Getting Started with Secure Software

Class 5: Secure Frameworks and Ecosystems

April 24, 2020

Jacob Beningo

Presented by:

DesignNews

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

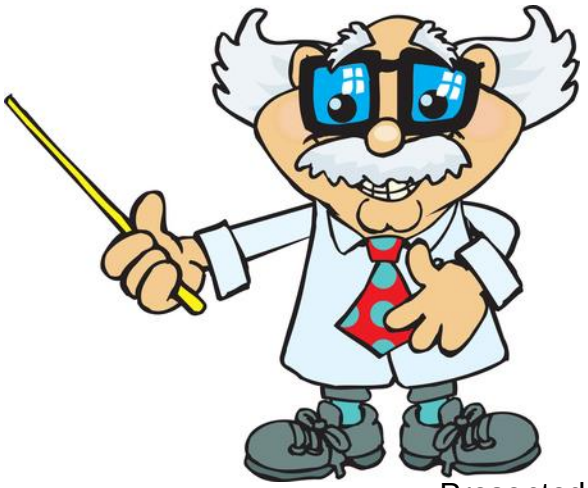
Course Overview

Topics:

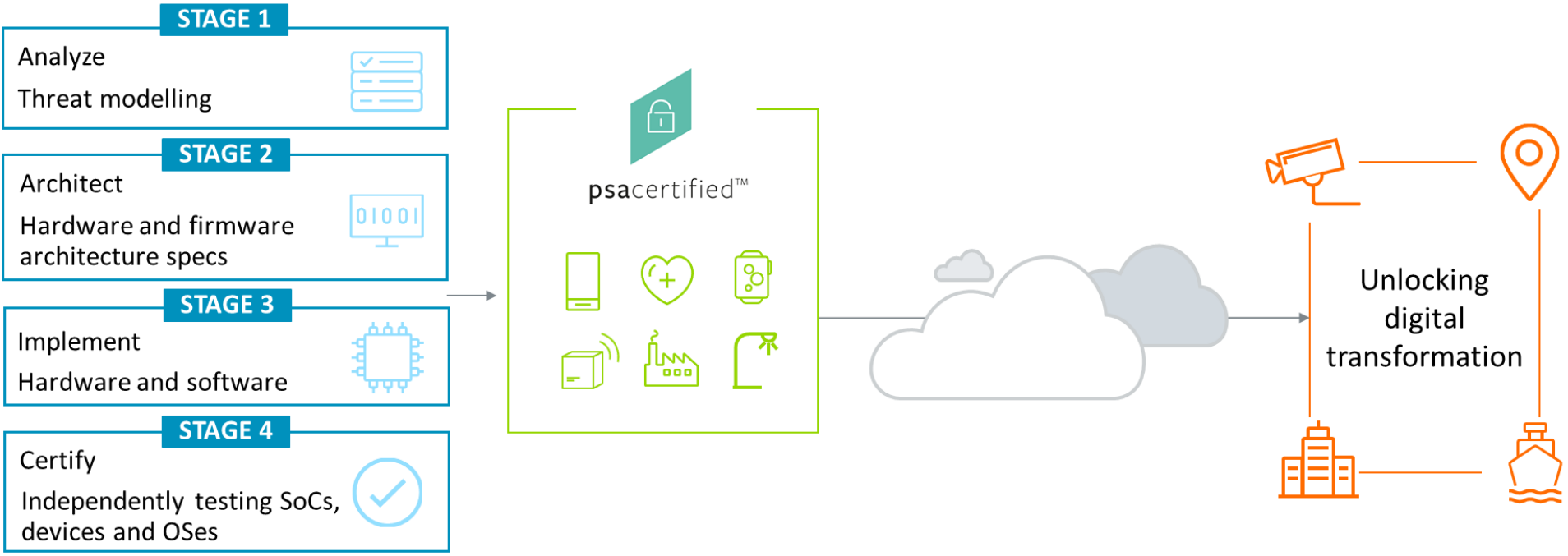
- Introduction to Platform Security Architecture (PSA)
- Performing a Security Threats Analysis
- Architecting a Secure Solution
- Secure Boot and the Root-of-Trust
- **Secure Frameworks and Ecosystems**

Session Overview

- Trusted Firmware M (TF-M)
- Door Lock Example
- TrustZone Frameworks
- The Challenges



