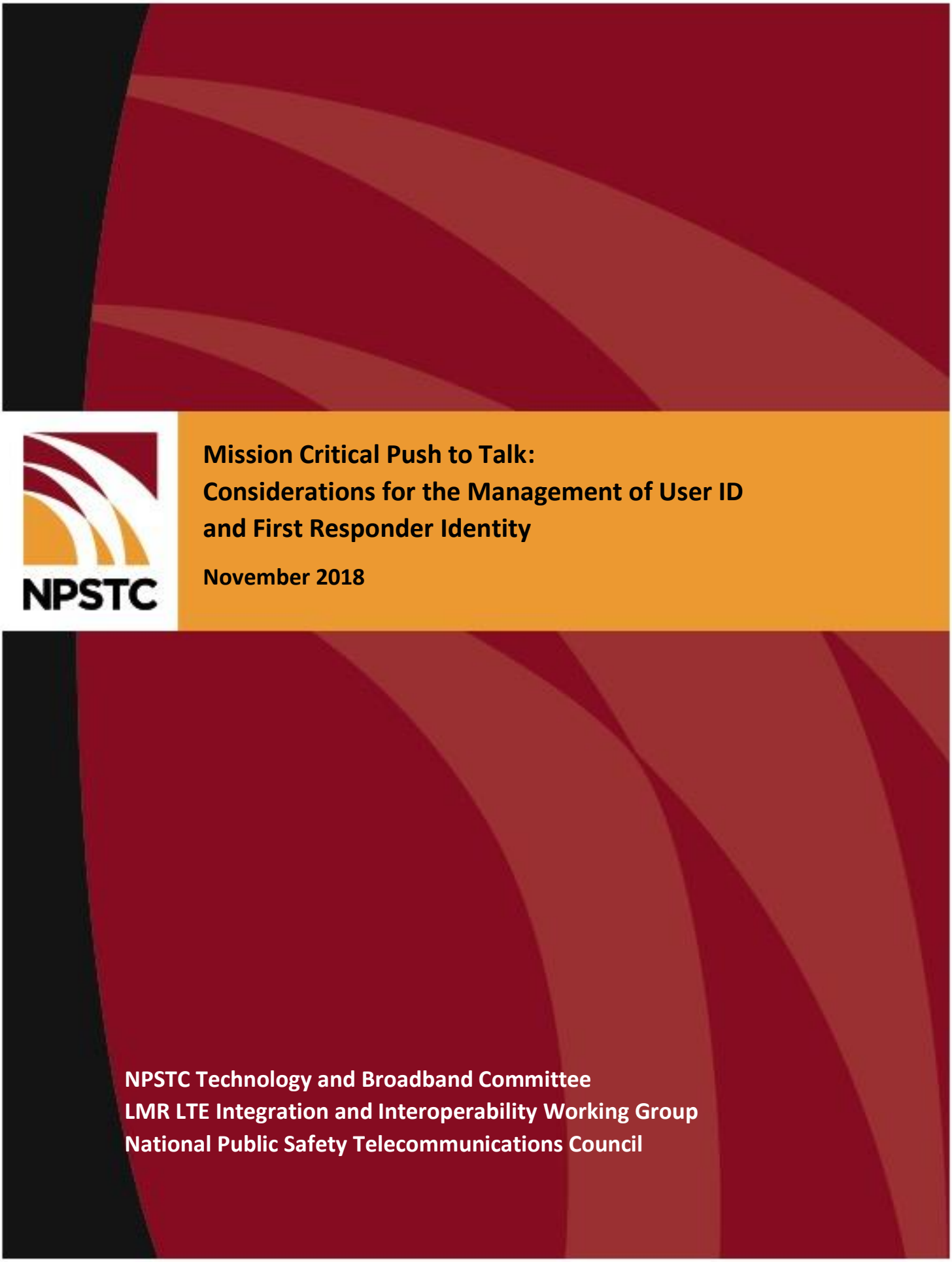


Mission Critical Push to Talk: Considerations for the Management of User ID and First Responder Identity

November 2018

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

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 the identity of a first responder and how that identity is managed within the MCPTT service.

Identity is a critical component of first responder safety. Today, most public safety Land Mobile Radio (LMR) systems support the transmission of a Unit ID which is used by communications center personnel and field supervisors to verify which first responder is communicating. That identity information is crucial during high-risk events and other emergencies. For example, the provision of Unit ID in public safety LMR systems allows backup units to be immediately dispatched even though a police officer's radio transmission for help was garbled. Unit ID also allows for the immediate identification of a first responder who has activated the Emergency Call button during a crisis in which they cannot transmit a voice message. Finally, Unit ID allows agencies to identify and immediately disable a lost or stolen device which may be used to interfere with public safety radio communications.[1]

Identity, Credentialing, and Access Management (ICAM) solutions are also an important component of the NPSBN. ICAM comprises the tools, policies, and systems that allow an organization to manage, monitor, and secure access to protected resources.[2] ICAM will impact the NPSBN in a number of ways and may play a role supporting user sign on to all Mission Critical services, including MCPTT. However, this report is focused exclusively on the MCPTT application and how a first responder's identity is managed. This report, therefore, does not speak to the relationship between ICAM, Single Sign On, and the MCPTT User.

