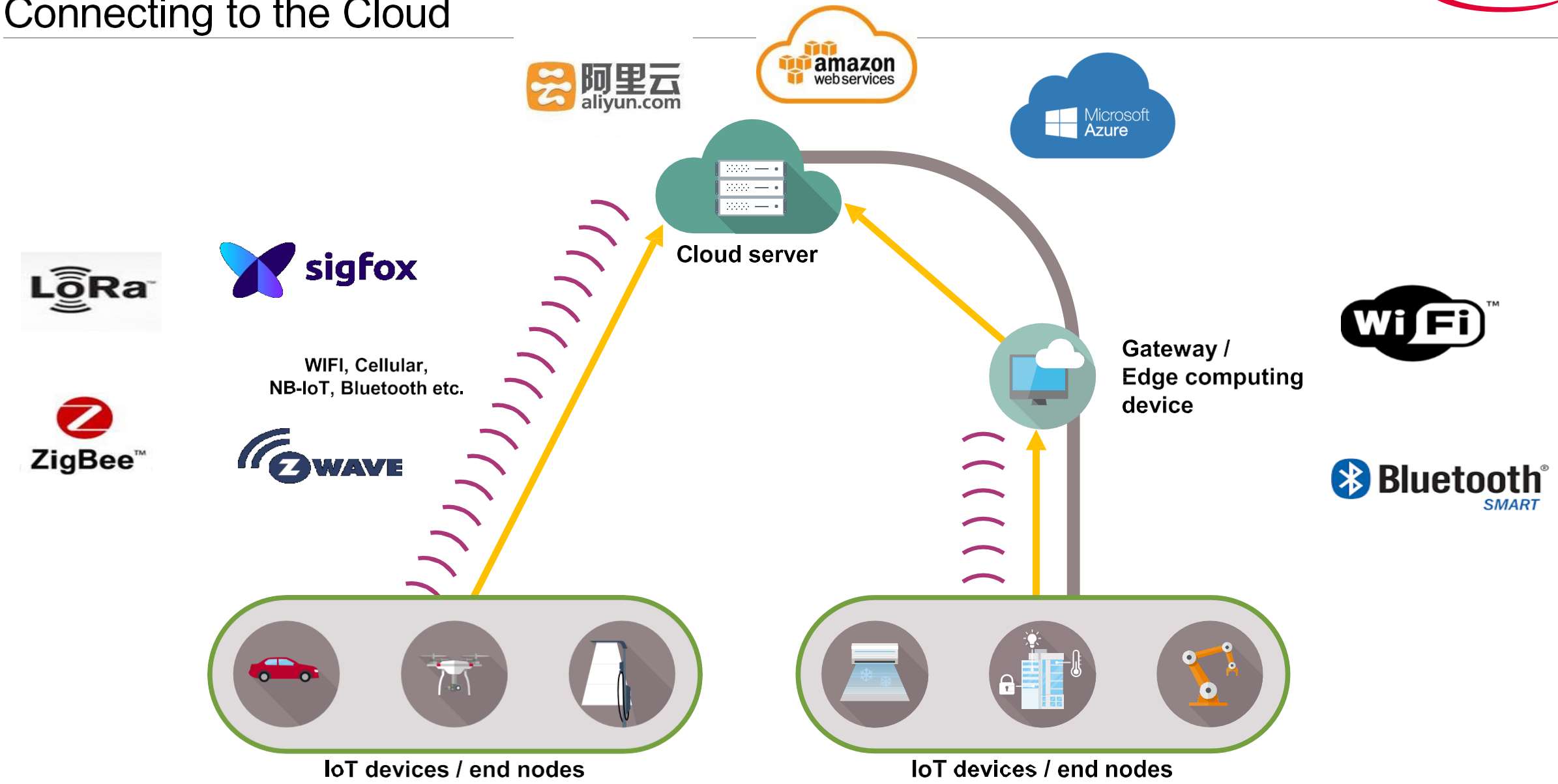
INFINEON : IoT Cyber Security (PSoC 64 - Optiga Trust M Solution)

Mauro Bottura - Connected Secure Systems Marketing SW Europe

Connecting to the Cloud



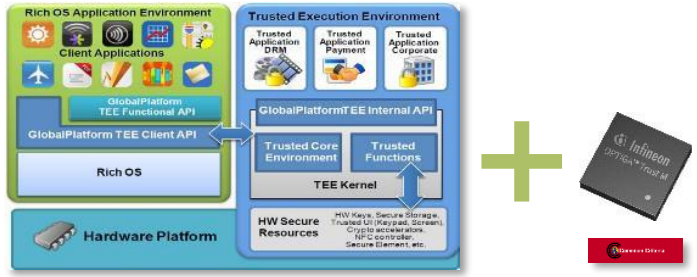
Protection of Assets : Levels of Protection

eSE

Software + Hardware Trust Anchor + Certified Tamper Resistant

Common Criteria

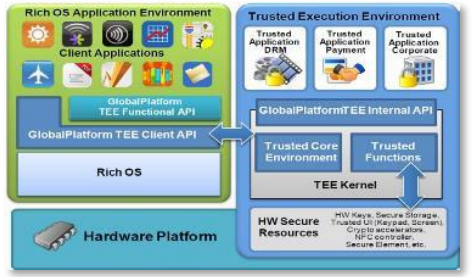
Using Secure Element for tamper-resistant Hardware Trust Anchor



