

Cypress PSoC® 64 Secure Microcontrollers

THE FOUNDATION FOR IoT SECURITY

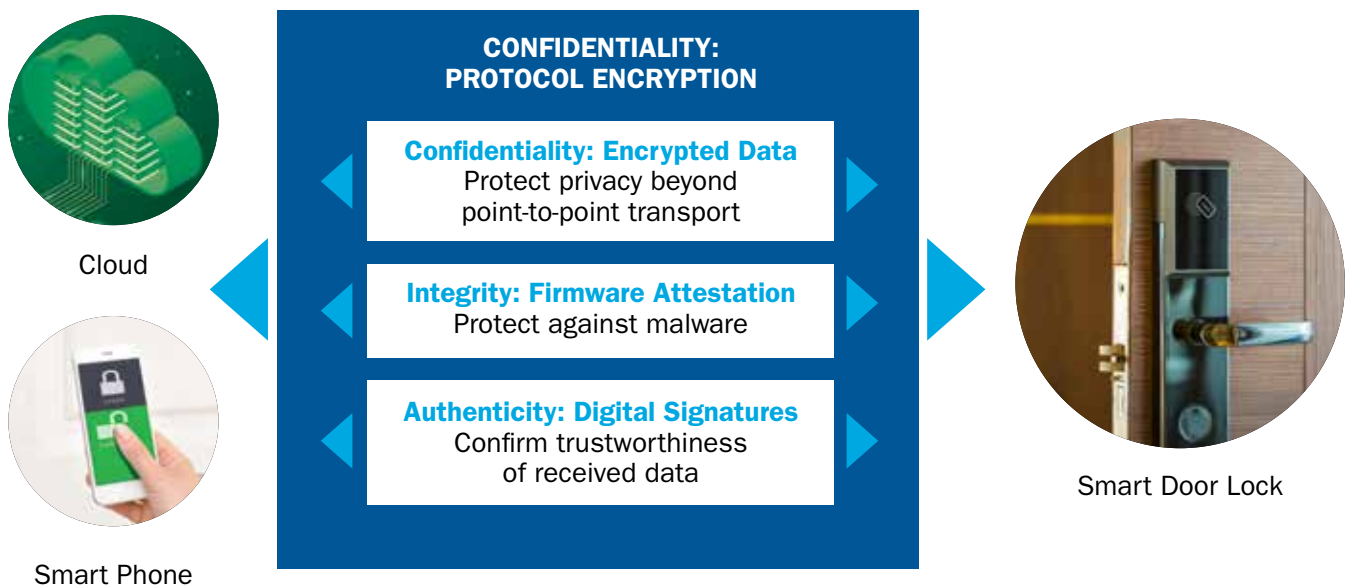
WWW.CYPRESS.COM/PSOC6SECURITY



SECURITY MATTERS FOR IoT APPLICATIONS

DESIGNING SECURE IoT DEVICES IS COMPLICATED

Hacks, data breaches, security vulnerabilities. News headlines regarding security are becoming an every day occurrence in this constantly-connected world. It isn't a question of whether or not your connected IoT device will be attacked, but a question of when. IoT developers need to incorporate security into their connected product design from the beginning. You can't wait till a security breach destroys your brand reputation to incorporate robust security features.

