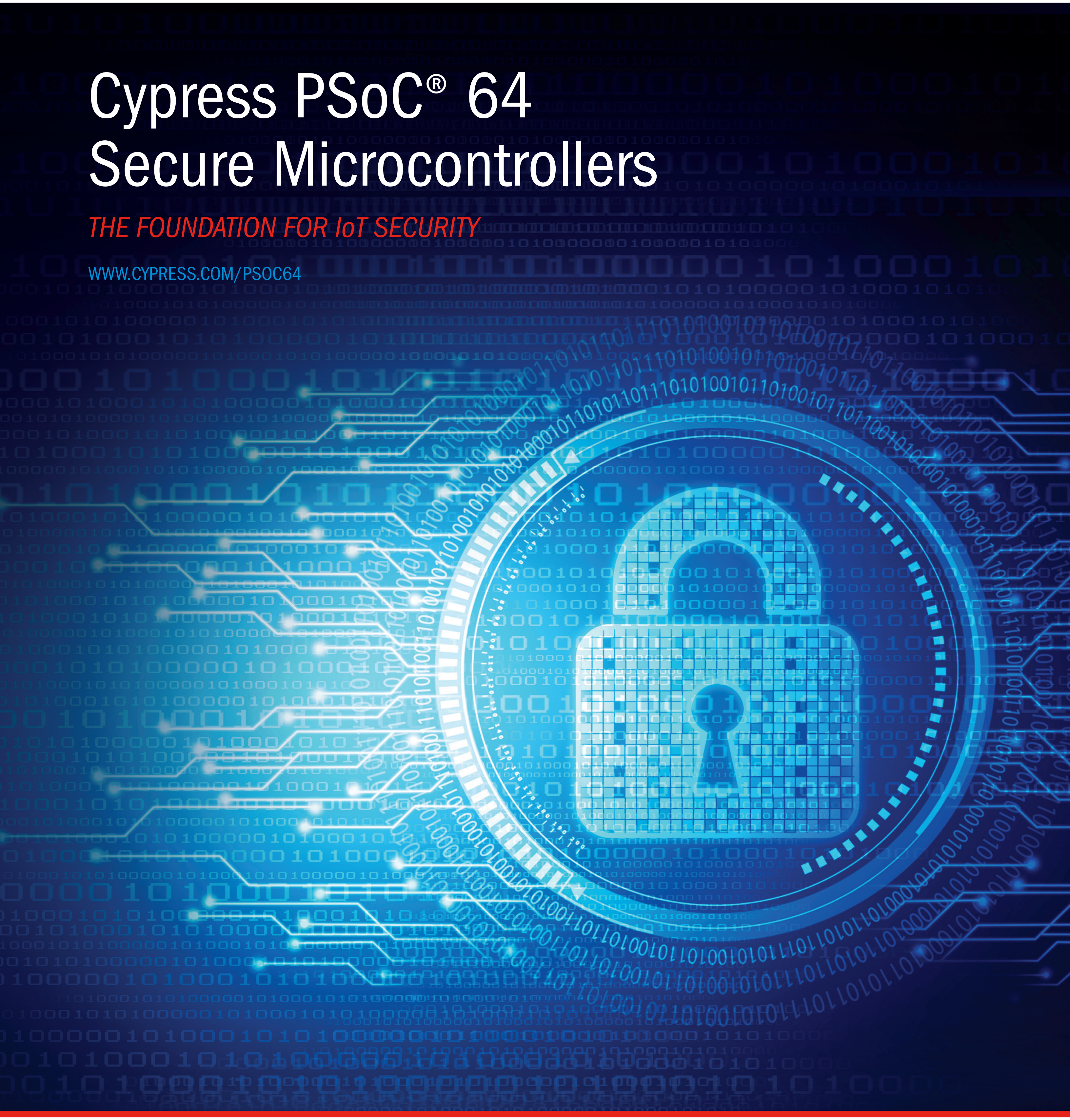
CYPRESS®
EMBEDDED IN TOMORROW™

Cypress PSoC® 64 Secure Microcontrollers

THE FOUNDATION FOR IoT SECURITY

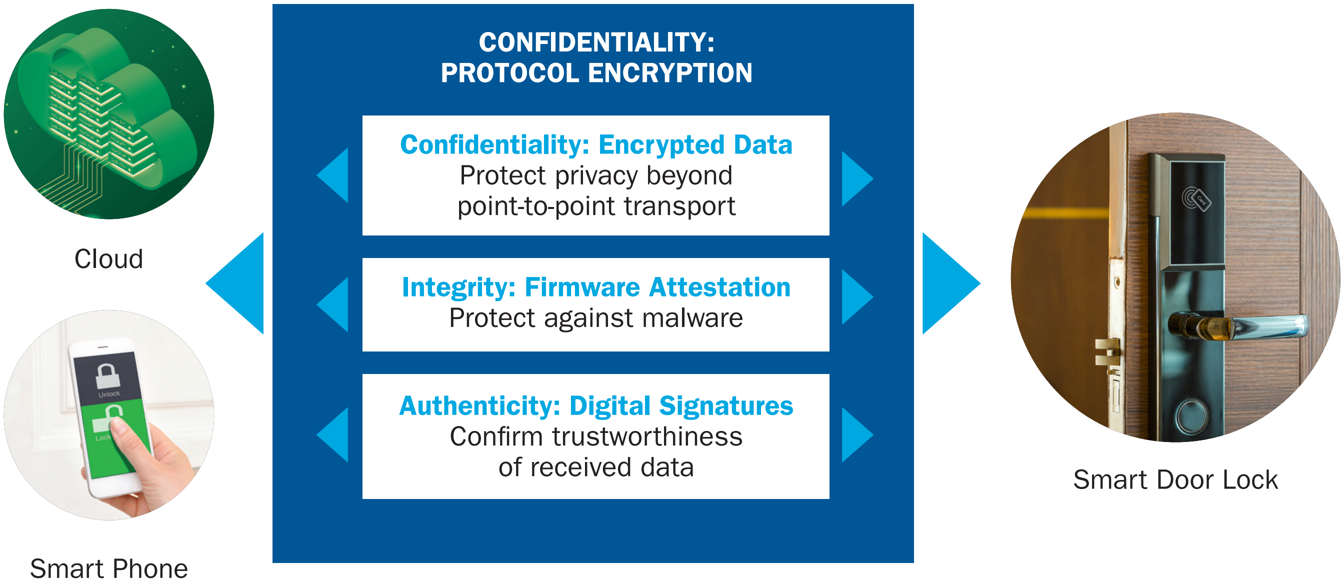
WWW.CYPRESS.COM/PSOC64



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.



CONFIDENTIALITY: PROTOCOL ENCRYPTION

Confidentiality: Encrypted Data
Protect privacy beyond point-to-point transport

Integrity: Firmware Attestation
Protect against malware

Authenticity: Digital Signatures