TEE

Software + Hardware Extensions

TEE OS runs separate from the general Rich OS - but still using the same HW platform



Host

Purely software protection

Storage and processing is done within application running on Android on host

[Owner: Mike Volkmann Doc ID: EU CSS-ICW Presentation Vers.:]

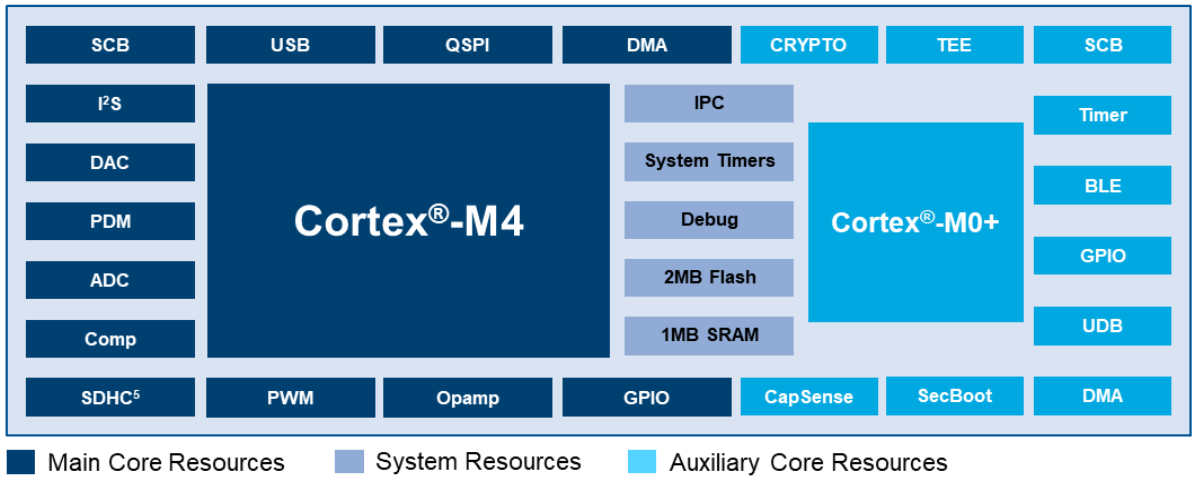
PSoC 64 Logically Secure MCU
(TEE Security level)

PSoC 6 Family - Purpose Built, Low Power, Secure MCU for the IoT

PSoC 6 Dual-Core MCU Architecture

Cortex®-M4 Usage Examples:

RTOS
Displays
Sensor Analytics
Audio Interface
USB/BLE HCI[4]



Cortex®-M0+ Usage Examples:

BLE Stack
CapSense
Secure Functions
I/O Data Control
Sensor Aggregation

PSoC 6 bridges the gap between application processors and standard microcontrollers

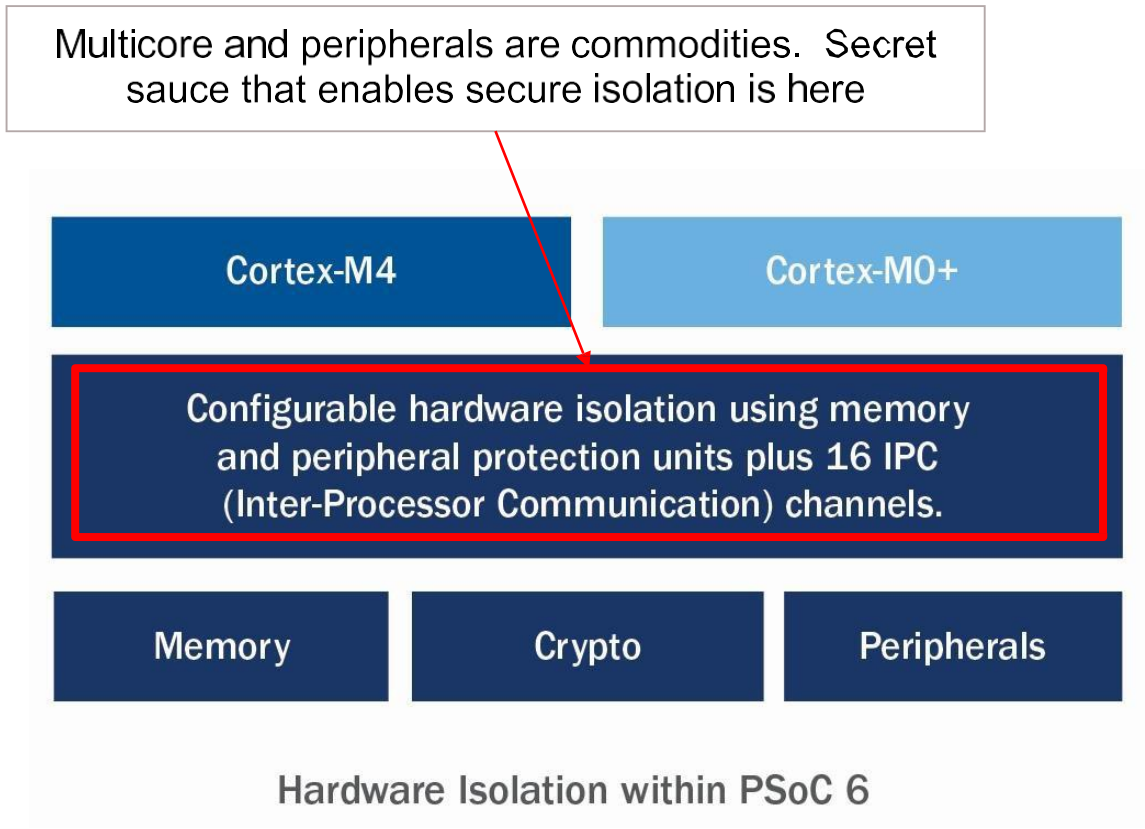
PSoC 64: Built on the PSoC 6 Security Architecture