The NPSBN will allow first responders to communicate almost anywhere in the U.S. using MCPTT. This capability enables two-way voice communications far beyond the range of local public safety LMR systems. This impacts identity management in that first responders will be able to communicate with almost any other public safety agency operating on the NPSBN across a very large geographic area. Communications Center personnel in a Public Safety Answering Point (PSAP) must be able to immediately visualize identity information for any first responder who contacts them on an MCPTT talkgroup. A law enforcement officer who is traveling through a neighboring state would be able to use MCPTT to easily contact a local PSAP[3] and request assistance. If the officer radioed an urgent call for help the receiving communications center must have sufficient identity information in order to respond. An

---

[1] LMR P25 systems may also transmit GPS location data, which is critical in a crisis situation.

[2] https://www.gsa.gov/policy-regulations/policy/information-integrity-and-access/identity-credential-and-access-management

[3] This capability is partially available today using designated LMR nationwide public safety interoperability channels but is problematic depending on the frequency band in use and whether a PSAP is monitoring the channel.

ambiguous Unit ID appearing on a telecommunicator's dispatch console would not provide sufficient information to identify the officer or their home agency and could delay an emergency response. In addition to supporting itinerant public safety personnel who are passing through multiple jurisdictions, the transmission of meaningful identity information is also essential for first responders who routinely provide automatic aid to nearby agencies and who respond greater distances to provide mutual aid.

This report notes that first responder identity is tracked in an entirely new way with MCPTT. In public safety LMR systems, the user's device is the basis for the Radio ID and additional translation is necessary to match the radio device to the current user. In MCPTT, first responders log into the application with a unique ID that identifies them individually.[4] This ability to identify the individual first responder will be critical as new technologies and capabilities are developed. For example, software applications can provide customized support based on the specific user including the ability to only respond to an individual first responder's voice.

However, the management of identity within MCPTT can be complicated by the wide range of options that exist. Fortunately, a set of international technical standards[5] for MCPTT provide great flexibility in the creation and assignment of first responder identity. For the MCPTT service, the three main user identifiers are:

1. **MCPTT User ID** is a structured and unique ID designed to identify the first responder.
2. **MCPTT Alias** is designed to store additional identity information.
3. **MCPTT Functional Alias** is designed to dynamically display the specific role the first responder has been assigned, which may include their placement in the Incident Command System (ICS) structure.

Each of these MCPTT data fields are described in greater detail elsewhere in this report. However, it is important to note that the MCPTT User ID is the only data field of the three that must be unique from every other MCPTT user.

A survey was conducted of the public safety agencies participating in the development of this report to determine what specific elements of a first responder's identity were considered essential.[6] The resulting recommendation offered five core elements[7] that should be present in every MPCTT User ID:

---

[4] There is a complex set of 3GPP standards, including Standard 23.280 (R16), which provide more detail on these definitions and other user and service IDs.

[5] The 3rd Generation Partnership Project (3GPP) sets standards for LTE and for a wide range of mission critical services, including MCPTT.

[6] Chapter 3 includes a discussion of the various data elements that were identified.

[7] These five core identity elements are considered the minimum necessary to identify a first responder. They do not represent all of the other identity elements that may be desired by public safety agencies.

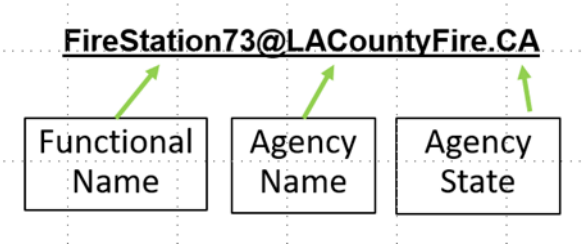
1. User First Name
2. User Last Name
3. Agency assigned ID Number/Badge Number
4. Agency Name
5. Agency State[8]

The structure of an MCPTT User ID resembles an email address and supports a lengthy character string. It is important to note that typical agency email addresses should not be used because they do not contain sufficient information. For example, using the recommended elements above, a deputy working for the King County, Washington, Sheriff's Office may have an MCPTT User ID of John.Smith.79332@KingCountySheriff.WA

A separate set of data elements were recommended as the minimum necessary for MCPTT specialty devices that are not assigned to an individual first responder. Examples of specialty devices include radios in hospital emergency departments, fire stations, and mobile command posts, which may be accessed by a group of authorized users. Three identity elements should be present in every MCPTT User ID associated with these specialty devices:

1. Functional Name
2. Agency Name
3. Agency State[9]

For example, a radio in a Los Angeles County fire station may have an MCPTT User ID of: **FireStation73@LACountyFire.CA**



[8] The Agency State element would support the use of "US" for federal government agencies. Federal use of MCPTT was not in the scope of this report and no recommendations are made regarding how federal agencies may manage MCPTT identities.

[9] See footnote #6 regarding the use of "US" to support federal agency identifiers.

The report also concluded that the final format selected for the MCPTT User ID should be standardized to ensure consistency across all agencies. Variations in the sequence and type of data elements in an MCPTT User ID could lead to confusion and prevent rapid identification of a first responder in an emergency. It was for these reasons that this report recommends creation of a standard governing the MCPTT ID structure.

