

Soteria-G3

Summary

Soteria-G3 is the firmware that implements the hardware cryptography in the CEC173x Trust Shield family of real-time root of trust controllers. Soteria-G3 plus the CEC173x can be used in conjunction with any Application Processor (AP) to extend the root of trust and enforce a secure boot process in the platform.

Key Features

Secure Boot

Soteria-G3 supports NIST 800-193-compliant secure boot and secure updates for up to two APs in parallel to ensure boot firmware authenticity.

Multi-SPI Image Support

Soteria-G3 supports multiple code images that can optionally be stored in separate external SPI Flash devices. Images and encryption are user configurable.

Golden SPI Image Support

It also supports reading backup images (also known as golden images) in the event of an update failure or code compromise.

SPI Bus Monitoring

It allows real-time monitoring of data bus traffic to enforce user-customized rules for what opcodes are allowed to run.

Key Revocation

Soteria-G3 allows up to 32 unique public/private key pairings to replace a compromised private key.

Rollback Protection

After any firmware update, older versions of code can be prevented from running in the future to prevent exploitation of previously patched security vulnerabilities.

Crypto Library Support

Soteria-G3 supports a suite of asymmetric cryptographic algorithms, including:

- SHA-2, SHA-256 and SHA-512
- RSA-1024 to RSA-4096
- ECDSA and EC-KCDSA
- Ed25519

I²C Platform Communications

Soteria-G3 supports I²C as a peripheral host interface. This interface enables Security Protocol and Data Model (SPDM)-compliant attestation, firmware image crisis recovery, debug modes and NIST 800-193 Platform Firmware Resiliency guidelines.

Transfer of Ownership

When refurbishing or transferring a platform, the original owner can initiate an ownership transfer command to protect their device secrets. The original owner's private key encrypts this command. It can be initiated via arbitration or after the platform has been transferred.

Lifecycle Management

A platform may have one or more owners over its lifetime. Each owner may customize the images that are permitted to run on the system. Lifecycle management protects features and secrets at every stage of the lifecycle, including raw, test, development, production, Return Merchandise Authorization (RMA) and End of Life (EOL).

Secure I²C/UART Crisis Recovery

A crisis occurs when a system is unable to advance past secure boot due to corruption or the unavailability of code images. Soteria-G3 supports recovery from a crisis by using a command that is encrypted by the owner's private key to force an image update.

Attestation Support

Soteria-G3 leverages the CEC173x's SRAM-based Physically Unclonable Function (PUF) to enable SPDm-compliant component attestation.

Certifications

Soteria-G3 code is cleared by MISRA, checked by Coverity® and CERT® C code analysis and certified by third-party penetration tests.

Availability

Soteria-G3 is available through a Software License Agreement with Microchip. Contact your [local sales representative](#) for more information.

Learn More About the Trust Shield Solution

- [Trust Shield Family Sell Sheet](#)
- [Trust Shield Product Page](#)

Soteria - G3 Firmware Topography

