catalyst communications technologies

Technology Milestones

Transcoded Encryption

Catalyst explored security considerations as part of its SBIR Award from the Department of Homeland Security to develop a Broadband Interoperability Platform (BIOP) that would allow communications between end users on different push-to-talk systems on broadband networks, such as FirstNet® Built with AT&T and Southern Linc's CriticalLinc™. We recognized an environment where Push-to-Talk over Broadband (PTToB) systems would not be making deep, system-level connections any time in the near future. Given the diverse mix of 3GPP and proprietary PTToB solutions available in the market, the BIOP that connects them must function as a neutral gateway for managing agency traffic between systems. The gateway must be able to obtain and protect access credentials and cryptographic information for each system with which it interfaces. For this reason, in addition to having a compatible interface (messaging, vocoders, etc.) a BIOP must be given access credentials by **each** interoperating system in order to provide interoperability between agency users on two or more systems.

We developed considerable insight into the current PTToB encryption capabilities specified by the 3GPP standards, implemented to varying levels of completeness by the major service providers. Our research pointed to the following major policy elements that should be considered for the BIOP solution for encrypted, cross-system PTToB services. Conclusions we present are:

September 2025

1. Utilize a "Transcoded BIOP" solutions for encrypted cross-system PTToB services. Recognize that this mode of operation will need to be the dominant mode for several years to come for 3GPP-compliant services and is required to accommodate non-3GPP PTToB services.

2. Leverage the BIOP to serve as a Security Gateway providing edge protection for security and policy functions and provide proxy capabilities to hide network topologies as well as accommodations for non-3GPP standard interfaces.

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. Some carriers and vendors have embraced the 3GPP encryption recommendations more completely than others, such that **there are significant differences in how each PTToB solution implements encryption**. The transcoded approach helps to mitigate issues caused by varying encryption implementations for both media and signaling by making the BIOP the endpoint for each interoperable PTToB system, but these varying encryption mechanisms between solutions are just another example of an interoperability barrier that the BIOP must overcome.

Our analysis emphasized the 3GPP standards for MCPTT which began to address the need for interoperability in 2018 (Release 15). Unfortunately, the rollout of PTToB service offerings in the United States has significantly outpaced the development of standards. The evolving standards created by 3GPP for interoperable encryption (including Release 17 in 2021 and 2022) depend on complex server-to-server interfaces that won't be implemented by US carriers in the short term who report to be currently implementing portions of Releases 13 to 15, depending on the carrier. Our recommendation is to leverage portions of these established, deployed standards to create a BIOP that can be used on current PTToB service offerings.

Our objective for this project was to create a solution that supports 3GPP standards-compliant offerings but can also accommodate proprietary PTToB service offerings as well. To allow interoperability between standards-compliant and proprietary services, the BIOP needs to act as the endpoint for security mechanisms of the non-3GPP system as well as the 3GPP-compliant system, protecting the security of data for each.

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.

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 as shown below in Figure 1. Our research indicates that a much cleaner and more flexible BIOP solution that leverages existing security mechanisms without E2EE for the intervening years is what is required to meet the needs of Public Safety and Federal agencies.

