



The
Public Safety[®]
Network 
EMPOWERING PUBLIC SAFETY WITH LIFE SAVING TECHNOLOGIES



A Public Safety Agency Roadmap for Successful Mission Critical Push-to-Talk (MCPTT) Implementation

Introduction

Starting this year, public safety agencies across the United States will be able to leverage smartphone-based push-to-talk for mission critical operations. Mission Critical Push-to-Talk (MCPTT) provides the features and functionality traditionally used in connection with land mobile radio (LMR) systems but adapted for LTE mobile devices and networks. This functionality will be fully operational on FirstNet, which was built with AT&T. This nationwide communications platform will provide public safety with both the core communications functionality it has come to rely on and the enhanced broadband capabilities that modern first responder agencies need.

As we enter 2020, many public safety agencies are expanding their mobile initiatives — moving away from an informal bring-your-own-device (BYOD) approach, and toward issuing smartphones as core tools for every law enforcement officer, firefighter, paramedic and emergency medical technician (EMT).

In planning this transition, it is critically important for agencies to incorporate MCPTT in their technology roadmap. In the midterm, MCPTT on smartphones will complement existing LMR systems. However, as the technology matures over the next decade, it's anticipated that MCPTT will begin to replace and improve upon LMR systems, bringing significant cost savings for agencies. In addition, the deployment of modern smartphones to all personnel will enable on-the-go access to key computer-aided dispatch (CAD), situational awareness apps, automatic location/routing tools and records management systems (RMS).

This guide will describe the core features and the benefits of MCPTT and offer recommendations for public safety agencies to plan and execute a successful transition to rugged smartphones with built-in MCPTT capabilities.



What Is MCPTT?

Before looking at how public safety agencies can incorporate MCPTT into their operations, it's important to understand how it came about and what capabilities it will provide.

MCPTT is governed by the Third Generation Partnership Project's (3GPP) Mission Critical Push-to-Talk over LTE standards, starting with Release 12 and continuing through Release 14, which was finalized in 2017.

MCPTT was designed specifically to meet public safety's mission critical voice communication requirements, including reliable connectivity with low latency, high-quality audio, security and encryption, support for one-on-one and group calling, broadcast calling, emergency alerts, caller identification and direct device-to-device communications. The 3GPP Release 15 includes additional enhancements to these capabilities, including remotely initiated call requests, location tracking, and the creation of emergency zones. These capabilities will be extended to a wider business sector with the completion of Release 16, which is currently in development by 3GPP.

Public safety's use of mobile broadband networks with rugged smartphones and MCPTT provides significant benefits over LMR systems on their own. Specifically, it enables:



The ability to **leverage a single device for all voice communications** and data applications



The **integration of public safety applications** with devices running mobile-enabled operating systems and user interfaces



Cost savings through reduced capital investment and the ability to leverage **economies of scale** for hardware and applications available within the mass market, but ruggedized for public safety



Nationwide coverage across an LTE network with priority, preemption, encryption and hardening



True interagency, nationwide, city, county, state and federal **interoperability**

Innovation Spotlight: Samsung's Galaxy XCover FieldPro

Samsung is leading the way with the introduction of MCPTT-capable mobile technology. The Galaxy XCover FieldPro was designed specifically for first responders, with a rugged design, high performance and a field-ready feature set.

Durability: Tested against MIL-STD-810G standards for drops, shocks and vibrations

Water resistance: IP68-certified for dust and water resistance

Battery Life: Full-shift, field-replaceable batteries plus grab-and-go, pogo-pin charging

Dedicated PTT Buttons: Glove-friendly physical keys for PTT, navigation and emergency connection for quick access on the move

Security: Samsung Knox security down to the chip level to meet CJIS, NIAP and HIPAA requirements

Biometrics: Ergonomic fingerprint sensor for secure, fast device authentication

FirstNet Ready: Available on FirstNet, the nationwide communications platform built with and for first responders.

Included Accessories: Comes with FirstNet PTT ear-tube headset and belt clip, as well as drop-in desk charger and spare battery



Overcoming Interoperability Challenges With MCPTT

Leveraging rugged smartphones with MCPTT creates a unique synergy where public safety retains the benefits associated with traditional radio systems, while enhancing them with rich broadband and LTE capabilities through a single high-performance device.

