CYPRESS

PSoC® 6
THE SECURE MCU

PSoC 6 MCUs incorporate a hardware-based root-of-trust and hardware-accelerated cryptography enabling embedded security for the IoT Edge. PSoC 6 MCUs support:

Secure Storage
- Protect Identity
- Protect cryptographic keys
- Protect firmware
- Protect data at rest

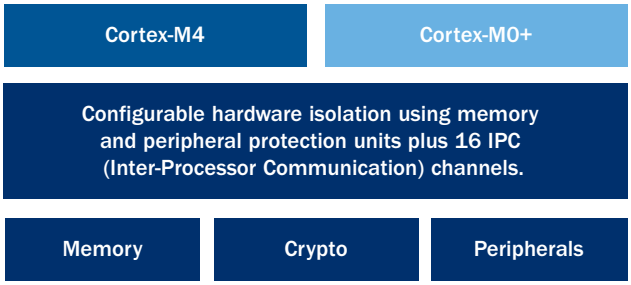
Secure Operation
- Secure device onboarding
- Secure authentication
- Secure boot
- Secure firmware updates

Secure Communication
- Protect transmitted data
- Authenticate data packets

PSoC® 6 FEATURES

SECURITY FEATURES
- Secure execution environment for trusted applications
- Incorporated secure-element functionality with isolated cryptographic operations and isolated key storage
- Hardware-accelerated cryptographic operations include AES, 3DES, RSA, ECC, SHA-256 and SHA-512, and True Random Number Generator (TRNG)
- Optional pre-installed credentials for secure boot

MICROCONTROLLER FEATURES
- Asymmetric dual-core Arm® Cortex® -M4 (150 MHz) and Arm Cortex-M0+ (100 MHz)
- Up to 4096KB Flash, 512KB SRAM
- Industry-leading ultra-low power design that consumes as little as 22-µA/MHz in active power mode
- Best-in-class flexibility with wired and wireless connectivity options, software-defined peripherals, and CapSense® capacitive sensing



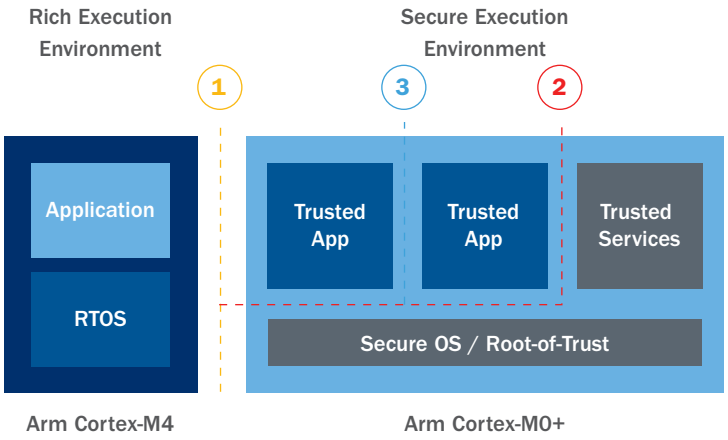
Hardware Isolation within PSoC 6

WWW.CYPRESS.COM/PSOC6SECURITY

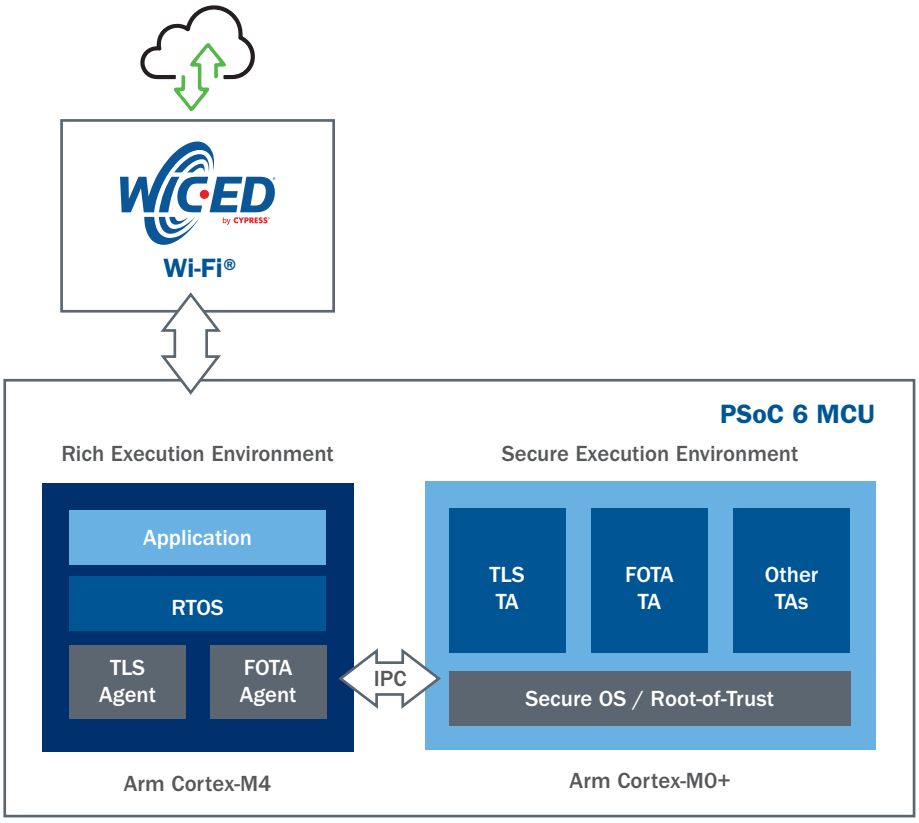
CYPRESS EMBEDDED IN TOMORROW™

HARDWARE-BASED ISOLATION

1. Secure Execution Environment: PSoC 6 MCUs provide a secure execution environment for trusted applications. The Cortex-M0+ core is dedicated to this environment. It communicates to the Cortex-M4 that supports the rich execution environment through IPC channels.
2. Root-of-Trust Isolation: Root-of-Trust operations and trusted services are further isolated within the secure execution environment, protecting the integrity and confidentiality of the root-of-trust.
3. Trusted Application Isolation: Each Trusted Application within the secure execution environment can be isolated from each other, reducing the available attack surface.



SECURE IoT APPLICATION EXAMPLE



In this example, the general application runs in the rich execution environment. To set up a secure TLS (Transport Layer Security) connection and to support a secure Firmware-Over-the-Air (FOTA) update feature, TLS and other trusted applications operate in the secure execution environment. Isolation between the trusted apps further reduces the attack surface. Other TAs can be added to support unique security functions required by the cloud application.

LEARN MORE WWW.CYPRESS.COM/PSOC6SECURITY

Cypress Semiconductor Corporation
198 Champion Court, San Jose CA 95134
phone +1 408.943.2600 fax +1 408.943.6848
toll free +1 800.858.1810 (U.S. only) Press “1” to reach your local sales representative

002-22926 Rev.*A