This report does not address how MCPTT User ID may be affected when a first responder is operating off network in Pro Se (Direct Mode). The report is also silent on what options may exist to identify the specific MCPTT device a first responder is using if they are carrying multiple devices. Answers to these questions, and others, are dependent on further research and testing and on implementation decisions to be made by the FirstNet Authority and AT&T.

The NPSBN will provide an array of new technologies for public safety communications, including voice, data, and video; while 3GPP, the international standards group, is creating and refining a number of requirements for Mission Critical services. It is important to note that the NPSBN and the supporting standards are still evolving. **There are a number of significant operational and technical issues that must wait for the finalization of MCPTT network design and for the completion of additional standards work.** For those reasons, this report is a high-level examination of how MCPTT may impact public safety agencies. The information contained in this report is accurate as of its publication date and the reader should check for subsequently published documents that may address some of the items that are unresolved.

This document concluded that a minimum set of MCPTT identity components must be used by all public safety agencies in a standardized way. Use of these identity components also must be expanded to include Extended Primary users and others who are authorized to use the MCPTT service. Elements of this report are applicable to any use of MCPTT regardless of the network on which it is deployed.

Finally, it is recommended that the FirstNet Public Safety Advisory Committee (PSAC) review this document and provide additional input to the First Responder Network Authority and AT&T.

1. Introduction

This report is a follow up to the recently completed LMR LTE Integration and Interoperability Report[10] published by NPSTC on January 8, 2018.

In that report, several follow-up actions were proposed to further study the impact of MCPTT on public safety agencies. Those recommendations were approved by the NPSTC Governing Board and included the following topics:

1. MCPTT User ID management
2. MCPTT impact on nationwide interoperability channel capabilities
3. Encryption issues with MCPTT and encryption interworking with LMR and LTE
4. LTE and MCPTT console issues

This report addresses the first action item regarding MCPTT User ID Management. Another NPSTC Working Group is currently addressing the impact of MCPTT on nationwide interoperability channel access. Work to address encryption issues and to study MCPTT consoles will occur sequentially following completion of this document.

The LMR LTE Integration and Interoperability Working Group met for 7 months between April and October 2018 to learn how MCPTT standards address first responder identity and to study the potential impact to public safety agencies. Presentations were received to better understand how LMR User IDs are leveraged by public safety agencies today and how 3GPP standards create a foundation for MCPTT profiles and user identity. Standards development is also underway in a joint working group operated by the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) to examine how LMR and MCPTT networks may be interworked. That group will examine the ability of MCPTT IDs to be exchanged with first responders are operating on LMR.

Management of first responder identity is a cornerstone to all efforts involving first responder safety and device security. Chapter 2 discusses the important role of Unit ID and other resources to effectively respond to emergency and crisis situations.

From a safety perspective, identity involves the need to rapidly understand which first responder is communicating and, in some cases, from which device a first responder is communicating. Management of first responder identity is complicated by the wide range of device assignment practices used by public safety agencies:

1. Assigned Device: A device that is used exclusively by a single first responder on a permanent basis. First responders may also be using more than one assigned device simultaneously.

[10] This report may be accessed on the NPSTC website at www.npstc.org

2. Shared Device: A device that is exchanged among different first responders, including hand off of a device at shift change between day and evening unit personnel.
3. Simultaneous Use Device: A device that is used by more than one first responder simultaneously (e.g., MCPTT radio in a fire truck occupied by four firefighters).
4. Functionally Assigned Device: A device which is used by a group of personnel in an assigned area (e.g., an MCPTT device in a hospital emergency department, mobile command post, or fire station).
5. IoT Device: A device which supports first responder safety, which may be on a first responder's uniform or vehicle, and which may be capable of generating a distress call through the MCPTT application on behalf of the first responder.

Lengthy discussions were held on the minimum data elements needed to identify a first responder in an emergency. It was noted that other types of responders may also access public safety MCPTT talkgroups and need to be identified as they communicate or activate their emergency button. For example, secondary responders (also known as "Extended Primary" users) from public transportation and utilities may play a critical role at an incident scene. **Therefore, all authenticated users of the NPSBN who have been authorized to use the MCPTT service must have a standardized User ID.**[11]

A survey of public safety agencies participating in the Working Group was conducted which captured a large set of potential identity components**. While a minimum identity data set is recommended in this report, it is acknowledged that agencies may need to add other components to the MCPTT User Identity to meet their unique operational needs.**

It is important to note that MCPTT manages the identity of users in a very different way than public safety LMR systems and existing Push-To-Talk-Over-Cellular solutions. A first responder signs into an MCPTT application with their unique credentials and establishes their identity. In LMR systems, the first responder's radio may transmit a string of data that identifies the device they are holding.[12] MCPTT identity is also managed differently than existing Push to Talk over Cellular applications used by some public safety agencies, which typically use a cellular phone number to identify the device.

During the development of this report, additional issues and concerns were highlighted which relate to the need for a standardized first responder identity to support public safety operations.

[11] Use of MCPTT, as with other Mission Critical Services, will require users to first authenticate (e.g., via some forms of credentials) with the Identity management server to retrieve tokens, which are then used to retrieve user profile information, including IDs, from the MCPTT server.

[12] In some LMR systems, no identity data is transmitted with the Push to Talk voice message.

