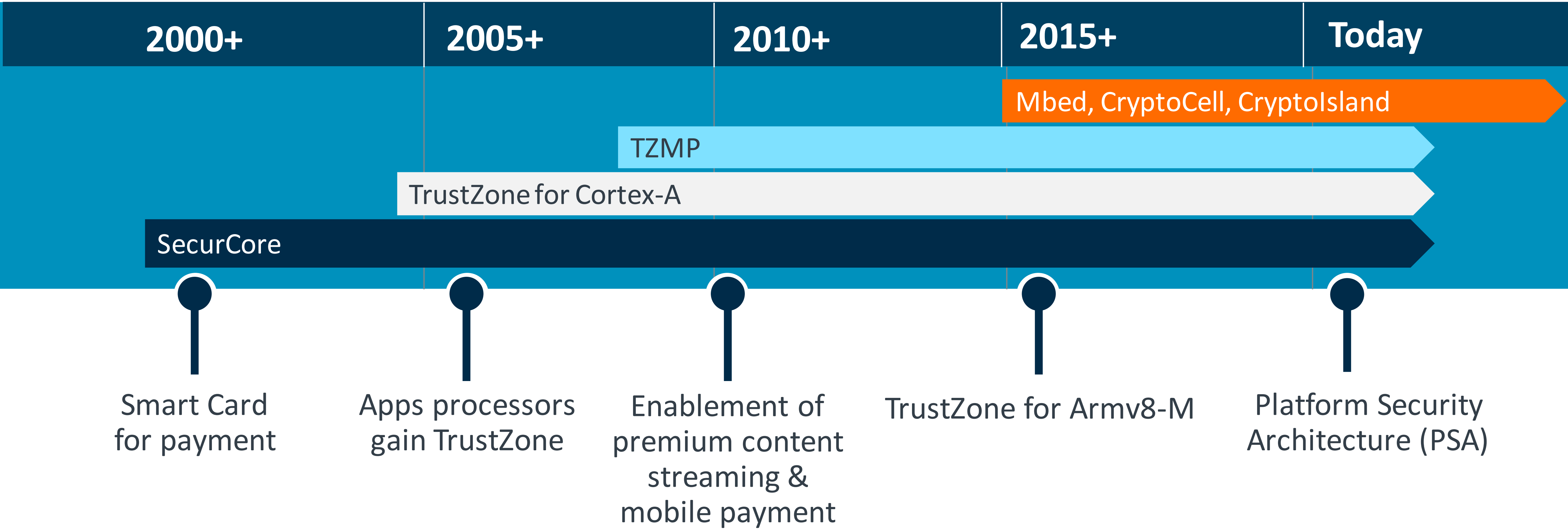
PSA: building trust in IoT

Ethan Zhang
Security Marketing Manager

Arm secure IP: Helping to protect billions of devices



2000+

2005+

2010+

2015+

Today

Mbed, CryptoCell, CryptoIsland

TZMP

TrustZone for Cortex-A

SecurCore

Smart Card for payment

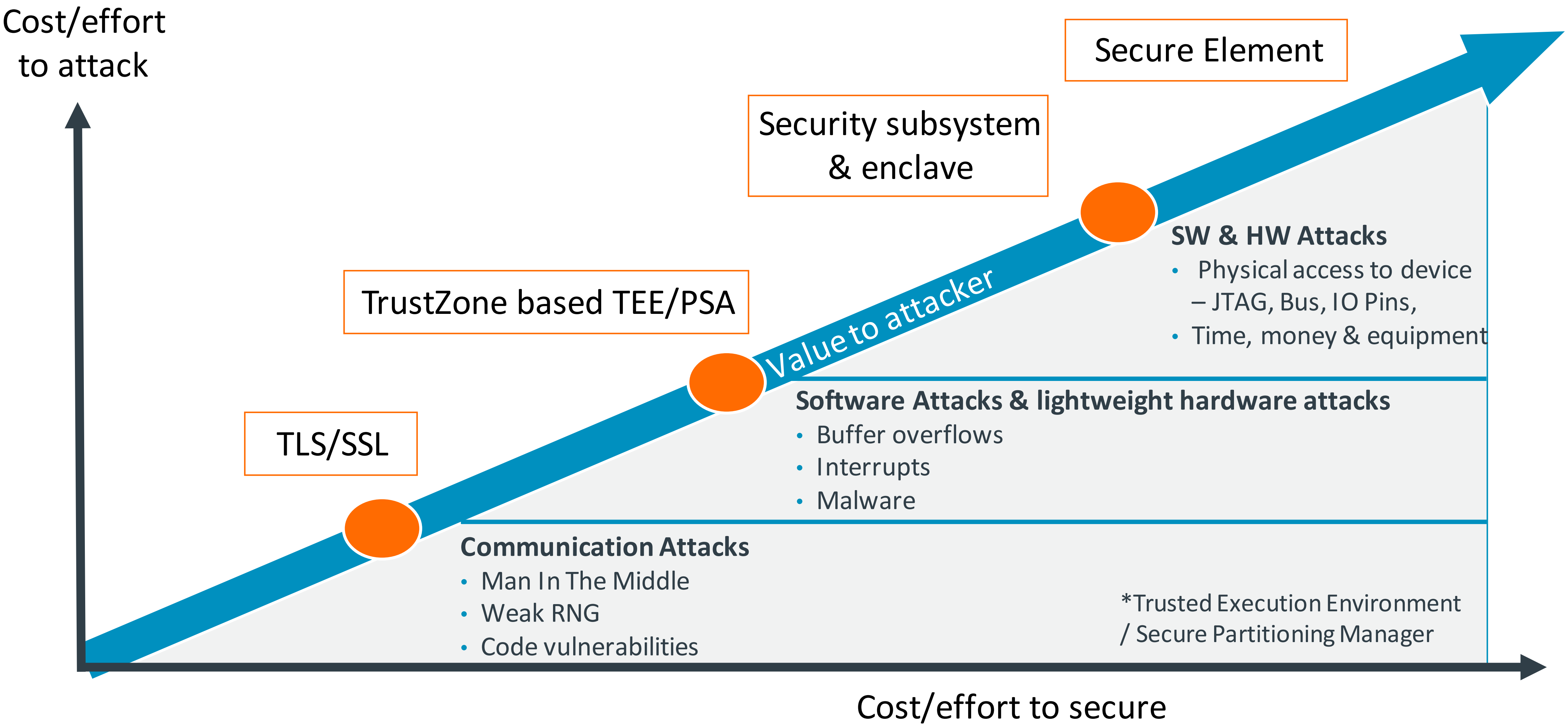
Apps processors gain TrustZone

Enablement of premium content streaming & mobile payment

TrustZone for Armv8-M

Platform Security Architecture (PSA)

How much security to fit your needs?



SW & HW Attacks

- Physical access to device – JTAG, Bus, IO Pins,
- Time, money & equipment

Software Attacks & lightweight hardware attacks

- Buffer overflows
- Interrupts
- Malware

Communication Attacks

- Man In The Middle
- Weak RNG
- Code vulnerabilities

*Trusted Execution Environment / Secure Partitioning Manager

ARM TrustZone Technology – A Security Foundation

Today

Authentication

Mobile Payment

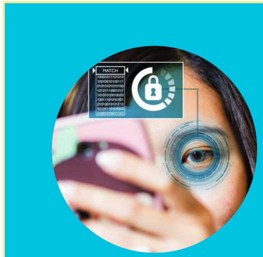
Content Protection

Enterprise Security

ARM TRUSTZONE

System Security

What can we learn from mobile & apply to IoT?

