Analysis and Recommendations for a Universal Interworking Function (UIWF) for Mission Critical LMR & LTE Networks

Final Report

November 29, 2018 - Version 1.1

Prepared for:

Department of Homeland Security (DHS)

Science and Technology Directorate (S&T)

Prepared by:

Murus Cybersecurity LLC

Under

SBIR Phase I Topic Number H-SB018.1-005

Contract

70RSAT18C00000040

Approved by:

THIS PAGE IS INTENTIONALLY BLANK

CHANGE HISTORY

Change	Version	Date
Initial release	1.0	10/26/20 18
Changes for Public Release Updated Conclusions/Recommendations	1.1	11/29/2018

Table of Contents

1 Executive Summary

Good progress is being made in the 3rd Generation Partnership Project (3GPP) in standardizing an Interworking Function (IWF) interface on the Mission Critical Push To Talk (MCPTT) side to support Land Mobile Radio (LMR)/Long Term Evolution (LTE) interoperability. Presently 3GPP Release 15 (LTE) and ATIS/TIA (Project 25 [P25] LMR) work is in progress, which is likely to result in providing some level of open-standard LMR to LTE capabilities.

The 3GPP standard will likely address the major requirements National Public Safety Telecommunications Council (NPSTC) documented. However, the development for the 3GPP IWF interface protocol will not be complete until late 2019. In addition to commercialization time, this means equipment implementing the 3GPP IWF will not likely be broadly available until 2021 at the earliest.

On an interim basis, many users are deploying pre-MCPTT systems. These have created interoperability islands between proprietary solutions. The migration path from these solutions to MCPTT is not uniformly clear. These systems enable core interoperability capabilities that include groups calls, individual calls, emergency calls, and PTT-ID. However, these pre-MCPTT systems, while perhaps based on open-standards (e.g., OMA POC in some cases), are not interoperable between themselves.

ATIS and TIA are jointly working on the development of the interface protocol to be used on the P25/LMR side of the IWF. It is unclear when this development will be done. In addition, 3GPP has postponed the completion of the IWF interface protocol until Release 16 due to pressures to advance 5G standards. Since the ATIS/TIA work depends on the Stage 3 completion of the IWF, the ATIS/TIA work cannot be completed until 2020 at the earliest.

There are several security related concerns especially for end-to-end encryption and user authorization. Both P25 and 3GPP have comprehensive security standards, however the protocols and algorithms of each system are not interoperable. A conversion function in the IWF is required or the LTE user equipment (UE) application will need to accommodate and support P25 security standards. No provision is made for non-P25 LMR interoperable security. Interoperable security solutions are destined to be ad-hoc unless these concerns are addressed.

While using the P25 Inter Radio Frequency Subsystem Interface (ISSI) to interface with the 3GPP IWF and the MCPTT system is the most straightforward path for large trunked system, this solution also has many compromises:

> The P25 ISSI is typically very expensive to procure and maintain, making this solution prohibitively costly for all but the largest P25 systems operators. They pose a significant commercial problem in that the ISSI license fees for the most popular P25 trunking systems is typically in the 6-digit U.S. dollar range, which puts the ISSI outside the budget of most small to medium size public safety agencies.
>
> The P25 ISSI does not natively support P25 conventional -- a mode that is used pervasively by federal law enforcement nationwide.
>
> The P25 ISSI does not address the many thousands of analog conventional channels used by public safety -- often for mutual aid interoperability. Approximately half of the public safety agencies in the USA are still using conventional (either Analog FM or P25 conventional). The ATIS/TIA joint project committee has not yet begun work on conventional interfaces, such as the P25 Fixed Station Interface (FSI) for integration with the 3GPP IWF.

Prioritization in favor of P25 trunking systems may further postpone the ability to integrate conventional LMR systems into the MCPTT ecosystem.

Although the scope of this report is LMR, we also considered the integration needs of dispatch consoles because they are an essential component to any public safety LMR system. Consequently, this report identifies several additional issues relevant to dispatch console integration, including the need for mission critical media outside of voice, the need for achieving MCPTT talk group adhoc creation and priority lift, and the need for access to talker ID meta data.

In light of the 3GPP IWF deployment delays and the gaps in support of non-P25 systems and dispatch consoles, we explored a standards-based alternative to LMR-LMR and LME-LTE interoperability that makes use of open standards already released, implemented, and tested to address some of the gaps in the envisioned solutions.

In this report, we describe an Universal Interworking Function (UIWF) solution that uses the MCPTT UE interface based on 3GPP Release 13, which was released in 2016 and is a mature interface for implementation. The UIWF solution can support the interoperation of any of the following five types of LMR and LTE systems:

- Analog FM conventional system
- P25 conventional system
- P25 trunked system
- MCPTT LTE system
- Non-MCPTT LTE system with an internal ISSI gateway

2 Introduction

This final report contains all the findings and results of the effort conducted by Murus Cybersecurity LLC in partnership with Zetron performed under a Small Business Innovative Research (SBIR) contract with the purpose of recommending a Universal Interworking Function (UIWF) for Mission Critical LMR & LTE Networks that would provide LMR-LMR, LMR-LTE, and Pre-MCPTT -MC LTE interoperability.

2.1 Contract Objective

The full objective of this SBIR is described in ***LMR LTE INTEROP Department of Homeland Security HQ FY18 SBIR Solicitation 7RSAT18R0000010***. In general, the solicitation asked to investigate and develop a reliable, secured, and standards-based LMR/P25 – LTE Mission Critical Network (e.g., MCPTT) interface service and address options consistent with P25, ISSI, P25 Common Air Interface (CAI), RoIP gateways, and donor radios.

More specifically, the intent of the contract was to determine the feasibility of developing an interface/ interworking solution for:

- The different LMR systems in use today; and
- The current LMR systems and new LTE systems being deployed.

The contractors were requested to analyze and define functionality/capabilities and call features not only between an LMR/P25 network and the 3GPP Mission Critical network (e.g., MCPTT), but also across multiple LMR/P25 networks with different technologies/functionality/features/capabilities.

The desired outcome was a solution matrix consistent with the NPSTC requirements that included performance and capability comparison of attributes such as voice quality, complexity, cost, security, ease of implementation protocol availability, and time-to-market.

This report documents all the team's research, analysis, major findings, and recommendations except for several specific proprietary recommendations and solutions. These proprietary recommendations and solutions are described in the Commercialization Report.

2.2 Contractors

Murus Cybersecurity LLC was the primary contractor and Zetron the commercialization partner. A brief biography of each company is shown below.

Murus Cybersecurity LLC

Murus Cybersecurity is a technology and management consulting company specializing in securing complex wireless networks and devices at the edge. It is made up of a network of independent technologists, innovators, and executives from the IT and telecom industries.

Zetron

Zetron was founded in 1981. Public Safety is the primary application for Zetron dispatch console products, and most of its systems are used in multi-agency dispatch centers, where the various agencies may be using completely disparate LMR systems.

3 Purpose of this Final Report

This report satisfies a key contract milestone deliverable. The purpose is to present all the analysis and work performed under this contract in a format that is informative and instructive to as large an audience as possible in the public safety industry.

4 Scope

This document reports on the analysis, activities, and efforts of the Phase I Topic Number H- SB018.1-005 in response to LMR LTE INTEROP Department of Homeland Security HQ FY18 SBIR Solicitation 7RSAT18R0000010. All analysis and work is limited to the six-month duration of the contract. As indicated in this report, there are several areas that require further analysis and effort.
The team made a best effort to focus on the issues that would have the greatest impact to the public safety industry.

5 Overview

In the execution of this contract, the team addressed questions like:

- What is the matrix of system types that need to be connected by this interworking function?
- What standards-based and proprietary wireline interfaces already exist?
- What is the minimum scope of services required to be supported by the interworking function?
- What are the existing IWF solutions and direct connected solutions?
- What are the functional, performance, and security requirements?
- What are the critical functional parameters supported across the IWF?
- What are the relevant standards that apply to a UIWF?
- What are the data streams and data types that need to transit the UIWF?
- What protocol translations need to take place in the UIWF?

The team further developed its reach to include perspectives and findings from government, industry, and users. The team observed the European Telecommunication Standards Institute (ETSI) MCPTT second plugtest event in Texas and developed insight into the state of interoperable technology aligned with the currently published 3GPP standards.

The team also developed a detailed interview plan to collect the most current information from industry experts to identifying gaps and needs relative to this project. The interviewees included experts from NPSTC, AT&T, and the FirstNet Authority.

The remainder of this document contains the team's research, analysis, major findings, and recommendations as follows:

Section 6 is a synopsis of the various standards, studies, and white papers the team reviewed and analyzed as part of research effort

Section 7 presents a summary of the radio technologies currently being used by Public Safety. It discusses current standard and non-standard interoperability solutions.

Section 8 looks at Over the Top (OTT) LTE interoperability solutions, including a table in Appendix C that compares OTT and pre-MCPTT solutions in terms of features, performance, and LMR support.

Section 9 discusses security concerns relative to interoperability. This section looks at the state of the standards' work addressing interoperability security discusses the gaps, risks, and mitigations.

Section 10 focuses on the interworking capabilities of the various systems including Analog FM, P25, MCPTT, and non-MCPTT systems. The section concludes with an analysis and a table of the Minimum set of interworking capabilities.

Section 11 compares the attributes of each interface that is considered in our proposed UIWF solution. Those interfaces include the P25 DFSI, P25 ISSI, MCPTT UE, and 3GPP IWF. We look at voice quality, security, complexity, ease of implementation, time to market, cost, and protocol availability.

Section 12 proposes an UIWF (Universal Interworking Function) solution for the communication of LMR systems with each other and the communication of LMR systems with LTE systems. This proposed solution supports five types of LMR and LTE systems: Analog FM conventional, P25 conventional, P25 trunked, MCPTT LTE, and Non-MCPTT LTE system with an internal ISSI gateway. The proposed UIWF solution can support LMR to LMR, LMR to LTE, and LTE to LTE interoperations.

Section 13 contains a summary of our conclusions and recommendations.

Appendices A and B contain a list of abbreviations and references respectively.

Appendix C contains a summary table of Pre-MCPTT and OTT products and solutions discussed in Section 8.

6 Existing and Developing Interoperability Standards

Standards making has made exceptional progress within 3GPP where a Technical Specification Group (TSG) has established a Service and System Aspect (SA) working group devoted to mission critical applications: TSG SA WG6. This working group has published many documents, including stage 2 (architecture) standards of Mission Critical (MC) Communication Interworking with Land Mobile Radio Systems (TS23.283) and interconnection between MC systems (TS23.280 and TS23.379). These architecture documents are included in Release 15, which was released in mid-2018. Implementation of these services will require completion of stage 3.

A final challenge to MC LTE-LMR interoperability is the fact that although 3GPP Release 15 includes the Mission Critical IWF, it is only at Stage 2 (definition of switching and signaling capabilities). Stage 3 (description of the organization of the network functions to map service requirements into network capabilities) is postponed to Release 16 scheduled for late 2019, which is not in time for the conclusion of this research project. Furthermore, FirstNet has plans to deploy 3GPP Release 13 initially in 2019, and it may be several years before it deploys infrastructure capable of supporting Release 15. This means that any near term LMR-LTE interoperability solution will likely be less than ideal on the LTE side for several years until Release 15 is deployed.

The purpose of this project is to develop the requirements, feature sets, architecture, and design analysis to establish the feasibility of a Universal Interworking Function (UIWF) that closes the gap between standards-based MC LTE and P25 DFSI/ISSI, as well as establish solutions for MCPTT to Pre-MCPTT and other LMR system types, providing a "shim" between these where necessary and productive. In addition to P25, ETSI Terrestrial Trunked Radio (TETRA) provides for a standards-based Inter-System Interface (ISI). These two LMR interfaces can be interworked with MCPTT via the MC IWF envisioned in 3GPP.

The next sections contain a synopsis of the various standards, studies, and white papers the team reviewed and analyzed as part of the research effort.

6.1 The NPSTC Reports

6.1.1 NPSTC_Public_Safety_LMR_LTE_IO_Report_20180108

Title: Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk – January 2018.

Summary: Public safety technical requirements involving mission critical voice communications specifically targeting operational interoperability between LMR and LTE MCPTT.

This report identifies forty-six (46) technical requirements (see Appendix A1 of the NPSTC report) and defines eight (8) use cases that demonstrate a basic interworking between public safety agencies operating on different technology platforms (see Appendix B of the NPSTC report). In addition, it contains an analysis of the requirements labeling each as mandatory or optional, and identifies the existing solutions or gaps (see Appendix A3 of the NPSTC report). These 46 technical requirements are the minimum essential requirements to be considered for the UIWF. NPSTC also reports that parity with P25 capabilities would also be a likely expectation of users (see Section 4.2).

6.1.2 Console_LTE_Report_FINAL_20140930[1]

Title: Public Safety Broadband Console Requirements – September 2014

Summary: This report defines the public safety requirements for the functionality and interfaces for command and control consoles connected to the LTE network. This document is intended primarily for use by FirstNet to fully understand the mission requirements of the public safety community and to

[1] To meet NPSTC's recommendations, a "console" would need access to MC-DATA and MC-VIDEO. Consoles are an essential part to a public safety communications system, whether LMR or LTE.

provide guidance on the design and Implementation of the Nationwide Public Safety Broadband Network (NPSBN).

This report identifies fifty-four (54) public safety requirements for dispatch center control systems relative to emerging broadband functions common to FirstNet. This report looks at new broadband services and features and does not attempt to examine existing public safety requirements for LMR dispatch systems. However, it is widely known that dispatch centers and dispatch functionality are an essential part of any public safety LMR voice network, and this is not expected to change as public safety agencies transition to LTE data networks capable of several media types, including voice and video. Therefore, this report supplies valuable information for the development of the UIWF features that may be hosted by dispatch center control systems.