- Public safety agencies need the capability to view a list of current users associated with a particular MCPTT talkgroup. This would include both traditional first responders as well as secondary responders (e.g., FirstNet Extended Primary users).
- First responders may be using more than one MCPTT device, which could include a vehicle mounted radio, a hand carried device, a tablet, and a smart phone. When a first responder transmits, it is important to know which device they used. For example, if a police officer calls for help at the scene of a burglary: Is the officer located at their vehicle, which is parked in front of the building, or are they on the 15th floor of the apartment building using their handheld device? It is currently unclear how a first responder's device information may be appended to their User ID.[13]
- Standardized identity for users of MCPTT also extends to non-human components. First responders may be using MCPTT talkgroups to query an Artificial Intelligence (AI) assistant for information or to make a request for service. For example, a police officer at the scene of a traffic crash may switch to a designated talkgroup and say, "One Rotation Wrecker." The AI system would use the officer's identity to look up the incident being worked and then notify the next wrecker company on the rotation list.
- Standardized identity information originating from MCPTT could also be used to implement specific policy templates, including those that relate to alerting and notifications. A firefighter's biometric monitoring system could customize the alerting threshold for a high heart rate alarm, so it was relevant for that specific firefighter based on their MCPTT ID.
- The MCPTT User ID may also be used to identify the authorized voice of a first responder and restrict voice access to the device by others.[14]

Most existing MCPTT industry solutions are based on Release 13 of the 3GPP standard. Work is underway to finalize Release 15 of the standard while additional revisions and new work is starting for Release 16. This informs public safety agencies that MCPTT will continue to evolve as the standards efforts refine existing capabilities and add new ones. **A key take-away of this report is the need for public safety agencies to be aware that MCPTT is a very different solution than LMR and that it is still evolving.**

2. Importance of First Responder Identity

The identification of each first responder is a critical factor for all public safety agencies and is especially important when using Push to Talk voice communications in tactical high-risk

[13] It should be noted that 3GPP standards provide for the transmission of GPS location information during each transmission. But identification of the specific device is still necessary in order to determine which one has been stolen or is malfunctioning.

[14] There are policy and technical issues surrounding voice access services, including use on shared devices. This item is noted as an example that the MCPTT User ID can support an array of other services and capabilities.

situations. From an MCPTT perspective, first responder identity is important because it provides real time information on who is communicating. It also allows for the identification of a first responder whose transmission is garbled or otherwise hard to understand. Identity supports the emergency alerting feature when a first responder is in trouble and cannot speak. Finally, it assists in the identification of lost and/or stolen devices, so they can be disabled.

MCPTT will eventually allow a first responder to travel virtually anywhere and contact a nearby PSAP for information or assistance, even if that PSAP is hundreds of miles away from their home agency. The management of first responder identity is therefore significantly complicated by the nature of the NPSBN, which moves this function from a localized agency specific operation to a single nationwide network.

Rapid identification of public safety personnel should be possible in all of the following situations:

- When using MCPTT to call for help
- When using their MCPTT Emergency Call Button
- When a sensor connected to their MCPTT device detects an emergency and calls for help on the first responder's behalf, using the MCPTT application
- When they are communicating with their home agency
- When they are communicating with mutual aid agencies
- When they are outside their local area

As noted above, identity solutions must also address devices that may use the first responder's MCPTT device to transmit data and alerts. A public safety IoT [Internet of Things] device attached to a law enforcement officer's belt may automatically detect that the officer is in a struggle and transmit an alert using the officer's LTE device as the transmission hub. That alert may leverage the MCPTT identity of the officer when notifying the PSAP. Another IoT device may detect that an EMS unit has been involved in a collision and transmit a data alert using the paramedics MCPTT identity. Some IoT devices and sensors will connect directly to cloud services using their own network connection to the NPSBN or via a separate IoT network. Those devices should also transmit a standardized identity of the user to the PSAP. Additional study is needed on best practices to manage those issues.

While there are a variety of ways in which identity is used by first responders and their devices, this report is focused exclusively on MCPTT and User Identity. However, it is important to note that the need for first responder identity extends to any NPSBN user who is able to access MCPTT. Extended primary users, which include public transportation, utilities, and public works, frequently need to communicate with first responders at the scene of a major incident. They will likely be authorized to access MCPTT interoperability talkgroups and will need to be identified for the same reasons as those noted for first responders.

Finally, beyond the need to standardize MCPTT identity processes, all devices and sensors will need to be provisioned with an appropriate and standardized identity. This includes any electronic component that may communicate with a public safety agency, including body worn cameras, IoT devices, and safety sensors.

3. MCPTT Standards and Identity Data Elements

The standards which define MCPTT were created by the 3rd Generation Partnership Project (3GPP) which continues to enhance and refine them. 3GPP is an international standard setting body that provides collaboration between groups of telecommunications organizations.

Most existing MCPTT industry solutions are based on Release 13 of the 3GPP standard. The FirstNet Authority has indicated that it will require MCPTT applications on the NPSBN to use Release 13 as the baseline. However, work is currently underway to finalize Release 15 and new work is starting to define Release 16. Public safety agencies should be aware that MCPTT will continue to evolve as the standards work refines existing capabilities and adds new ones.