SECURITY FEATURES

- **Hardware-isolated processing environment** for trusted applications
- **Integrated secure-element functionality** with isolated cryptographic operations and 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 (PSoC 64)

MICROCONTROLLER FEATURES

- Asymmetric dual-core Arm® Cortex®-M4 (150 MHz) and Arm Cortex-M0+ (100 MHz)
- Up to 2 MB Flash, 1 MB 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

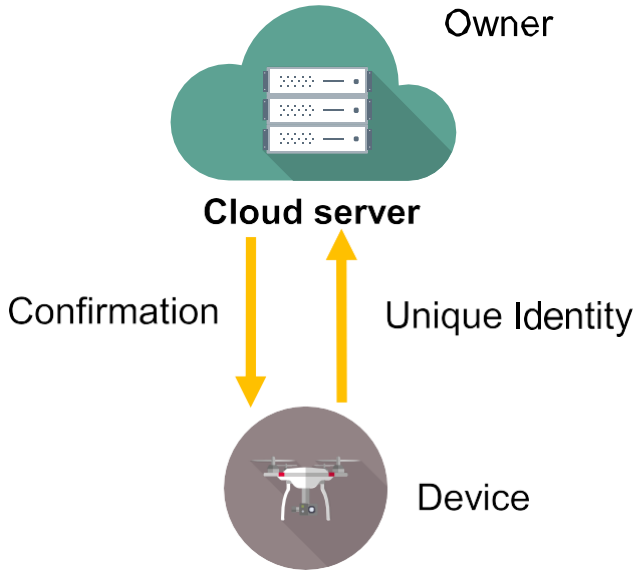
PSoC® 6 Portfolio

Programmable Line PSoC 61	Performance Line PSoC 62	Connectivity Line PSoC 63	Security Line PSoC 64
Arm® Cortex®-M4	Arm Cortex-M4, Cortex-M0+	Arm Cortex-M4, Cortex-M0+	Arm Cortex-M4, Cortex-M0+
Up to 2MB Flash, 1MB SRAM	Up to 2MB Flash, 1MB SRAM	Up to 1MB Flash, 288KB SRAM	Up to 2MB Flash, 1MB SRAM
			Preconfigured Secure Processing Environment (SPE) and Non-Secure Processing Environment (NSPE) (PSA API) Hardware-based Root-of-Trust (PSA L1) and Trusted Services Integrated RTOS + TF-M (PSA L2)
		Bluetooth Low Energy	
	Dynamic Voltage and Frequency Scaling for LP and ULP		
CapSense®, SAR ADC, DAC, LP COMP, OpAmps, UDBs, SCBs, TCPWMs, QSPI, I2S, PDC-PCM, USB, LCD, DMA, RTC, Efuse, PLLs, OSCs, GPIOs, Smart IO, Crytpo			