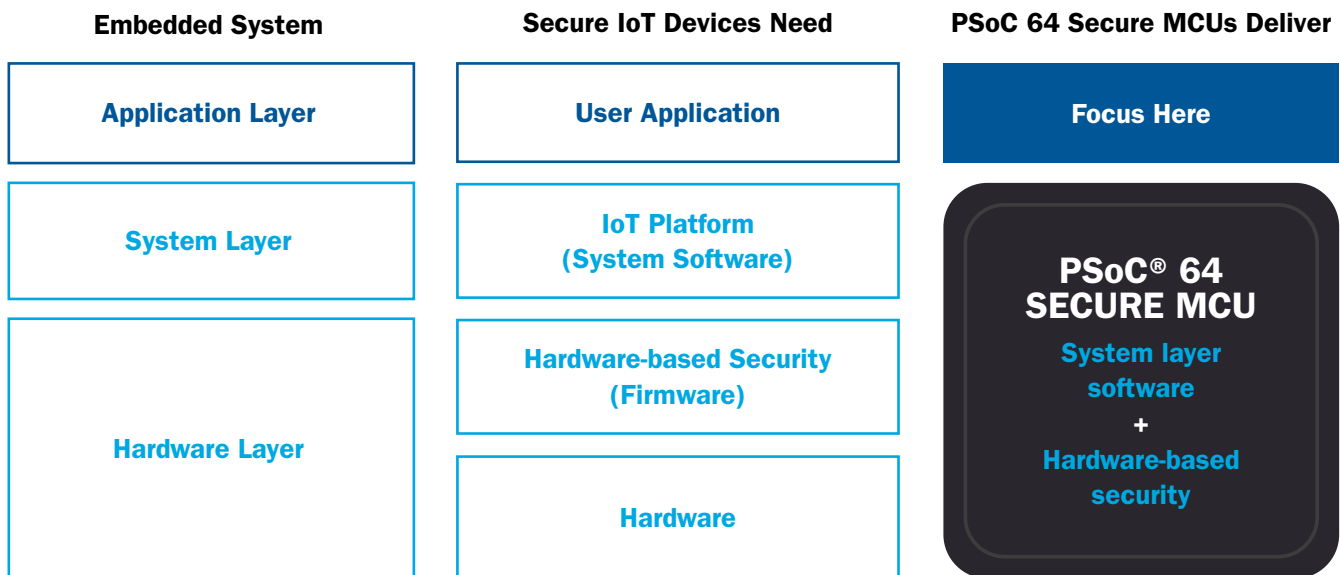


Designing reliable security features into your IoT device can be a daunting task. Let's take the example of a smart door lock. You not only have to worry about user data privacy, but also have to ensure that the lock itself can't be hacked. Adhering to the security principles of Confidentiality, Integrity, and Authenticity, you can build a rock-solid security framework that cannot be compromised.

70% of the most commonly used IoT devices have serious security vulnerabilities¹.

PSoC® 64 SECURE MCUs DELIVER SECURITY THAT JUST WORKS

Consumers expect IoT devices to evolve quickly. They want to see new features and capabilities delivered frequently, ideally using the same hardware platform. The extreme pressure to scale and evolve must be met without compromising quality and security. By using PSoC 64 Secure MCUs, you can focus on your IoT application to deliver the differentiation that your end-product deserves. PSoC 64 Secure MCUs integrate the award-winning, ultra-low-power PSoC 6 architecture with a well-structured, open-source IoT platform software to deliver a solution that works every time, all the time.