6.1.3 Related Draft NPSTC Reports In Progress

NPSTC's Public Safety LMR-LTE Interoperability Report contained several recommendations for additional research. Among them was the need for a nationwide standard for creation of PTT IDs by public safety agencies, and the need for nationwide LTE interoperability talk group names. Consequently, during the team's research, NPSTC launched two subcommittees to produce recommendations. Both subcommittees have drafted recommendations that are currently in review, with a goal to be published before the end of the year. Since one member of the team is a committee participant, we know of a relevant emerging recommendation: the need for dispatch consoles and receiving UEs to display meaningful meta data of the talker whose traffic they are monitoring (not just their ID). The draft recommendation is that this meta data include the talker's name, agency affiliation, and badge number.

6.2 3GPP Studies

6.2.1 3GPP TR 23.781 V15.0.0

Title: Study on migration and interconnection for mission critical services (Release 15)

Summary: This document looks at solutions to satisfy the requirements for interconnection and migration between Mission Critical systems. It may identify enhancements to be included in the Technical Specifications for those services. Requirements for this study are taken from the Stage 1 requirements, including 3GPP TS 22.179, 3GPP TS 22.280, 3GPP TS 22.281, and 3GPP TS 22.282.

6.2.2 3GPP TR 23.782 V15.0.0

Title: Mission Critical Communication Interworking between LTE and non-LTE Systems

Summary: This document looks at solutions suitable for interworking between LTE mission critical systems and non-LTE mission critical systems that satisfy the MCPTT requirements in 3GPP TS 22.179 and the MCData requirements in 3GPP TS 22.282 (Short Data Service [SDS] only).

This document identifies key issues and possible solutions to mission critical communication interworking between LTE and non-LTE systems. The document considers 24 key issues and 25 solutions (including highlighting **notable gaps**) including **encryption, key management**, and **vocoder reconciliation** – critical considerations for end-to-end security in a heterogeneous network. Finally, the document records conclusions on the issues. This study provides the background to TS 23.283 development and provides the starting points for development considerations for a UIWF.

6.3 Other Interoperability Requirements

6.3.1 3GPP TS 23.283

Title: Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2 (Release 15)

Summary: The objective of this technical specification is to specify interworking between MC systems and LMR systems that satisfy the MCPTT requirements in 3GPP TS 22.179, MCCoRe requirements in 3GPP TS 22.280, and the MCData requirements (SDS only) in 3GPP TS 22.282.

6.3.2 3GPP TS 22.179/23.179

Title: Mission Critical Push to Talk (MCPTT) over LTE; Stage 1 (22.179) & Stage 2 (23.179)

Summary: This document provides the service requirements for operation of the MCPTT Service. MCPTT makes use of capabilities included in Group Communications System Enablers for LTE (GCSE_LTE) and Proximity Services (ProSe), with additional requirements specific to the MCPTT Service.

6.3.3 3GPP TS 22.280/23.280

Title: Mission Critical Services Common Requirements (MCCoRe); Stage 1 (22.280) & Stage 2 (23.280).

Summary: This document provides the service requirements that are common across two or more mission critical services -- MCPTT, MCData, and MCVideo.

6.3.4 3GPP TS 22.282/23.282

Title: Mission Critical Data services over LTE. Stage 2 (23.282).

Summary: This document provides the service requirements for operation of the MCData service.

6.4 P25

6.4.1 LMR to LMR

For LMR systems, P25 has established a set of standards for digital mobile radio communications designed for use by public safety organizations in North America. P25 defined interface standards include:

- RF Sub-System (RFSS) – Core Infrastructure
- Common Air Interface (CAI) – Radio to Radio protocol
- Inter-Subsystem Interface (ISSI) – RFSS to other RFSS
- Telephone Interconnect Interface (Et) – PSTN to RFSS
- Network Management Interface (En) – Network to RFSS
- Data Host Interface (Ed) – CAD to RFSS
- Data Peripheral Interface (A) – Radio to Data Peripheral
- Fixed Station Interface (FSI) – Fixed Station to RFSS/Console
- Console Sub-System Interface (CSSI) – Console to RFSS

While the Association of Public-Safety Communications Officials (APCO) initiated Project 25, APCO authorized the Telecommunications Industry Association (TIA) to create the standards for the above interfaces.

With the advent of Mission Critical (MC) services within the LTE standards body, 3GPP, TIA and the Alliance for Telecommunications Industry Solutions (ATIS) have created a LMR/LTE joint project committee (JPC) to define the LMR side of the MCPTT LMR/LTE interworking. The LMR/LTE JPC is taking 3GPP's Release 15 IWF definitions and drafting an architecture document to outline P25 interworking with MCPTT. The JPC is focusing first on P25 trunking, but also plans to address P25 and Analog FM conventional. The JPC has a target goal of publishing their architecture document in June 2019, but manufacturers will require a follow-on protocol document to actually implement P25/MCPTT interworking. This cannot be completed until 3GPP Release 16 reaches Stage 3 (protocol definitions), which is not likely to occur until late 2019. It is the general expectation of industry participants in the JPC that the P25 ISSI will be used for P25 trunking system integration, and the P25 CSSI will be used for P25 console system integration. Conventional integration has not been discussed within the JPC much, but the assumption of the team is that the P25 Digital Fixed Station Interface (DFSI) will be used for conventional system integration.

The P25 has defined an Inter RF Subsystem Interface (ISSI) as a non-proprietary communications interface between P25 systems. TETRA has defined a similar standard interface called Inter System Interface (ISI). The ISSI standard is being evaluated to provide an initial UIWF feature set.

Although these standards provide a means for interoperability between P25 systems, few standards exist for radio technologies that do not comply with the P25 standards. Since there exists a substantial deployment of non-compliant P25 system in North America today, there is a need for an UIWF component that accommodates interoperability with non-P25 systems. The team views this need as a gap in the current MCPTT standards development efforts.

6.5 TETRA

6.5.1 ETSI TR 103 565 V1.1.1 (2017-10)

Title: TETRA and Critical Communications Evolution (TCCE); Terrestrial Trunked Radio (TETRA); Study into interworking between TETRA and 3GPP mission critical services

Summary: 3GPP is standardizing a set of mission critical services as applications working over 3GPP LTE systems. These services include speech PTT systems (MCPTT), data (MCData), and video (MCVideo) systems. Users have a need to interwork between TETRA and 3GPP MC systems for several reasons, which can include:

- Communication between different user groups who receive service from the different types of system;
- Use of both systems by the same set of users to allow selection of optimum radio coverage and services in any situation; and
- Migration from an existing TETRA system to a 3GPP MC system over a period of time, which may be long.

It is envisioned that an interworking function will be standardized as part of this work within ETSI TCCE to allow communication between TETRA and 3GPP MC systems. The present document provides considerations for realizing this interface.

6.5.2 ETSI TR 103 565-2 V1.1.1 (2018-05)

Title: TETRA and Critical Communications Evolution (TCCE); Interworking between TETRA and 3GPP mission critical services; Part 2: Security of interworking between TETRA and Broadband applications

Summary: TETRA users are adopting broadband technologies based on 3GPP LTE for critical communications to add new services and capabilities to their operations. TETRA systems are required to work alongside and together with such broadband critical communications systems to enable the users to benefit from the strengths of both technologies.

Interworking is necessary with both the developing suite of 3GPP Mission Critical applications including MCPTT and MCData applications, and with more general use of broadband networks for enhanced bandwidth and higher speed general data applications. The present document describes the security related aspects of such interworking between technologies. It contains use cases for secure interworking, security related issues, and potential security solutions

6.5.3 TETRA Connectivity to LTE (by TCCA, 2018)

The key issue addressed in this white paper is the interworking between these two worlds and especially the interworking and evolution of PTT services, the group communications being the key service in the LMR/PMR networks. The interworking requirements for connection to TETRA are described in Chapter 4 of the TCCA white paper.

6.5.4 2018_May_SFPG_Security_considerations_for_interconnection

Title: TCCA White Paper Security considerations for interconnection of TETRA and Mission Critical broadband systems

Summary: This paper is intended as information for the critical communications community who at present use TETRA systems, but also need to communicate using secure PTT systems over mission critical broadband and to communicate between TETRA and these broadband systems.

This paper provides an overview of how an MC broadband PTT system can be connected to a TETRA system for interworking without compromising the security of either system. The security aspects relating to authenticity, confidentiality, integrity, and availability are considered, together with issues of having an interface between two different technologies.

Interworking with legacy LMR/PMR systems is a 3GPP standardization item and is specified in 3GPP TS 23.283. This paper considers the security implications of these functions.

7 The State of Public Safety Interoperability

7.1 Public Safety System Types

The public safety radio systems used by first responders can be divided into four categories based on radio technologies and services: 3GPP MCPTT, commercial LTE, digital radio, and analog FM.

7.1.1 3GPP MC Services

3GPP has defined the following Mission Critical (MC) services for use by first responders. They can also be used for commercial applications. The Nationwide Pubic Safety Broadband Network (NPSBN) established by FirstNet is a 3GPP MCPTT based network. When used in multicast enabled networks (such as FirstNet’s Band 14), the MC group sizes are virtually unlimited; but MC services can also be used on non-multicast commercial networks where group sizes are limited.

7.1.1.1 MCPTT

MCPTT (Mission Critical Push-To-Talk) is the new global standard for PTT services over LTE networks. It is part of the 3GPP official releases (starting from Release 13). Unlike the existing over-the-top PTT services, which are heavily affected by the number of users on the same network, MCPTT ensures high- quality communications as it uses the VoLTE (Voice over LTE) network with the Evolved Multimedia Broadcast Multicast Services (eMBMS) and supports priority and preemption.

7.1.1.2 MCData

MCData defines a suite of Mission Critical Data services over LTE networks. It is part of the 3GPP official releases (starting from Release 14).

7.1.1.3 MCVideo

MCVideo defines a suite of Mission Critical Video services over LTE networks. It is part of the 3GPP official releases (starting from Release 14).

7.1.2 Commercial LTE

7.1.2.1 Push-to-talk over Cellular (PoC)

Push-to-talk over Cellular (PoC), defined by Open Mobile Alliance (OMA), is intended to provide rapid communications for business and consumer customers of cellular networks. PoC V2.0 allows audio, video, still image, text, and file shared with a single recipient or between groups of recipients as in a group chat session.

7.1.2.2 Push to Communicate for Public Safety (PCPS)

Based on PoC, OMA developed Push to Communicate for Public Safety (PCPS) to address the requirements of public safety community. PCPS includes PTT requirements, architecture, interfaces, and protocol standards for public safety communications purposes. PCPS incorporates LTE and supports multiple access technologies. It is based on the PoC Service Enabler. In 2015, PCPS was licensed to 3GPP to serve as the foundation of MCPTT standard in 3GPP Release 13.

7.1.2.3 Other Commercial LTE Systems

The currently deployed commercial LTE systems, including Kodiak, WAVE, ESChat, and Covia, are not MCPTT based. They can be considered pre-MCPTT systems. They use either Over-The-Top or carrier integrated solutions. Please refer to section 8 for a more detailed description of these systems.

7.1.3 Digital Radio

7.1.3.1 Project 25

Project 25 (P25) is a suite of standards for digital mobile radio communications designed for use by public safety organizations in North America. There are two phases: phase I uses the IMBE digital vocoder over FDMA channels; and phase 2 uses the AMBE+2 half-rate vocoder over TDMA channels.

7.1.3.2 TETRA

TETRA (Terrestrial Trunked Radio) is a European standard for a trunked radio system similar to P25. It is specifically designed for use by government agencies, public safety first responders (police forces, fire departments, and ambulance), transportation industry, and the military. It uses the ACELP digital vocoder over TDMA channels.

7.1.3.3 DMR

DMR (Digital Mobile Radio) is an open digital mobile radio standard defined by ETSI. It uses the AMBE+2 half-rate vocoder over TDMA channels. It is used in commercial products around the world and has become popular within the amateur radio community due to the relative lower cost and complexity compared to other digital standards such as P25 or TETRA.

7.1.3.4 dPMR

dPMR (Digital Private Mobile Radio) is a Common Air Interface (CAI) for digital mobile communications. It is an open, non-proprietary standard developed by ETSI. It is very similar to NXDN protocol implementation by JVC Kenwood and Icom.

7.1.3.5 TETRAPOL

TETRAPOL is a digital professional mobile radio standard, as defined by the Tetrapol Publicly Available Specification (PAS), in use by professional user groups, such as public safety, military, industry, and transportation organizations throughout the world. It is an open standard.

7.1.3.6 OpenSky

OpenSky is the trade name for a wireless communication system, invented by M/A-COM Inc., which is now a division of Harris RF Communications. OpenSky uses the AMBE digital vocoder over TDMA channels.

7.1.3.7 NEXEDGE

NEXEDGE, based on NXDN technology, is JVC Kenwood’s innovative digital conventional and trunked radio solution, designed to meet the highest demands of today’s communications environment and to provide users with a multitude of NEXEDGE-abilities to transform their operations. NEXEDGE uses the AMBE+2 half-rate vocoder over FDMA channels. There are 25 known deployments of NEXEDGE for public safety agencies in the USA.

7.1.3.8 IDAS

IDAS is Icom's digital land mobile radio system using the NXDN common air interface.

7.1.3.9 MOTOTRBO

MOTOTRBO is Motorola’s digital radio product marketed primarily to business/industrial users. The format is based on, and compatible with, the European 2-slot DMR standard and uses Time Division Multiple Access (TDMA) to effectively accommodate two simultaneous users.

