\

Broadband Interoperability Platform

From Catalyst Communications Technologies, Inc.

Final Report Summary
Department of Homeland Security
Science and Technology Directorate
Topic No. DHS221-004
Contract No. 70RSAT22C00000024

March 2023

WWW.CATCOMTEC.COM

Introduction

In 2018, Catalyst Communications Technologies won a contract with the Department of Homeland Security (DHS) Small Business Technology Research (SBIR) Program to investigate the feasibility of a standards compliant solution to enable communications between legacy land mobile radio systems and first responders using new Mission Critical Push-to-Talk applications on smartphones connected to LTE networks, including FirstNet® built with AT&T. Catalyst then won subsequent contracts with SBIR to develop a prototype of our proposed solution, and with PSCR – the Public Safety Communications Research division of the National Institute of Standards and Technology - to commercialize and market this solution. Products based upon this research and development work are currently being marketed under the IntelliLink™ Interworking brand.

In 2022, DHS SBIR published another solicitation to research the feasibility of whether and how these LTE smartphone users with push to talk applications – both standards based and proprietary – might communicate with each other, even if they were served by different network providers using different technologies. Building upon our experience and success with LMR LTE Interworking, Catalyst responded to this solicitation with a proposal to investigate the feasibility of broadband LTE to LTE Push-to-Talk Interoperability. Catalyst competed for and was awarded a contract; this research was completed in 2022, and this document is a summary of our research and the report we provided to DHS SBIR.

The addendum to this report includes a description of terms and discussion on security considerations.

Executive Summary

Our goal was to determine the technical feasibility of building a Broadband Interoperability Platform (BIOP) which can provide Push-to-Talk (PTT) voice interoperability between broadband systems for mission critical operations. From our research, we have demonstrated this feasibility and outlined a plan to build a prototype and gain acceptance from the service providers, their vendors, and the agencies that need this interoperability.

We divided the task into four Phases. We began with a thorough analysis of Public Safety's requirements as documented by the National Public Safety Telecommunications Council (NPSTC), supplemented by those from the US Department of Homeland Security (DHS) and our twenty-five years of experience providing Internet Protocol-based PTT dispatch and interoperability solutions. We identified sixty-one user requirements and over the course of this five-month project used them to derive specific requirements for the operation and administration of a BIOP. We researched leading Push-To-Talk over Broadband (PTToB) services to verify that the required features are generally available and to explore the

interfaces currently supported by those services. We then undertook an extensive analysis to evaluate the feasibility of end-to-end encryption and transcoded encryption. Encryption is a critical issue and, while end-to-end encryption is appropriate for LMR communications, it is a major barrier to a viable broadband interoperability solution.

After our encryption analysis, Catalyst analyzed six established interfaces that PTToB services could utilize for interoperability. We had success identifying the 3GPP "client" interface in our Interworking research, and we found that using a client interface enables a near-term solution that is highly likely to be accepted by the cellular carriers, their vendors, and other service providers. Specifically, we recommend using the 3GPP Mission Critical Push-to-Talk (MCPTT) Client interface[1] as specified by the Third Generation Partnership Project (3GPP) for compliant MCPTT services such as AT&T's FirstNet PTT. For PTToB services that are not 3GPP MCPTT compliant, we recommend the Telecommunications Industry Association's Console Sub-System Interface (CSSI) P25 standard[2]. Also, in this Phase we identified six significant barriers to prototyping a BIOP and explained how our approach, coupled with the existing technologies and relationships that we have with leading carriers in the US, uniquely positions Catalyst to successfully test and commercialize our solution.

The last phase of our research analyzed the work needed to address the essential operational and administrative requirements for the BIOP, derived from the sixty-one user requirements, and we developed a plan to gain acceptance from the service providers, their vendors, and the agencies that need this interoperability. In addition to solving the broadband-to-broadband PTT interoperability needs listed in the solicitation for this project, our approach seamlessly enables interworking of those services with a variety of LMR systems.

The balance of this paper describes the details and methodology of this research.