Two Key Attributes of a Secure IoT Device

DEVICE IDENTITY: binds the device to an owner

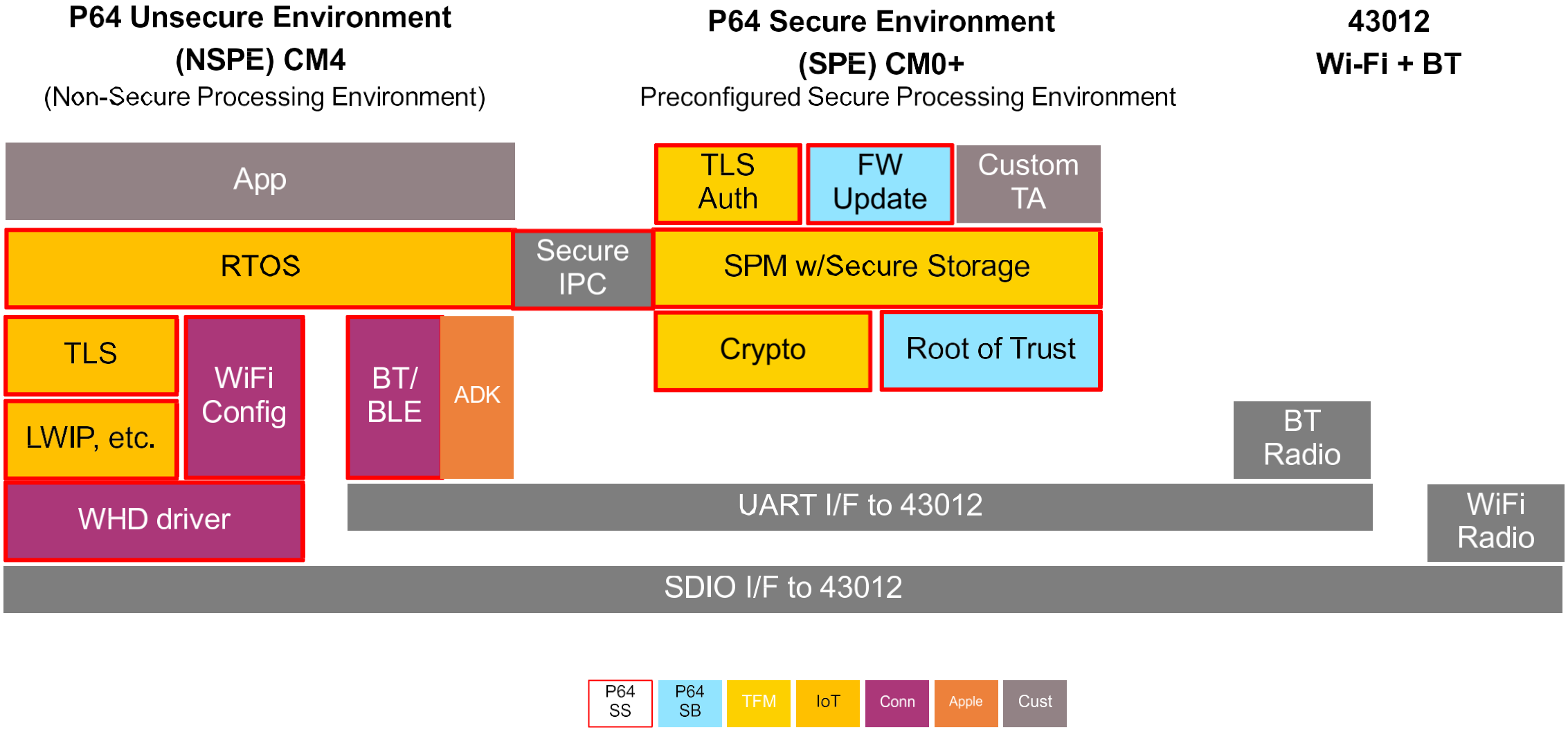
- PROVISIONING : Mechanism Providing Unique Identity
- ATTESTATION : Identity Confirmation to IoT platform
- SECURE BOOT
- FW UPDATES
- TLS : Transport Layer Security



RESOURCE ISOLATION: limits a given attack surface and protects access to keys

- PROCESSING ENVIRONMENTS
- APPLICATION
- SECURITY SERVICES : process to keep safe all devices into IoT system
- KEYS

Application Example – PSoC 64 Standard – AWS Product



Software security is just not enough

	Main CPU + Software	Main CPU + Software + Hardware
Crypto functionality	✓	✓
Strong isolation	STOP	✓
Security certified	STOP	✓
Tamper resistant	STOP	✓
Manufactured by security certified processes	STOP	✓
Personalized by security certified processes	STOP	✓

PSoC 64 + Optiga Trust – M SW Architecture
(eSE Security level)