PSA



PSA: enabling right-sized device security

Trusted Firmware M (TF-M)

TF-M Overview

TF-M includes:

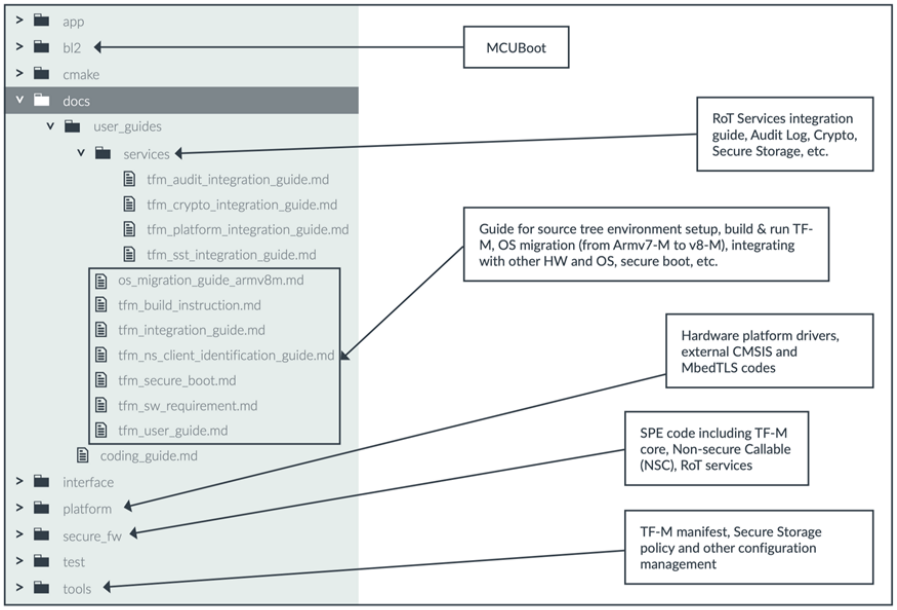
- Crypto Services
- Secure Storage Services
- Audit Logging Services

Implementation Guides and Code:

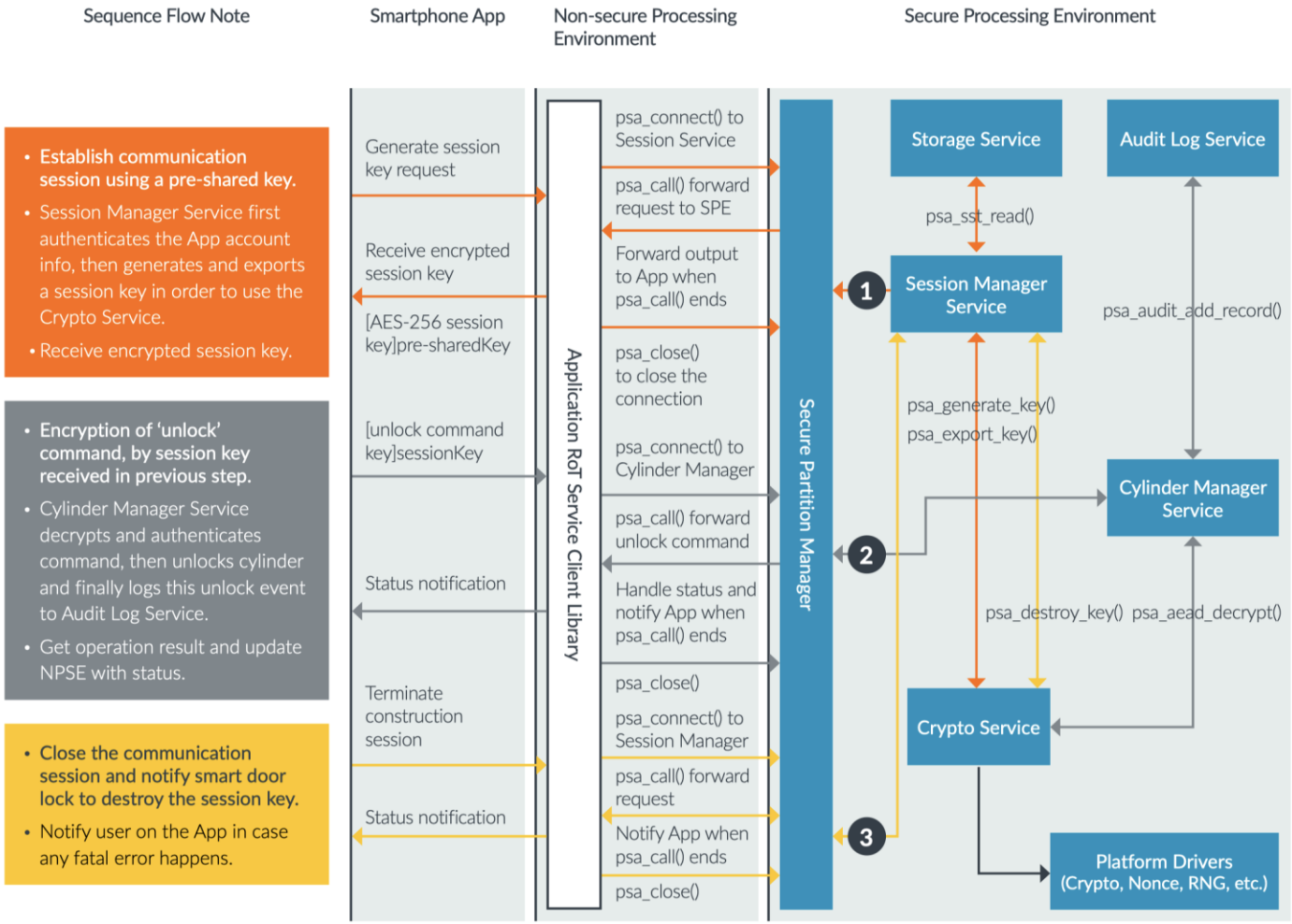
- tfm_user_guide.md provides a getting started guide for TM-M
- tfm_integration_guide.md discusses integration with device targets
- Can be cloned from :