In particular, leveraging MCPTT with smart mobile devices will greatly diminish the interoperability issues that have existed for years between and among radio networks. Traditionally, the United States has had more than 10,000 separate LMR networks¹ for public safety, creating substantial interoperability issues among jurisdictions and among law enforcement, fire, and emergency medical services (EMS) agencies.

MCPTT is built upon open international standards, which ensure interoperability today and into the future as the network is constantly upgraded. This important difference between LTE public safety implementation and the way that LMR has traditionally been implemented in the United States means there will be inherent operability between and among all users and agencies adopting MCPTT. Simply put, the operability among public safety agencies is similar to how people in the United States can successfully text friends, family and colleagues both domestically and in other countries, despite different networks and devices being used. The technologies used inherently allow users to communicate with one another. This is what MCPTT does for public safety users using mobile broadband. It is key that this new functionality be simple and easy to use, and it is.

With specialized devices such as Samsung's Galaxy XCover FieldPro, first responders will be able to use the push to talk button on the side of their smartphone to leverage the MCPTT functionality in the same way they always have with their traditional radios. In addition, the XCover FieldPro has an emergency "personnel down" button on the top of the device to enable emergency communications. This familiarity makes the operational transition to a hardened LTE device relatively easy with minimal training required, yet resulting in enhanced capabilities to the users.



¹ Based on 2012 recorded FCC license applications from public safety when first responder agencies were working to bring their LMR systems into compliance with the FCC's narrowbanding mandate. See <https://urgentcomm.com/2019/01/03/public-safety-lmr-licensing-activity-sets-new-low-during-2018/>

Why Transition to MCPTT?

Public safety is inherently a mobile workforce and this requires that agencies provide responders with the best mobile tools to support them as they respond to and engage in calls for service every day.

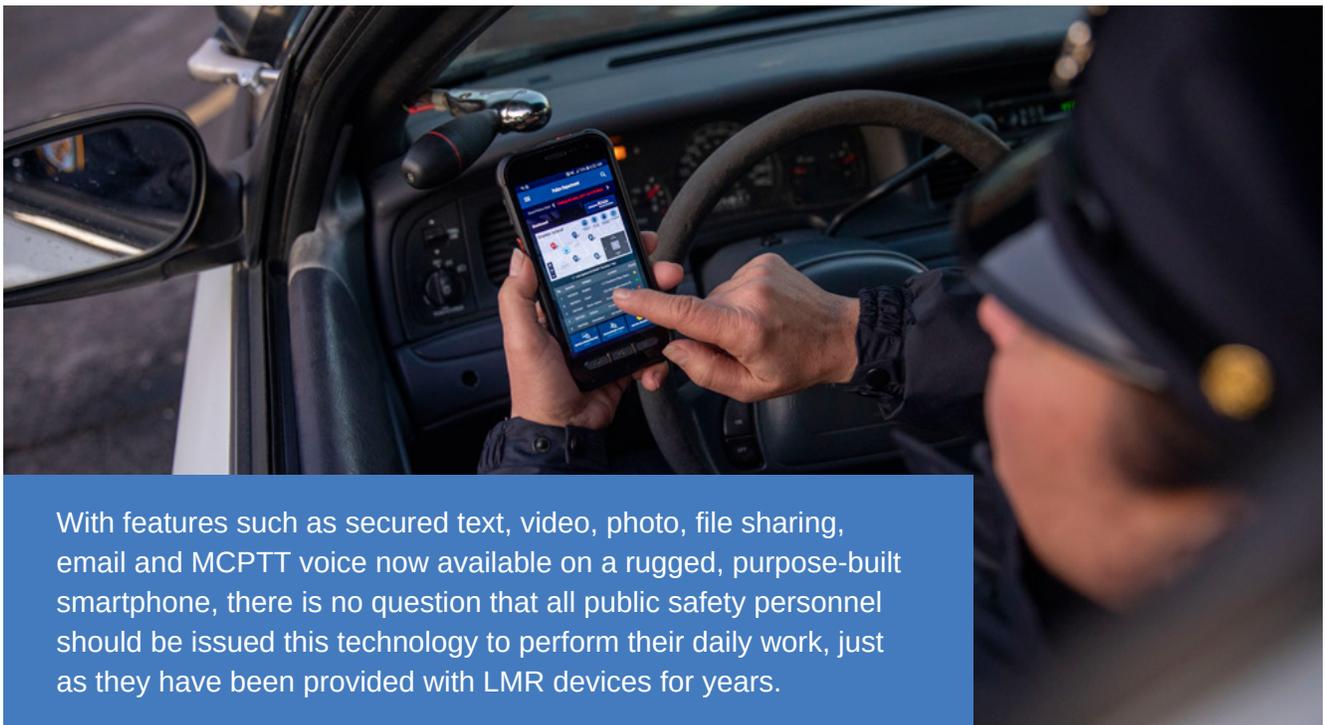
With features such as secure text, video, photo, file sharing, email and MCPTT voice now available on a rugged, purpose-built smartphone, there is no question that all public safety personnel should be issued this technology to perform their daily work, just as they have been provided with LMR devices for years.