OPTIGA™ Family Overview

OPTIGA™ - embedded security solutions

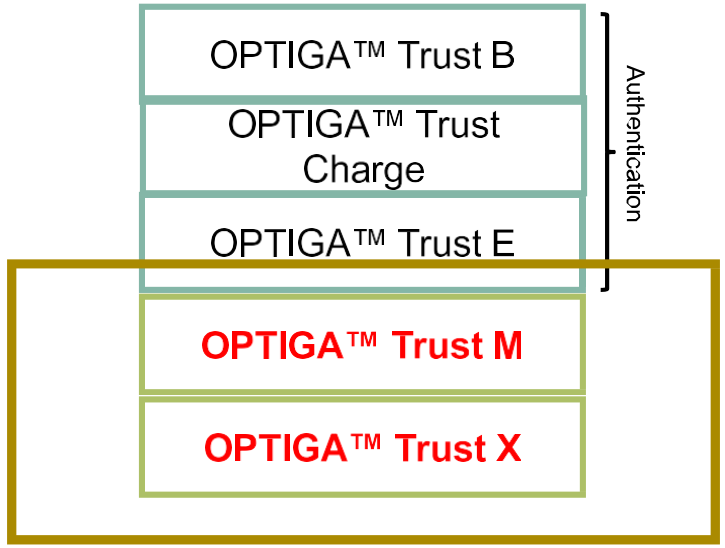
OPTIGA™ Connect

- OPTIGA™ Connect IoT
- OPTIGA™ Connect Consumer

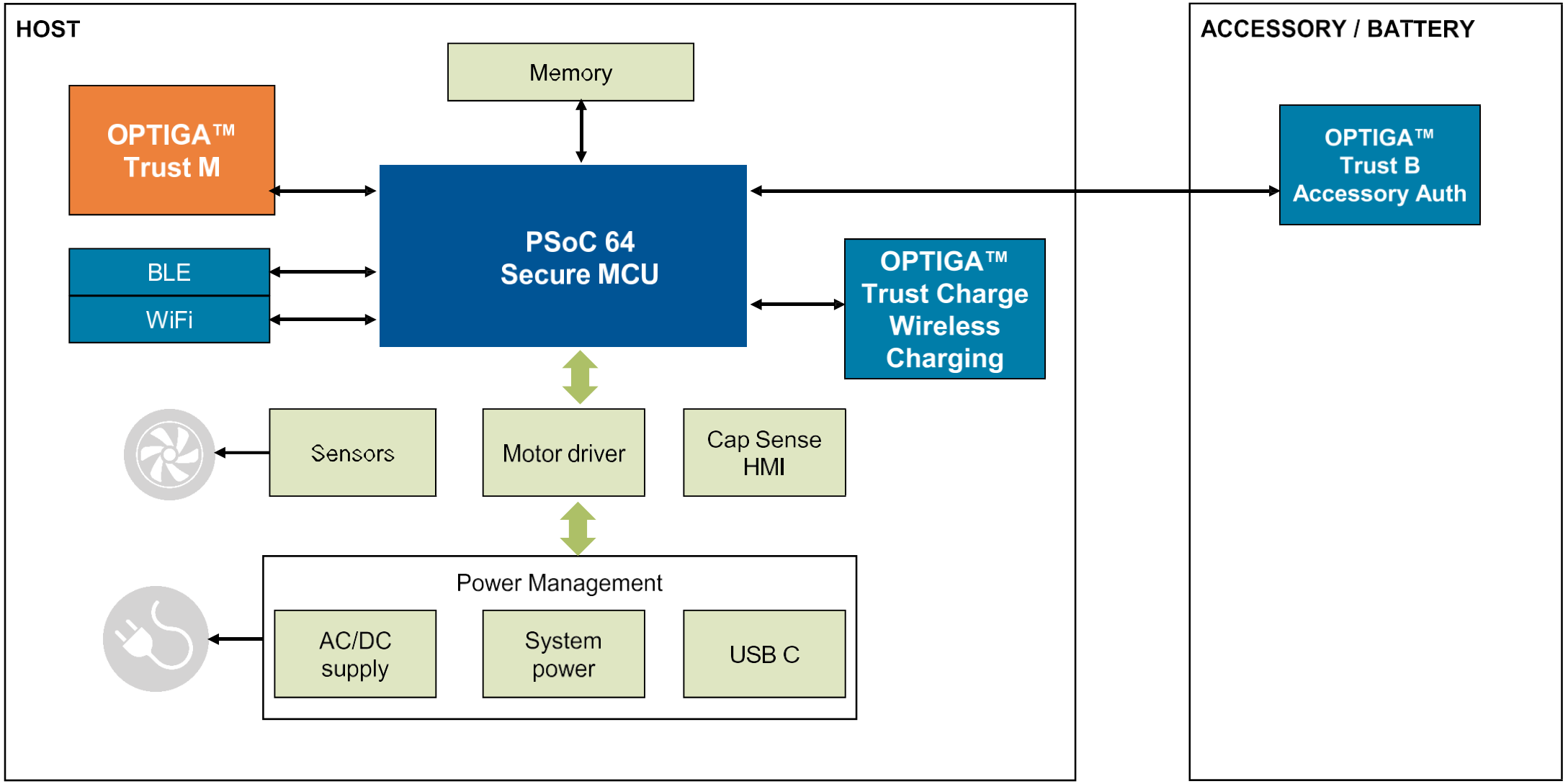
OPTIGA™ TPM

- OPTIGA™ TPM SLB
- OPTIGA™ TPM SLI - automotive
- OPTIGA™ TPM SLM - industrial

OPTIGA™ Trust

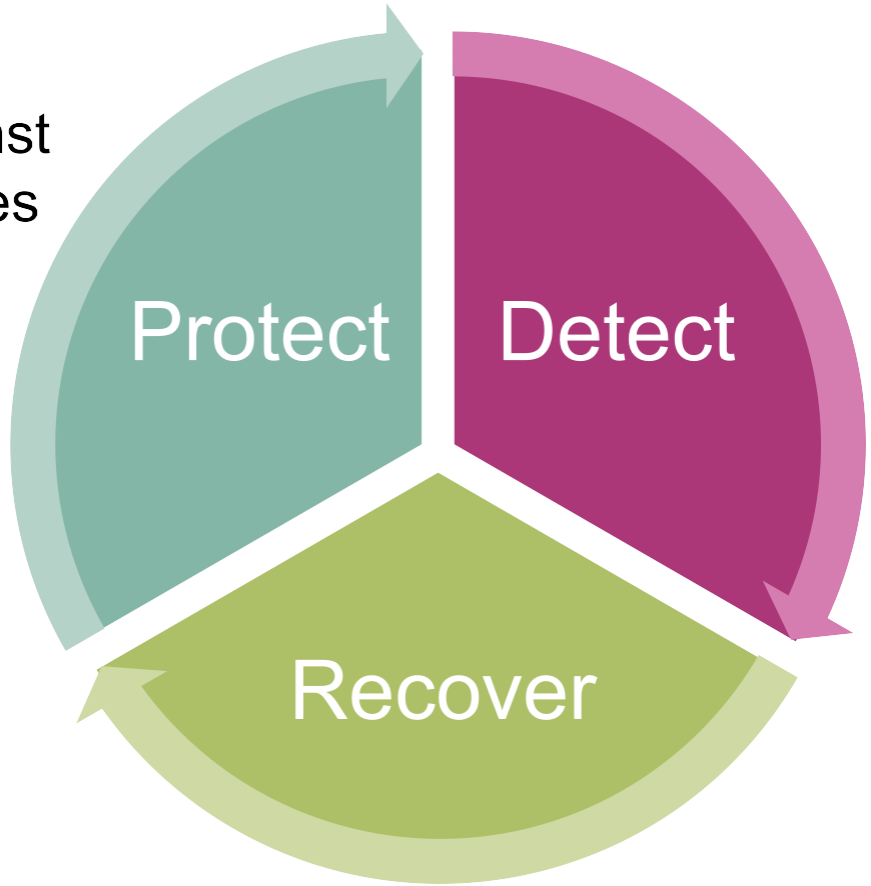


Infineon System Diagram: a typical connected IoT device



The main objective

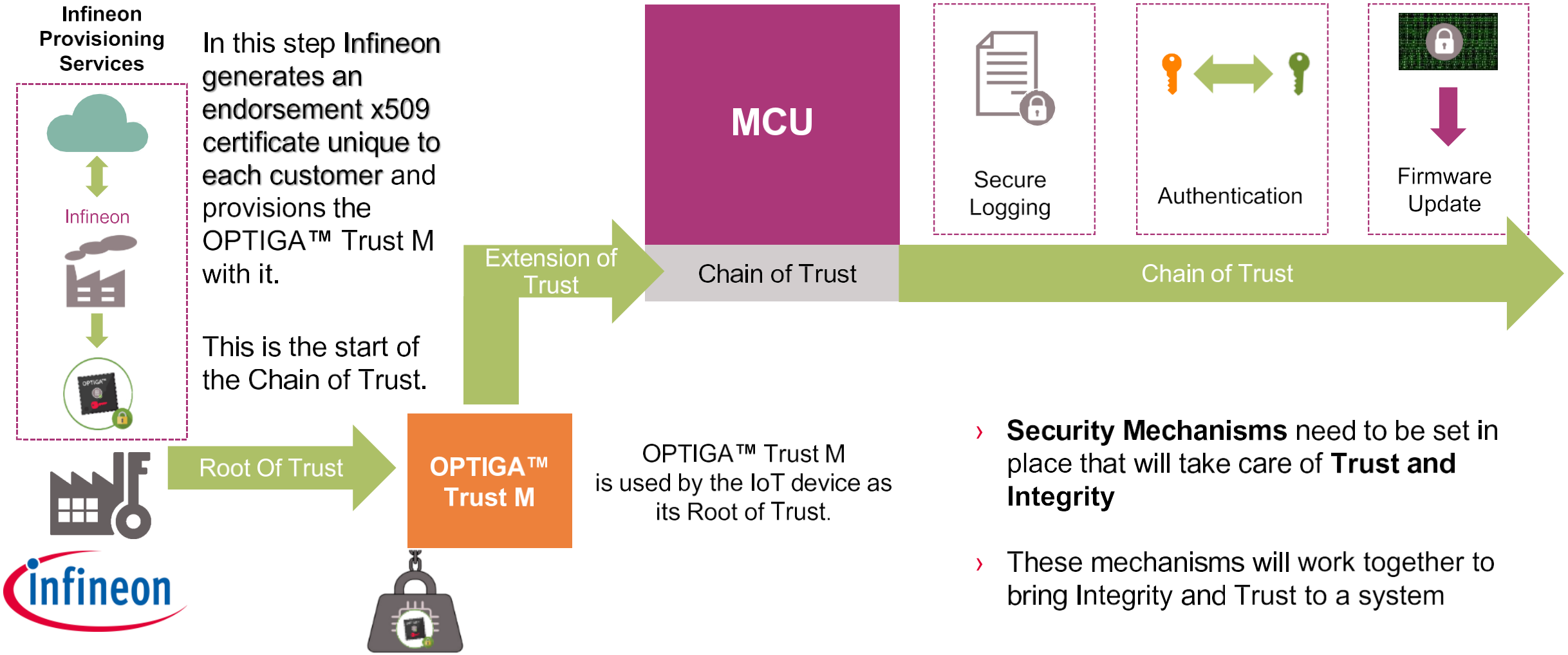
Provide protection against attacks for critical devices in the system



Detect when an attack has occurred and establish secured methods for logging it

Recover from attacks to a state of integrity and trust

OPTIGA™ Trust M
The foundation for a secured chain of trust



- **Security Mechanisms** need to be set in place that will take care of **Trust and Integrity**
- These mechanisms will work together to bring Integrity and Trust to a system