7.1.4 Analog Trunking

7.1.4.1 MPT 1327

MPT 1327 is an industry standard for analog trunked radio communications networks. It was developed in 1988 by the British Department of Trade and Industry (DTI), and is primarily used in the United Kingdom, Europe, South Africa, and Australia.

7.1.4.2 LTR

Logic Trunked Radio (LTR) is an analog radio system developed by EF Johnson in the late 1970s. It is distinguished from some common trunked radio systems in that it does not have a dedicated control channel.

7.1.4.3 PassPort

Motorola's PassPort is an analog trunking solution for secure, efficient, and reliable radio communications. It allows multiple talk groups to share limited spectrum, communicate over a wide area, and take advantage of system security features. It offers wider area coverage, automatic roaming, efficient channel expansion, electronic serial number protection, and other key benefits.

7.1.5 Summary Table

A summary of the various radio technologies and their features are shown below.

Radio Technologies	**PTT Systems**	**Standards/ Manufacturers**	**Features**
MC LTE	MCPTT	3GPP Standard	Group call, private call, emergency call, emergency alert, registration and authorization, affiliation, group management, dynamic regrouping, late entry, location service, encryption service, first-to-answer call, ambient listening, callback, supports multicast networks.
	MCData	3GPP Standard	Short data service (SDS), file distribution (FD).
	MCVideo	3GPP Standard	Group video call, private video call, video push, video pull.
Commercial LTE	Push-to-talk over Cellular (PoC)	Open Mobile Alliance (OMA)	Group call (pre-arranged, chat, ad-hoc), individual call, personal alert, multimedia (audio, video, images, and text), priority and preemption, dynamic regrouping, multicast/broadcast.
	Push to Communicate for Public Safety	OMA	Group call (pre-arranged, chat, ad-hoc), individual call, personal alert, multimedia (audio, video, images, and text), priority and preemption, dynamic regrouping, multicast/broadcast, invited party identity, incoming media barring.
	The currently deployed commercial LTE systems, including Kodiak, WAVE, ESChat, and Covia, are summarized in the Table in Appendix C.		
Digital Radio	P25	US Standard	Group call, private call, broadcast call, announcement call, PSTN Interconnect call, emergency call, emergency alarm, priority and preemption, dynamic regrouping, late entry, location service, encryption service, over the air rekeying, short data service.
	TETRA	European Standard	Group call, individual call, broadcast call, emergency call, priority and preemption, dynamic regrouping, late entry, encryption service, ambience listening, discreet listening, telephone type supplementary services.

Radio Technologies	PTT Systems	Standards/ Manufacturers	Features
Digital Radio, continued	DMR	European Standard	Group call, individual call, broadcast call, all call, late entry, talking party identification, encryption service, data services (including AVL).
	dPMR	European Standard	Group call, individual call, status call, data call, short data call, status polling, short data polling.
	TETRAPOL	European Standard	Individual call, multi-party call, emergency call, PABX/PSTN call, dynamic regrouping, call forwarding, call transfer, priority and preemption, ambient listening, late entry, talking party identification, encryption service, over the air rekeying.
	OpenSky	Harris	Group call, individual call, system call, emergency call, selective call, emergency alert, patch/simulselect, high availability, interest signaling, provisioning, registration.
	NEXEDGE	JVC Kenwood	Group call, individual call, broadcast call, interconnect call, all call, emergency call, data call, location service, encryption service, short data service, registration. There are 25 known deployments of NEXEDGE for public safety agencies in the USA.
	IDAS	Icom	Group call, individual call, emergency call, location service, simple encryption, status message, short data message, talk back, radio stun, kill, and revive.
	MOTOTRBO	Motorola Solutions	It has the following system types: Direct Mode, Single Site Conventional, IP Site Connect, Capacity Plus, Capacity Max, Connect Plus. Features offered depend on system type.
Analog	MPT 1327	European Standard	Group call, individual call, status messages, short data messages.
	Logic Trunked Radio (LTR)	EF Johnson	Selectable systems and groups, receive priority ID codes, RIC repeater interconnect ID codes, system scan, group scan, proceed tone, transmit inhibit, free system ringback, busy queuing, system search, transpond, call indicator, horn alert, time-out timer.
	PassPort	Motorola Solutions	Electronic serial number protection, automatic registration, seamless roaming, radio inhibit, private selective call, automatic vehicle location (AVL).

Table 7.1-1 Radio Technology Features

Table Notes: (1) Group sizes are typically restricted to between 100 and 250 users on commercial LTE PTT solutions, and non-multicast MCPTT solutions. Only multicast LTE networks (e.g., FirstNet Band 14) will allow group sizes comparable to what LMR supports today. Thus, only FirstNet Band 14 with MCPTT is a candidate for replacing LMR functionality.

7.2 Standard Interoperability Solutions

For interconnecting the same type of public safety radio systems, in North America, there is the P25 Inter RF Subsystem Interface (ISSI) created to enable P25 RFSSs built by different manufacturers to be connected into wide area networks so that users on different P25 networks can communicate with each other. ISSI is an open standard. In Europe, there is the TETRA Inter-System Interface (ISI) created to connect different TETRA networks, like ISSI for P25. ISI is also an open standard.

In P25, the Console Subsystem Interface (CSSI) is the standard interface created to connect a P25 console subsystem to an RFSS. The Digital Fixed State Interface (DFSI) is the standard interface created to connect a digital fixed station of a conventional P25 system to a console system.

For LMR/LTE interoperation, on the LTE side, 3GPP has defined the Interworking Function (IWF) interface for connecting an MCPTT system to LMR systems. The requirements of IWF (stage 2) have been defined. However, the protocols to be used to implement IWF (stage 3) have not been defined. On the LMR side, neither TIA nor ETSI has defined an interworking function interface for connecting a P25 or TETRA system to an MCPTT systems. This is a gap that we are trying to fill with the solutions proposed in this project.

7.3 Non-Standard Interoperability Solutions

There are standard interfaces defined for interconnecting same type of radio systems, such as the P25 ISSI or TETRA ISI. However, except the 3GPP IWF, there is no standard interface defined for interconnecting dissimilar radio systems. Some non-standard or near de-facto standard interfaces or products have been created to solve the LMR/LMR or LMR/LTE interoperability issues, including the DHS RIC-M (Radio Internet-Protocol Communication Module) and RoIP (Radio over IP) gateways. In the case of RIC-M, it is used to convert the analog voice and V.24 serial signal output by a Motorola conventional ASTRO base station to the P25 DFSI format so a DFSI capable console can control and communicate with a conventional base station. In the case of RoIP gateways, they are used to convert analog voice to digital voice using a standard form of VoIP protocols based on SIP and RTP, but these protocols become proprietary with the addition of non-standard PTT capabilities (the DHS BSI [Bridging Systems Interface] protocol is an exception but is implemented in very few RoIP gateways). Both RIC-M and RoIP gateways are usually used to solve the interoperability issue for conventional systems. The RoIP gateways can be used also for trunking systems when interfaced to donor radios that are part of a trunking system.

The following table lists the non-standard interoperability products that are offered by various vendors.

Product Name	Manufacturer	Brief Description	Note
MOTOBRIDGE	Motorola Solutions	MOTOBRIDGE is a scalable, cost-effective IP-based solution for quickly establishing communications between disparate systems in support of emergency response and day- to-day operations. MOTOBRIDGE provides connectivity to any disparate radio system, all with the same gateway unit. Systems that support the P25 standard, as well as other technologies, can be linked together for interoperable communications.	None
R-NIC	Mutualink	Mutualink's Radio Network Interface Controller (R-NIC) Series of Secure Controllers support the integration of fixed station or mobile radio transceivers irrespective of their operating frequencies or protocols. Variants of the R-NIC series provide support for standard fixed station interfaces including DC or EIA Tone Remote Control and E&M signaling in either 2 or 4-wire configurations.	None
IntelliLink Gateway	Catalyst	The IntelliLink Gateway can link multiple talk groups or channels across frequency bands and over the air protocols including DMR, P25, LTR, SmartNet, EDACS, analog conventional, and others.	Limited to narrowband radios only (analog conventional and digital trunked). No support for LTE radios, including MCPTT.
ACU-1000	JPS Interoperability Solutions (formerly Raytheon)	The ACU-1000 interoperability gateway enables communications by cross-connecting each device's base-band audio. Includes VoIP/RoIP technology to provide a means for regional, state, multi-state, and national interoperability.	Scalable and field configurable. Controlled using the ACU Controller software provided. Three different methods of operation for system redundancy

Product Name	Manufacturer	Brief Description	Note
Universal Communications Platform (UCP) Gateway	Lockheed Martin	The UCP gateway is an IP based gateway product designed to provide interoperability between radio systems (Tactical and LMR both secured and non- secure) and other communication devices including cellular telephones, landline telephones, commercial VoIP phones, etc.	None
T. BRIDGE	TASSTA	T. BRIDGE provides a middleware solution to help businesses to overcome the challenges of integration by interconnecting a PMR System with TASSTA's features.	None
Stratus	Codan	Codan Stratus is the first deployable P25/LTE hybrid solution that leverages the strengths of both technologies to provide secure mobile voice networks.	Support end to end encryption
IPICS	Cisco	Cisco IP Interoperability and Collaboration System (IPICS) is a platform that enables users to bring their own devices into the world of PTT communications in Cisco Unified Communications (UC) environments. Cisco IPICS bridges the worlds of land mobile radio and UC, providing the ability for communication between desperate devices such as traditional and digital radio, Android, and Apple iOS devices.	None

Table 7.3-1 Non-standard interoperability products

Several LMR manufacturers are approaching the interoperability solution from the handset end, by producing hybrid (combined) LMR and LTE handsets, or by integrating separate LMR and LTE handsets via bluetooth connections. These handset-based solutions are beyond the scope of this analysis.

8 Over-The-Top LTE Interoperability Solution

8.1 Existing Over-The-Top LTE Systems

8.1.1 Kodiak Networks

Kodiak is a carrier-integrated PTT-over-cellular solution. Kodiak Networks is a provider of broadband PTT services for commercial customers.

Kodiak partners with mobile network operators globally to offer its cloud-based PTT solution and management platform, which operates over 4G LTE, Wi-Fi, and 3G networks. Kodiak was acquired by Motorola in 2017 and has since merged Motorola’s WAVE 7000 solution with Kodiak. Kodiak claims to have a migration path to MC-PTT and has been named as the MC-PTT provider for UK’s Emergency Services Network (ESN). At the 2018 APCO show, Kodiak announced a “Critical Connect” service that acts as a cloud-based ISSI hub for interconnecting ASTRO 25 systems to each other, and to LTE. Kodiak only plans to support connection to Motorola ASTRO 25 LMR systems which puts into question whether their ISSI implementation is truly P25 compliant.

Kodiak accommodates LMR interoperability via the P25 ISSI, CSSI and proprietary RoIP gateways (for non-P25 systems). Additional functionality (such as location) is available via proprietary APIs. Kodiak supports both Android and iOS and offers a dedicated purpose PC client dispatcher app. Although Kodiak is used by multiple cellular carriers in the USA, commercial issues prevent cross carrier operation. Thus, interoperability via a single common solution has not been achieved in this case.

8.1.2 WAVE

Motorola’s WAVE Broadband Push-To-Talk enables those on radios, smartphones, tablets, and laptops to communicate with one another in a seamless fashion. WAVE was available in three tiers; 3000, 5000, and 7000. WAVE 3000 and 5000 are primarily extensions of Motorola’s ASTRO 25 LMR networks (much like Harris’s BeOn). WAVE 7000 was deployed by some cellular networks as a network integrated POC service (a competitor to Kodiak until Motorola bought Kodiak), but has recently been retracted by Motorola in favor of new developments by Kodiak.

8.1.3 Enterprise Secure Chat (ESChat)

ESChat is a full featured PTT over cellular application that includes private, ad hoc and group PTT calling, text and image messaging, and real-time location reporting. It offers pre-MCPTT Over-The-Top PTT with LMR interoperability via the P25 ISSI, the DMR AIS, and proprietary RoIP gateways. It was among the first apps to be FirstNet Certified. It is also the PoC engine behind several situational awareness apps.
ESChat has also private labeled their app for several other vendors. ESChat offers both Android and iOS apps, and a primitive, dedicated purpose PC dispatcher client.

8.1.4 Covia Labs Push-to-Talk

Covia Labs Push-to-Talk is a rich-media communications software product that supplements existing public safety radio communications systems using cost effective commercial mobile phones and carrier networks.

8.1.5 Summary Table

The proliferation of Over-The-Top (OTT) or Pre-MCPTT systems has added complexity to the PTT interoperability picture. The table in Appendix C summarizes the OTT or Pre-MCPTT systems we have researched.

8.2 Proposal for Over-The-Top LTE Interoperability Solution

An examination of the Google Play and Apple stores shows several dozen OTT systems. Those shown in the table Appendix C appear to be the prevalent systems that may be viable for LMR interoperability. As far as is known, except for privately labeled products that may have a common source, no two OTT vendors are able to interoperate. Even if public safety agencies purchase the same OTT solution, separate subscriptions make it problematic to coordinate common talk groups needed for interoperability. However, OTT solutions do traverse carriers, and can be a solution for cross-carrier operation.

After analyzing the LMR interoperability support for OTT or Pre-MCPTT systems, our key finding is it is quite common for an OTT or Pre-MCPTT system to support P25 ISSI for LMR interoperation. Therefore, our UIWF solution should support the interoperation with OTT or Pre-MCPTT systems via the standard based P25 ISSI.

9 Interoperability Security Concerns

The NPSTC report entitled, “Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk (NPSTC Report),” contains important operational requirements relative to interoperability security concerns. However, the nature of the security issues is never discussed. The document stops short of categorizing or prioritizing. Largely based on the technological limitations and the LMR heritage, the document places a heavy focus on encryption, but leaves little guidance for recommendations on authentication and authorization -- perhaps the most critical area to define a scalable multi-network, nationwide interoperability solution.