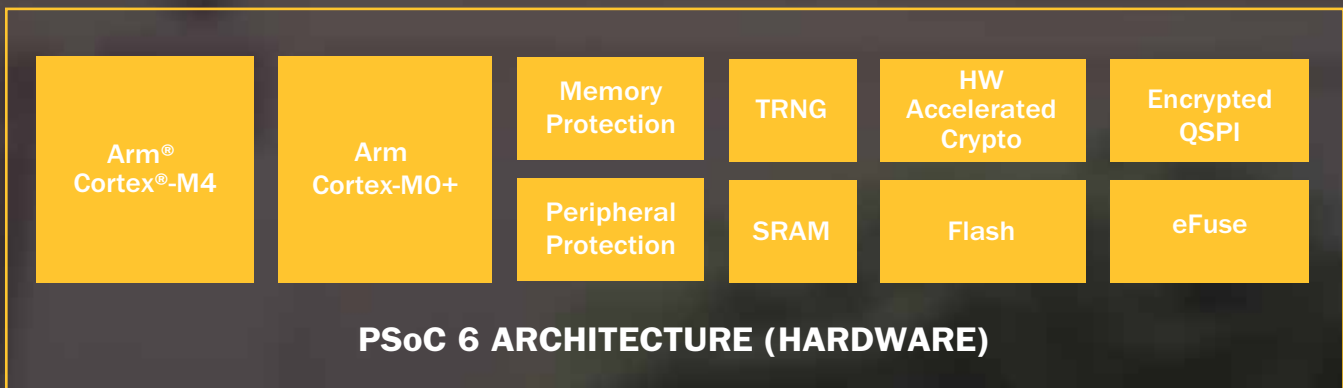
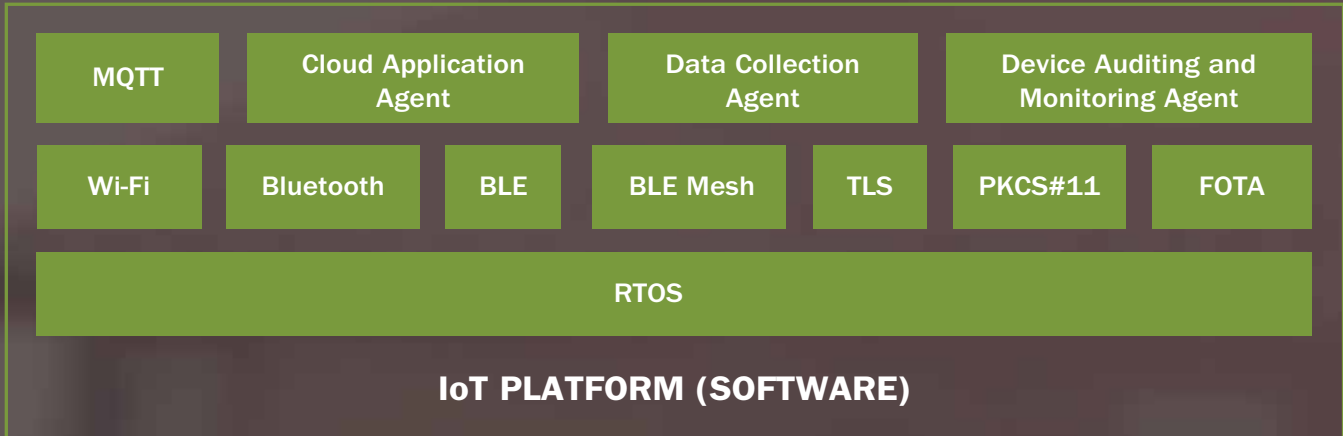
Cypress has an extensive portfolio of industry-leading Wi-Fi connectivity devices that deliver a rock-solid wireless user experience. PSoC 64 Secure MCUs include the communication firmware that supports our Wi-Fi devices. The combination of PSoC 64 Secure MCUs and Cypress' Wi-Fi devices provides a best-in-class IoT application solution.

50%

of enterprise executives believe IoT devices could become their network's most significant security risk².

ACCELERATE YOUR IoT DEVELOPMENT

PSoC 64 Secure MCUs combine IoT platform software, a root-of-trust with secure services, and the ultra-low power, hardware-based security capabilities of the PSoC 6 MCU architecture. By bringing these pieces together, PSoC 64 Secure MCUs provide a secure foundation for cloud-based applications. Combined with Cypress' wireless connectivity devices, you get a total cloud application solution that gets you to market fast.





IoT PLATFORM

IoT platform software consists of fully integrated and validated cloud functions including MQTT, data collection, and device auditing. Secure cloud functions such as Transport Layer Security (TLS), Firmware Over the Air Updates (FOTA), and key management using PKC11 are also included. Wireless stacks supporting Cypress' industry-leading wireless connectivity portfolio are also available.



ROOT-OF-TRUST WITH SECURE SERVICES

The root-of-trust provides the trust anchor to support the secure boot chain of trust, along with additional security services such as mutual authentication, attestation, and other security services.