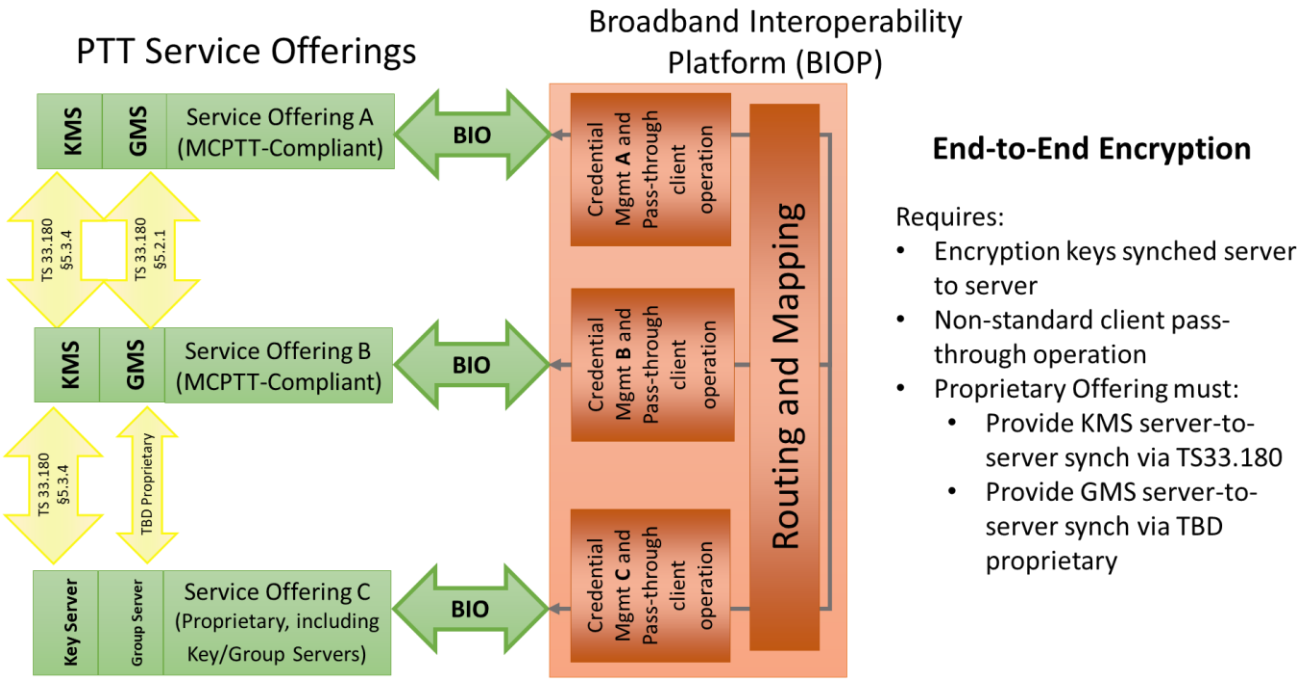

Figure 1 - End-to-end Encryption with Server-to-Server KMS and GMS Connections

In the land mobile radio (LMR) industry, there is a certain degree of dogma associated with the concept of end-to-end encryption and as we move forward to integrate LMR with other systems, its necessity needs to be able to survive technical scrutiny. We have heard uncompromisingly over the years about the need for end-to-end encryption for Project 25 LMR systems so that critical communications can be kept secure. Catalyst agrees with that requirement for LMR, but as we ponder the unification of LMR and broadband as well as broadband-to-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 (i.e., 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 "tricks" 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 was 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 forever.

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.

The effort required to develop a Transcoded BIOP encryption solution will be markedly lower than the effort required to develop E2EE. The main issue related to transcoded encryption will be hardening the BIOP both programmatically and physically for the proper protection, handling, and disposal of cryptographic materials, but these efforts are focused within the BIOP itself and thus will cause minimal change or impact to PTT service offerings. 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. Figure 2 below again helps to visualize the transcoded encryption approach, without a server-to-server connection.

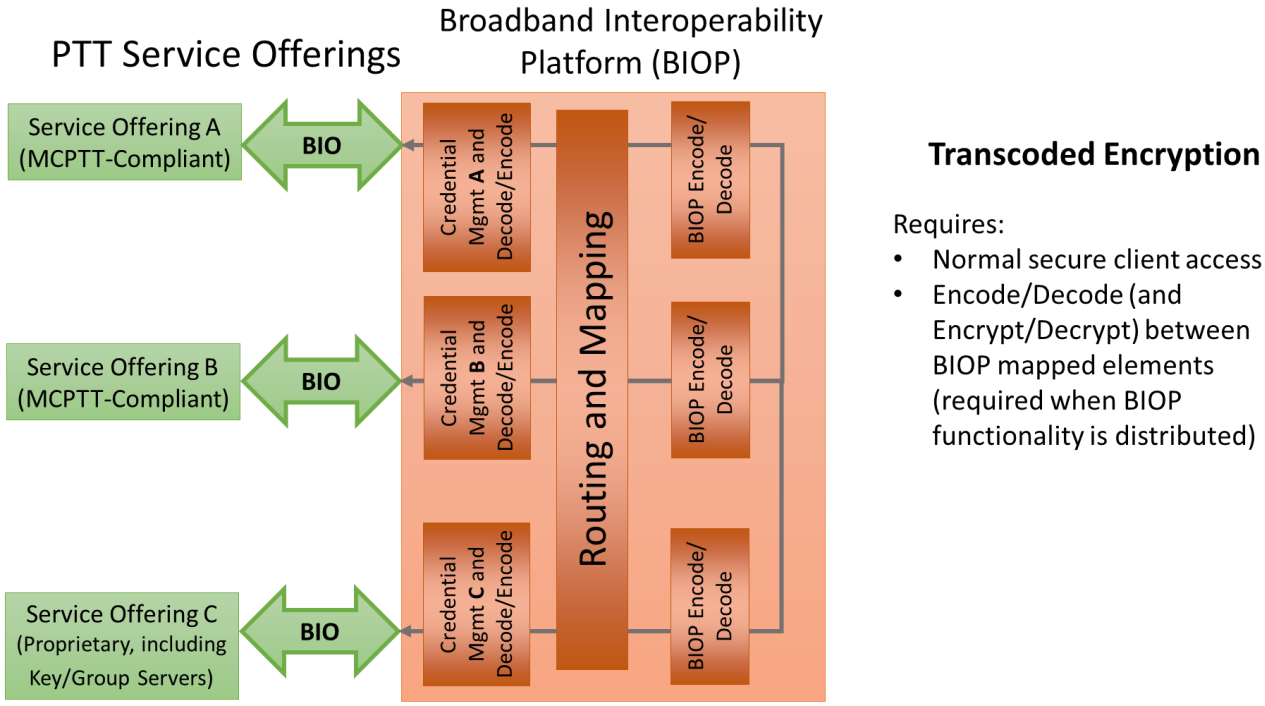

Figure 2 - Transcoded Encryption without Server-to-Server Connections

An important advantage of transcoded encryption is that it utilizes the existing authentication, authorization, and encryption mechanisms across multiple service providers whether 3GPP-compliant or proprietary. Another advantage of transcoded encryption is that it "unhooks" the BIOP from the 3GPP standards process such that BIOP implementation will not have to wait for a particular release (or adoption of same by the service providers) in order to provide encrypted MCPTT across multiple PTToB systems.