Within the NPSTC document, there is no security risk analysis or discussion and no reference to existing standards or security frameworks. There is no discussion of “lessons learned” for existing LMR or LTE security solutions. Gaps are identified and requirements to close those gaps are listed, but many of the difficult issues are not addressed. The report defers to FirstNet to solve the interoperability security problem. In section 5 “Conclusions and Recommendations,” the report talks about the importance of voice encryption, but states there are many technical and policy issues that need addressing especially when LMR-LTE talkgroups are involved and there is a need for “end-to-end” encryption. The recommendation is deferred to FirstNet and suggest they publish guidance on options for managing encryption and instruct on the need for LTE devices to support P25 vocoder to enable end-to-end encryption.

The NPSTC report also points out that there is a technical, standards, and policy gap that must be addressed relative to managing encryption in a nationwide network. It recommends that this issue be studied by an LMR LTE Integration and Interoperability Working Group.

The TCCA White paper entitled “Security considerations for interconnection of TETRA and Mission Critical broadband systems (TCCA White paper) was reviewed with the expectation of gaining more insight into interworking security issues, but its lack of depth provided little additional information.

Both the NPSTC report and the TCCA White paper emphasized encryption (and transcoding) as the principle means for security interconnecting LMR and MCPTT system.

9.1 Standards Base Risks

The NPSTC report requires standards-based authentication of a user and device. It contains three requirements on authentication. The requirements are very high level and ask for a "mechanism" for authentication to be in place. The NPSTC report requires local control policies determine authorized users and devices, and authorization to connect to system resources. The requirements governing how to authorize a device or user are left undefined. More research and development is required in this area to develop a truly scalable solution capable of nationwide, cross-system interoperability.

3GPP standards require identity-based encryption for MCPTT key establishment. This is incompatible with symmetric key based LMR key management like that defined for P25. This makes true end-to-end encryption through the IWF difficult.

The NPSTC report emphasizes the need for supporting encryption through the IWF. The report identifies two types of encryption solutions:

1. LMR/LTE Common Encryption: Use of the same encryption and voice coding components on both the LMR and LTE devices; and
2. LMR/LTE Dissimilar Encryption: Use of one type of digital encryption and vocoder on the LMR network and a different type of encryption and vocoder on the LTE network.

Both solutions come with security risks. For common encryption, LTE applications would need to support LMR symmetric key management and encryption processes. LTE devices may not be physically equipped to provide adequate protection for the symmetric keys. For dissimilar encryption, the IWF would be required to perform decryption acting as a security gateway between the MCPTT system and the LMR systems. This would require careful implementation and physical security measures to prevent exposing the plaintext to possible compromise. The IWF would also need to store and protect the encryption keys for both systems.

The 3GPP TR 23.782 V15.0.0 (2017-06) Technical Report 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on mission critical communication interworking between LTE and non-LTE systems (Release 15) identifies several key Issues with solutions including Key Agreement and Key Management.

Protection of encryption keys is essential for maintaining voice and data confidentiality. Until issues with end-to-end encryption and key management through the UIWF are resolved, there is risk of implementation vulnerabilities.

The 3GPP TS 23.283 V1.0.0 (2017-12) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2 (Release 15) contains the following interworking requirements for key management:

- Mechanism to securely (i.e., authenticity, integrity, confidentiality) share an LMR E2EE traffic key for a private call session between a party in an MCPTT system and a party in the LMR system;

- Mechanism to securely convey to group members, the LMR E2EE key or set of LMR E2EE keys associated with an MC service group or set of MC service groups, to be used for encryption of interworking group calls spanning the multiple systems;
- Mechanism to securely share with temporary group members in MC systems, the LMR E2EE key(s) associated with a temporary MC service group to be used in interworking group calls spanning the multiple systems;
- Key management solutions shall not preclude the ability of an IWF to allow one or more individual Mission Critical Organizations from having sole control over and sole access to LMR E2EE traffic keys used for the entity's media traffic and users' key encryption keys (UKEKs or KEKs);
- Key management solutions shall support the ability of the IWF to decrypt/re-encrypt the media traffic for one or more groups; and
- For deployments where Mission Critical Organizations wish to use LMR E2EE mechanisms when interworking with LMR users:
    - a mechanism to securely provision an MC service client with the user's UKEK or KEK; and
    - a mechanism to convey LMR OTAR or OTAK message contents.

These requirements are not sufficient to result in a secure solution implementation. More work is needed to define the aspects of the required “mechanisms.” If details of the actual solution are left open to interpretation, the resulting implementation may not be secure.

9.2 MC LTE to P25 Implications

There are several technical and business challenges with LMR/LTE common voice coding. First, the narrowband vocoder will have poorer audio quality than the broadband voice coding. This means that for optimum quality, the LTE device would need to support two vocoding methods: one for talkgroups with interoperability, and one for MCPTT only communication talkgroups. This also introduces undesirable coupling in the end device. TETRA and P25 / DMR use different vocoders, meaning the end LTE device might need to support a portfolio of different vocoders. Presently, the narrowband vocoder used in P25 is licensed and its licensing cost would likely limit the distribution model of MCPTT applications and increase their cost.

These vocoding challenges make the need for dissimilar vocoding between LMR and LTE the only realistic solution that can be commercialized. Since the audio coding of the MCPTT system and the narrowband LMR system are different, the audio must be transcoded, and as such the audio payload must also be trans-crypted.

The NPSTC report requires the IWF to support end-to-end encryption including flexible key management with little or no human interaction.

A more comprehensive document about interworking security considerations is ETSI TR 103 565-2 V1.1.1 (2018-05) “TETRA and Critical Communications Evolution (TCCE); Interworking between TETRA and 3GPP mission critical services; Part 2: Security of interworking between TETRA and Broadband applications.” This document contains security considerations for interworking between TETRA and 3GPP standardized mission critical broadband systems. It is also applicable to the 3GPP mission critical systems interworking with LMR systems.

This document teaches a more comprehensive end-to-end security solution through the IWF applied to communications between LMR devices and MCPTT clients. It requires that MCPTT system and clients support LMR protocols, vocoder, and mechanisms. This appears to be the best near-term approach to an IWF E2EE solution.

ETSI TR 103 565-2 V1.1.1 (2018-05) also presents an encryption translation solution that requires the IWF to have an end-point identity and be provisioned with public and private master keys to enable identity based key management to take place on the 3GPP side. The IWF would also be provisioned with the LMR key sets that support all the key management processes including OTAK. Both solutions are viable for supporting voice and data confidentiality across the IWF, but come with risks presented in the previous section.

It should be noted that the 3GPP standards consider MC media encryption independent of LMR E2EE techniques and MC media encryption can be applied in addition to LMR E2EE.

9.3 Multilevel Security (MLS)

There is clearly a need for the IWF to support Multilevel Security (MLS). MLS must first be defined through policy and doctrine before it can be effectively implemented. These policies do not yet exist.

9.4 Security Tenets and Mitigations

The ESTI standard ETSI TR 103 565-2 V1.1.1 (2018-05) contains security tenets for the IWF that serve as over-arching requirements for the security solutions aimed at mitigating the threats to LMR/LTE interoperability.

Each system will need to manage its own security aspects, such as authorization, authentication of users or devices, and protection of signaling and traffic information. End-to-end encrypted material should not be blocked by either system.

The two main security tenets of ETSI TR 103 565-2 V1.1.1 (2018-05) are:

- *"The solution should not affect security for any users of either system that are not involved in interworking with the other system."*
- *"The solution should maintain as high a level of security as possible for users that are involved in interworking communications with users in the other system."*

In addition, a security policy, auditing, and reporting will need to be defined in support of any IWF security solution – *"… which details which types of communication are permissible for interworking, and whether specific procedural measures are needed for these communications. Users need to be aware whether a call includes other users who are connected via an interworking interface."*

Monitoring and filtering requirements to record events will need to be defined and applied. This will reduce the IWF vulnerability to a variety of attacks and will create auditable records. A policy is needed to specify how often these records are examined and to define a response to a security event.

ETSI TR 103 565-2 V1.1.1 (2018-05) identifies threats to the interworking function, as shown in the Table 9.4-1 below, and presents solutions to mitigate these threats as described in the following paragraphs.

Threat Type	Threat Manifestation
Masquerade/impersonation	System impersonation IWF impersonation Client impersonation User impersonation
Eavesdropping	Eavesdropping in other system Eavesdropping on external links between systems Eavesdropping IWF links within a system Eavesdropping within IWF
Ambience listening invoked across IWF	
Traffic Analysis	Traffic analysis in other system Traffic analysis in intersystem link Traffic analysis within IWF
Denial of Service	Excessive traffic in other system Improper use of high priority calls DoS of IWF DoS of key management
Manipulation/Insertion	Traffic modification Signaling modification Signaling insertion Mapping modification Configuration modification False response
Extraction	Keys extraction from IWF Keys extraction from TETRA terminals Keys extraction from high assurance MC terminals Key extraction from COTS MC terminals
Replay	Traffic replay Signaling replay
Repudiation	Repudiation

Table 9.4-1 Threats to the Interworking Function

The solutions presented in ETSI TR 103 565-2 V1.1.1 (2018-05) to mitigate these risks are discussed below.

Service Authorization can be handled by each system, authorizing users to join groups connected to groups in the other system. The IWF should also manage an address book for both systems. This can provide additional authorization for interworking.

Each system should carry out its own authentication locally. A trust structure will allow each system to verify and trust that a connected user or device in the other system has been correctly authenticated.

Both the systems connected to the IWF and the IWF will need to verify the authenticity of the connection independently.

Each system will need to protect signaling from eavesdropping, and to protect integrity of signaling. LMR has several means of signal protection such as air interface encryption, while MCPTT uses SIP bodies (XMLenc) and HTTPS for signaling plane protection, and SRTCP for floor control.

The IWF will need appropriate physical and procedural protection to prevent it from becoming a point of attack.

MCPTT uses SRTP to protect speech between clients:

- Secret group key for group communications.
- Session keys for private calls.
- Identity based encryption for key management.
- The AES GCM algorithm implementation is used for traffic encryption.
- There is additional air interface encryption provided by the LTE network between the device and the eNodeB.

LMR uses air interface encryption as specified in ETSI EN 300 392-7:

- Keys provided as part of the air interface authentication and OTAR functions.
- Additional end to end encryption can be overlaid, using a variety of algorithms.
- Keys are provided in advance of communications by LMR key management processes and not negotiated at the start of calls.

Specification and implementation of the UIWF will require much more thorough work on security at scale. Implementation is critical for any secure design. How a security function is implemented is just as important as what is implemented. To that end, the following list of general principles should be applied when implementing the UIWF:

- Use the NPSTC Use Cases and other resources to clarify the mission of the UIWF in functional terms.
- Categorize and analyze the information flowing through the UIWF.
- Perform a risk analysis.
- Review LMR security solutions for lessons learned.
- Determine the mitigating security functions needed.
- Synthesize the solution architecture.
- Determine the control points – technical, business, political, procedural, etc.
- List the policies that will govern operation.
- Identify the standards that will govern the security functions.

9.5 Security Requirements and Constraints

Additional requirements that should be considered relative to the IWF are found in 3GPP TS 33.180: "Security of the mission critical service" and are shown below:

- [33.180 MCX-A.5-004] A radio user should be told as soon as possible that they are, or have been, subject to Ambient Listening and the reason why the functionality was activated. The fact they have been informed, by whom and when, should be recorded in a suitable log.

- [33.180 MCX-A.8-001] An authorized MCX User shall be able to obtain the information necessary to derive the group security context for the MCX Group while an MCX Group communication is on-going. As a result, the MC User shall be able to listen to the group communication within 350ms. This requirement applies for both on-network and off network MCX operations.
- [33.180 MCX-A.12-001] User authentication and authorization interoperability between different networks and different manufacturers' clients and servers shall satisfy the requirements for mission critical roaming and migration.
- [33.180 MCX-A.13-006] End to end security of an MCX Service Group communication (including in Partner MCX Service Systems) shall be based on parameters obtained from the MCX Service system where the MCX Service Group is defined (R-6.17.2-007 [47]).
- [33.180 MCX-A.13-007] All Mission Critical Users shall be authenticated with their home identity management service prior to authentication or authorization with a partner domain.

10 Interworking Capabilities

10.1 Analog FM Conventional System Interworking Capabilities

In an analog FM conventional system, the voice sent over the air is analog, modulated via analog FM method. Besides voice, some type of in-band signaling (i.e., in the voice band) can be used to carry PTT ID and simple radio control messages. Examples of in-band signaling formats are MDC-1200, 5/6 tones, GE-Star, and FleetSync. Among them, MDC-1200 is the dominative format used in North America.

Currently, there is no interworking standard for interconnecting the analog FM conventional systems. Based on the system manufacturer and in-band signaling format used, the information available at a base station could be analog voice only, analog voice plus raw in-band signal, and analog voice plus decoded in-band signal. The most basic interworking capability that an analog FM conventional system can provide is the analog voice. Some systems can provide analog voice plus raw in-band signal capabilities. Others can provide analog voice plus decoded in-band signal capabilities. To support interoperation with the analog FM conventional systems, our proposed solution includes a protocol converter or gateway to convert the analog signal of FM base stations to an IP-based open standard protocol. This analog FM gateway takes the 4-wire E&M or 2-wire Tone Remote Control signal from an analog base station on one side and converts it to a standard-based IP protocol on the other side for interfacing to UIWF. With the help of this gateway, our proposed solution is capable of supporting the interworking with the analog FM conventional systems.