Providing first responders with a reliable and rugged smartphone enables all departmental applications, including CAD, RMS and other applications, to be accessible remotely in the field. Additionally, by consolidating computing around the smartphone — as seen with Samsung's DeX in Vehicle solution — departments are reducing the number of endpoints, and therefore the device management burden and risk of data breach.

Augment with Broadband Technology

Public safety organizations will in most cases maintain both LMR and MCPTT systems during the transitional phase until LMR ramps down over the next decade. However, taking advantage of MCPTT as an immediate parallel network with a legacy LMR voice-only network produces:

- Individual first-responder location data on emergency scenes, improving safety and effectiveness
- A completely redundant voice communications network alongside the existing LMR network that now has the same functionality as existing LMR technology plus additional rich data applications
- A secure, multimedia-rich data platform for emergency dispatch, situational awareness and real-time data coming from NG911 and additional data repositories (ADR) directly to responders in the field
- LMR handset emergency functions also available on the rugged smartphone



With features such as secured text, video, photo, file sharing, email and MCPTT voice now available on a rugged, purpose-built smartphone, there is no question that all public safety personnel should be issued this technology to perform their daily work, just as they have been provided with LMR devices for years.

Guidance for Agency Integration of a Rugged MCPTT Solution

Like any complex technology migration, a phased approach for implementation is most effective for transitioning to MCPTT. Change management requires good preparation and planning with appropriate follow-up and should be implemented incrementally to maximize effectiveness.

Public safety agencies can begin with an inventory of the mobile needs of all personnel. While planning to outfit all personnel with an agency-issued MCPTT-capable smartphone, it is important to also assess the need for other connected devices and the specific role of all personnel. For example, agencies should consider whether frontline personnel may need smartwatches and other internet of things (IoT) devices. It is also important to review whether desktop computers and/or laptops could be phased out in favor of today's powerful mobile devices that can potentially meet all the needs of public safety personnel.

MCPTT Migration Planning Checklist

- ✓ Assess the technology currently assigned to each member of your department — from desktop computers to in-vehicle laptops, mobile hotspots, body cameras and LMR
- ✓ Determine whether the interworking capabilities are in place for a legacy LMR system to interface through a gateway to MCPTT devices
- ✓ Evaluate LTE/LMR integration vendors and costs and conduct testing of the preferred solution to ensure interworking between LMR and MCPTT
- ✓ Assess the capabilities of new or existing department-issued smartphones for use with MCPTT
- ✓ Match mobile device options against current operational roles and needs, considering frontline personnel, supervisors, leadership and command personnel, and other nonfrontline personnel
- ✓ Update your communication policies and procedures to ensure that MCPTT is addressed in all areas of department policy and procedure
- ✓ Evaluate existing software used by your department to determine capabilities available on smartphones, including CAD, RMS, Automatic Vehicle Location systems (AVL), secure communications and situational awareness apps
- ✓ Consider smartphone charging needs, in-vehicle, in-station and at-home, and plan to stock spare batteries for long-running operations
- ✓ Develop device cleaning policies, including for particulate matter from smoke and fire, as well as blood-borne exposure and pathogens
- ✓ Evaluate necessary smartphone accessories, including external speakers/microphones, earpieces and uniform holders
- ✓ Deploy mobile security and management tools to ensure local device protection, timely security updates, effective locking and wiping of lost or stolen device

