MOTOROLA SOLUTIONS

WAVE™ Security

Keeping your critical communications safe

STATEMENT OF CONFIDENTIALITY / DISCLAIMER

The information disclosed herein is confidential and proprietary to Motorola Solutions, Inc., and is being furnished under a valid license agreement. This document may not be disclosed to third parties without the prior written consent of Motorola Solutions, Inc. The recipient of this document shall respect the security status of the information.

Version 1.2

Introduction

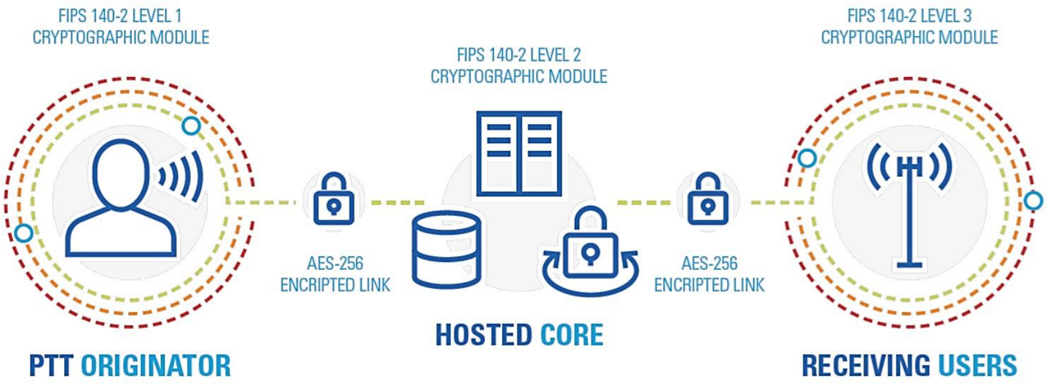
Protecting critical communication from unauthorized access is key to the success of any business, organization, or government agency. That's why WAVE™, Motorola Solutions' cloud-based, carrier-independent broadband push-to-talk (PTT) service supports multiple levels of authentication and security to keep your sensitive communication private and protected.

Security for Broadband PTT

WAVE provides comprehensive security at both the device and the network. With an end-to-end approach to security, we ensure that all broadband PTT voice traffic and signaling information remains free from unauthorized eavesdropping, monitoring or recording, and that WAVE users can make secure PTT calls across the globe on any 4G/LTE, 3G, or Wi-Fi network.

Network-level

WAVE utilizes FIPS 140-2 Level 2 compliant cryptographic algorithms to protect users from unauthorized call interception and monitoring, as well as providing secure alerting and contact management. During the Transport Level Signaling (TLS) and Datagram Transport Layer Security (DTLS) handshakes, the WAVE PTT mobile application and server negotiate the level of security supported during both signaling and media sessions.



The following security functions are supported in the cryptographic libraries of the WAVE PTT mobile application:

- All signaling, media and administration data sessions negotiate with servers using the highest level of encryption: Advanced Encryption Standard (AES)-256
    - Signaling (SIP)

  - Media (RTP/RTCP)
  - HTTPS admin data
- Authenticated ciphers supported:
  - AES_128_CBC_SHA
  - AES_256_CBC_SHA

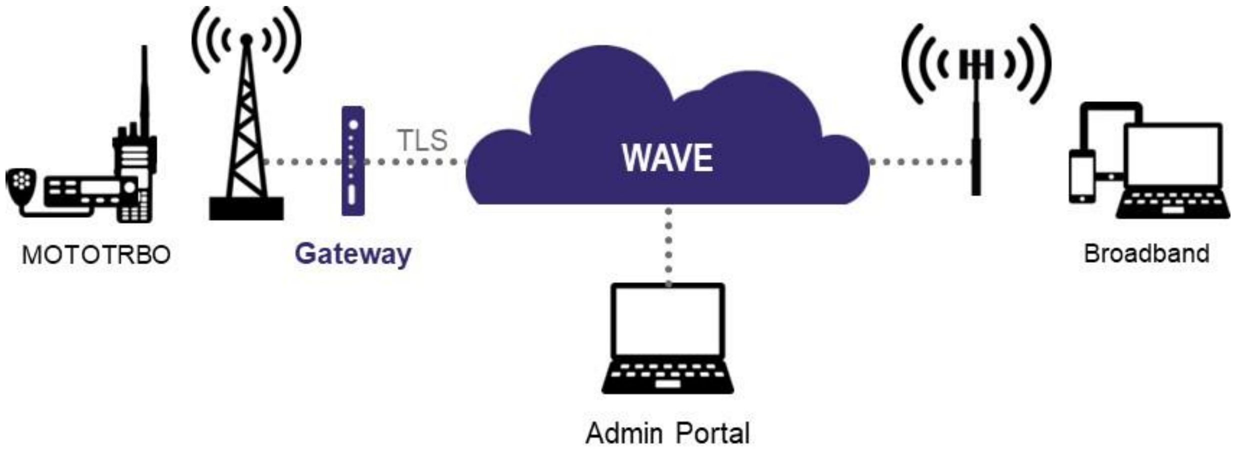
AES-256 is used to encrypt all voice traffic and signaling information traveling between the Broadband PTT application and the gateway server at the broadband PTT data center. Sessions are decrypted and intelligently distributed to the appropriate Broadband PTT servers. PTT communications leaving the data center toward the end devices are re-encrypted in compliance with FIPS 140-2 cryptographic modules, ensuring that all communications between the data center and PTT user devices remains secure.

Device-level

On the device, the broadband PTT application uses the Advanced Encryption Standard (AES)-256 to encrypt all locally stored data, including authentication credentials, configuration, and settings. The locally stored data can be decrypted by the WAVE PTT mobile application only on the specific device on which it was encrypted, and the PTT application will not log sensitive data such as username, password, configuration values received from the server, or PTT application configuration values.

Security for LMR Interoperability

Providing seamless communications between broadband PTT users and those on Land Mobile Radio (LMR) networks introduces a new component, the WAVE Gateway to the configuration. The Gateway, deployed at the customer premise, uses TLS to provide a secure connection to the WAVE server. HTTPS is used for the secure exchange of configuration information between the Gateway and the portal.



Summary

WAVE offers a highly scalable and simplified approach to ensure maximum security for your sensitive communications. First, WAVE resides in geographically dispersed data centers that follow the SSAE 16, PCI DSS, and HIPPA security compliancy standards. Second, our end-to-end methodology utilizes FIPS 140-2 cryptographic modules, AES-256 encryption for all voice and data signaling, ensuring that all your critical PTT communications remain secure, available only to the originator and the intended recipients.