The Privoro SafeCase

The first high-security, intelligent smartphone case.

Smartphone vulnerabilities continue to plague security professionals as threat actors turn to these devices as a vehicle to access sensitive organizational information. From the chip layer, to firmware, operating system and apps, the entire ecosystem of these mobile devices is under constant attack.

Enter the Privoro SafeCase, the first smartphone case to enable truly trusted services around off-the-shelf mobile devices, beginning with the iPhone 7 and 8.

The SafeCase and supporting solution elements.

TRUSTED HARDWARE

High-security hardware – isolated from a user's smartphone

ANTI-SURVEILLANCE

Protection against audio and video surveillance

SECURE MANAGEMENT

Cloud-integrated policy management tools

PRIVORO®

The SafeCase Technical Detail

TRUSTED HARDWARE

Hardware root of trust

- A unique key pair is generated, bound and exclusively contained within a single secure chip.
- Built and provisioned within a US-based, ITAR-compliant facility utilizing embedded supply-chain protections.

Trusted execution environment

- Secure boot
- Secure firmware
- Secure updates
- Code signing

Tamper protection

- The SafeCase is physically sealed and tamper-resistant.
- The SafeCase has a variety of protections against side-channel attacks.

Isolated components

- Closed-system architecture.
- The SafeCase's processor is used exclusively for running authenticated firmware.

Motion sensors

A nine-axis inertial measurement unit (IMU) – which includes a three-axis gyroscope, accelerometer and magnetometer.

Wireless data technologies

WiFi, Bluetooth and NFC – enable communication with local devices, including the paired smartphone.

- Permanent wireless disablement option available.

Digital signal processor

- For audio quality, voice masking and audio path control.

GPS module

- Enables location tracking for policy management purposes.

ANTI-SURVEILLANCE

Protection from audio and video surveillance

- Audio protection: The SafeCase utilizes patented, proprietary technology to ensure that a conversation's content (the words spoken) and context (accents, tones, number of participants, etc.) are unidentifiable to even the most sensitive audio forensic equipment.
  - High-security, TRNG-based audio masking
  - Adaptive audio masking
  - Microphone-specific jamming
- Camera/video protection: A physical barrier over each of the smartphone's cameras prevents unwarranted third parties from observing or recording any visual data in the device's vicinity.

SECURE MANAGEMENT

Cloud-integrated management tools

- User management: The Portal provides administrative tools to manage new and existing users.
- Device management: The Portal allows for optional automated provisioning and status tracking.
- Policy management: The Portal makes it easy to establish and enforce policies at the individual, group or organization level.
- Non-repudiation: SafeCase events are recorded in a non-repudiable audit log.

Secure Communications

- Dual-tunnel encryption: Secured using a NIST-compliant, third-party-reviewed cryptographic architecture.
- Use of NIST-approved algorithms at CNSA-approved strengths to provide high assurance against cryptographic attacks.
- Perfect forward secrecy: Unique keys for each communication session are generated from verified ephemeral keys to protect communications against future compromise of participant's identity keys.

MODULAR BACKPACKS

Extending SafeCase functionality and specialized services

Additionally, SafeCase's processing, sensing and communication capabilities serve as building blocks for the development of additional features and services, both via the SafeCase itself or through detachable hardware backpacks. Privoro welcomes third party inquiries who wish to build on the SafeCase platform.

PRIVORO®