There are a variety of identification systems and schemes associated with public safety communications. It should be noted that MCPTT requires that a user be signed into the application to use the service. This is different than with LMR devices where anyone can pick up the radio and make a transmission or activate the Emergency Call Button. This is because security for all LTE Mission Critical Services is bound to the user and not the device.[15]

To access MCPTT, a first responder must initiate a series of specific steps, which are described below in general terms:[16]

- A first responder **turns on** their device (the network sees that it is an authorized device and allows it to connect).
- A first responder **unlocks their phone** (with a PIN number or biometric data) to access applications and services.
- A first responder **opens the MCPTT application** and signs in with their credentials (and is then authorized to use the application).

While not addressed in this report, Identity, Credentialing, and Access Management (ICAM) solutions play a role in the management of first responder devices and may support a "Single Sign On" (SSO) solution. SSO would enable multiple software applications to receive log on credentials without the first responder having to sign in to each one individually. There is an

[15] It should be noted that while this approach provides enhanced security, it will not be possible for a first responder or citizen to pick up a device and call for help if that device is not logged in and authenticated.
[16] The three steps identified provide a high-level overview of a more complicated process with multiple steps.

extensive set of 3GPP standards related to MCPTT that govern all of these processes. Additional standards also exist for a wide range of other mission critical services.

Current 3GPP standards[17] establish three ways to identify an MCPTT user:[18]

1. MCPTT **User ID**
2. MCPTT **User Alias**
3. MCPTT **Functional Alias**

Each of these data fields is controlled by the public safety agency that provisions the user. This information is stored in a first responder's MCPTT User Profile, which is maintained on an MCPTT Server. This data is not hard coded to the device as is the case with LMR radio identity information.

The following sections provide specific information on each of these MCPTT identity elements:

MCPTT User ID. The first data element used to manage identity is the MCPTT User ID. 3GPP standards require that the User ID be unique (e.g., it cannot match any other MCPTT User ID). The User ID is formatted as a Uniform Resource Identifier (URI) and is structured like an email address[19] (e.g., John.Smith@OrangeCountyFire.FL). The MCPTT User ID structure provides significant flexibility for the creation of a first responder's identity.

MCPTT User Alias. The MCPTT User Alias is a free text data field.[20] It has no prescribed data structure and the data is not required to be unique. It could be used to store supplemental information based on local agency needs. For example, an agency could use this data field to hold a secondary identity for the user (like a permanently assigned CAD Unit Number) or it could be used to store additional contact information (like their cell phone number). This data field may also be used to store information on a first responder's credentials and special skills.

MCPTT Functional Alias. The MCPTT Functional Alias is a new capability that is included in 3GPP Release 15. It allows a local agency to assign a specific functional role to a first responder. This is designed to be dynamic in nature and updated on an as needed basis. For example, a unit at the scene of a warehouse fire could be designated as the "incident commander" while another unit could be designated as the "evacuation supervisor." This could support the ability to assign an ICS position[21] to specific first responders based on their role at the scene of the emergency. It could also be used by public safety agencies for other purposes. This data field is

[17] See 3GPP Standard 23.179 and subsequent revisions for information on MCPTT Release 13.

[18] 3GPP standards also define various group identifiers and attributes for each user.

[19] The URI will support approximately 2,000 characters in overall length, and each specific element of the User ID is limited to 57 characters.

[20] The URI will support approximately 2,000 characters of data.

[21] The National Incident Management System (NIMS) has a structured set of roles and responsibilities for personnel operating at the scene of an emergency.

also designed to look like an email address. 3GPP standards note that the Functional Alias data should be structured and used in a consistent way, but the standard does not prescribe a set of valid entry codes for this data field. The Functional Alias could be designed so that an assignment is selected from a drop-down list of standardized options.

Specific recommendation on the use of these three data fields is provided in Chapter 4.

Public safety agencies will need to access the identity information contained in each of the three data fields. These fields are a part of a larger MCPTT User Profile, which contains additional information.[22] It is likely that industry will create an interface that will feed MCPTT data into an agency's CAD system (or other technology) where additional data mapping can occur and where this data can be aggregated with other information.

This approach may provide the same type of data translation that occurs today when radio ID data is exported from a public safety LMR system into another database or technology platform. For example, MCPTT data may be converted by the agency's CAD system to display the first responder's current CAD Unit ID (instead of their specific personal identity). Vendor software could access multiple databases and provide important information to the PSAP, beyond what is available from the MCPTT system. This process is further described in Appendix A.

In order to fully leverage the first responder identity information described in this chapter, public safety agencies may need additional capabilities, including:

- The ability for PSAPs to immediately visualize identity information of any user who is communicating on an MCPTT talkgroup.
- The ability for the PSAP to visualize additional information about a first responder that may be contained in the MCPTT Alias or MCPTT Functional Alias.

4. Recommendations for MCPTT Identity Management

This chapter offers specific recommendations for the management of first responder identity in MCPTT. These recommendations are based on a review of various MCPTT data fields and follow lengthy discussion on the minimum amount of information that a communications center would need in order to identify a first responder in distress. Beyond first responder safety, public safety agencies will also use MCPTT identity information on a daily basis to support operations. While the main focus of this chapter is on identification of first responders, it is important to note that Extended Primary and other critical infrastructure users of MCPTT must also adopt the same standardized approach. These other entities may be communicating with

[22] 3GPP Release 15, Section 24.484 provides a complete list of the XML data elements included in the User Profile.

first responders on public safety interoperability talkgroups and must be identified for safety and operational reasons.