A Phased MCPTT Rollout

Deploying MCPTT-capable smartphones across a large first-responder agency should be planned in several phases. Here's a roadmap for phasing a rollout across three to six months:

Roll out initially to training, administration and nonfrontline personnel. This initial rollout will allow for the processes and procedures to be worked out with personnel responsible for training, communications, logistics and support and ensure that all new procedures are documented. This should not be rushed and can logically be done over a 30-to-60-day period. All issues should be thoroughly addressed and worked through before proceeding to transitioning supervisors and command personnel.

Expand to first-line supervisors and command personnel. Supervisors and command personnel must lead by example. They should become strong users of the new technology and should be ready and able to answer questions of frontline personnel before going to an agency-wide implementation. This will likely be an additional 30-to-60-day implementation and use period.

Deploy to frontline personnel. This should be conducted after incorporating all of the lessons learned from the above, and tried and tested practices for your agency. All policies, procedures and user guides should be distributed prior to full deployment. This will likely be another 30-to-60-day implementation and use period.

Support documentation and an effective communications plan are key to a successful rollout. This should include:

- ✓ Frequently asked questions (FAQ) document
- ✓ Policies and procedures manual/repository
- ✓ Simple and clear user guide
- ✓ Laminated quick reference card
- ✓ Clear escalation path for help and issues, including a phone-and-email help desk

Smartphones Are Already Essential to Agency Operations

Today's first responders all carry a smartphone already, whether it is a personal device or an agency-issued device. They use it for many aspects of their personal life and many aspects of their work life. They use it for voice, video and text chats. It is their go-to device to order coffee, buy airline tickets, get driving directions, etc. Because they already use it every day for almost everything, the learning curve for using a smartphone at work is minimal.

First responders consider a smartphone essential. Ask any of them if they have ever gone to work without their device, and what they would do if they left home without their smart device. The answer is, almost without exception, turn around and head home to get it or ask a family member or friend to drop it by the station.

Another good way to assess the critical nature of smart devices is to ask your entire leadership team to pull out their smartphones and put them in airplane mode. Then request that they do not turn them back on for 24 hours. The looks on their faces will tell you just how important that device and that connectivity is to support their operational role as well as their other daily activities.



Reduced Cost, Increased Capabilities

The migration from LMR to smartphones with MCPTT has the potential to yield significant reductions in capital expenditure over the next decade. Powerful smartphones and tablets cost less than \$1,000 each, which is much less than the \$2,500 to \$6,500 for a full-featured LMR. When then considering the associated LMR licensing and infrastructure, the cost savings achieved with smart mobile solutions is significant. The “as-a-service” model for mobile devices, in which agencies pay a monthly fee for a fleet of devices, also gives many agencies more purchasing discretion since they are now incurring only OpEx costs instead of having to budget for large-scale CapEx investments.

In one California agency, a fire chief recently assigned smartphones (with LMR integration) to some of his nonfrontline staff, repurposed their existing radios, and saved his department \$360,000 annually.² In another, the fire chief opted to provide smartphones for his nonfrontline staff instead of paying for an LMR upgrade and saved \$950,000. The savings achieved by leveraging smart mobile technology can be invested into other complementary technology solutions or can be used to offset operational expenses in other areas.



Powerful, rugged smartphones cost less than \$1,000 each – much less than the \$2,500 to \$6,500 for a full-featured LMR.

Reliability and Increased Capabilities

Moving to agency-issued rugged smartphones with MCPTT provides a completely capable, all-in-one communications system to complement your department’s LMR network. This MCPTT capability, along with applications, photos, video and other multimedia capabilities, provides a robust separate communications platform and network, providing your agency with greatly improved resiliency and capability, with both mission critical voice and data as well as photo and video applications. Plus, mobile devices provide a built-in upgradability with software that is regularly updated and remotely pushed to each device, significantly reducing maintenance costs and complexity. This ensures they remain secure and improves the usability and capability of the device over time.