Terminology

There are several terms used here that are used frequently in this market and industry, but the meanings are different depending on the writer. The following definitions and clarifications, therefore, are presented:

---

[1] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=623

[2] 6 TIA TR-8 is the engineering committee responsible for developing the TIA-102 series of P25 Standards in collaboration with the P25 Steering Committee and public safety users

1. We use the term "**interoperability**" for connecting two or more diverse PTToB systems together.
2. We use the term "**interworking**" to describe connecting LMR and LTE systems together.
3. 3GPP specifications also use the "interworking" term as well as the term "interworking function".
4. 3GPP uses the term "**interworking function**" to describe an entity that connects the interworked LMR and LTE systems together and in some cases more generally to mean connecting non-3GPP compliant systems to 3GPP compliant systems.
5. We use the term **BIO Interface** for the interface used for Broadband Interoperability, connecting to a broadband system.
6. We use the term **BIOP (Broadband Interoperability Platform)** to describe the entity that connects the interoperating LTE systems together using the BIO interface.
7. If a solution is required that enables both interoperability and interworking functionality, we refer to it as a **harmonizing solution**, since it is interconnecting both between and among LMR and broadband systems.

Broadband Interoperability Feature Requirements

Catalyst defined a baseline PTToB feature set and Interoperability Requirements to be used in subsequent tasks to define and validate an appropriate interface into diverse Broadband PTT Offerings. Catalyst derived these requirements by drawing on input from the following customer-side sources representing the needs of First Responders with emphasis on Public Safety:

- National Public Safety Telecommunication Council (NPSTC) publications that address the role of PTToB systems:
  - *Considerations for Mission Critical Push to Talk (MCPTT) Consoles, July 3, 2020*
  - *Public Safety LMR Interoperability with LTE Mission Critical Push to Talk report, January 8, 2018*
- Department of Homeland Security (DHS) PTT Requirements Interoperability spreadsheet that lists PTT features and priorities

Figure 1 illustrates Catalyst's high-level architecture for a BIOP interface that could connect users of several representative PTToB service offerings to provide interoperability functionality. These particular PTToB systems were chosen as representative of the industry and market.

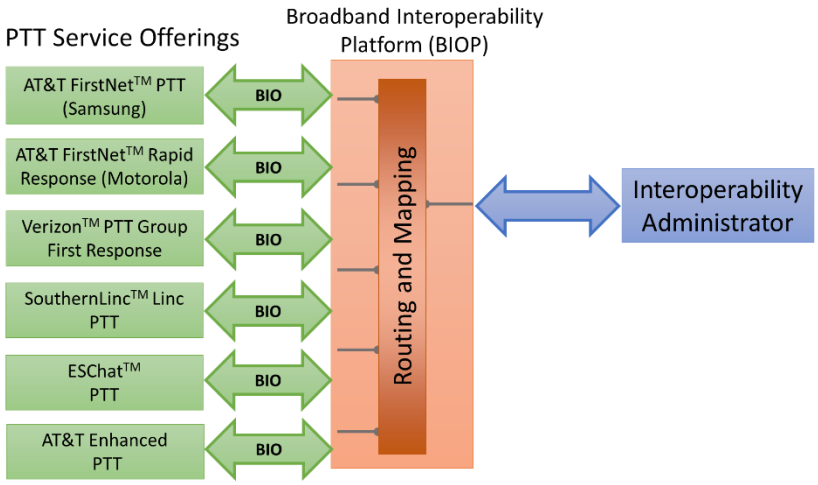


Figure 1: Catalyst's high-level architecture

For the 3GPP service offerings, we have assumed connecting using a 3GPP compliant interface for Interoperability (IO) and so the interface for IO for the service offering would support the same feature set as any other component using that interface. For the proprietary service offerings, however, in addition to reporting the feature set enjoyed by a 3GPP compliant interface, we will need to consider the feature set accessible through a third-party interface. We scored these requirements based upon the feature sets available in the market, and we did so in the aggregate – our report does not identify individual feature sets available from individual service providers or vendors but summarized the number of vendors that provided that feature. Twenty-three features derived from the analysis were scored at 7 or greater.

Security Policy

As determined through Catalyst's analysis, a key feature that must be provided by the BIOP is the ability for users of PTToB services to communicate securely and privately with each other, regardless of the underlying network, PTT application, or PTT service provider. This secure, "cross-network" communications capability requires support for encryption of media, metadata, and signaling transmissions. Figure 2 illustrates our analysis.