This report recommends the use of a specific MCPTT data field as the primary location for first responder identity. It further recommends a core set of data elements which should be considered the minimum necessary to identify a first responder. These recommendations represent the collective input of public safety agencies and other stakeholders based on operational requirements

It is recommended that the MCPTT User ID be adopted as the standardized location to store primary information about a first responder's identity.

Public safety agency representatives were surveyed to determine which specific pieces of identity data should be considered essential in order to identify a first responder or MCPTT device in an emergency. Two groups of user equipment were identified. They include MCPTT users who are assigned a specific device and use their personal log-on credentials, and MCPTT consoles and specialty devices, which are shared by multiple users and which do not have an individual user signed on. Each of these two groups have unique identity requirements that must be addressed separately.

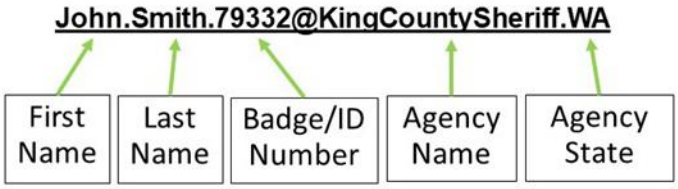
Group 1: MCPTT Individual Users

This is a typical user configuration where a first responder signs into the MCPTT application on a device issued to them. This may be a permanently assigned device or a shared device that they are using for their shift. Five identity data elements are recommended as the minimum necessary to identify these first responders:

MCPTT ID ELEMENT	EXAMPLE	Comment
Responder First Name	John	
Responder Last Name	Smith	
Responder ID Number	79332	Agency assigned Badge or ID number
Agency Name	King County Sheriff	The full agency name should be used and not the agency's city or county name.
Agency State[23]	WA	The first responder's home agency state would be necessary to identify the correct public safety agency, especially if an itinerant user called for help outside of their local area.

[23] The suffix "US" could be used to identify federal agencies, but this report does not make specific recommendations for federal users of MCPTT.

An example of the MCPTT User ID resulting from this recommendation would be:
John.Smith.79332@KingCountySheriff.WA



Group 2: MCPTT Consoles and Specialized Uses

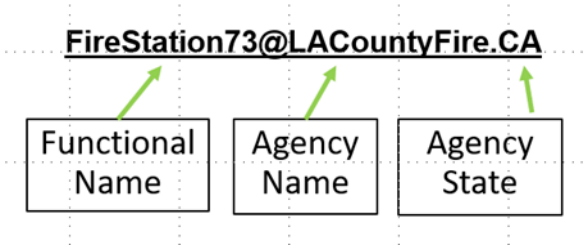
This MCPTT configuration supports dispatch consoles and other specialized equipment. In some cases, as with MCPTT consoles, the public safety agency may want a functional name to be displayed (e.g., "Patrol West") vs. the name of the dispatcher staffing the console. In other cases, MCPTT radios may be located in hospital emergency departments, fire stations, emergency operations centers, and mobile command posts. Those MCPTT devices would be used by a group of authorized personnel and a functional name would be preferred over the display of the name of a single first responder.

Three identity elements are recommended as the minimum necessary for this group:

MCPTT ID ELEMENT	EXAMPLE	COMMENTS
MCPTT Functional Name	FireStation73	This identifies where the MCPTT application is to be used.
Responder Agency Name	LACountyFire	This identifies the home public safety agency.
Responder Agency State[24]	CA	This identifies the first responder's home agency state.

Examples of the MCPTT User ID resulting from this recommendation would be:
FireStation73@LACountyFire.CA (shown in the table above)
HarborviewED@KingCountyEMS.WA
MobileCommandPost1@GainesvillePolice.FL
PSAPSupervisor@AtlantaPolice.GA

[24] See footnote #21 regarding the use of the suffix "US" to support federal users.



Beyond the minimum data fields recommended in this report, the issue of data formatting and sequence must be addressed to ensure consistency across the wide variety of public safety agencies and other entities who will use MCPTT.

This report recommends the standardized sequence noted in the above examples. This includes first name followed by a period, the last name followed by a period, the Agency ID/Badge number following by the "@" symbol, followed by the agency name and a period, and then the identity of the state the public safety agency is in. The use of standard U.S. postal code assignments for the state would also support cross border interoperability with Canada as their provinces also use two letter postal codes that are unique to those used in the U.S. This suggested format must be vetted by the FirstNet Authority and AT&T to ensure that it will meet the technical requirements for MCPTT implementation. Further, the FirstNet Authority's Public Safety Advisory Committee (PSAC) should review these recommendations and provide input.[25]

A standardized approach to the creation of MCPTT User IDs is essential in order to achieve the goal of rapid identification of a first responder in an emergency. Variations in the MCPTT User ID could lead to confusion and delay the arrival of assistance in an emergency. For example, in the absence of a standard, a public safety agency may elect to use the first responder's email address as their MCPTT User ID. This would result in a wide range of different formats and missing information. For example, a firefighter working for the City of Kent, Georgia, may be assigned the following MCPTT User ID by the agency administrator:

- **John.Smith@KentFire.GA**
  (correct User ID syntax based on recommendations in this report)
- **John.Smith@Kent.GA**
  (no agency name assigned)
- **John.Smith@KentFire.gov**
  (no state identified, there may be multiple cities named Kent)
  (use of "gov" at end of User ID to emulate email address)
- **John.Smith@CityofKent.GA**
  (variation of the city name)

[25] These recommendations could also be shared with other LTE operators including public safety broadband networks in adjoining countries.