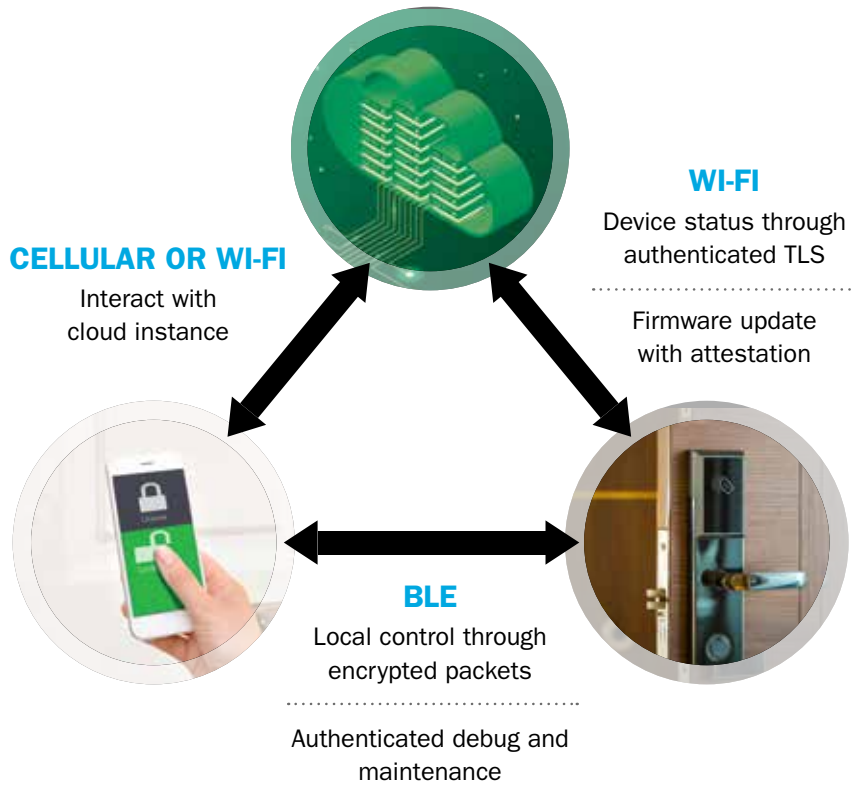
ULTRA-LOW-POWER PSoC 6 ARCHITECTURE

Key hardware features includes isolated resources such as dual cores, hardware accelerated cryptography, true random number generation, memory protection units, peripheral protection units, and non-volatile memory for an immutable identity. The architecture also includes an encrypt-on-the-fly, external flash interface to support secure firmware updates.



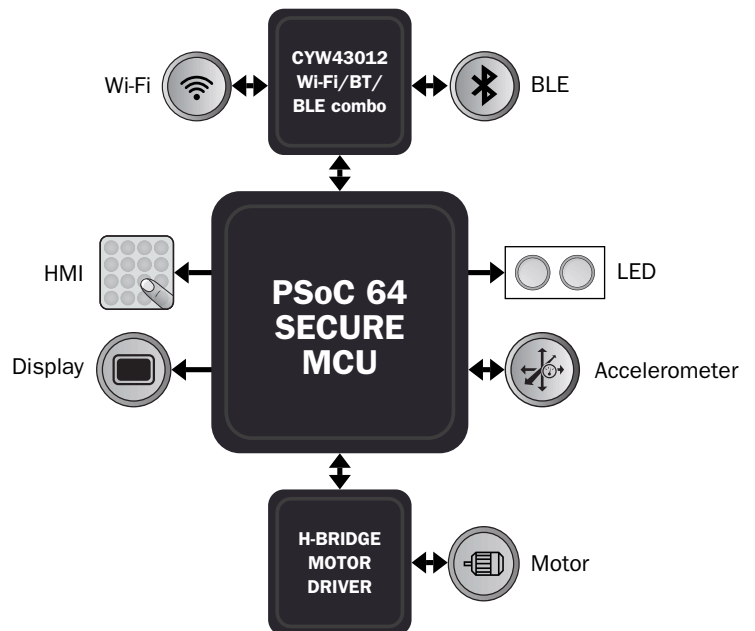
USE CASE EXAMPLE: SMART DOOR LOCK

Below is an example of a smart door lock. The lock is connected through Wi-Fi to the cloud through a secure TLS connection and can be remotely controlled through a mobile device. The lock is authenticated to the cloud and can confirm its hardware and software status through attestation, enabling secure over-the-air firmware updates. In addition, local control of the lock can be performed through an authenticated device using BLE.