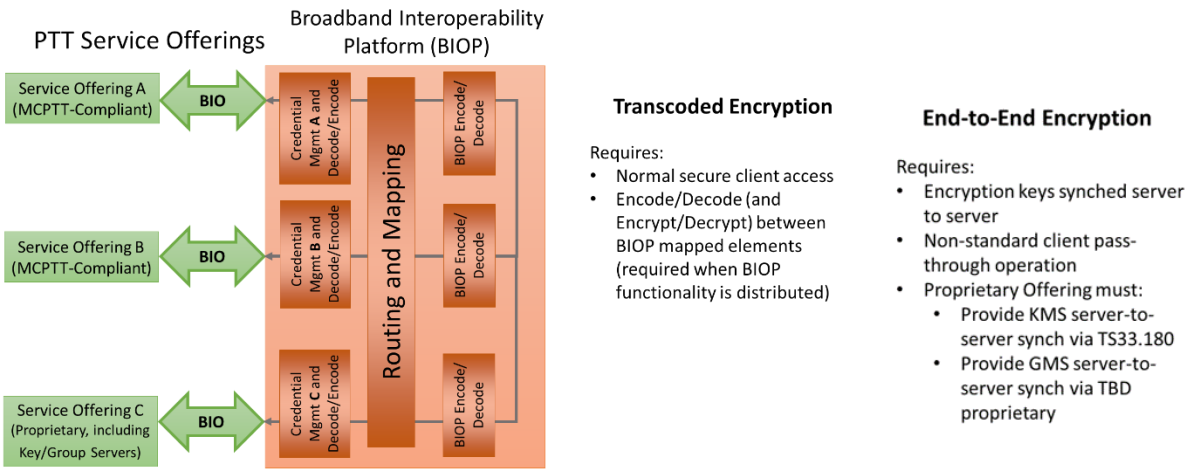


Figure 2: Security Considerations for the BIOP

Catalyst evaluated the feasibility of managing encryption between disparate PTT Service Offerings and concluded that the only feasible approach in the short term is to use ***Transcoded Encryption*** where the BIOP itself is the endpoint for interoperating PTToB systems. While one of this project's goals was to prioritize creating a solution that supports End to End Encryption (E2EE), our conclusion is that transcoded encryption provides the most feasible approach. It breaks the signal path into secure segments in which the BIOP makes secure connections to PTT systems, decrypts the data using the originating system's encryption key, and then re-encrypts using the target system's encryption key before securely forwarding information to that system. The effort required to develop a Transcoded BIOP encryption solution will be markedly lower than the effort required to develop E2EE. We note that the handling of these materials by the BIOP is essentially no different than any other client application (including mobile clients) that currently connect securely to MCPTT servers.

In our research, we found that only a standards-based server-to-server approach for sharing encryption keys is viable for E2EE and is, at best, many years off. The algorithms, keys, and voice codec must be the same at both ends for end-to-end encryption and this approach only applies to communication between two fully compliant MCPTT systems. The approach that Catalyst is recommending uses a standard, agency-specific, connection that can be accessed without large extensions to functionality or exposing the inner workings of the system. The addendum to this report provides additional information.

The Interface Specification

At the outset, it is important to understand there are operational differences between the various interfaces to different PTToB systems and to understand how those differences impact how interoperability will work. Catalyst has conducted extensive evaluation and analysis of two different approaches to interoperability:

• A deep system-to-system connection

• A more modest connection between independent client connections into different systems.

There are substantial operational, philosophical, and obtainability differences between these two interface types: the first is used to connect and tightly integrate systems together and the second is used to give users access into a given system. Rather than depend on the complexity and complicity needed by the server-to-server approach, our approach is to leverage the simplicity of the client interface to provide interoperability between diverse systems that cannot/will not integrate in the short term.

Catalyst identified six candidates for the BIO interface; they are:

1.3GPP Interfaces
   a. MCPTT Client interface specified in 3GPP TS 23.379[i] & TS 23.280[ii]
   b. MCPTT Interworking Function Interface (IWF) specified in 3GPP TS 23.283[iii]
   c. MCPTT Server to Server interface MCPTT-3 specified in 3GPP TS 23.379[i]
2.LMR Interfaces
   a. Project 25 Inter RF Subsystem Interface (P25 ISSI accessed using CSSI[iv])
   b. Project 25 Digital Fixed Station Interface (P25 DFSI[iv])
3.Generic IP Interfaces
   a. An RTP[v] or RTCP[vi] "connection" either "nailed up" or with SIP session control

Catalyst evaluated each of these interfaces against the Recommended Interoperability Requirements for PTT Service Offerings that were derived in Task 1. We provided insights into the feasibility of each requirement on whether it is required for basic, advanced, or encryption interoperability requirements. By studying these factors both individually and in aggregate, we can begin to determine which interface or interfaces might be best at integrating diverse systems together to meet the requirements of a BIOP. We scored each interface, however while the absolute scores are instructive, we must also judge which interfaces fulfill all essential requirements and which ones are more feasible for vendors and carriers to support. Table 1 and Figure 3 provide the results of this analysis.