- **John.Smith@KentFireOperations.GA**
  (variation including the fire department's division name)

It should also be noted that public safety agencies may need to include additional identity data elements based on their unique operational needs. For example, a metropolitan sized public safety agency with a large number of personnel may desire to include the specific division that the first responder is assigned to. Other agencies may want to include the rank of the first responder to help identify personnel who are authorized to take command of an incident.

Public safety agencies may also need to include additional data elements beyond the functional name for MCPTT specialty devices. For example, an agency may want to include the hardware device name (MDC1210), the type of device (laptop), and the device's installed location (Vehicle 1213) as they create the User ID for the device.

These additional data elements could be accommodated by adding them to the end of the standardized MCPTT User ID. In this way, interfaces and APIs could receive a structured data stream of the core identity elements. Public safety agencies could still leverage the use of the additional data elements by working with their technology vendors to modify their interface applications.[26]

The two other MCPTT Identity Elements, **MCPTT Alias** and **MCPTT Functional Alias** are also available for use by public safety agencies. The MCPTT Alias data field is unstructured free text and allows an agency to store any type of information it desires.

The **MCPTT Functional Alias** allows a public safety agency to assign a dynamic task to a first responder. For example, it may be used to note that the user is a member of the command staff. It may also be used on a dynamic basis to flag an MCPTT user as the Incident Commander at the scene of an emergency. This real time update may be initiated by the communications center (via an interface from the agency's CAD system or other technology system). There are a number of unresolved issues with the Functional Alias, including a decision on whether to place structured status information in a drop-down menu to ensure consistent utilization by public safety agencies. If this data field is left unstructured, public safety agencies will invariably use any text entry format or abbreviations that they desire. This would make it difficult for the PSAP or the COML to identify key members of the ICS structure. For example, if selected members of the Incident Command team needed to have their priority level uplifted, it would be difficult to quickly identify them if each agency used their own nomenclature and abbreviations. It is therefore recommended that this data field be standardized, and public safety agencies should select options from a drop-down menu.

[26] An example of how P25 LMR data is leveraged by public safety agencies today is included in Appendix A.

5. Conclusions and Next Steps

The nationwide coverage provided by the NPSBN will allow public safety personnel using MCPTT to communicate with almost any other agency, including those far removed from their traditional service area. Personnel providing mutual aid or traveling through another agency's service area may need to request urgent assistance or request additional information about their assignment. A key component of first responder safety is the ability for the PSAP to immediately determine the identity of those users, especially those in distress. This report provides high-level recommendations on the potential use of various MCPTT data fields to create a standardized approach to managing first responder identity.

This report is also designed to increase awareness of these issues by public safety agencies as they consider implementation of PTT and MCPTT services and to raise awareness with key stakeholders, including local, regional, tribal, and state coordinating entities.

Finally, it should be noted that many questions surrounding the implementation of MCPTT cannot be answered at this time as 3GPP standards are updated and as the FirstNet Responder Authority and AT&T finalize the MCPTT system design and architecture.

The following recommendations are made:

Recommendation #1: The MCPTT User ID should be the designated data field for first responder identity and should also be used by Extended Primary users.

Discussion: Of the three data fields available in MCPTT, the User ID is the most logical choice to assign for first responder identity because it requires a unique ID. It is critically important that any NPSBN user who has access to MCPTT be identified in a standardized way. This includes Extended Primary users who represent secondary responders including transportation, utilities, and other critical infrastructure support entities.

Recommendation #2: A minimum set of core identity components should be designated as mandatory during the creation of MCPTT IDs.

Discussion: While public safety agencies may need flexibility to include additional data elements in the User ID, a minimum set of mandatory identity components must be established. These minimum components should be sufficient to identify a first responder who is communicating with a public safety agency that is not their home organization. This report offers recommendations on a set of mandatory elements for MCPTT users and a different set for MCPTT consoles and other specialty devices. Extended Primary users must also adopt these core identity components to prevent ambiguity in their MCPTT display identity when they communicate with public safety agencies.

Recommendation #3: The MCPTT User ID data field should be standardized so that public safety agencies will enter the required information in a specific structured order.

Discussion: Identity information must be provided quickly and in a standardized format during an emergency. Personnel in the PSAP should not receive identity information in varying formats based on individual agency preferences. While this report does not recommend a specific entity to create the standardized identity structure, the FirstNet Authority should make that determination and leverage the expertise of the PSAC and other public safety associations and organizations. The local control software used to provision new user accounts on the NPSBN should be programmed to require that identity information be formatted in the correct manner.

Recommendation #4: The MCPTT Functional Alias data field should be standardized and public safety agencies should select options from a dropdown menu. Consideration should be given to ensure that this data field has sufficient flexibility to be used for day-to-day operations as well as during major incidents.