https://git.trustedfirmware.org/trusted-firmware-m

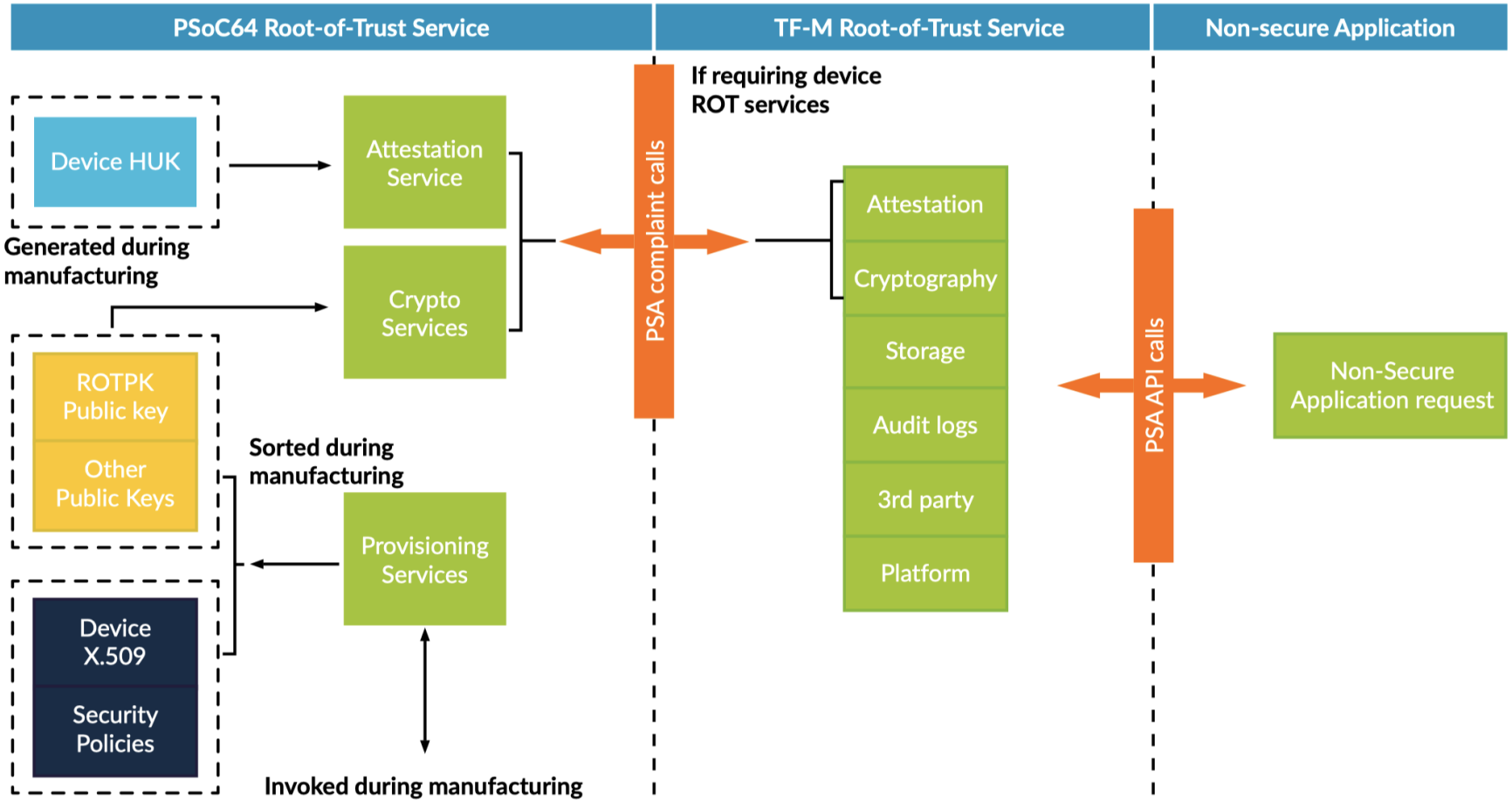
TF-M Code Source Tree