10.2 P25 Interworking Capabilities

P25 systems can be divided into P25 conventional systems and P25 trunked systems. For P25 conventional systems, the best option to interconnect those systems is via their base stations using the standard P25 DFSI protocol. For P25 trunked systems, the best option to interconnect those systems is using the standard P25 ISSI protocol. Table 10.2 -1 below lists the interworking capabilities of both P25 DFSI and P25 ISSI. An entry that is marked “No” in the table means this capability is not supported.

Capabilities		P25 DFSI	P25 ISSI
Mobility Management	Registration	No	Yes
	De-registration	No	Yes
	Affiliation	No	Yes
	De-affiliation	No	Yes
Voice Services	Group call: non-emergency	Yes	Yes
	Group call: emergency	Yes	Yes
	Announcement group call	No	Yes
	System group call	No	Yes
	Individual call with availability check: non-emergency	No	Yes
	Individual call without availability check: non-emergency	Yes	Yes
	Individual call with availability check: emergency	No	Yes
	Individual call without availability check: emergency	Yes	Yes
	PTT floor control	No	Yes
Supplementary Data Services	Emergency alarm	Yes	Yes
	Emergency alarm cancel	Yes	Yes
	Group emergency cancel	Yes	Yes
	Call alert (i.e., page)	Yes	Yes
	Short message (via 16-bit message code)	Yes	Yes
	Status query (response with 28-bit status fields)	Yes	Yes
	Status update (via 2 8-bit status fields)	Yes	Yes
	Radio unit monitor	Yes	Yes
	Radio check	Yes	Yes
	Radio detach (i.e., de-register)	Yes	Yes
	Radio inhibit	Yes	Yes
	Radio un-inhibit	Yes	Yes
Call Control	Priority call	Yes	Yes
	Dynamic regrouping: group regrouping	No	No (work in progress)
	Dynamic regrouping: individual regrouping	No	No (work in progress)

Capabilities		P25 DFSI	P25 ISSI
Call Control, continued	Audio takeover and console priority	Yes	Yes
	ID display: individual ID	Yes	Yes
	ID display: group ID	Yes	Yes
Security Services	Encryption	Yes	Yes
	Authentication	No	Yes
	Key management	No	Yes
Data Services	Location service	Yes (limited)	Yes (limited)
	Over-the-air-rekeying (OTAR)	Yes	Yes

Table 10.2-1 Interworking capabilities of P25 DFSI and P25 ISSI

The P25 location service is different from the 3GPP MCPTT location service. In P25, an SU (Subscriber Unit) sends its location data to a Location Service Host System for processing and achieving. During a group call, the P25 system does not provide the current talker's location to group members and the interested console systems. The 3GPP MCPTT has a better location service. In MCPTT, the MCPTT server can provide the current talker's location information to all affiliated members including console UE.

Currently in P25, dynamic regrouping (group or individual regrouping) is only supported on P25 CAI. It is not supported on the DFSI or ISSI interface. TIA is currently working on creating the ISSI regrouping protocol. In MCPTT, dynamic regrouping is a fully supported feature, and is supported on the MCPTT UE interface.

P25 supports Supplementary Data Services for sending emergency alarm, call alert, and short message, and for checking and controlling radio units. MCPTT does not have the equivalent radio control services.

10.3 MCPTT Interworking Capabilities

3GPP has defined the requirements for an IWF interface on the LTE side between the LMR and MCPTT systems in Release 15. Figure 10.3 – 1 below shows the functional model of this interface.

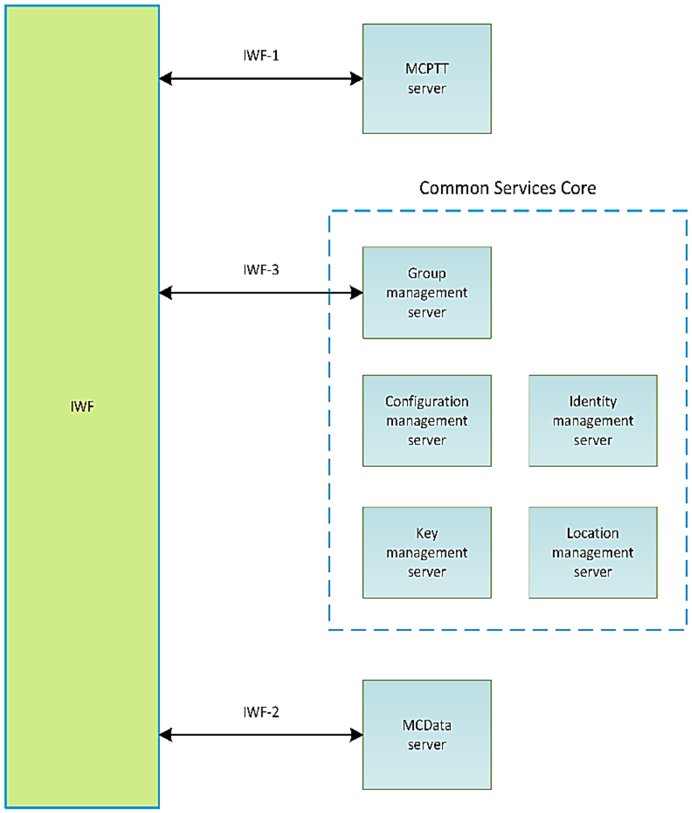

Figure 10-1 3GPP IWF interface of Release 15

There are three reference points defined in the diagram. The IWF-1 reference point, between the IWF and the MCPTT server, provides a peer to peer interconnection between the LMR and MCPTT systems. The IWF-2 reference point, between the IWF and the MCData server, provides a SDS interconnection between the LMR and MCData systems. The IWF-3 reference point, between the IWF and the Group Management Server, provides a group management interconnection between the LMR and MCPTT systems.

Even though 3GPP has defined the IWF requirements, it has not defined the IWF protocol. Therefore, IWF cannot be implemented due to the unavailability of its protocol. An alternative option is to replace the IWF interface with the wireline MCPTT UE interface defined in Release 13, which was released in 2016 and available for implementation now. The main difference between the 3GPP IWF and the MCPTT UE for use in UIWF is the 3GPP IWF is a peer to peer (i.e., server to server) interface, while the MCPTT UE is a client to server interface. With the 3GPP IWF, interworking groups can be homed in either the LMR system or the MCPTT system. With the MCPTT UE, all interworking groups must be homed in the MCPTT system. That is, the MCPTT server is the controlling server for all interworking groups when the MCPTT UE model is used. The following diagram shows the wireline MCPTT UE functional model defined in Release 13.

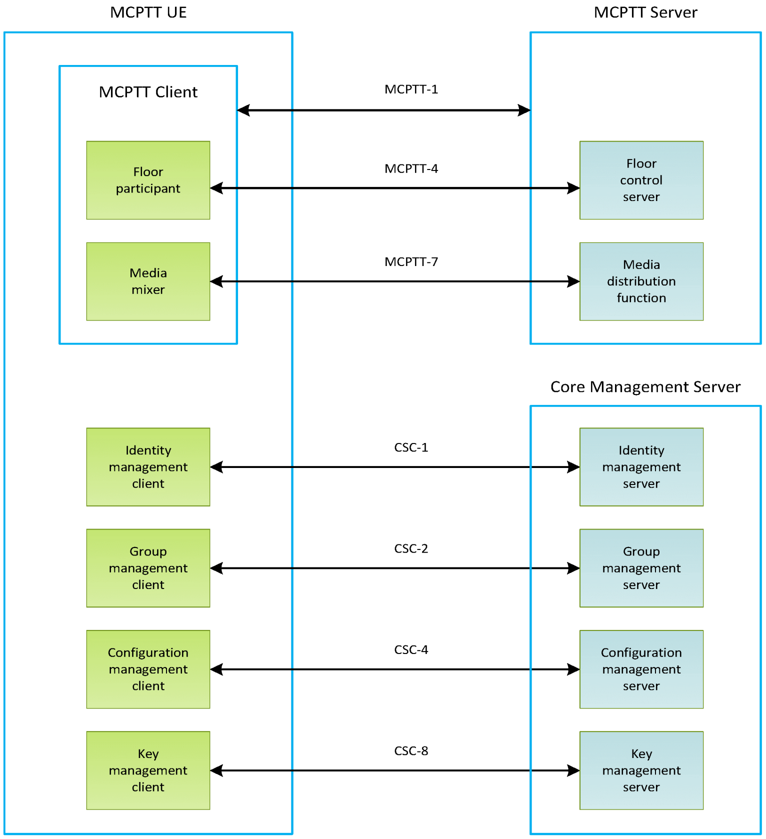

Figure 10-2 MCPTT UE interface of Release 13

The following table (Table 10.3 -1) provides a quick summary of those reference interfaces shown in Figure 10-2 MCPTT UE interface of Release 13 above.

Interface	Description	Main Function
MCPTT-1	The MCPTT-1 interface is between the MCPTT UE and the MCPTT Server. It is used for MCPTT application signalling for establishing call sessions in support of MCPTT.	Call session establishment
MCPTT-4	The MCPTT-4 interface is between the floor participant of UE and the floor control server in the MCPTT Server. It provides floor control signaling between the floor control server in the MCPTT server and the floor participant of UE over a unicast bearer.	PTT floor control

Interface	Description	Main Function
MCPTT-7	The MCPTT-7 interface is between the media mixer of UE and the media distribution function in the MCPTT Server. It is used to exchange unicast media between the media distribution function of the MCPTT server and the media mixer of the MCPTT client.	Media distribution
CSC-1	The CSC-1 interface is between the identity management client of UE and the Identity Management Server. It provides for the authentication of the common services core to the MCPTT client and subsequent authentication of the user to the common services core on behalf of applications within the application plane.	Identity management service
CSC-2	The CSC-2 interface is between the group management client of UE and the Group Management Server. It supports the configuration of group related data at the group management client of UE.	Group management service
CSC-4	The CSC-4 interface is between the configuration management client of UE and the Configuration Management Server. It provides the configuration information required for MCPTT services to support the configuration of UE.	Configuration management service
CSC-8	The CSC-8 interface is between the key management client of UE and the Key Management Server. It provides a means for the key management server to deliver security related information (e.g., encryption keys) to the key management client of UE.	Key management service

Table 10.3-1 Description of MCPTT UE reference interfaces

We use the MCPTT UE interface defined in Release 13 in our UIWF solution on the LTE side for interfacing to the MCPTT system. Besides the differences on client to server model versus server to server model and group home choice (in MCPTT only or in either LMR or MCPTT), the supported capabilities for LMR/LTE interoperation by the MCPTT UE and 3GPP IWF interfaces are very similar. Table 10.3-2 below lists and compares those supported capabilities. The MCPTT UE interface defined in Release 13 does not support three capabilities in Table 10.3-2 *-2MCPTT interworking capabilities* group configuration for interworking, location service (defined in Release 14), and SDS (defined in Release 14).

Since the 3GPP IWF protocol is not available for implementation, we propose using the MCPTT UE interfaces defined in Release 13 in our UIWF solution on the LTE side for interfacing to the MCPTT systems.

Capabilities		MCPTT UE	3GPP IWF
Group affiliation		Yes	Yes
Group regrouping		Yes	Yes
Group configuration for interworking		No	Yes
Group call		Yes	Yes
Group broadcast		Yes	Yes
Chat group call		Yes	Yes
Private call		Yes	Yes
Late entry		Yes	Yes
Short Data Service		No (not in Release 13)	Yes (via MCData)
Voice encryption		Yes	Yes
Simultaneous calls (i.e., scan)		Yes	Yes
Location service		No (not in Release 13)	Yes
Full duplex voice (private call only)		Yes	Yes
Talker ID (without alias)		Yes	Yes
Floor control	Floor request	Yes	Yes
	Floor granted	Yes	Yes
	Floor rejected	Yes	Yes
	Floor request cancel	Yes	Yes
	Floor idle	Yes	Yes
	Floor release	Yes	Yes
	Floor taken	Yes	Yes
	Floor revoked	Yes	Yes
	Floor acknowledgement	Yes	Yes
	Queue position info	Yes	Yes
	Queue position request	Yes	Yes
	Unicast media stop request	Yes	Yes
	Unicast media resume request	Yes	Yes

Capabilities		MCPTT UE	3GPP IWF
Prioritization and pre-emption	Emergency group call	Yes	Yes
	Imminent peril group call	Yes	Yes
	Emergency alert	Yes	Yes
	Losing audio	Yes	Yes

Table 10.3-2 *-2MCPTT interworking capabilities*

10.4 Non-MCPTT Interworking Capabilities

In this document, we define a non-MCPTT system being any LTE system that does not conform to the 3GPP MCPTT standard, including any OTT or Pre-MCPTT systems such as Kodiak, WAVE, ESChat, and BeON. There is no standard way defined to interconnect a non-MCPTT system and an MCPTT system. As we found out in this research project, it is quite common for an OTT or Pre-MCPTT system to contain a P25 ISSI gateway in its system for LMR/LTE interoperation. Since our proposed UIWF solution supports ISSI, we can interconnect a non-MCPTT system that offers an ISSI interface. What capabilities are supported on the ISSI interface depend on the type of non-MCPTT system deployed. Different types of non-MCPTT systems may offer some different capabilities over their ISSI interface. Using UIWF, the interworking capabilities of a non-MCPTT system can be accessed via its ISSI interface. Our proposed solution will only support a non-MCPTT system that has an internal ISSI gateway for LMR/LTE interoperation.