Confirm trustworthiness of received data

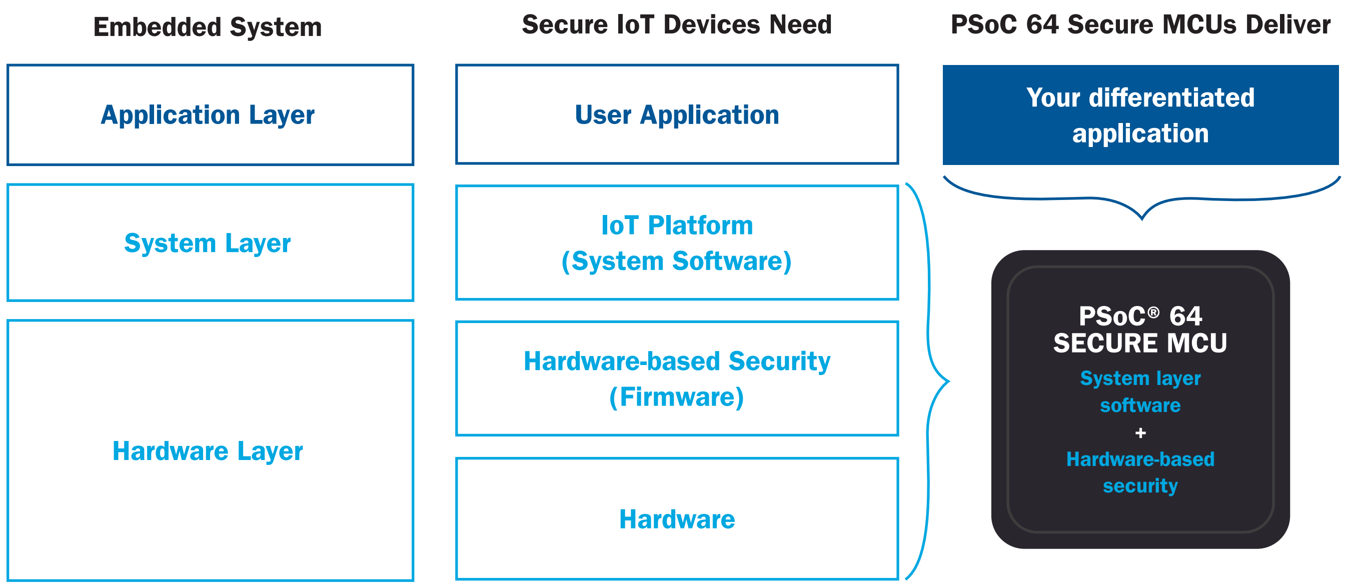
Designing reliable security features into your IoT device can be a daunting task. Let's take the example of a smart door lock. You not only have to worry about user data privacy, but also have to ensure that the lock itself can't be hacked. Adhering to the security principles of Confidentiality, Integrity, 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 vulnerabilities[1].