Root of trust
Internal countermeasures for highest security

Logical Attacks

e.g. protocol fuzzing, Jamming, replay, …

Side Channel Attacks

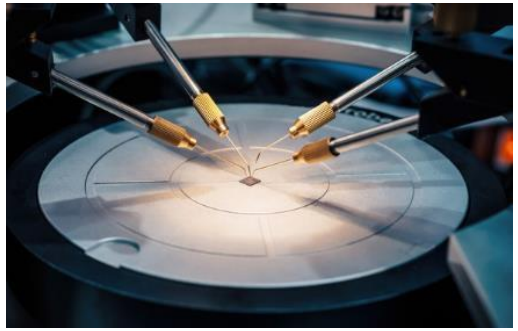
e.g. SPA, DPA, Spectre, Meltdown

Fault Injection

e.g. Spiking, radiation, light attacks, clock manipulation, DFA

Invasive Attacks

e.g. FIB manipulation, micro-probing, …



Countermeasures

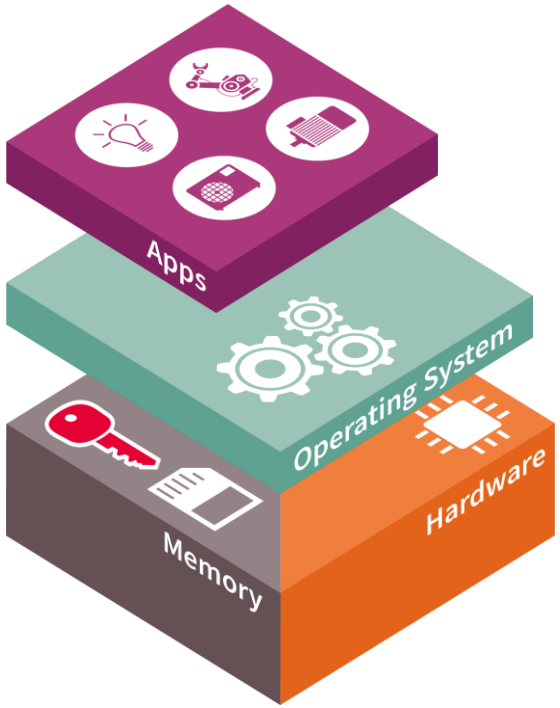
PKI, digital signatures, encryption, CMAC, blockchain, MISRA C-CERT coding guidelines…	runtime invariant SW implementation, randomized processing in HW and SW, dual-rail HW implementation, encrypted computation…	double computation, all safety HW measures…	Tamper protection, implanted ROM, full-custom design

Software

Hardware

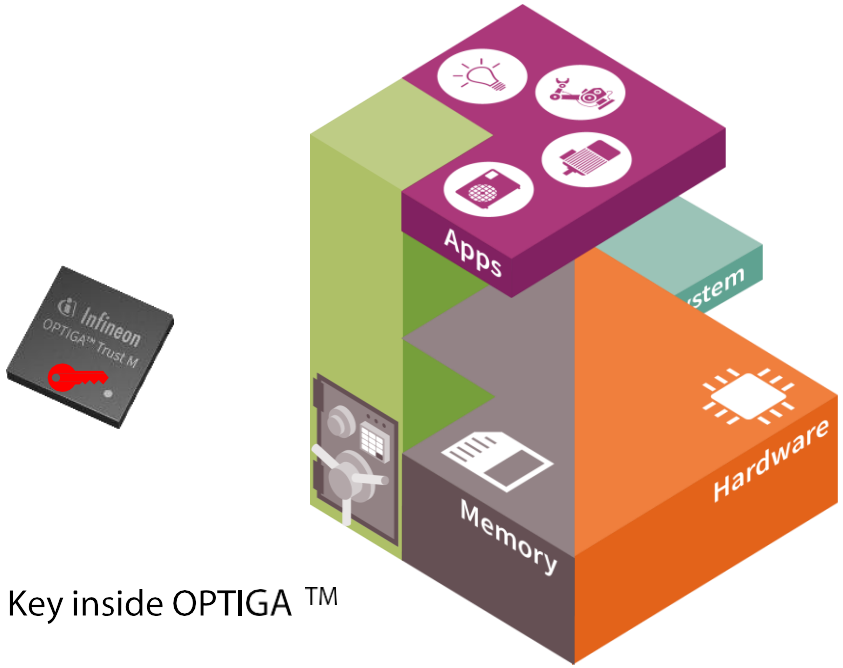
Trusted execution environments and software security is not enought

