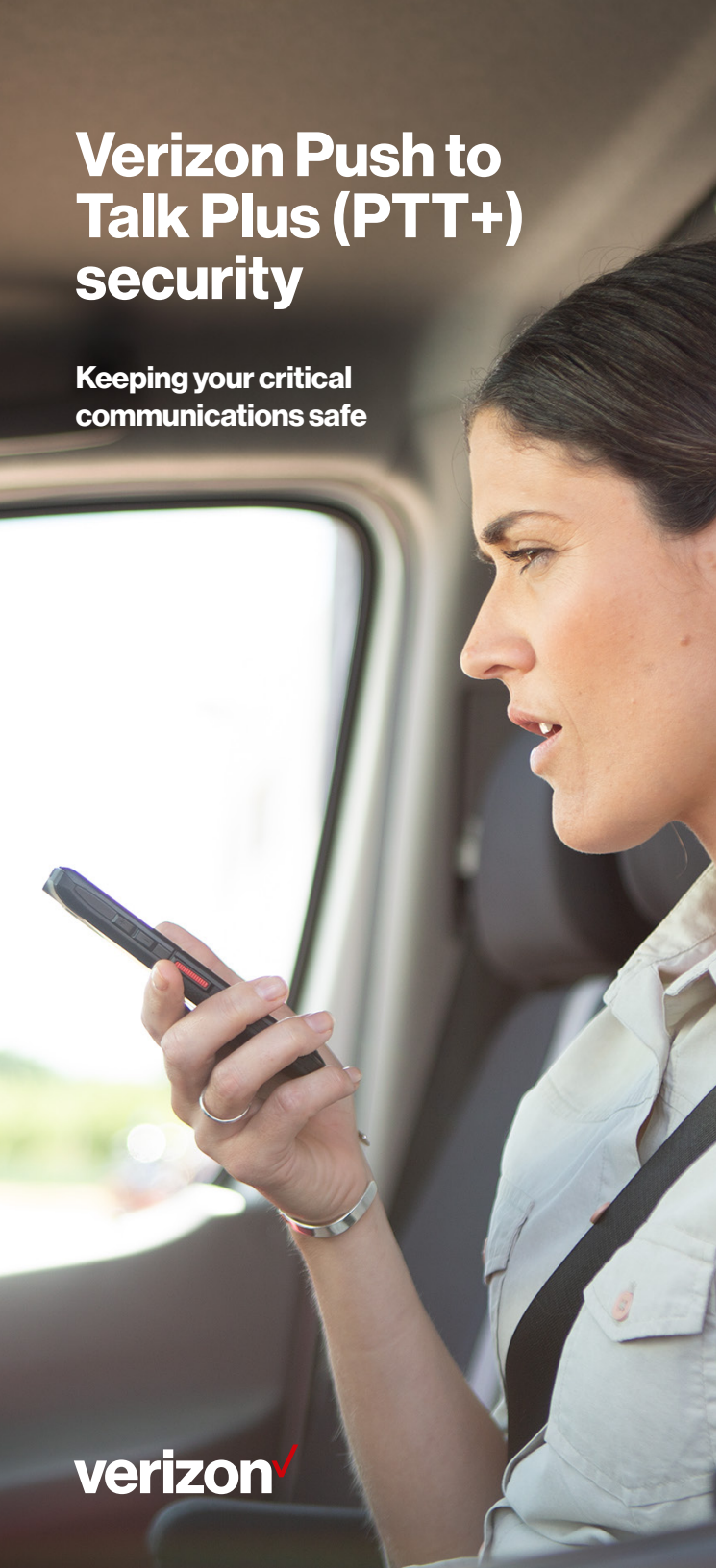


Verizon Push to Talk Plus (PTT+) security

Keeping your critical communications safe

verizon

Introduction

Protecting critical communication from unauthorized access is key to the success of any business, organization or government agency. That's why Verizon supports multiple levels of authentication and security to keep your sensitive communication private and protected.