² <https://urgentcomm.com/2019/01/11/fire-chief-encourages-early-firstnet-adoption-cites-cost-savings-potential-mission-critical-use-in-2024/>

Six Public Safety Mobile Use Cases

To illustrate the beneficial impacts of smartphones in an agency, consider these public safety use cases:

1

Public safety answering points (PSAPs) can now send a photo of a missing child or a wanted suspect to an entire police department in seconds, accessible on smartphones, asking officers to be on the lookout for the individual for faster identification and location resolution.

2

Law enforcement agencies may now share real-time camera feeds from their security cameras to inform critical situations as they are unfolding in the field. CAD and dispatch information that was traditionally sent to a laptop computer mounted in a patrol car can now be sent to an officer's handheld device and wearable with the data and information needed to respond.

3

Police officers have the ability to use the high-quality cameras on their smartphones to capture photos or videos of accident scenes for evidence collection and situational awareness, and then can use apps to log additional details and upload them across secure platforms to their RMS.

4

For wildland firefighters, rugged MCPTT-capable smartphones bring expanded crew safety and dynamic situational awareness capabilities. Device durability combined with a smartphone display to easily review weather information and drone video of the direction and path of a fast-moving wildland fire make tactical operations considerably safer for personnel with faster fire suppression.

5

Under the new Emergency Triage, Treat and Transport (ET3) methodology for community paramedicine, EMS agencies must be able to conduct video telemedicine in a patient's home to be able to meet the program's requirements and to provide the advanced care that is needed. A smartphone can enable a paramedic to embrace the new demands of out-of-hospital care.

6

Rugged mobile devices can meet the demands of EMS personnel who are en route to an incident or outside in a difficult environment where devices may be dropped, or scraped against steel at an accident scene. Smartphones become the baseline communication platform that allows EMTs and paramedics to share real-time patient vital signs, photos, voice reports, ECGs and videos with emergency rooms, as well as with specialty treatment teams.

Conclusion

MCPTT, enabled by rugged smartphones like Samsung's Galaxy XCover FieldPro, will become the foundation for public safety communications in the years to come. Public safety should focus now on developing a migration plan for a seamless transition and successful implementation of MCPTT into agency operations.

The goals and objectives of the transition are to ensure widespread access to mobile broadband capabilities and applications to complement legacy LMR systems. In the near-term, LMR systems will continue to operate alongside MCPTT for redundancy, with gateways providing integrations with the new MCPTT LTE solutions. Public safety leaders will be able to comprehensively support a mobile-first environment, utilizing both LMR and LTE broadband.

For leadership, this is about reducing risk and providing the right tools for the mission. Agencies can reduce risk by having two parallel and interworking voice communications systems for their first responders, while also lowering costs and increasing capabilities. Knowing that communications systems often fail in some capacity during major incidents, having redundant systems that leverage separate technologies and backbone networks to provide MCPTT in the field is much more reassuring from a risk reduction perspective and to the responders themselves.

The smartphone is already ubiquitous for first responders in their personal lives. Some agencies have yet to provide this capability for emergency personnel even though there is now a prioritized, preemptive and secure communications network for public safety that permits easy sharing of video, photos and other data. Public safety fell behind in taking advantage of the available technologies on the market because of the lack of assured connectivity to the cloud and is only now truly able to leverage many of the benefits of cloud connected platforms that mainstream society has been relying on for years. This technology gap narrows more every day.

With the availability of high-speed, secure broadband networks, MCPTT capability running on rugged smartphones, and an ever-growing suite of public safety solutions, public safety agencies are finally in position, both practically and financially, to take advantage of what the communications ecosystem now offers and lead the way in mobile-first operations.

The Public Safety Network has relationships with clients focused on empowering public safety with life-saving technologies, some of which may have contributed to, or helped fund content. Our work for our clients includes, without limitation, helping develop strategies, conducting research, content development, education and training, and sharing best practices, business models and innovative technology for first responders. The views, analysis, research, and opinions contained herein are our own unless otherwise specifically noted.