Interface	Numeric Overall Efficacy	Overall Efficacy Text
3GPP Client I/F	3.669	Medium/Medium-High
3GPP IWF	2.977	Medium
P25 ISSI	2.746	Medium/Medium-Low
P25 DFSI	2.000	Medium-Low
RTP/RTCP	1.015	Low
3GPP Server-to-Server	4.731	High

Table 1 – Overall Scoring of the Six Interfaces Against BIOP Requirements

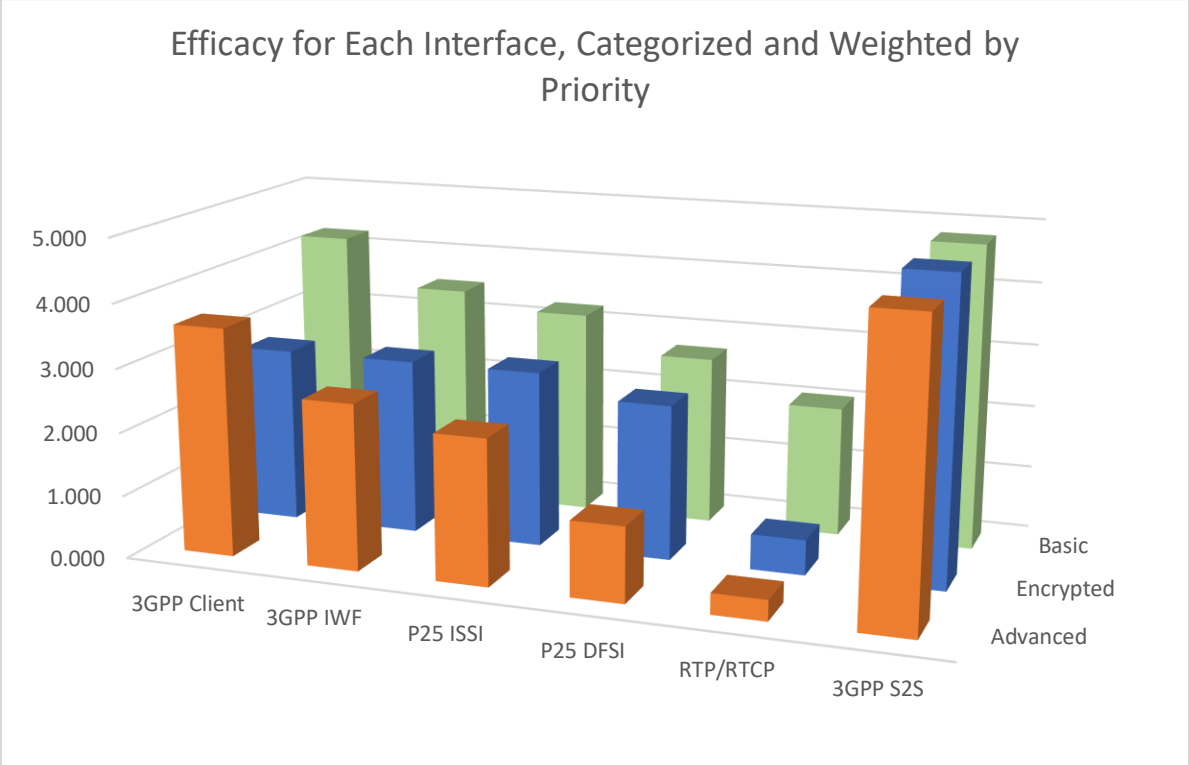


Figure 3 - Efficacy for Each Interface, Categorized and Weighted by Priority

Table 1 shows information numerically and Figure 3 graphically, respectively, on the distribution of efficacy when classified as Basic, Encrypted, and Advanced requirements.