10.5 Minimum set of Interworking Capabilities

In this section, we investigate and recommend the minimum set of capabilities needed to support LMR/LTE interoperation. The source of capabilities that we use for analysis comes from the P25 DFSI and ISSI, which represent the LMR side, and the MCPTT UE and 3GPP IWF, which represent the LTE side. The MCPTT UE interface considered here is a wireline UE interface based on the 3GPP Release 13, where MCData and MCVideo services are not supported. We consider the MCPTT UE interface in our UIWF solution because the protocol of this interface has been released and is available for implementation, while the protocol of 3GPP IWF interface is still undefined. We have shown the capabilities of the P25 DFSI and ISSI and the capabilities of the MCPTT UE and 3GPP IWF in the previous sections. The following (Table 10.5-1) puts together the capabilities of those interfaces in one table for easy comparison.

Capabilities	P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Registration	No	Yes	Yes	Yes
Group affiliation	No	Yes	Yes	Yes
Group configuration for interworking	No	No	No	Yes
Group call	Yes	Yes	Yes	Yes
Group broadcast	No	Yes	Yes	Yes
Chat group call	No	No	Yes	Yes
Private call	Yes (limited to the same frequency channel)	Yes	Yes	Yes

Capabilities		P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Dynamic regrouping		No	No (work in progress)	Yes	Yes
Late entry		No	Yes	Yes	Yes
Short Data Service		Limited (via Packet Data Service)	Limited (via Packet Data Service)	No (not in Release 13)	Yes (via MCData)
Voice encryption		Yes	Yes	Yes	Yes
Key management		Yes	Yes	Yes	Yes
Simultaneous calls (ie, scan)		No	Yes	Yes	Yes
Location service		Limited	Limited	No (not in Release 13)	Yes
Full duplex voice (private call only)		No	No (protocol supports but not commonly implemented)	Yes	Yes
Talker ID (without alias)		Yes	Yes	Yes	Yes
Console talkspurt identifier		No	Yes	No	No
Floor control	Floor request	No	Yes	Yes	Yes
	Floor granted	No	Yes	Yes	Yes
	Floor rejected	No	Yes	Yes	Yes
	Floor request cancel	No	No	Yes	Yes
	Floor idle	No	No	Yes	Yes
	Floor release	No	Yes	Yes	Yes
	Floor taken	No	No	Yes	Yes
	Floor revoked	No	No	Yes	Yes
	Floor acknowledgement	No	No	Yes	Yes
	Queue position info	No	No	Yes	Yes
	Queue position request	No	No	Yes	Yes
	Unicast media stop request	No	No	Yes	Yes

Capabilities		P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Floor control, continued	Unicast media resume request	No	No	Yes	Yes
	Transmit wait	No	Yes	No	No
	Transmit mute	No	Yes	No	No
	Transmit unmute	No	Yes	No	No
Prioritization and pre-emption	Emergency call	Yes	Yes	Yes	Yes
	Imminent peril call	No	No	Yes	Yes
	Emergency alert	Yes	Yes	Yes	Yes
	Losing audio	No	Yes	Yes	Yes
	Priority call and pre-emption	No	Yes	Yes	Yes
P25 Supplementary Data Service	Emergency alarm	Yes	Yes	Yes	Yes
	Call alert (i.e., page)	Yes	Yes	No	No
	Short message (via 16-bit message code)	Yes	Yes	No	No
	Status query (response with 2 8-bit status fields)	Yes	Yes	No	No
	Status update (via 2 8-bit status fields)	Yes	Yes	No	No
	Radio unit monitor	Yes	Yes	No	No
	Radio check	Yes	Yes	No	No
	Radio detach (i.e., de-register)	Yes	Yes	No	No
	Radio inhibit	Yes	Yes	No	No
	Radio un-inhibit	Yes	Yes	No	No

Table 10.5-1 Interface capabilities comparison

To determine the minimum set of capabilities needed to support LMR/LTE interoperation, we find the common capabilities that are supported by the P25 DFSI, P25 ISSI, MCPTT UE, and 3GPP IWF. The P25 DFSI is chosen to represent the source of interworking capabilities on the LMR side for the conventional radio systems. The P25 ISSI is chosen to represent the source of interworking capabilities on the LMR side for the trunked radio systems.

The MCPTT UE and 3GPP IWF are chosen to represent the source of interworking capabilities on the LTE side. The result of the minimum set of capabilities, derived from the common capabilities of the four interfaces considered, is shown in Table 10.5-2. Although the P25 DFSI, used only by the P25 conventional systems, is not as capable as the other three interfaces, we list it in the table for the completeness of all the interfaces considered in our solution. We show in the table the "feature readiness" of each capability under each interface considered. A "No" in the "feature readiness" column means this capability is limited or still under development. There are two "No" assigned in the "feature readiness" column under the P25 ISSI. The reasons are explained below:

- Dynamic regrouping: The P25 ISSI currently does not support dynamic regrouping. The protocol for dynamic regrouping over ISSI is under development now (note the protocol for dynamic regrouping over P25 CAI has been defined and released).
- Location service: The P25 location service is limited. In P25, a subscriber unit sends its location data to a Location Service Host System for processing and achieving. During a group call, the P25 system does not provide the current talker's location to group members or the interested console systems. While in MCPTT, the MCPTT server can provide the current talker's location information to all affiliated members including console UEs.

Minimum Set of Capabilities	Feature Readiness			
	P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Registration	Not supported	Yes	Yes	Yes
Group affiliation	Not supported	Yes	Yes	Yes
Group call	Yes	Yes	Yes	Yes
Group broadcast	Not supported	Yes	Yes	Yes
Private call	Yes (limited to the same frequency channel)	Yes	Yes	Yes
Dynamic regrouping	Not supported	No	Yes	Yes
Late entry	Not supported	Yes	Yes	Yes
Voice encryption	Yes	Yes	Yes	Yes
Key management	Yes	Yes	Yes	Yes
Simultaneous calls (i.e., scan)	Not supported	Yes	Yes	Yes
Location service	No	No	No (not in Release 13)	Yes

Minimum Set of Capabilities	Feature Readiness			
	P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Talker ID (without alias)	Yes	Yes	Yes	Yes
Floor control	Not supported	Yes	Yes	Yes
Emergency call	Yes	Yes	Yes	Yes
Emergency alert	Yes	Yes	Yes	Yes
Losing audio	Not supported	Yes	Yes	Yes
Priority call and pre-emption	Not supported	Yes	Yes	Yes

Table 10.5-2 Minimum set of interworking capabilities

11 Attributes Comparison Among Interworking Interfaces

In this section, we compare the attributes of each interface that is considered in our proposed UIWF solution. Those interfaces include the P25 DFSI, P25 ISSI, MCPTT UE, and 3GPP IWF. The following describes each attribute comparison among those interfaces.

Voice quality: One of the most important factors that affect the overall communication voice quality is the voice codec used to compress the voice samples for transmission. In the P25 ISSI protocol, voice can be compressed by either the IMBE (the P25 full rate vocoder) or the AMBE+2 half rate vocoder. The IMBE vocoder compresses a 16-bit linear PCM stream into a 4.4 kbit/s bit stream, while the AMBE+2 half rate vocoder compresses a 16-bit linear PCM stream into a 2.45 kbit/s bit stream. Both vocoders operate on the input voice sampled at 8kHz rate. Due to the combination of narrowband and low bit rate, the voice quality provided by the IMBE or AMBE+2 vocoder is considered mediocre compared to broadband voice, yet sufficiently good for today’s public safety use. The P25 DFSI supports the same IMBE vocoder. In addition, it supports the G.711 u-law codec to compress the PCM voice when the radio system is analog FM. At the 64 kbit/s bit rate, the voice quality provided by the G.711 u-law codec is considered good. The MCPTT system uses the AMR-WB codec to compress the voice samples. AMR-WB supports 9 different bit rates, ranging from 6.60 kbits/s up to 23.85 kbit/s. It operates on the input voice sampled at 16kHz rate. Due to the use of a higher sampling rate, the voice quality provided by the AMR-WB codec is considered very good (i.e., HD quality). Both the MCPTT UE and 3GPP IWF interfaces support the AMR- WB codec.

1. Security: Both the P25 DFSI and ISSI support the same private key encryption scheme, where voice can be encrypted with 256-bit AES keys using the output feedback mode (OFB). In P25, there are two ways to distribute encryption keys to radios: manual key loading or over-the-air rekeying (OTAR). Manual key loading is performed by using a key fill device to physically connect to a radio to download encryption keys into the radio. OTAR is performed by using a Key Management Facility

(KMF) to remotely send encryption keys to a radio via P25 CAI. In the P25 DFSI, analog voice can be transmitted using the u-law G.711 format after digitally sampled. When transmitted in the u- law G.711 format, voice cannot be encrypted. MCPTT employs an identity-based encryption scheme to distribute shared secrets to interested parties. Traffic encryption keys are derived from the shared secrets after being received in the MCPTT clients. In MCPTT, the Key Management Server is used to manage the creation and distribution of shared secrets. After traffic encryption keys are derived in the MCPTT clients, voice can be encrypted with 128-bit AES keys using the Galois counter mode (GCM). How traffic encryption keys are derived is specified by the Secure Real-time Transport Protocol (SRTP).

2. Complexity: The P25 DFSI is the simplest interface protocol among the interfaces considered in our solution. It is used between a P25 fixed station and its host device such as a console. On a DFSI interface, only one voice stream can be sent in each direction at any given time. To support DFSI in UIWF, there has to be one DFSI host implemented in UIWF to communicate with a DFSI base station. One DFSI interface can only support one talkgroup or channel group. Compared to DFSI, the P25 ISSI is a much more complicated interface protocol. It is used to interconnect two P25 RFSSs. To support ISSI in UIWF, there has to have one RFSS controller implemented in UIWF to communicate with another RFSS controller in a P25 system. One ISSI interface can support many P25 talkgroups. The 3GPP IWF is based on a server to server model. To support 3GPP IWF in UIWF, there has to be one MCPTT server implemented in UIWF to communicate with the MCPTT server of the primary MCPTT system. In addition, UIWF has to communicate with the MCData server of the primary MCPTT system in order to support the Short Data Service. The 3GPP IWF consists of three sub-interfaces: IWF-1, IWF-2, and IWF-3. The complexity of the 3GPP IWF is high. The MCPTT UE interface is based on a client to server model. To use the MCPTT UE interface in UIWF, there has to be one or more MCPTT UE instances implemented in UIWF to communicate with the MCPTT server and also the common core management servers of the primary MCPTT system. The MCPTT UE interface consists of MCPTT-1/4/7 and CSC-1/2/4/8 sub-interfaces defined in Release 13. The complexity of the MCPTT UE interface is also high.

3. Ease of implementation: The P25 DFSI is the easiest one to implement among the interfaces considered in our solution since its complexity is low. The implementation of the P25 ISSI can be considered moderate. In UIWF, we do not need to implement all the ISSI features. We only need to implement the required ISSI features to support LMR/LTE interoperation. The MCPTT UE interface considered for use in our solution is defined in the 3GPP Release 13. Compared to the P25 ISSI, it uses more modern and advanced technologies in almost every area, including registration, authentication, encryption, and broadband multimedia. This makes it more complex and difficult to implement than ISSI. Even though the protocol of the 3GPP IWF has not been defined, it is expected that its implementation will be on the same difficulty level as the MCPTT UE interface. The 3GPP IWF requires the use of a server to server interface, instead of client to server. However, to use the 3GPP IWF, we still need to implement the UE functions inside UIWF to simulate the MCPTT clients.

4. Time to market: Since the P25 DFSI is the easiest one to implement, it has the fastest time to market. For the P25 ISSI, only the required ISSI features for LMR/LTE interoperation are needed. Therefore, the development time for ISSI can be cut down dramatically. The time to market for ISSI

is considered medium. As the MCPTT UE interface uses more modern and advanced technologies, it requires a longer time to develop the interface protocol. The time to market for the MCPTT UE interface is considered slow. Because the protocol of the 3GPP IWF has not been defined, its time to market is unknown. It is expected that we will need to wait at least two to three years to start seeing the interworking products that support the 3GPP IWF.

5. Cost: The end-user license cost of the P25 ISSI is expensive. Many small public safety agencies cannot afford the P25 ISSI. Also, there is high disparity on the implementation of the P25 ISSI protocol. Almost every RFSS manufacturer has its own way of implantation on some ISSI features. Due to high cost and high disparity, the number of the actual ISSI deployments has been low, but is growing. Compared to ISSI, DFSI is a much less expensive solution since it is a much simpler interface. MCPTT is a new broadband technology for mission critical applications. It is expected that the cost of the MCPTT UE based solution will not be cheap. Even though the 3GPP IWF based solution is not available for implementation, the expected cost for such solution is not cheap either.
6. Protocol availability: The protocols of the P25 DFSI and ISSI was released and implemented by equipment manufacturers years ago. Many public safety agencies are currently using the P25 DFSI or ISSI based systems. The MCPTT UE interface defined in the 3GPP Release 13 was released in 2016. Several MCPTT equipment vendors are currently developing the MCPTT UE interface in their products. It is expected that the Release 13 based UEs and systems will be available in 2019. The stage 2 of the 3GPP IWF interface was released this year. However, the stage 3 of this interface, where the detailed protocol and procedures are defined, is still under development. They will be defined in the 3GPP Release 16. Currently, the protocol of the 3GPP IWF interface is not available for implementation.

Table 11-1 below summarizes the attribute comparison described above among each interface protocol considered in our proposed solution.