Trusted execution environments



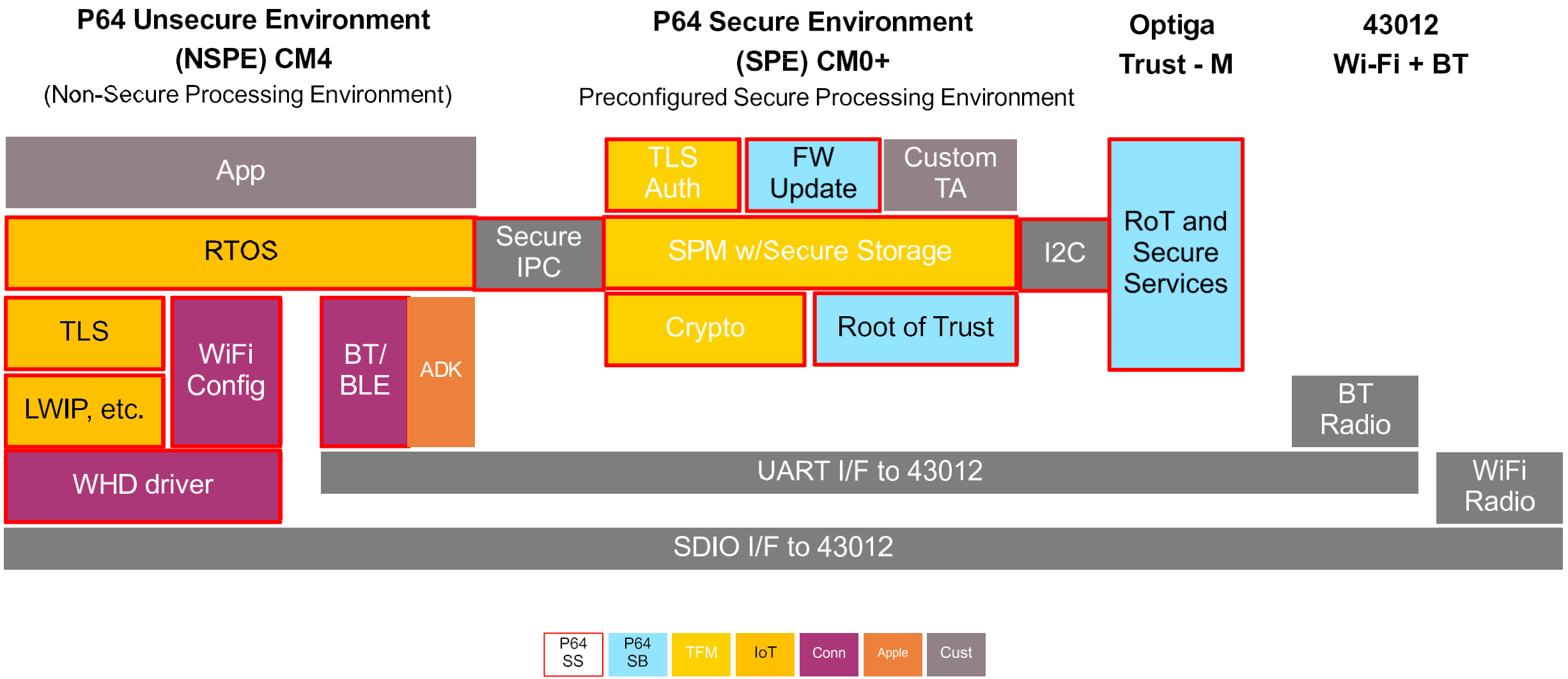
Protection Key inside standard memory

OPTIGA™ Trust M and Trusted Execution Environments complement each other, achieving the highest level of security



Protection Key inside OPTIGA ™

Application Example – PSoC 64 + Optiga TrustM – AWS Product



Conclusion

- **WHAT DOES OPTIGA TRUST DO FOR A NON-SECURE MCU**

It stores keys in a logical and physically secure domain, therefore, an attacker cannot get the keys and clone them.

- **WHAT OPTIGA TRUST DOES NOT DO FOR A NON-SECURE MCU**

It does not logically prevent an attacker from taking over the MCU, therefore, an attacker can take over the MCU but the he cannot get access to the keys in the Optiga Trust to clone the now compromised IoT device.

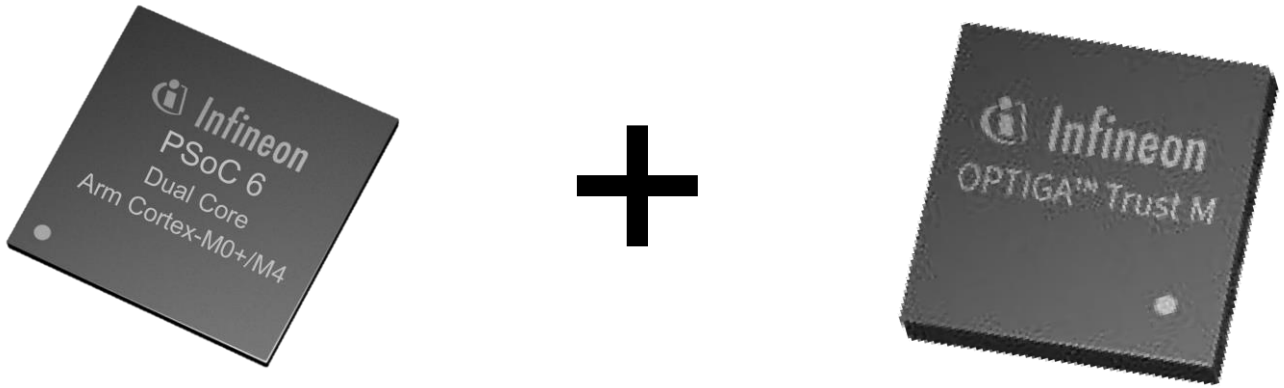
- **A SECURE MCU LIKE PSOC 64**

Is able to prevent the compromise of the MCU.

Conclusion

PSOC64 + OPTIGA TRUST M

is the best combination to prevent the compromise of the MCU and physical attack to the keys



Part of your life. Part of tomorrow.