Table 1 shows information numerically and Figure 3 graphically, respectively, on the distribution of efficacy when classified as Basic, Encrypted, and Advanced requirements. The classifications are as follows:

a. ***Basic*** – this requirement is needed for basic interoperability. A BIO interface into a proprietary system might only provide these more basic features: voice, talkgroup, etc.
b. **Advanced** – this requirement may not be essential to operation, but brings additional functionality for agencies that require it.
c. **Encrypt** –this requirement classification is separate from the others since, for instance, if voice is encrypted, you cannot do basic voice functionality without it. Unlike LMR systems where some systems routinely operate unencrypted, virtually all PTToB support encryption and most run with it enabled at all times.

The calculation used for these categorized scores is also a weighted average using the Catalyst Priority to give greater weight to High priority requirements. As would be expected, the simplest interface, RTP/RTCP, can meet some of the basic requirements, but very few of the advanced ones. The server-to-server interface is again the highest ranked in all of these categories, representing an ideal system-to-system interface.

What these evaluations do not show is what is implicitly the most important consideration of all - for a given interface would carriers and PoC vendors consider adopting the interface for the use-cases described? Getting buy-in and access for a BIO interface from all or most Service Offering Providers is more important than specific features, capabilities, or even specific requirements. These next paragraphs discuss this overarching requirement of commitment to making access available by carriers and vendors.

In North America, it would be extremely difficult to get server-level interoperability connections between all solutions from all Service Offering Providers. Our high-level characterization of the 3GPP Server-to-Server interface describes in an idealized way how MCPTT application servers might be connected together. The MCPTT-3[i] interface is designed primarily to connect sibling MCPTT application servers together for load-sharing and geographic distribution. Because MCX involves many server entities beyond MCPTT itself used for functions like Key Management, Group Management, Identity Management, etc., a working server-to-server interface between disparate systems and carriers would be incredibly challenging. It is beyond the scope of this high-level evaluation to examine these intricacies in greater detail, but the Broadport Report[3] details a plan for tying MCPTT

[3] Frequentis (Broadport) Consortium End of Phase Report
Broadway Phase 2 V1.0 2021-5-7

systems together for interoperability and their analysis includes many system elements and even LTE components that they indicate would be needed for direct system-to-system interoperability.

The impracticality in the short term of a direct server-to-server interface between systems points to a more modest, client-based interface that scored a close second to the server-to-server interface. As far as getting buy-in from vendors and carriers, the best buy-in is no need for commitment or agreement – i.e., utilize technology and access methods already available from the carrier or vendor. The reason that Catalyst considers the client, transcoded approach particularly attractive in today's environment is not strictly for technical reasons but for practical reasons. A secure Client Interface-based BIOP interoperability solution that operates between two or more PTToB service providers and supports encryption as part of its interoperability function provides a flexible mechanism for meeting BIOP requirements while not exposing service providers' network topologies.

The huge downside of the direct server-to-server approach is that it requires total cooperation and integration between vendors and carriers to a degree that Catalyst judges to be impractical in North America. Even if the competitive barriers between US carriers could be overcome, based on our direct experience and in-depth knowledge of the North America's PoC technology, we judge a Broadport type of system-to-system connection here to be many years in the future.

The 3GPP Client interface, however, is only naturally applicable for 3GPP MCPTT-Compliant PTToB providers. It is possible that a proprietary PTToB system provider might be motivated to synthesize and maintain a 3GPP-Compliant Client that accesses their proprietary system, although this seems unlikely and impractical for the most part. What is practical and available today, however, and is in the vein of "no need for buy-in," is an LMR interface into their product that many proprietary PTToB service providers may also provide into their system. Often this is implemented as a P25 ISSI connection on their system that can be accessed through a dispatch console using CSSI. When the BIOP uses a CSSI client connection to the service provider's emulated ISSI that homes the PTToB talkgroups and users, it functionally works much like the 3GPP client interface. Based on the scoring of interfaces, the ISSI interface has the potential of providing a significant amount of PTToB interoperability between systems. Although the interface is not capable of providing as rich an interoperability experience as the 3GPP Client Interface, it scores almost as well, especially for Basic functionality.

To summarize: the interface that Catalyst recommends for the BIOP, when connecting to 3GPP MCPTT-Compliant PTToB systems, is the 3GPP Client Interface. When connecting to non-3GPP MCPTT Client PTToB systems, we recommend using the most full-featured P25 LMR interface available. The BIOP architecture should anticipate that eventually some PTToB services will be connected via the Server-to-Server interface and that some

collection of agencies will use those two services plus a third. The BIOP architecture and management tools should anticipate how those three services might be connected and coordinated.