Attributes	P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Voice quality	Mediocre (with P25 vocoder), or good (with G.711 codec)	Mediocre (with P25 vocoder)	Very good (with AMR-WB codec)	Very good (with AMR-WB codec)
Security	Voice encryption with AES-256 (with P25 vocoder) or no encryption (with G.711 codec)	Voice encryption with AES-256	Voice encryption with AES-128	Voice encryption with AES-128
Complexity	Low	Medium	High	High
Ease of implementation	Easy	Medium	Difficult	Difficult (expected)
Time to market	Fast	Medium	Slow	Unknown (since protocol is not defined yet)

Attributes	P25 DFSI	P25 ISSI	MCPTT UE	3GPP IWF
Cost	Low	High	High	High
Protocol availability	Yes	Yes	Yes	No

Table 11-1 Interface Attribute Comparison

12 Universal Interworking Function Solution

In this section, an UIWF (Universal Interworking Function) solution is proposed for the communication of LMR systems with each other and the communication of LMR systems with LTE systems. For the LMR systems to be supported for use in North America, only P25 systems (conventional or trunked) and the analog FM conventional systems are considered in the proposed solution. The reason to include the support for the analog FM conventional systems is the reality that there are still many organizations and agencies using this type of legacy systems today. We do not want to ignore the need for LMR/LTE interoperation of those organizations and agencies.

Only standard-based protocols are considered for use in the proposed UIWF solution. We believe the three most important wireline protocols for enabling LMR/LTE interoperation in North America are P25 DFSI, P25 ISSI, and MCPTT UE interface (based on 3GPP Release 13). The proposed UIWF solution supports these three open standards to interconnect LMR and LTE systems.

The base stations of analog FM conventional systems do not communicate with their hosts (e.g., console systems) using IP protocols natively. To support interoperation with the analog FM conventional systems, a protocol converter or gateway is needed to convert the analog signal of FM base stations to an IP-based open standard protocol. This analog FM gateway would take the 4-wire E&M or 2-wire Tone Remote Control signal from an analog base station on one side and convert it to a standard-based IP protocol on the other side. With the help of this gateway, the proposed UIWF solution is capable of supporting the analog FM conventional systems.

P25 systems have two different types: conventional and trunked. To interoperate with a P25 conventional system, the P25 DFSI protocol can be used. A P25 conventional system with a DFSI base station can connect to UIWF via DFSI for LMR/LTE interoperation. To interoperate with a P25 trunked system, the P25 ISSI protocol can be used. A P25 trunked system supporting ISSI can connect to UIWF via ISSI for LMR/LTE interoperation.

We divide LTE systems into two types: MCPTT and non-MCPTT. An MCPTT system is an LTE system that conforms to the 3GPP MCPTT standard, such as the National Public Safety Broadband Network (NPSBN) established by FirstNet and operated by AT&T. A non-MPCPTT system is any LTE system that does not conform to the 3GPP MCPTT standard, including any OTT or Pre-MCPTT systems such as Kodiak, WAVE, ESChat, and BeON. To interoperate with an MCPTT system, the standard-based wireline MCPTT UE interface should be used. This implies the MCPTT system to be interoperated should offer a wireline MCPTT UE interface. UIWF can connect to an MCPTT system using a wireline MCPTT UE interface for LMR/LTE interoperation. This wireline MCPTT UE interface should be based on 3GPP

Release 13, which was released in 2016 and available for implementation. The 3GPP IWF interface is not considered in the proposed solution because the protocol is still under development and not available for implementation.

Our research shows that it is quite common for an OTT or Pre-MCPTT system to include a P25 ISSI gateway inside its system to support LMR/LTE interoperation. Since the proposed UIWF solution already supports ISSI, it is an obvious choice to interconnect a non-MCPTT system using the standard-based ISSI. This requires that the non-MCPTT system to be interconnected by UIWF should contain a P25 ISSI gateway internally. UIWF can connect to a non-MCPTT system using ISSI. A non-MCPTT system without an internal ISSI gateway is not supported by the proposed solution.

Figure 12-1 shows the interconnection diagram of the proposed UIWF solution. On the left side of the diagram, the LMR systems, including the analog FM conventional system and the P25 conventional and trunked systems, are supported. On the right side of the diagram, two different types of LTE systems are supported: the MCPTT LTE system and the non-MCPTT LTE system. The center of the diagram is UIWF, which implements the functions of DFSI Host, P25 RFSS Controller, and MCPTT UEs, and performs protocol conversion, ID translation, and message routing. Between the analog FM conventional system and UIWF, the analog FM gateway is used to convert the 2-wire or 4-wire analog signal to an IP-based open standard protocol.

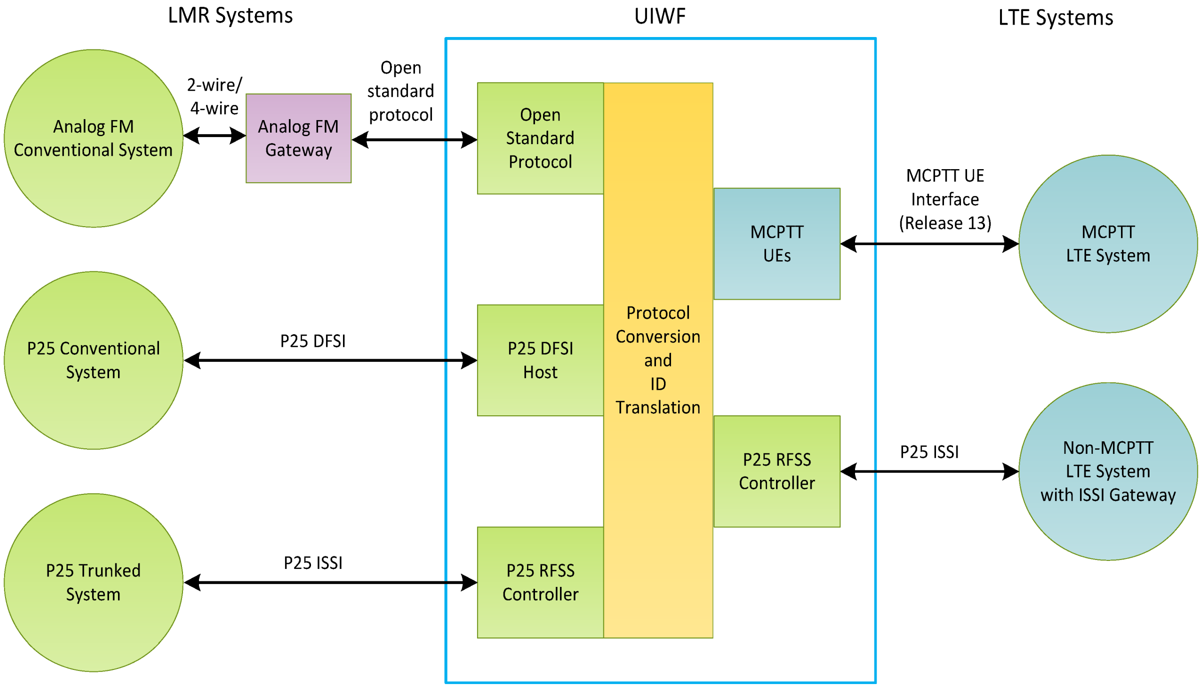

Figure 12-1 Universal Interworking Function solution

With the functional model shown in Figure 12-1, the proposed UIWF solution can support the interoperation of any of the following five types of LMR and LTE systems:

- Analog FM conventional system
- P25 conventional system
- P25 trunked system
- MCPTT LTE system
- Non-MCPTT LTE system with an internal ISSI gateway

The proposed UIWF solution can support LMR to LMR, LMR to LTE, and LTE to LTE interoperations.

The DHS RIC-M can be used to convert V.24 serial signal output by a Motorola conventional ASTRO base station to the P25 DFSI signal. Since the proposed UIWF solution already supports DFSI, a conventional LMR base station that supports V.24 protocol can be connected to UIWF for LMR/LTE interoperation via the use of RIC-M.

13 Conclusions and Recommendations

13.1 LMR to Pre-MCPTT LTE

- Today, open-standard interfaces exist that enable interoperability between P25 LMR trunking systems and pre-MCPTT LTE broadband PTT systems. These systems enable core interoperability capabilities that include groups calls, individual calls, emergency calls, and PTT-ID. **However, these pre-MCPTT systems, while perhaps based on open-standards (e.g., OMA POC in some cases), are not interoperable between themselves.** The only cross-vendor, pre-MCPTT interoperability available is via a common connection to a shared LMR interoperability solution.
  The best solution to this problem is probably to migrate pre-MCPTT users to MCPTT once it becomes available, which will allow cross-vendor interoperability (although it may not solve the commercial problem of cross-carrier MCPTT interoperability).

- Solutions also exist for interoperability between non-P25 LMR systems, but these solutions tend to rely on **proprietary RoIP gateways that do not adhere to any formal LMR open standard and tend to only support voice** (without talk group selection, without emergency indications, and without PTT-ID).
  Pre-MCPTT solution providers should be made aware of and encouraged to use the already available LMR wireline interfaces that can serve the same purpose as RoIP gateways but using open-standards (e.g., the P25 DFSI). The DHS-sponsored RIC-M may be a viable gateway for this purpose.

13.2 LMR to NPSBN MCPTT LTE

- Presently, 3GPP Release 16 (LTE) and ATIS/TIA (P25 LMR) work is in progress, which is likely to result in providing some level of open-standard LMR to LTE MCPTT interworking. Work on the LTE IWF has been slowed down within 3GPP due to 5G priorities. Although 3GPP has completed Stage 2 (architecture design), Stage 3 (protocols) is not expected until late 2019. ATIS/TIA have indicated that their goal is to publish their first document June 2019, but this will only cover architecture (equivalent to 3GPP Stage 2). ATIS/TIA cannot complete their protocol definitions until 3GPP completes their IWF protocol definitions, which means that **2020 is the earliest that LMR standards for 3GPP Release 16 IWF will be available**. Until then, the only open standard interfaces available on NPSBNs will be Release 13 and 14; both of which are UE/Client-centric with limitations explained elsewhere in these conclusions.

It is essential that these standards bodies continue their work until there is sufficient capabilities to meet user requirements.

- It is estimated that **approximately half of the public safety agencies in the USA are still using conventional (either Analog FM or Project 25 conventional).** ATIS/TIA work to date has been focused on P25 trunking. Although ATIS/TIA leadership have stated their intentions to address conventional LMR (both P25 and Analog), **no work has yet started for conventional interworking**. *ATIS/TIA should make plans to support the P25 DFSI, which can provide both Analog FM and P25 Conventional systems access to MC-PTT.*
- While the P25 ISSI/CSSI hold promise as enablers towards solving the technical interoperability problems for LMR/LTE integration, **they pose a significant commercial problem in that the ISSI license fees for the most popular P25 trunking systems is typically in the 6-digit US dollar range with significant ongoing maintenance costs, which puts the ISSI outside the budget of many small to medium size public safety agencies.**

  Either industry should seek a more affordable alternative, or manufacturers will need to significantly reduce the price of their ISSI licenses. Changing the ISSI fees from a one-time capitol expense to pure ongoing operating expense might help some agency budgets, but unless the lifetime costs for the ISSI drop significantly, it will likely prevent many P25 trunking user agencies from integrating with FirstNet or other MCPTT-capable networks.
- While Project 25 standards do support location services, it is via a P25 Data Interface rather than the ISSI/CSSI, and **at present, the ATIS/TIA joint committee is not considering the P25 Data Interface in its LTE interworking plans.** Furthermore, the existing P25 location services standards define how to receive the location of field radios and send that data to a data server. However, **no P25 standards exist to define sending location data out of the server to dispatch consoles or CAD/GIS systems**, which are the preferred systems for conveying this information to users. The only solutions that exist for this today are via proprietary interfaces subject to potentially restrictive license terms. *Industry members participating in the Project 25 standards development may want to consider alternate methods of conveying location information, possibly including transporting it with voice. Also, Project 25 Tier 1 and Tier 2 Location Services standards should be updated to close the server-to-console location service data gap. As the standards update process can take several years, other options may need to be explored such as selecting one manufacturer's proprietary solution as an interim defacto standard.*

- The only accessible LTE-side interface solutions available at this time are based on 3GPP Release 13 soon to be enhanced with Release 14. Both **Release 13 & 14, being UE/Client-centric, base their Talker ID on the credentials of the user logged into the client app. However, an LTE gateway for LMR systems must show the Talker ID of the originating LMR user, rather than one fixed Talker ID representing all LMR users. This is likely to prevent the transport of Talker ID from LMR to LTE, which would prevent meeting one of NPSTC's major LMR/LTE Interoperability recommendations.**

  Since Release 13 & 14 may have to exist in NPSBN networks for several years, solutions to this problem need to be explored with 3GPP and MCPTT solution providers, avoiding proprietary work-arounds if possible.

13.3 Dispatch Integration with NPSBNs

- An essential function of any public safety dispatch console is to display to dispatchers the identity of the field units that they are hearing.[2] In today's LMR systems, this identity is translated from a numeric SU ID to a meaningfully descriptive alias retrieved from a local radio-programming database, typically conveying the talker's role. However**, in an LTE NPSBN, user alias (metadata) is contained in a central provisioning server, and 3GPP standards may not have provisions to access this information externally.** Thus, there may be no open-standard method for dispatch consoles to access talker ID alias.

  3GPP and those who influence 3GPP should be requested and encouraged to develop an open-standard interface to allow each individual agency's dispatch center to access MCPTT talker meta-data information. Until then, open-source APIs should be developed to give dispatch systems access to the needed information.

- NPSTC has identified the need for a NPSBN capability not previously available on LMR systems: the ability to dynamically adjust the network access priority of field users based on their present role and incident assignment (aka "lift"). Only systems in the local dispatch center know the incident assignment of its individual users and this is typically the agency's Computer Aided Dispatch (CAD) system. Although FirstNet offers a proprietary API to address lift, **3GPP-defined open standard interfaces may lack the ability to allow CAD systems to inform the NPSBN of a user's incident assignment and associated dynamic priority.**

  3GPP and those who influence 3GPP should be requested and encouraged to develop an open-standard interface to allow each individual agency's dispatch center to influence the dynamic priority of users responding to local incidents. Until then, open-source APIs should be developed to give dispatch systems access to the needed information.