SMART DOOR LOCK

- PSoC 64: Ultra-low power, secure dual-core MCU
- CYW43012: Ultra-low power 802.11ac + Bluetooth 5.0 combo
- Maximize battery life
- Integrate HMI and sensor hub functionality with PSoC 64
- Works with any IoT platform and cloud host



PSoC 64 SECURE MICROCONTROLLER PORTFOLIO

PSoC 64 is a line of MCUs within the PSoC 6 family with integrated security functionality. Devices can be pre-configured for secure boot operation, along with options for secure cloud connections.



	PSoC 62/63	PSoC 64	PSoC 64	PSoC 64
Memory	Flash: 512KB - 2MB, SRAM: 160KB - 1MB			
Cryptography	Hardware accelerated: Symmetric: AES, 3DES; Asymmetric: RSA, ECC; Hashing: SHA-256, SHA-512; True Random Number Generator (TRNG)			
Cortex-M4 Fully Open	✓	✓	✓	✓
Cortex-M0 + Fully Open	✓			✓
Secure Boot		✓	✓	✓
Attestation		✓	✓	✓
TLS			✓	✓
FOTA			✓	✓
Integrated Cloud Support			✓	✓
Target Developer	Wants to use secure features in PSoC 6 but will "roll their own" security firmware	Wants a preconfigured device root of trust	Wants secure cloud connectivity that "just works"	Wants standard features but wants to add own trusted applications

PSoC 64 FEATURES

RICH EXECUTION ENVIRONMENT

The Cortex-M4 processor in PSoC 64 MCUs is used to establish a rich execution environment for you to develop your differentiated application. IoT platform software libraries are available to establish secure connection to the cloud.

**PSoC 64
SECURE MCU**

IoT Platform Software
+
Root of Trust and
Secure Services

SECURE EXECUTION ENVIRONMENT

The Cortex-M0+ processor in PSoC 64 MCUs is used to establish a secure execution environment used to perform secure operations isolated from the rich execution environment.

HARDWARE-BASED ROOT-OF-TRUST AND TRUSTED SERVICES

Further isolated within the secure execution environment is a hardware-based root-of-trust with trusted services. The root of trust includes hardware-accelerated cryptography, true random number generation (TRNG), and secure storage. Trusted services that utilize the hardware-based root of trust include secure boot, attestation, Transport Layer Security (TLS), and firmware over-the-air (FOTA) updates.

DEVELOPING YOUR SECURE IoT DESIGN WITH PSoC 64 MCUS

1

DEVELOP YOUR APPLICATION

Develop your IoT application using a full-featured PSoC 6 development kit.



CY8CKIT-062-WIFI-BT (PSoC 6 + CYW4343W)

2

DEVELOP YOUR SECURE BOOT AND PROVISIONING CREDENTIALS

Use a secure MCU to develop the secure properties of your IoT application.



CY8CPROTO-064-SB

3

GO TO PRODUCTION

Cypress has partnered with HSM providers that can help you get your secure IoT design into production. Services include secure device provisioning and key management.



ABOUT CYPRESS

Cypress is the leader in advanced embedded system solutions for the world's most-innovative automotive, industrial, home automation and appliances, consumer electronics and medical products. Cypress' programmable and general-purpose microcontrollers, analog ICs, wireless and USB-based connectivity solutions and reliable, high-performance memories help engineers design differentiated products and get them to market first. To learn more, go to www.cypress.com.