Managing the Interface

Administration in our proposed system requires that each system retains its own talkgroups and users and each system must administer them themselves. In the 3GPP-compliant system, the interoperability user (normally a dispatch user who can receive and transmit on multiple talkgroups simultaneously) is given access by the administrator to certain talkgroups and users. The BIOP is essentially a trusted user on multiple PTToB systems, and each system connection works as a dispatch user who has access to multiple talkgroups. It is up to the BIOP to define and configure which talkgroups on the connected systems are interoperable groups and which pairs of groups on the two systems interoperate with each another.

We also propose a structured naming convention for interoperable talkgroups (and perhaps even users) so that administrators and users of these broadband interoperable systems can instantly know who is talking and what PTToB system they are coming from. Without requiring any new functionality or signaling on the PTToB system, having each agency utilize a common, structured naming convention for these interoperable talkgroups will have the effect of unifying the systems and providing a structure and basis for creating, managing, and understanding interoperability. By leveraging this somewhat mundane, basic feature that inherently exists for each of these systems, proprietary or standards-compliant, we can provide some structure for interoperability that would allow an administrative tool, having access to all of this data, to differentiate between local talkgroups and interoperable talkgroups.

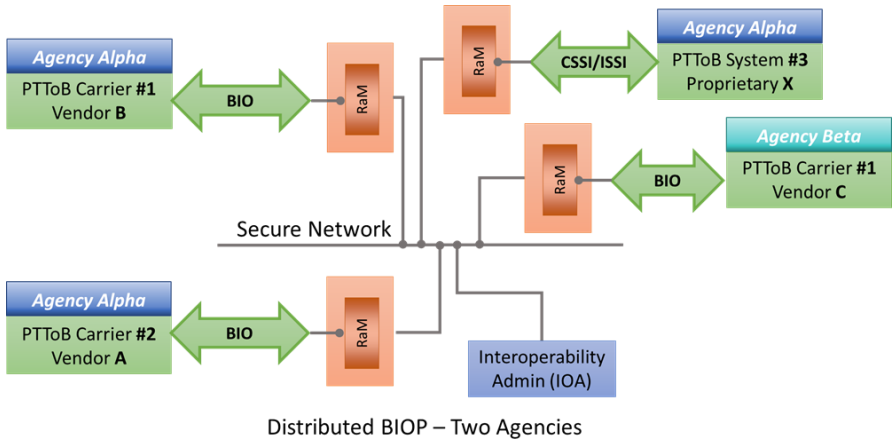
In MCPTT-Compliant systems, one of the key features that clients have access to is that, when connecting to the PTToB system, a wealth of information is downloaded to the client at connection time. This information includes other users on the system, talkgroups that the user has access to, and even the users that are members of those talkgroups (by contrast, this information is generally not available in an LMR system). Because the administrator on each system sets up this information and has a large degree of freedom in defining talkgroup names (and, to some degree, user names) these names can be used to provide structure and implicit information for interoperability. Catalyst recommends beginning this work by analyzing the 2018 NPSTC report "Mission Critical Push-to-Talk (MCPTT) Considerations for Interoperability Talkgroup Naming and Management."[4]

[4] https://www.npstc.org/download.jsp?tableId=37&column=217&id=4172&file=NPSTC_

Building BIOP Systems

The BIOP design that Catalyst envisions integrates disparate systems that are not tied together at the system level, but still must access them in secure and established ways before interoperability can be achieved. Some interfaces into a carrier or vendor's system might be expected to reside at the carrier's facility, but, because the entire purpose of the BIOP is to connect disparate systems together, this is not feasible. Instead, it is recommended that the BIOP hardware be located at a physically secure location maintained by the agency that is using it for interoperability. This follows a pattern already established for interworking where the LMR side of the interworking solution is usually physically constrained due to coverage or security considerations to be located at the agency's location.