[2] NPSTC is drafting a MCPTT-ID Report "*Considerations for the Management of User ID and First Responder Identity*" as a follow on to their Public Safety LMR LTE Interoperability Report. It should be published before the end of this year. The draft report recommends the ability for dispatch consoles to display the name, badge number, and agency of field units whose incoming traffic they are receiving.

- NPSTC has identified the need for dispatch consoles to know the membership of the MCPTT talk groups they are dispatching[3]. **3GPP standards may not have provisions for conveying MCPTTtalk group membership to dispatch consoles** via open standard interfaces.

  3GPP and those who influence 3GPP should be requested and encouraged to develop an open-standard interface to allow each individual agency's dispatch center to access talk group membership information. Until then, open-source APIs should be developed to give dispatch systems access to the needed information.

- The existing 3GPP Release 13 & 14 open standard interfaces that will be available in the near term are designed for User Equipment (UE) Client applications, not for dispatch center applications. While it may be imperative for field devices to be secure and require credentialed log in, **it may be unproductive to require dispatcher-initiated credentialed log-on in dispatch centers where the facility rather than the user equipment is secure**. The urgent nature of dispatching causes most dispatch centers to disable credentialed log-in on their dispatcher workstations so that dispatchers can instantly take a seat and begin dispatching. Presently, **with the restrictions of 3GPP Release 13 & 14 interfaces, and/or policies of carriers that deploy them, it may be difficult or impossible to disable dispatcher-initiated credentialed log-in**.

  3GPP and/or NPSBN carriers should find ways to work around the log-in requirements for dispatch scenarios. (e.g., using machine-initiated log-on such as used for IoT devices). Release 15 & 16 IWF interfaces should not be viewed as the solution to this because IWF only supports voice, and dispatch systems will also need access to MC-DATA and MC-VIDEO.

13.4 Security Concerns

- There is a major incompatibility in security functionality between LMR systems and LTE systems. Furthermore, **a large number of the public safety agencies in the USA are still using analog conventional systems for which a standardized security solution does not exist.** 3GPP has addressed the security incompatibility for P25 compliant systems with two possible solutions. However, **what is needed is a single interoperable and universal solution that address the need for interoperating with both P25 and analog conventional LMR**. **This is a notable gap toward achieving secure Public Safety interoperable communications. Unless this gap is addressed more earnestly, interworking with LMR systems could result in exposing Public Safety LTE communications to security vulnerablies in spite of the advanced security algorithms and protocols defined by 3GPP.** *Considering the current state of deployment of FirstNet, a short term and long term approach to a security solution is needed. In the short term, Proxies and/or Gateways connected to the existing LTE interoperable interfaces could translate, regulate, and isolate communications between LMR and LTE. In the long term, the lack of security in many LMR systems must be addressed. The IWF should incorporate the functional roles of security translation and regulation to minimize the threat to not only the LTE system, but also the end-to-end communications.*

[3] From the draft NPSTC MCPTT-ID Report "*Considerations for the Management of User ID and First Responder Identity.*"

Appendix A: Abbreviations

Abbreviation	Definition
3GPP	The 3rd Generation Partnership Project
AES	Advanced Encryption Standard
AMBE	Advanced Multiband Excitation
AMR-WB	Adaptive Multi-Rate Wideband
BSI	Bridging Systems Interface
CAI	Common Air Interface
CSC	Common Service Core
CSSI	Console Subsystem Interface
DFSI	Digital Fixed Station Interface
DMR	Digital Mobile Radio
E2EE	End-to-End Encryption
E&M	Ear and Mouth signaling
ETSI	European Telecommunication Standards Institute
GCM	Galois Counter Mode
GCSE	Group Communication Service Enabler
HTTP	Hyper Text Transfer Protocol
ICE	Interactive Connectivity Establishment
IMBE	Improved Multi-Band Excitation
ISSI	Inter RF Subsystem Interface
IWF	Interworking Function
KEK	Key Encryption Key
LMR	Land Mobile Radio
LTE	Long Term Evolution
MBMS	Multimedia Broadcast and Multicast Service
MC	Mission Critical
MCPTT	Mission Critical Push To Talk
MLS	Multi-Level Security
NPSBN	National Public Safety Broadband Network

Abbreviation	Definition
NPSTC	National Public Safety Telecommunications Council
OMA	Open Mobile Alliance
OTAK	Over The Air Keying
OTAR	Over The Air Rekeying
OTT	Over The Top
P25	Project 25
PCM	Pulse Code Modulation
PoC	Push To Talk over Cellular
ProSe	Proximity-based Services
PTT	Push To Talk
QoS	Quality of Service
RF	Radio Frequency
RFSS	RF Subsystem
RIC-M	Radio Internet-Protocol Communication Module
RoIP	Radio over Internet Protocol
SBIR	Small Business Innovative Research
SDS	Short Data Service
SIP	Session Initiation Protocol
SRTP	Secure Real-time Transport Protocol
SU	Subscriber Unit
TETRA	Terrestrial Trunked Radio
TRC	Tone Remote Control
TSG	Technical Specification Group
UE	User Equipment
UIWF	Universal Interworking Function
UKEK	Unique Key Encryption Key
URI	Uniform Resource Identifier

Appendix B: References

[1] National Public Safety Telecommunications Council: “Public Safety Land Mobile Radio (LMR) Interoperability with LTE Mission Critical Push to Talk”, 2018.

[2] National Public Safety Telecommunications Council: “Public Safety Broadband Console Requirements”, 2014.

[3] 3GPP TR 21.905: “Vocabulary for 3GPP Specifications (Release 14)”.

[4] 3GPP TR 23.781: “Study on migration and interconnection for mission critical services (Release 15)”.

[5] 3GPP TR 23.782: “Mission Critical Communication Interworking between LTE and non-LTE Systems (Release 15)”.

[6] 3GPP TS 23.283: “Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2 (Release 15)”.

[7] 3GPP TS 22.179: “Mission Critical Push to Talk (MCPTT) over LTE; Stage 1 (Release 14)”.

[8] 3GPP TS 23.179: “Functional architecture and information flows to support mission critical communication services; Stage 2 (Release 13)”.

[9] 3GPP TS 22.280: “Mission Critical Services Common Requirements (MCCoRe); Stage 1 (Release 15)”.

[10] 3GPP TS 22.282: “Mission Critical Data services (Release 16)”.

[11] 3GPP TS 33.179: “Security of Mission Critical Push To Talk (MCPTT) over LTE (Release 13)”.

[12] 3GPP TS 33.180: “Security of the mission critical service (Release 15)”.

[13] 3GPP TS 26.179: “Mission Critical Push To Talk (MCPTT); Codecs and media handling (Release 13)”.

[14] TIA-102.BACA-B: “Project 25 Inter-RF Subsystem Interface Messages and Procedures for Voice Services, Mobility Management, and RFSS Capability Polling Services”.

[15] TIA-102.BACD-B: “Project 25 Inter-RF Subsystem Interface (ISSI) - Messages and Procedures for Supplementary Data”.

[16] TIA-102.BAHA-A: “Project 25 Fixed Station Interface Messages and Procedures”.

[17] TIA-102.BAAA-A: “Project 25 FDMA – Common Air Interface”.

[18] TIA-102.AACA-A: “Project 25 Over-The-Air-Rekeying (OTAR) Messages and Procedures”.

[19] ETSI TR 103 565: “Study into interworking between TETRA and 3GPP mission critical services”.

[20] ETSI TR 103 565-2: “Interworking between TETRA and 3GPP mission critical services; Part 2: Security of interworking between TETRA and Broadband applications”.

[21] TCCA: “TETRA Connectivity to LTE”.

[22] TCCA White Paper: “Security considerations for interconnection of TETRA and Mission Critical broadband systems”.

[23] Kodiak Networks

[24] Motorola Solutions WAVE information: https://www.motorolasolutions.com/en_us/products/broadband-push-to-talk.html

[25] ESChat website: https://www.eschat.com

[26] Covia Labs

[27] Etherstack website: https://www.etherstack.com/us

[28] Harris website: https://www.harris.com

[29] Voxer website: http://www.voxer.com

[30] TASSTA website: http://www.tassta.com

[31] Orion Labs website: https://www.orionlabs.io

[32] Azetti Networks website: http://www.azetti.com

[33] StreamWIDE website: http://www.streamwide.com

[34] Push to Talk International website: http://www.ptti.co.uk

Appendix C: Summary Table OTT or Pre-MCPTT systems

NOTE: The information contained in this table has not been verified by each pertinent company and may not represent the most current information.

OTT or Pre-MCPTT System	Company	Brief Description	Features
Kodiak Networks	Motorola Solutions	Kodiak is a leading provider of carrier-integrated broadband PTT solutions that provide fast, seamless group or one-to-one communications over LTE/4G, 3G, and Wi-Fi networks. Kodiak Broadband PTT is a key part of the Motorola Solutions suite of integrated communications applications, delivering voice, video, and data communications at the push of a button to get the right information to the right people at the right time in the moments that matter. Used by AT&T, Verizon, and Sprint.	Sub-second call setup, high voice quality, multimedia messaging, location-based services on device, encryption based on AES-256, real- time presence, multiple application modes, one-touch calling, voice message fallback, late-join/re-join functionality, support for pre-defined and ad-hoc group calling, call preemption via supervisory override, PTT/cellular interaction, broadcast calling, talkgroup scanning with priority, alerts
WAVE 5000	Motorola Solutions	WAVE 5000 enables interoperable PTT communication across broadband and radio networks and devices so that critical, time-sensitive information flows quickly and securely between mobile workers and teams. https://www.motorolasolutions.com/en_us/products/broadband - push-to-talk.html	Voice, text, photos, video, cloud based subscription, cloud deployment, subscription service, on premise deployment, fully virtualized software, extensive two-way radio interoperability, managed services available, software upgrades included, service level agreements (SLAs)

OTT or Pre-MCPTT System	Company	Brief Description	Features
ESChat	SLA Corporation	ESChat (Enterprise Secure Chat) is a popular PoC app that offers an enhanced OTT service. Private labeled via other companies under many other names. https://www.eschat.com	Secure push to talk voice, secure group messaging, live location tracking, bread crumb tracking, RoIP: LMR radio integration, PC dispatch, cloud or customer hosted
Push-to-Talk	Covia Labs	Push-to-Talk is a rich-media communications software product that supplements existing public safety radio communications systems using cost effective commercial mobile phones and carrier networks. It addresses local law enforcement need to supplement public safety radio communications systems.	Voice, video, text, GPS location, maps
LTE25	Etherstack	Etherstack's LTE25 solution bridges LTE networks and existing APCO P25 narrowband networks with an integrated, push-to-talk solution. https://www.etherstack.com/us	Mission critical, high availability solution, listen to multiple talkgroups simultaneously, PTT group calls within the LTE network, talk directly to the dispatch center, priority and emergency calls supported, end-to-end encryption between LTE & P25, location services allows LTE & P25 units to be tracked, uses native P25 vocoder, runs on COTS LTE Android platforms, reduced cost of ownership, geographically diverse disaster recovery node, fast call setup times between P25 & LTE devices

OTT or Pre-MCPTT System	Company	Brief Description	Features
BeOn	Harris	BeOn is an application that extends the capabilities of LMR network to smartphones, tablets, and PCs—providing PTT communications far beyond the boundaries of regional radio systems and opening affordable PTT communications to new user groups. It has been designed to mimic the features of P25 radio networks. https://www.harris.com	Display location of LMR radios, full AES end-to-end encryption, group voice call, individual voice call, distress indication, announcement group calls, instant recall/call logging, console/supervisory override, talkgroup scanning, late call entry, P25 confirmed call, priority/preemptive support, P25 OTAR key management, console patch/simulselect, group location, user presence indication, location privacy, BeOn text messaging
Voxer	Voxer	Voxer is the leading walkie talkie app for high-performance teams and distributed workforces. http://www.voxer.com	Talk instantly with your team, never have to repeat yourself, voice, photo, and video messaging, manage who hears what, no limits on channels or range, no roaming charges, no contracts, use any carrier, organize users into functional teams, robust message control features

OTT or Pre-MCPTT System	Company	Brief Description	Features
TASSTA	TASSTA	TASSTA, a German company, provides professional push-to-talk communication over broadband solution. http://www.tassta.com	Group, individual and priority calls, encryption, ease of administration, multi-platform clients and accessories, task management system, GPS location, GPS route, indoor localization, bridge to PMR, voice recording and call history, alarming, mandown, LWP, message, file exchange and alerts, remote camera and mic control, redundancy
Orion Pro	Orion Labs	Orion Pro is a new kind of push-to-talk solution for organizations that need real-time coordination and fast answers without distractions. https://www.orionlabs.io	Unlimited range, one-to-one & groups, hardened security, simple powerful design, real-time location, unlimited users, advanced administration & management, real-time language translations, voice search company databases, voice-based automations

OTT or Pre-MCPTT System	Company	Brief Description	Features
Azetti	Azetti Networks	Azetti PTT is a professional PTT client compatible with OMA standards that turns your smartphone or tablet into a walkie talkie. http://www.azetti.com	Voice recording, priority calls, group call, one-to-one call, instant messages, instant personal alert, contact list, accepted/blocked list, GPS location, user’s status & presence
Team on the Run	StreamWIDE	Team on the Run is a comprehensive business communication solution that allows instant connection between remote teams. http://www.streamwide.com	Private and group conversations to communicate with relevant team members, VoIP calls, push-to-talk, geolocation, corporate directory, video streaming, video call, task management
POC-IT	Push to Talk International	POC-IT Push to Talk allows you to create private channels and groups for instant group communications without boundaries, to members of your private group. http://www.ptti.co.uk	Unknown