Security for Verizon Push to Talk Plus

The Verizon Push to Talk Plus (PTT+) solution provides comprehensive security at both the device and network levels. With an end-to-end approach to security, Verizon helps protect PTT+ voice traffic and signaling information traveling over Wi-Fi networks from unauthorized eavesdropping, monitoring or recording.

Network level

Over Wi-Fi networks, Verizon uses Federal Information Processing Standards (FIPS) 140-2 level-1–compliant cryptographic algorithms to help protect users from unauthorized call interception and monitoring, as well as to provide secure alerting and contact management.

The Verizon PTT+ 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 Verizon PTT+ application and are used under the following conditions:

- PTT+ over Wi-Fi:

  Call signaling, media and contact/group management sessions negotiate with servers using FIPS 140-2 level-1 validated ciphers: Advanced Encryption Standard (AES)-256 within Transport Layer Security (TLS) v 1.2.

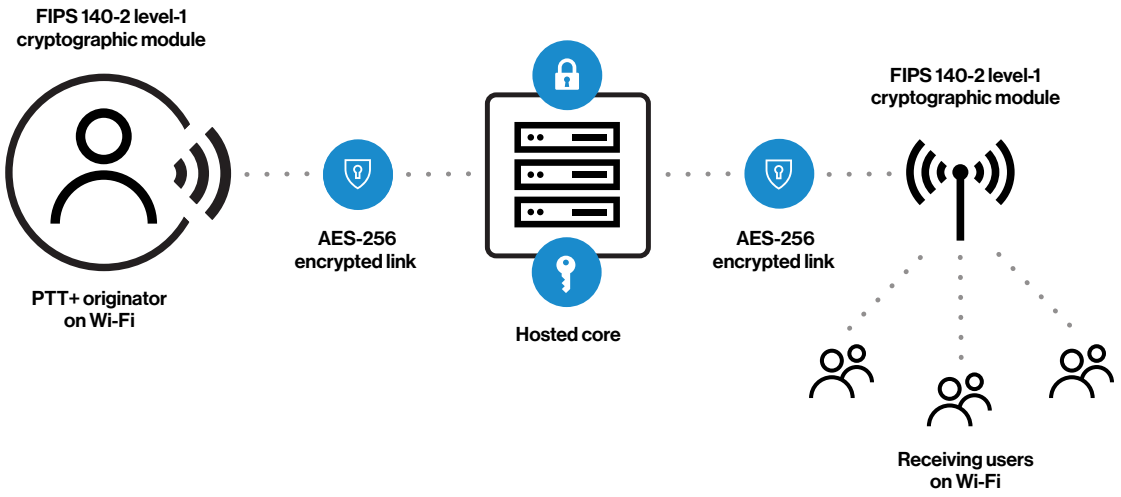
  – Signaling: Session Initiation Protocol (SIP)

  – Media: Real-time Transport Protocol (RTP)/ Real-time Transport Control Protocol (RTCP)

  – HTTPS XML Configuration Access Protocol (XCAP) data

- PTT+ over 4G LTE/cellular:

  Call signaling and media travel over plain User Data Protocol (UDP), using the security inherent in the Verizon 4G LTE network. Contact and group management is conducted over HTTPS/TLS v 1.2 using FIPS 140-2 level-1 validated ciphers.



