Name : Carlos Fernandez
Email: cfernandez@tasstaamericas.com
Contact: +1 (917) 816-4057

TASSTA Americas
3400 Lakeside Dr. # 510 | Miramar | FL | 33027

Date: April.09.2024

To whom it may concern

Subject: Encryption on TASSTA Americas PTT platform

TASSTA is a German company with more than 10 years in the radio communications market and has the cutting-edge technology for "Mission Critical" radio communication systems with the MCPTT (Mission Critical PTT) Platform on public and private LTE networks. The system supports encryption with the highest level of reliability approved by the standard.

TASSTA has a strategic agreement with Servivasa for security communications systems and is the technology behind the PTT ONE brand.

TASSTA is certified by FIRSTNET in the United States, which is a requirement to be used by American law enforcement. As part of the FIRSTNET certification process, the tool must comply with requirements for source code security, application distribution, and encryption in transit.

Below, we set out the security guarantees that TASSTA provides to its Public Safety clients.

Cybersecurity and source code protection

TASSTA follows NIST guidelines based on cybersecurity best practices. The National Institute of Standards and Technology (NIST) standards help organizations protect their data and network.

During software generation, TASSTA uses *Micro Focus Fortify*, which ensures that the software meets compliance objectives for internal and external security mandates, including 800+ vulnerability categories for SAST that enable compliance with standards such as OWASP Top 10, CWE/SANS Top 25, DISA STIG, and PCI DSS.

Security in the distribution of the application

Regarding the delivery of the application to the end customer, we are approved for:

- The Google Play Store is the world's first distribution platform for Android apps. All Android apps undergo rigorous security testing before appearing on Google Play.

- The Apple App Store reviews all apps and app updates submitted to the App Store to determine if they are reliable, work as expected, respect user privacy, and are free of malicious content. TASSTA for iOS has successfully passed the review and is available in the store.

Of course, TASSTA can deliver the Android APK application to the end customer for distribution outside the public application system.

Encryption of communications

The secure and private use of the TASSTA application on third-party networks is ensured by encrypting all data exchanged at a transport layer using TLS 1.2 with military-grade AES 256 encryption keys.

It should be noted that there is an additional layer of protection, which is normally used in highly sensitive organizations, such as the Armed Forces, which is another military-grade AES256 encryption at the application layer. Individual users can create and distribute keys so that they can talk privately without any other user of the system being able to eavesdrop, not even such communications are available to TASSTA or the system's recorders.

Application Access Protection

Access to the TASSTA server is protected by username/password with the possibility of using the IMEI of the devices as a second authentication factor. This will prevent someone from logging in with potentially stolen credentials if they use a different device.

I thank you in advance for the attention you will be given to this letter. I reiterate my willingness to answer any questions or queries and we attach a presentation about our company

Best regards,

Carlos Fernández Alonso, CEO