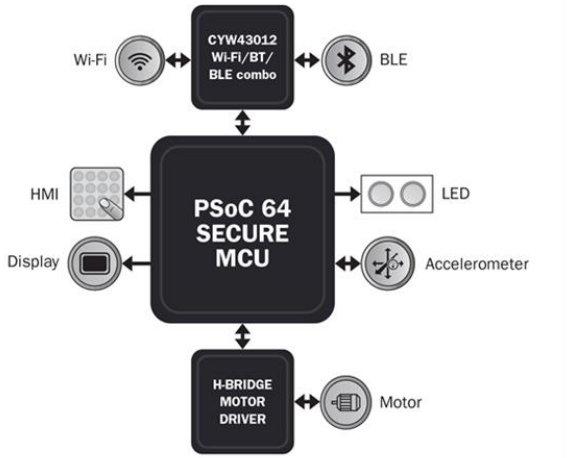
Smart Door Lock Unlock Operation

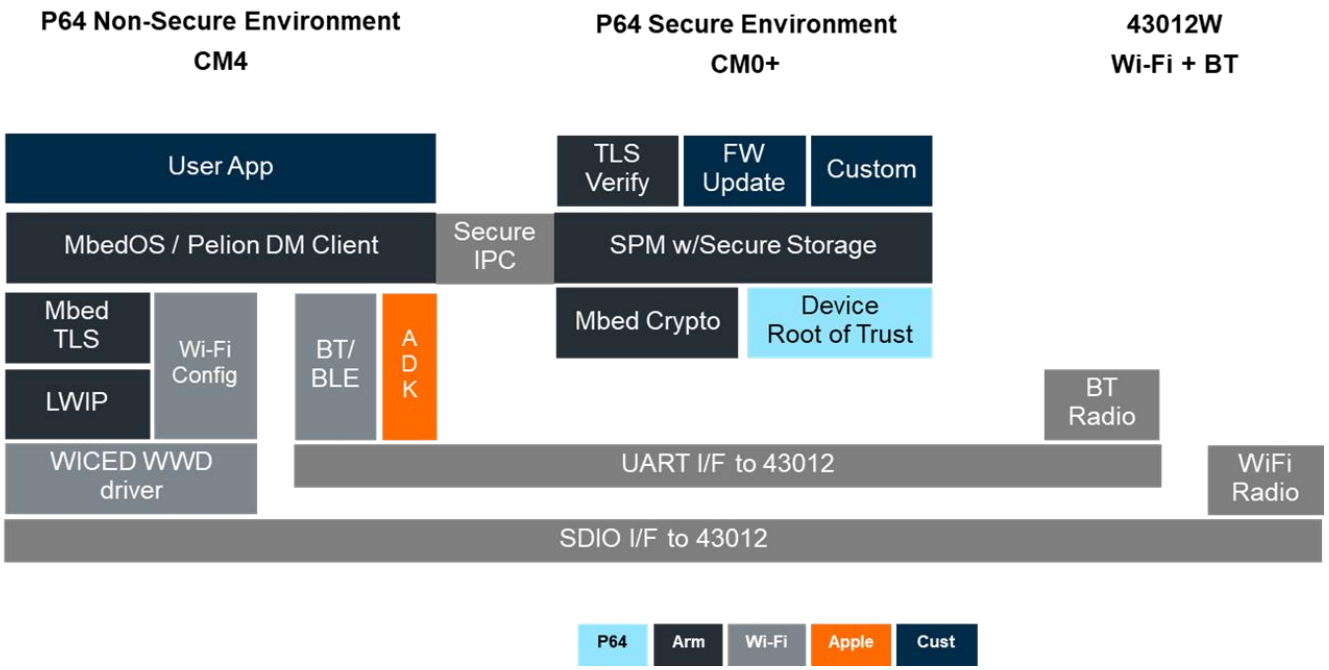