Discussion: The MCPTT Functional Alias field is a new feature offered by 3GPP in Release 15 and is designed to track the functional task assigned to a first responder at an incident scene. For example, an MCPTT user may be assigned as the Incident Commander. 3GPP designed this data field to support a set of fixed selections which would standardize the format of the information, but decisions on selection options would be left the entity implementing the service. If this data field is instead used for unstructured free text entries, it will dramatically reduce the functionality. This report advocates for the creation of structured data selections but does not offer specific suggestions for content. This issue needs greater study by a larger set of stakeholders to achieve a consensus on an appropriate list of incident functions.

Recommendation #5: Additional research should be conducted to determine what issues may impact first responder identity when the MCPTT user is in **Direct Mode**.

Discussion: There are many questions surrounding the use of direct mode proximity services in MCPTT, which are also known as “Pro Se.” Pro Se allows for direct device-to-device transmission of voice, data, and video. It is unclear at this time how the MCPTT User ID will be transmitted when a first responder switches to direct mode.

Recommendation #6: Additional research should be conducted to determine how a first responder may be identified when they are using **two or more MCPTT devices** at the same time.

Discussion: It is highly likely that first responders may be equipped with more than one device that is capable of accessing MCPTT. This may include a handheld device, a vehicle mounted device, and a tablet. If a first responder radios for emergency assistance, the PSAP must be able to determine from which device the call for help originated. It is unclear at this time how the MCPTT application may leverage information on the device hardware in conjunction with the MCPTT User ID.

Recommendation #7: Consideration should be given to creating a standardized framework that will manage the identity of other technology and public safety IoT components which connect directly to the NPSBN or other networks and bypass the MCPTT application.

Discussion: As with MCPTT, these devices need to be provisioned with a standardized identity that is meaningful to personnel in the PSAP. This includes any electronic component that may communicate with a public safety agency and/or generate alerts, including body worn cameras, IoT devices, and safety sensors.

Recommendation #8: The PSAC should examine additional ways to leverage first responder identity information, including the ability for the PSAP to determine which users are associated with an MCPTT talkgroup.

Discussion: MCPTT will allow any first responder, or Extended Primary User, to contact other agencies on talkgroups designated for that purpose. Because this capability allows multiple personnel from multiple agencies to share a talkgroup in an emergency, the PSAP must be able to determine who is on that talkgroup.

Finally, it is recommended that this report be forwarded to the FirstNet PSAC, SAFECOM, DHS's Office of Emergency Communications (OEC) and the Science and Technology (S&T) Directorate, and the National Council of Statewide Interoperability Coordinators (NCSWIC) for their consideration.

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. More than 200 members of the public safety community contributed to, or reviewed, this report including first responders and representatives of industry and academia.

APPENDIX A: Example of Public Safety Agency Use of P25 LMR Push to Talk (PTT) Data

The following examples illustrate how some public safety agencies share P25 PTT data via CAD system interfaces to fully determine first responder identity. This same approach could be used with MCPTT solutions in which MCPTT User ID data is shared with CAD systems and other applications and databases to aggregate information needed to manage an emergency response. For this to be effective, the MCPTT User ID data must be formatted consistently to be used by the agency interface or API.

Example 1: First responder, John Smith, transmits a radio call for help to the PSAP using a P25 radio.

1. John Smith transmits an emergency request for back up to the PSAP using the radio in his patrol car, but the voice transmission is distorted due to background noise and yelling.
2. An interface links the P25 Radio System with the public safety agency's CAD system and each radio transmission results in the Radio ID being shared with the CAD system along with GPS location data.
3. The CAD system receives PTT Radio ID 11827 from the mobile radio in John Smith's patrol car.
4. The CAD system matches this Radio ID (11827) to a radio installed in Police Department Vehicle 1234 (V1234).
5. The CAD system then matches Vehicle 1234 as the patrol car assigned to Officer John Smith, Badge Number 6789.
6. The CAD system then determines that Badge Number #6789 is on duty as CAD Unit "1Adam12."
7. "1Adam12" is displayed on the dispatcher's console in the same instant that the officer makes his radio transmission.

Example #2: First responder, John Smith, activates the emergency call button on his radio.

1. John Smith quickly presses the orange button on his portable LMR radio during a fight with a suspect in which he cannot make a voice transmission.
2. An interface links the P25 Radio System with the public safety agency's CAD system.
3. An Emergency Call Button activation results in the Radio ID and GPS location data being shared with the CAD system accompanied with an alert flag to note the emergency.
4. The CAD system receives an Emergency Call Button alert from Radio ID 12999.

5. The CAD system matches this Radio ID (12999) to a portable radio assigned to Officer John Smith, Badge Number #6789.
6. The CAD system then determines that Badge Number #6789 is on duty as CAD Unit "1Adam12."
7. The CAD system activates an audible and visual warning, and the CAD Unit "1Adam12" is displayed on the dispatcher's console flashing in red.
8. The CAD system then retrieves the incident record for the call that 1Adam12 is assigned to and displays the call information for the dispatcher.
9. The CAD system retrieves the incident location and/or the Automatic Vehicle Location (AVL) data for 1Adam12 and displays a pop-up map, which includes the GPS location shown for the radio device.

Example of CAD System Display: **Emergency Alert Received**
Unit: **1A12**
Current Incident: **F18093927** (a copy of the CAD incident record opens up)
Current Location: A **map display zooms** to the location of the incident and/or to the AVL location