[1] HP Security Research

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.



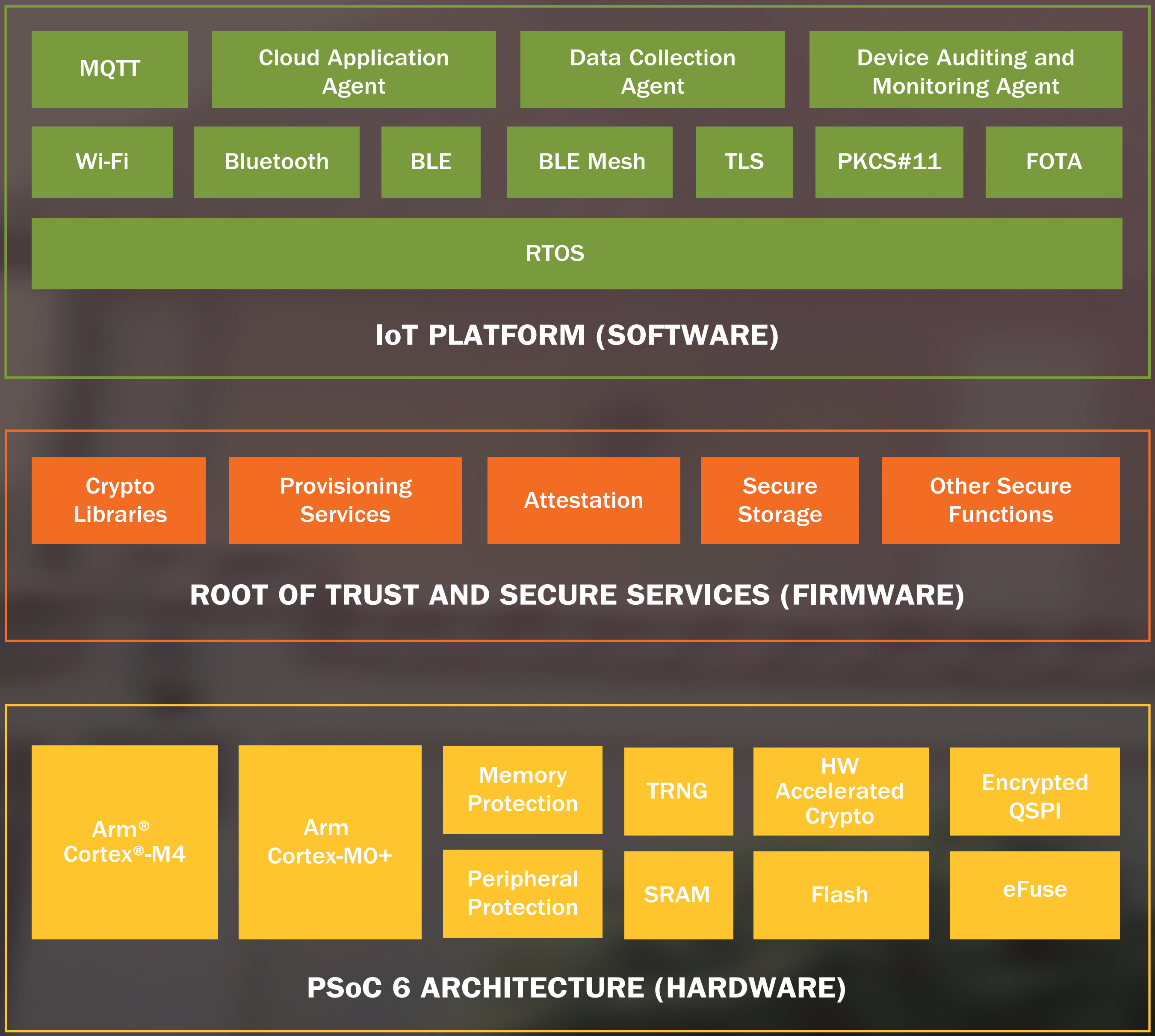
Cypress has an extensive portfolio of industry-leading Wi-Fi connectivity devices that deliver a robust wireless user experience. PSoC 64 Secure MCUs include the communication firmware that supports our Wi-Fi devices. The combination of PSoC 64 Secure MCUs and Cypress' Wi-Fi devices provides a best-in-class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

50% of enterprise executives believe IoT devices could become their network's most significant security risk[2].

