report

Appendix A: MCPTT Console Functionality Discussion List

During many months of discussion, the Working Group identified features and issues that should be addressed by MCPTT console manufacturers. While many of these items reflect existing LMR console functionality, there are also issues in how new MCPTT features will be implemented as well as identification of proposed new capabilities. This list was designed based on discussions in the Working Group is not meant to be indicative of all functions and features.

MCPTT Console Functionality:

- Workflow issues, including those created at the start and end of shift, and when communications center personnel "cover" for each other during breaks, and how the workload is dynamically redistributed (and shared) including during major events.
- Patching LMR talk groups to MCPTT talk groups
- Patching LMR talk groups to individual MCPTT Subscriber Units
- Patching individual LMR Subscriber Units to individual MCPTT Subscriber Units
- Patching individual LMR Subscriber Units to individual MCPTT talk groups
- Patching calls between carriers, between different talk groups within the same carrier, and between LMR and LTE.
    - Whose ID to pass during a patch?
    - Who owns the setup and tear-down of a patch?
- Managing Emergency declarations across LMR and MCPTT systems
- Tracking locations of LMR and MCPTT Subscriber Units.
- Understanding the location of field personnel who have multiple devices sending location data.
- Aggregation of location data coming from MCPTT and LMR users to create common situational awareness
- Multiselect (or Simul-Select) LMR talk groups to MCPTT talk groups
- Management of "multi-select transmit" in which an MCPTT console needs to transmit a message over several MCPTT talkgroups at the same time. Does 3GPP require a regrouping of users to a single talkgroup or can it be accomplished in other ways?
- Multi-System Transmit, in which consoles will communicate (transmit) to multiple first responders, who may be operating on different MCPTT talkgroups (or on different MCPTT solutions, or on MCPTT and LMR).
- Management of audio latency issues between adjacent MCPTT consoles in which an MCPTT console dispatcher is transmitting and the dispatcher sitting near them is monitoring the same talkgroup. (e.g., is there an echo effect based on the type of console integration)
- Management of, and display of, the Talker ID[33] on the MCPTT console. 3GPP provides for different ways to identify a user, which may be an individual first responder (e.g., a user) or it may be a functional name (e.g. a console).
- Management of 3GPP standardized console features which may have been implemented in different ways by the various providers (e.g., MCPTT provider, API provider).

[33] NPSTC Report on User ID Management, http://npstc.org/download.jsp?tableId=37&column=217&id=4169&file=NPSTC_MCPTT_UserID_181109.pdf

    - Example: 3GPP provides for the delivery of multiple streams of audio to the UE device. How this is implemented by the MCPTT provider and/or API vendor will impact how the console provider allows a dispatcher to monitor/control/communicate on multiple MCPTT talkgroups simultaneously.
- Use of "non 3GPP access connections" to facilitate additional functionality:
    - Logging of voice and meta data during MCPTT transmissions, including MCPTT private call sessions between 2 users.
    - To allow management of LMR and MCPTT encryption.

<u>New MCPTT Specific Capabilities:</u>

- Group Management (representing the biggest departure from traditional LMR console capabilities):
    - Handling "foreign" mutual-aid roamers from jurisdictions outside of the home agency's region – how to become aware of them, now to incorporate them into active incident talk groups, etc.
    - Viewing all participants in an MCX group
    - Viewing which MCX groups a participant is in
    - Viewing user presence
    - Ad-hoc group creation/formation (individual & group re-grouping) – incident-based and otherwise.
- AVL Mapping (& GIS integration) [available on a limited basis in some LMR systems]:
- Geo-based individual regrouping (from a geo-fence)
- Public Safety Internet of Things (PS IOT) integration
- Video integration
- Simultaneous monitoring of multiple talk groups, with independent volume control and independent speaker/headset assignment.
- Simultaneous transmissions to multiple talk groups
- Cross-console & cross-channel muting
- Handling Emergency & Imminent Peril activations
- Talker and Talk Group ID display
- Text Messaging
- Recording of voice, data and video (& logging recorder integration)