Smart Door Lock

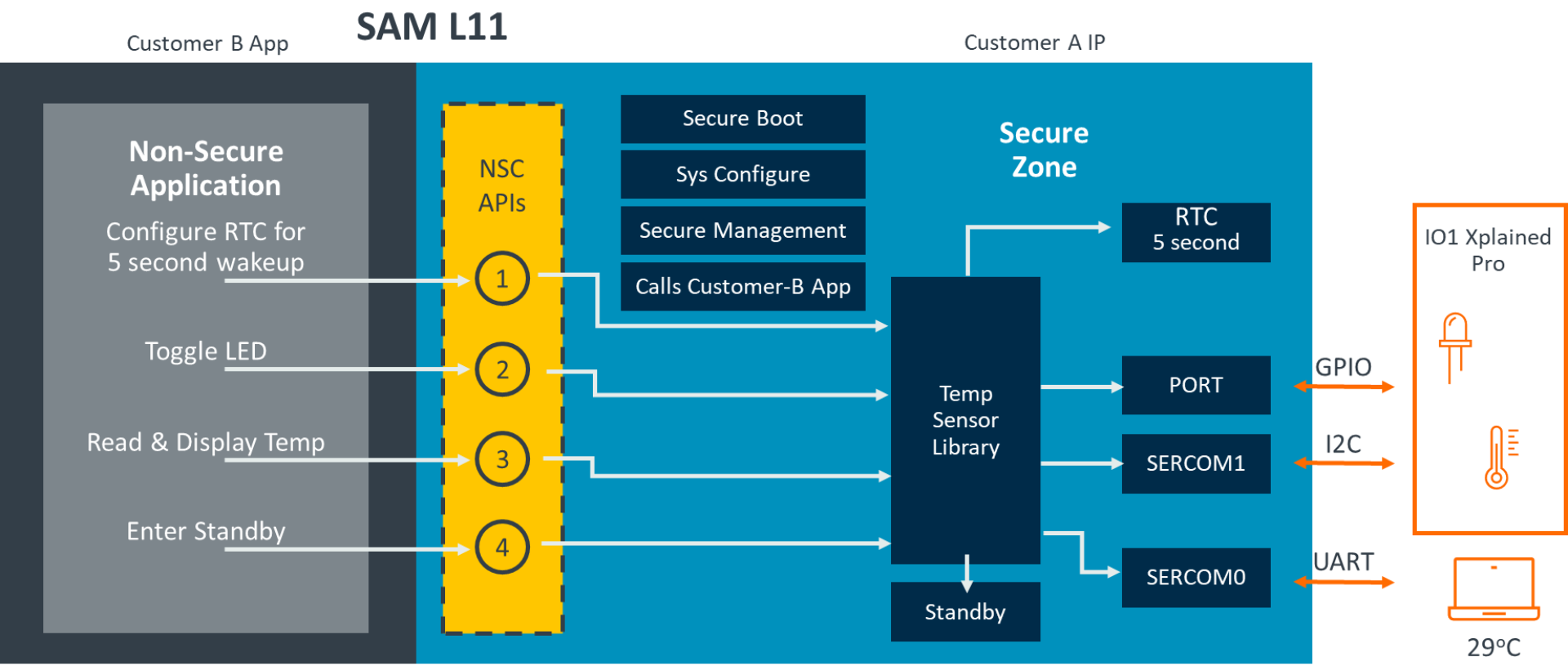


Smart Door

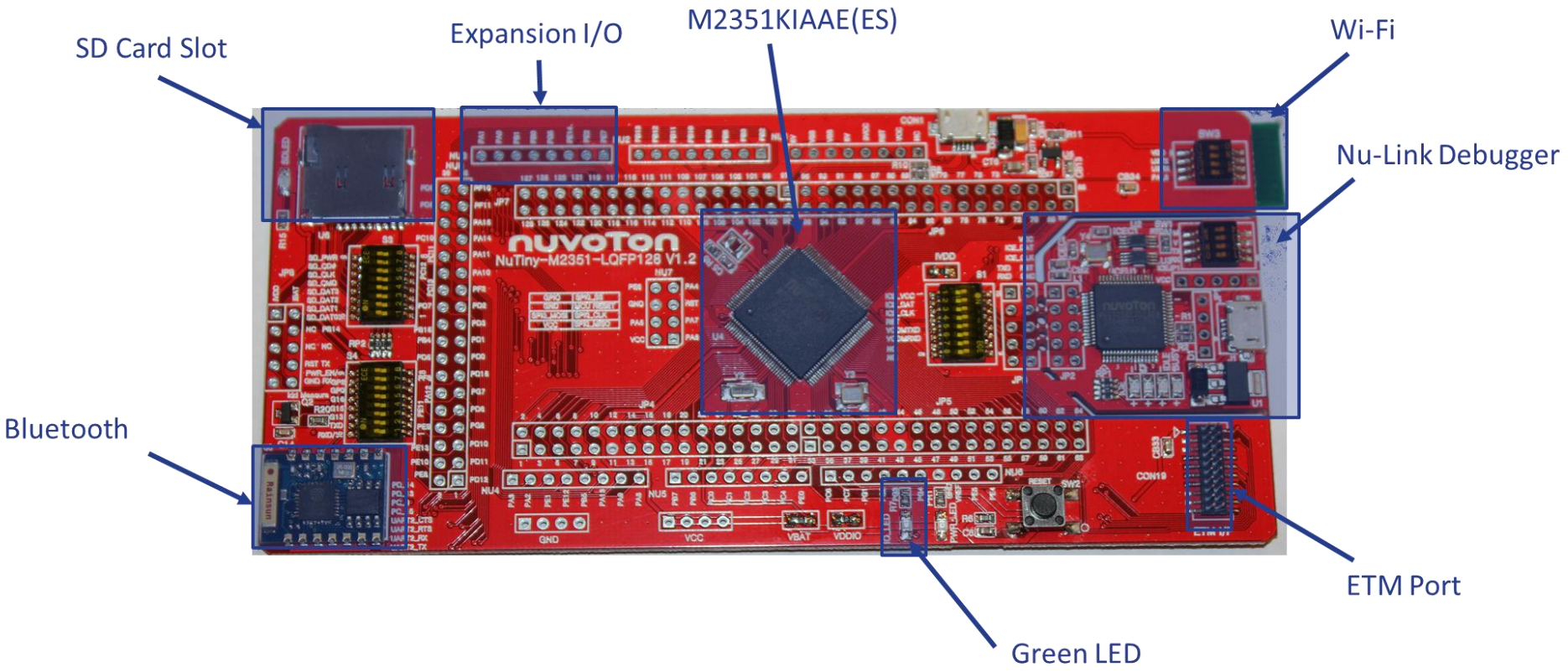

CYW43012
Wi-Fi/BT/
BLE combo
Wi-Fi
BLE
PSoC 64
SECURE
MCU
HMI
LED
Display
Accelerometer
H-BRIDGE
MOTOR
DRIVER
Motor