[2] Tripwire/Atomik Research

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.



MQTT | Cloud Application Agent | Data Collection Agent | Device Auditing and Monitoring Agent

Wi-Fi | Bluetooth | BLE | BLE Mesh | TLS | PKCS#11 | FOTA

RTOS

IoT PLATFORM (SOFTWARE)

Crypto Libraries | Provisioning Services | Attestation | Secure Storage | Other Secure Functions

ROOT OF TRUST AND SECURE SERVICES (FIRMWARE)

Arm® Cortex®-M4 | Arm Cortex-M0+ | Memory Protection | TRNG | HW Accelerated Crypto | Encrypted QSPI

Peripheral Protection | SRAM | Flash | eFuse

PSoC 6 ARCHITECTURE (HARDWARE)

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

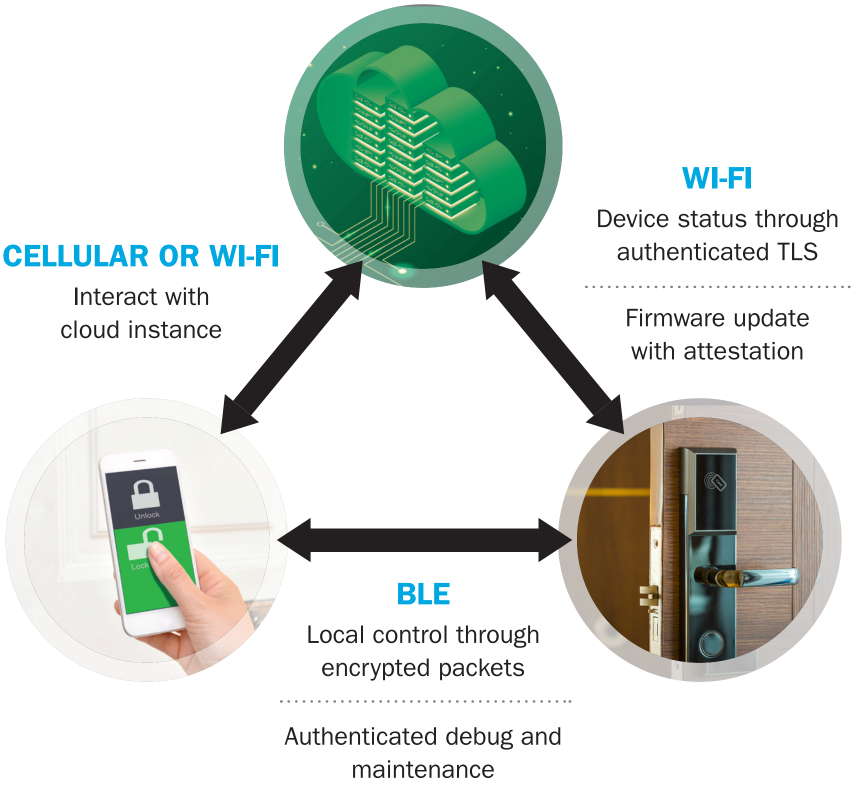
The root-of-trust provides the trust anchor to support the secure boot chain of trust, along with additional security services such as provisioning, attestation, and secure storage.

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.