At a systems level, a Broadband Interoperability system architecture connecting Four PTToB Systems from Two Agencies Interoperating can be represented thusly:



Distributed BIOP – Two Agencies

Figure 4: Four PTToB Systems connected via the BIOP

Catalyst expects that for the foreseeable future, interoperability between PTToB systems and interworking between PTToB and LMR systems will be the rule rather than the exception. The BIOP equipment for interoperability and the equipment used for interworking will not only be collocated but also integrated together architecturally. With this architecture, the distributed BIOP acts as a harmonizing solution, allows LMR to LMR interoperability, broadband to broadband interoperability, and LMR to broadband interworking, in any combination that the agency requires. The IOA (Interoperability

Administrator in the above diagram - essentially a Dispatch Console) also has simultaneous access to all of these diverse technologies. The Administrator or Dispatcher sees a talkgroup from any of the systems as the same as a talkgroup from any other system. This holds true visually as well as operationally.

Operations And Administration

In the BIOP itself, a call on one system's talkgroup that is configured as interoperable with a talkgroup on a different system causes a chain of events to occur that results in that call being forwarded and heard on a second system.

It should be noted that the mechanics of forwarding such a call, whether it is interoperability between PTToB systems or interworking between a PTToB and an LMR system, are non-trivial and require a significant amount of sophistication and coordination between systems. The sequencing and precise degree of coupling and synchronization between systems is a software technology and codebase that Catalyst has been perfecting starting with its LMR-to-LMR interoperability solutions for more than two decades.

In the BIOP system that we propose, each system retains the administration of its own talkgroups and users. In both 3GPP-compliant and proprietary systems, the user whose credentials are used to make a client connection to a PTToB system can receive and transmit on certain talkgroups with certain users. The BIOP is essentially a trusted user on multiple PTToB systems and on each system acts as a user who has access to certain talkgroups and users. It is up to the BIOP to define and configure which talkgroups on the connected systems are Interoperable (IO) groups and which IO group on one system interoperates with which IO group on another. The administration of these interoperability connections by customers in the Public Safety space are often managed in conjunction with the dispatch console by the Dispatcher. This is because Dispatchers are generally in operational charge of events and have the situational awareness to quickly and accurately create these new interoperability connections and to disable them when they are no longer needed.

As the NPSTC LTE Console Report[5] states, one of the greatest differences between the LMR and LTE systems is the ability to add new users (including from other agencies) and new talkgroups on-the-fly and the BIOP must be able to connect, recognize and register these new components on multiple, connected systems and to efficiently provide interoperability between them. There will be a need for a BIOP administrator who provides some of the more static and planned components of this critical functionality, but the back-end administration technician lacks the connection to unfolding events and the

[5] https://www.npstc.org/download.jsp?tableId=37&column=217&id=3205&file=Console_LTE_Report_FINAL_20140930.pdf

24/7 role of the Dispatch Center Shift Commander or an experienced Dispatcher. Hence our approach empowers each agency to control which individuals (Administrators, Technicians, Dispatchers, etc.) are allowed to enable and disable interoperability.

Summary and Going Forward

This paper describes and discusses the results of a research contract awarded by the Department of Homeland Security Science and Technology Directorate to investigate the feasibility of a Broadband Interoperability Platform connecting disparate Push to Talk over Broadband systems. We determined that such as solution can be developed, and recommend that, when connecting to 3GPP MCPTT-Compliant PTToB systems, the 3GPP Client Interface be used, and when connecting to non-3GPP MCPTT Client PTToB systems, the most full-featured P25 LMR interface available be used.

Many of the capabilities that are described in this paper as the BIOP are already available and working with Catalyst's solution today. However, there is still much work to do to make that solution satisfy additional essential requirements and to work with more PTToB vendors.

The Phase I Research described in this document is step one in a three Phase approach promoted through the Small Business Innovation Research program offered by the federal government. In late 2022, DHS issued a solicitation for Phase II of this program – further research and prototype development. Catalyst has provided a detailed proposal to DHS and expects to be awarded a contract for it by the second quarter of 2023. If awarded, that research, along with the development of the prototype solution described in the paper, will occur over the subsequent twenty-four months.

§

Addendum –

Abbreviations

3GPP	3rd Generation Partnership Project
BIO	Broadband Interoperability
BIOP	Broadband Interoperability Platform
CSSI	Console Subsystem Interface
DFSI	Digital Fixed Station Interface
DHS	Department of Homeland Security
E2EE	End-to-End Encryption

ISSI	Inter RF Subsystem Interface
IWF	Interworking Function
KMF	Key Management Facility
LMR	Land Mobile Radio
LTE	Long Term Evolution
MC	Mission Critical
MCX	Referring to 3GPP MCPTT, MCVideo, MCData, services collectively
MCPTT	Mission Critical Push To Talk
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
P25	Project 25
PTT	Push-to-Talk
PTToB	Push-To-Talk over Broadband
SBIR	Small Business Innovative Research
TIA	Telecommunications Industry Association
UE	User Equipment