P64 Non-Secure Environment
CM4
P64 Secure Environment
CM0+
43012W
Wi-Fi + BT
User App
TLS Verify
FW Update
Custom
MbedOS / Pelion DM Client
Secure IPC
SPM w/Secure Storage
Mbed TLS
Wi-Fi Config
BT/ BLE
ADK
Mbed Crypto
Device Root of Trust
LWIP
BT Radio
WICED WWD driver
UART I/F to 43012
WiFi Radio
SDIO I/F to 43012
P64
Arm
Wi-Fi
Apple
Cust

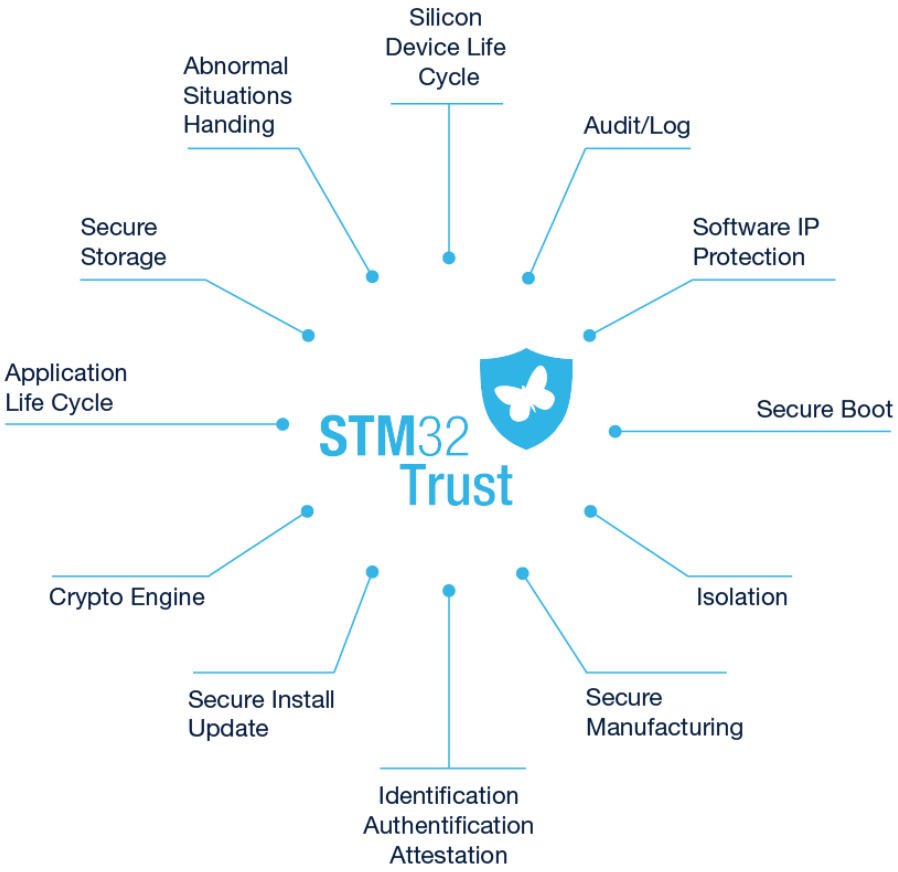
TrustZone Example - Microchip



TrustZone - Nuvoton

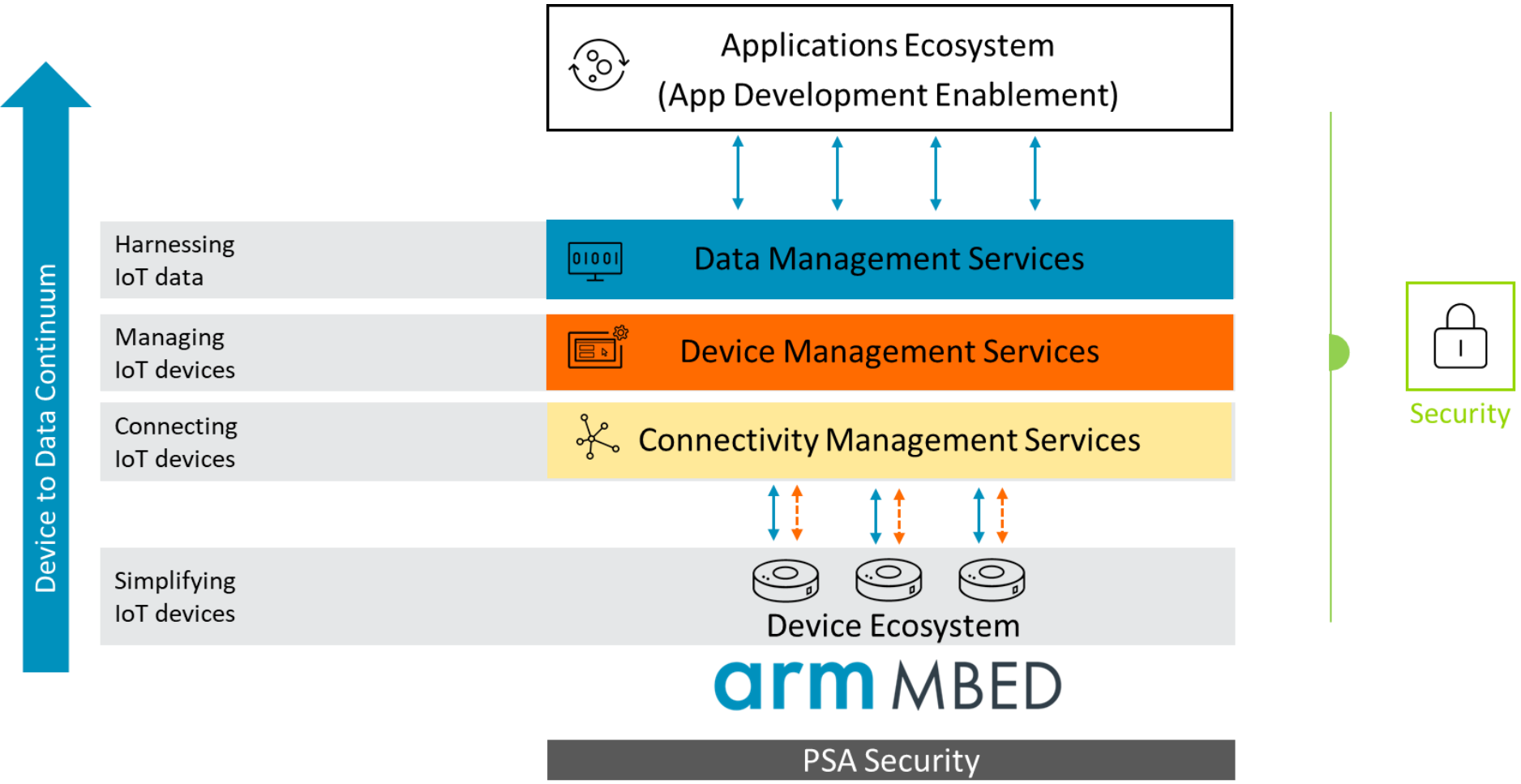


TrustZone – STM32

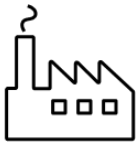


NUCLEO-L552ZE-Q

Pelion IoT Services Platform



Pelion IoT Services Platform

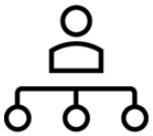


1 Factory provisioning

- Configuring devices with **trusted** unique identity
- Device receives bootstrap credentials

2 Commissioning

- **Securely** configuring network credentials and operational parameters



4 Regular Use – Sense/send data

- Normal life device operation
- Controlling access **securely** to devices in the field

3 Onboarding

- Device connects to **bootstrap service** to get registration credentials

5 Regular Use – Update device

- **Securely updating** device software remotely
- Security model describes system relationships and responsibilities

6 Retire/decommission

- Removing devices from the service (End of life)

Challenges Facing Developers

- Security can be expensive to implement throughout a device's lifecycle.
- IoT device security is difficult to manage at scale.
- Security specialists are expensive and in short supply, particularly for smaller businesses and start-ups.
- The security landscape is ever-evolving, with new attack vulnerabilities continuously emerging.
- A lack of confidence in the data being passed to, and from, sensors and actuators.

Additional Resources

- Beningo.com
  - Blog, White Papers, Courses
  - Embedded Bytes Newsletter
    - http://bit.ly/1BAHYXm
- Platform Security Architecture:
  - www.arm.com/psa
- Threat-based analysis method:
  - www.cypress.com/psoc6security

From www.beningo.com under

- Blog > CEC – Getting Started with Secure Software