CELLULAR OR WI-FI

Interact with cloud instance

WI-FI

Device status through authenticated TLS

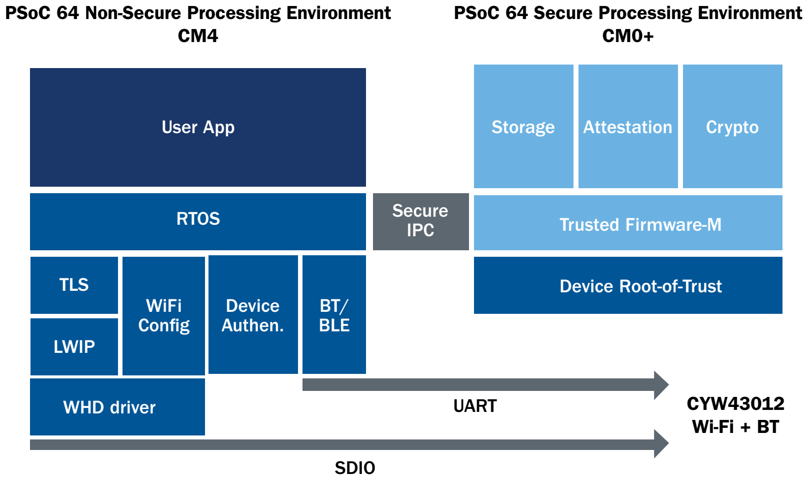
Firmware update with attestation

BLE

Local control through encrypted packets

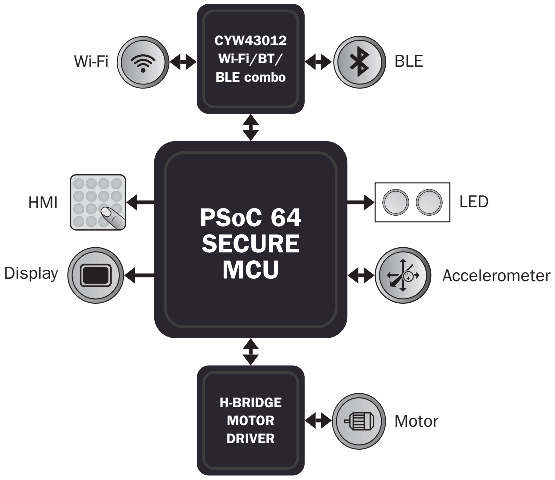
Authenticated debug and maintenance

SMART DOOR LOCK EXAMPLE



PSoC 64 Non-Secure Processing Environment CM4

PSoC 64 Secure Processing Environment CM0+



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® 64 Secure Boot | PSoC® 64 Standard

	Secure Boot	Standard
PSoC	PSoC 64Bx	PSoC 64Sx
Flash Memory	Flash Memory: 512KB - 2MB	
Bluetooth Low Energy	Available in 1MB Flash device only	
Hardware-accelerated Crypto	AES, RSA, ECC, SHA2, TRNG	
Certifications	PSA L1, FIPS 140-2	PSA L2, FIPS 140-2*
NSPE	✓	✓
SPE	✓	✓
Root-of-Trust	✓	✓
Secure Bootloader	✓	✓
Attestation	✓	✓
Trusted Firmware-M (TF-M)	Contact Cypress	✓
Cloud Integration		✓
Target Developer	Wants a pre-configured device root-of-trust	Wants secure cloud connectivity that "just works"

*Q3 2020

PSoC 64 FEATURES

NON-SECURE PROCESSING ENVIRONMENT

The Cortex-M4 processor in PSoC 64 MCUs is used to establish a non-secure processing 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 PROCESSING ENVIRONMENT

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

HARDWARE-BASED ROOT-OF-TRUST AND TRUSTED SERVICES

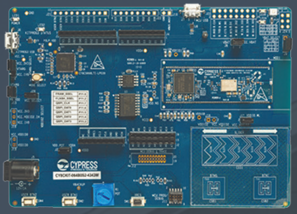
Further isolated from secure processing environment is a hardware-based root-of-trust with trusted services. The root of trust includes hardware-accelerated cryptography, true random number generation (TRNG), and secure storage. Trusted services that utilize the hardware-based root of trust include secure 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 64 development kit. Platform Security Architecture (PSA) APIs allow access to secure functions from your application.

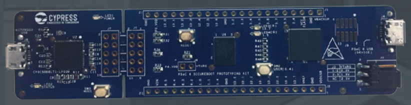


PIONEER KITs:
CY8CKIT-064B0S2-4343W
CY8CKIT-064S0S2-4343W

2

DEVELOP YOUR SECURE BOOT AND PROVISIONING CREDENTIALS

Cypress provides secure provisioning tools that help you develop your security scheme and credentials. Tools include provisioning scripts, key generation APIs for development, and templates for device security policies.



PROTOTYPING KITS:
CY8CPROTO-064B0S1-BLE
CY8CPROTO-064B0S1
CY8CPROTO-064B0S3

3

GO TO PRODUCTION

Cypress had partnered with HSM providers that can help you get your secure IoT design into production. Services include transferring the Root-of-Trust ownership from Cypress to you, injecting user assets, and programming devices at scale.

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.

CYPRESS®
EMBEDDED IN TOMORROW™

© 2019-2020 Cypress Semiconductor Corporation. All rights reserved. All other trademarks are the property of their respective owners.