Security Considerations Discussion

The Case for End-to-End Encryption for Broadband Interoperability

In the LMR industry, the concept of end-to-end encryption is well known and widely accepted but as we move forward to integrate LMR with other systems, its necessity needs to be able to survive technical scrutiny. The need for end-to-end encryption so that critical communications can be kept secure has partly driven the wide adoption of Project 25 LMR systems. Catalyst agrees with that requirement for LMR, but as we study the unification of LMR and broadband as well as broadband and broadband, it is worthwhile recounting the reasoning behind that approach for P25 LMR:

1. While Project 25 standards were in their formative stages, manufacturers were being asked to move from digital systems that used proprietary vocoders and signaling to ones that, over-the-air, used a published standard such that, anyone with a radio receiver in coverage that had access to that published

standard (scanner manufacturers) could listen to (and theoretically participate in) any conversation.

2. Because these communications were over-the-air such that you couldn't restrict access to them in a given coverage footprint, this standards-based approach ***forced*** any communication that needed to be secure to be encrypted, since proprietary implementations could no longer obscure it.
3. In LMR, any approach that did not encrypt and decrypt at the end-points had to deal with unencrypted communications somewhere along the signal path, usually between repeaters, likely unsecured and, again, over the air. Repeaters were not intelligent devices that would normally be able to manage secure communications between each other nor were they collocated, so managing keys at the end-point devices was deemed the only viable approach.

Although broadband communication on mobile phones is over the air, radio frequency eavesdropping of the type described above that is trivial in conventional analog radio systems, and still vulnerable in trunked, digital P25 systems, is much more difficult in the very dynamic and heavily-encrypted cellular world. LTE, 5G, Wi-Fi, wired connections, VPN, and other technologies generally make it very difficult to snoop over-the-air. The most successful snooping is done by devices connected on the same network, but, in these situations, transcoded encryption should arguably be more secure than using a single, infrequently changed symmetric key. That key could be compromised (especially if it has to be communicated to end-point devices in the cellular world), and then could be utilized at any point where the bad actor could get access to the signal chain.

It is beyond the scope of this study to analyze this exhaustively, but the point of this short discussion is that it is worth examining the risks and rationale of extending this LMR-centric approach to a very different technological landscape. Further, Catalyst believes the coup-de-grâce for bringing this approach to interworking, which in turn brings it to broadband interoperability, is that the common vocoder requirement forces narrowband audio quality on all interoperable broadband talkgroups on broadband devices.

This is more than a technical or theoretical issue and question, but one of marketing in a world where users are asking why they should adopt PTToB and move away from LMR. Today's users are hearing high-definition audio everywhere: VoIP phones, mobile phones, even on Microsoft Teams and Zoom teleconference calls. Crystal clear audio and virtually no background noise is the norm for today's user. For an analogy, you may have a movie on VHS tape and have access to the same movie on a streaming service. Your teenager is going to complain mightily (and justifiably) if you force him to watch it on VHS when he knows he can stream it in HD. Similarly,

using narrowband, voice-optimized codecs on a broadband system, even though at a point in time on LMR this audio was declared to be "good enough" (against the judgment of some analog users), does not move the industry forward by leveraging the superior capabilities of the new technology.

---

[i] 3GPP TS 23.379 V15.3.0 (2018-04) Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2 (Release 15)

[ii] 3GPP TS 23.280 V15.3.0 (2018-04) Common functional architecture to support mission critical services; Stage 2 (Release 15)

[iii] 3GPP TS 23.283 V15.0.0 (2018-04) Mission Critical Communication Interworking with Land Mobile Radio Systems; Stage 2 (Release 15)

[iv] Project 25 interface standards for ISSI, CSSI, DFSI etc. are maintained by Telecommunication Industry Association (TIA) and are available at (http://www.tiaonline.org/)

[v] H. Schulzrinne, et al., "RTP: A Transport Protocol for Real-Time Applications," Network Working Group, July 2003. https://www.ietf.org/rfc/rfc3550.pdf

[vi] C. Huitema, "Real Time control Protocol (RTCP) attribute in Session Description Protocol (SDP)," Network Working Group, October 2003. https://tools.ietf.org/html/rfc3605