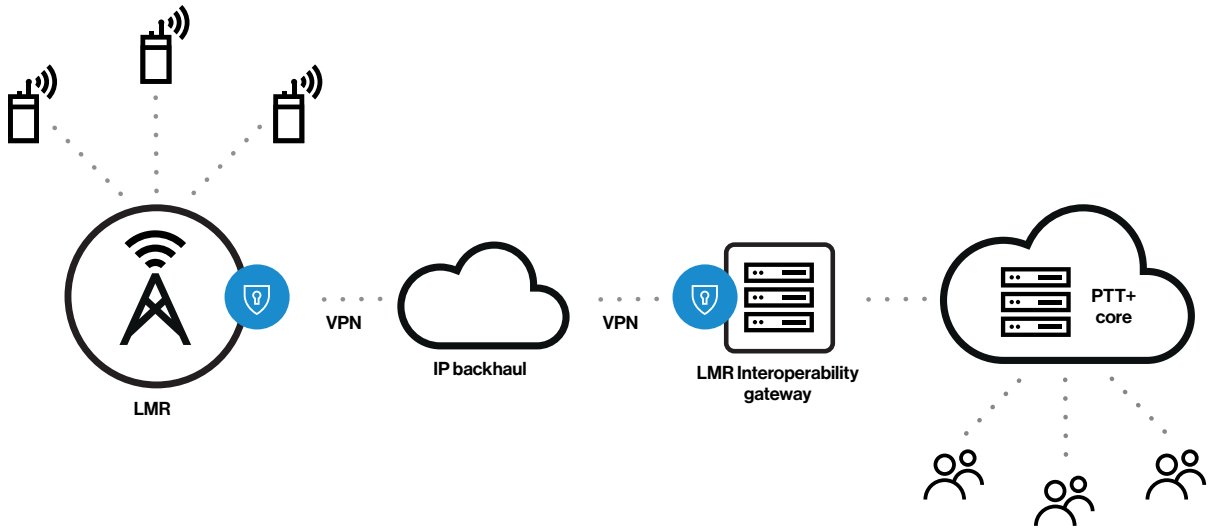
AES-256 is used to encrypt Wi-Fi voice traffic and signaling information traveling between the Verizon PTT+ application and the gateway server at the data center. Sessions are decrypted and intelligently distributed to the appropriate PTT+ servers. PTT+ communications leaving the data center toward end devices are re-encrypted to maintain compliance with FIPS 140-2 cryptographic modules, helping to keep communications between the data center and PTT+ user devices secure.

Device level

On the device level, the Verizon PTT+ application uses AES-256 to encrypt locally stored data, including authentication credentials, configuration and settings. The locally stored data can be decrypted by the PTT+ 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 Land Mobile Radio (LMR) Interoperability

Providing seamless communications between Verizon PTT+ users on Wi-Fi networks and those on Land Mobile Radio (LMR) networks calls for a new component, the interoperability gateway to the system. While the interoperability gateway is linked to the PTT+ server through a direct and dedicated connection, the link between the gateway and the customer's LMR system requires the use of a virtual private network (VPN) tunnel with AES-256 encryption.



VPN

A VPN provides a simple and widely available method to extend specific internet traffic between two networks securely. VPNs supported on the interoperability gateway have the following requirements:

- Site-to-site VPN (one to primary and one to geo)
- Dynamic Multipoint VPN (DMVPN)
- IPsec over Generic Routing Encapsulation (GRE)
- Border Gateway Protocol (BGP) or Open Shortest Past First (OSPF) running inside the VPN tunnels
- Public IPs to public IPs (Traffic from P25 systems must come with Network Address Translation, so the gateway only sees public IPs.)

Encryption

Verizon PTT+ calls to LMR users are encrypted while traversing the Wi-Fi network. The session is terminated at the interoperability gateway and decrypted due to the differences in voice codecs used by PTT+ and LMR. Once decrypted, the audio is then inserted into the 256-bit encrypted VPN tunnel and forwarded to the LMR system.

Summary

Verizon offers a highly scalable and simplified approach to help keep your sensitive communications private and protected. First, the Verizon PTT+ solution resides in geographically dispersed data centers that follow the Statement on Standards for Attestation Engagements (SSAE) No. 16, Payment Card Industry Data Security Standard (PCI DSS) security compliance standards. Second, the PTT+ end-to-end methodology over Wi-Fi networks utilizes FIPS 140-2 cryptographic modules, AES-256 encryption for noncellular voice and data signaling, and VPN tunnels for connections to customer premises components to help keep your critical PTT+ communications secure and available only to the originator and the intended recipients.