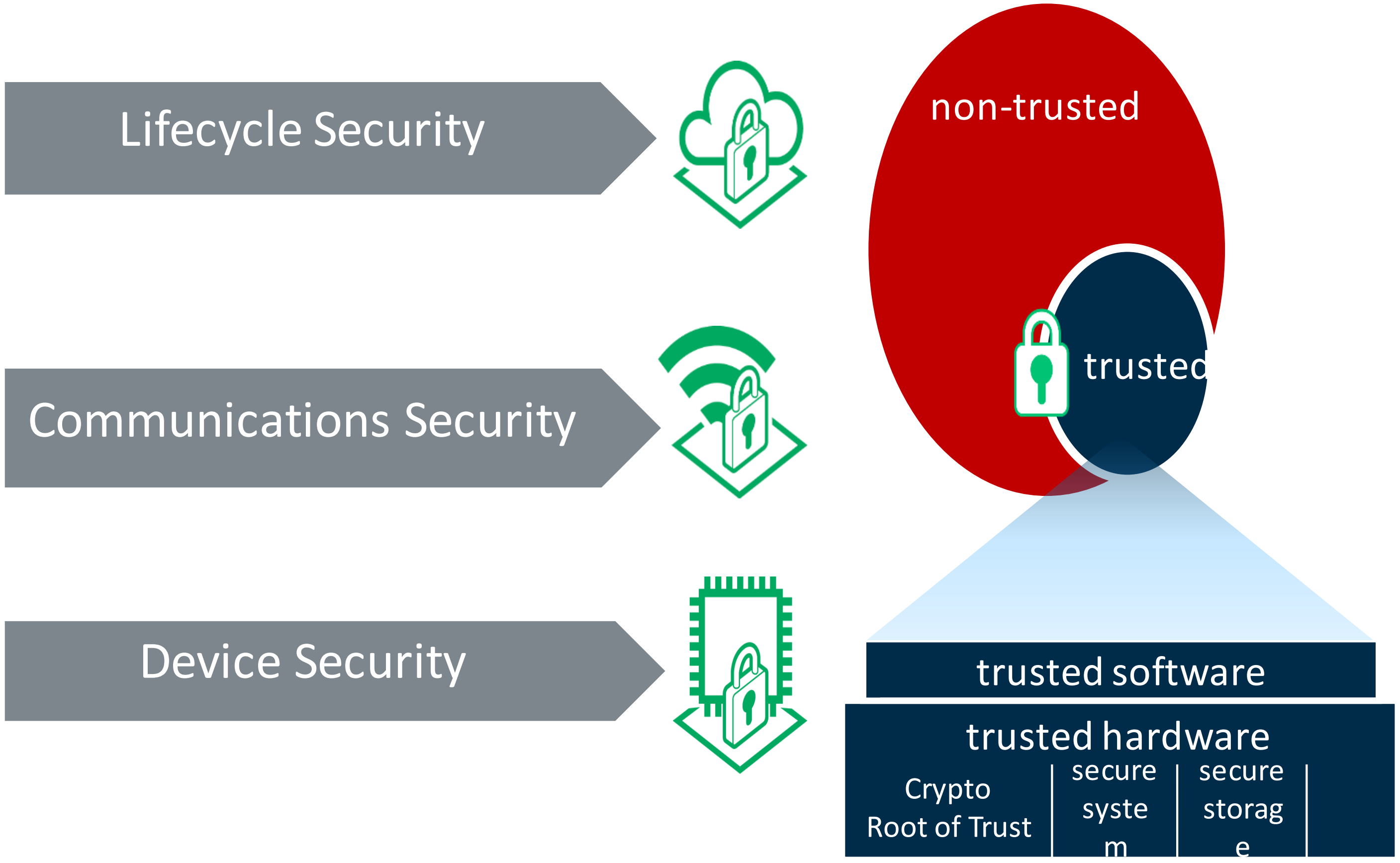


Authentication

Mobile Payment

Content Protection

Enterprise Security

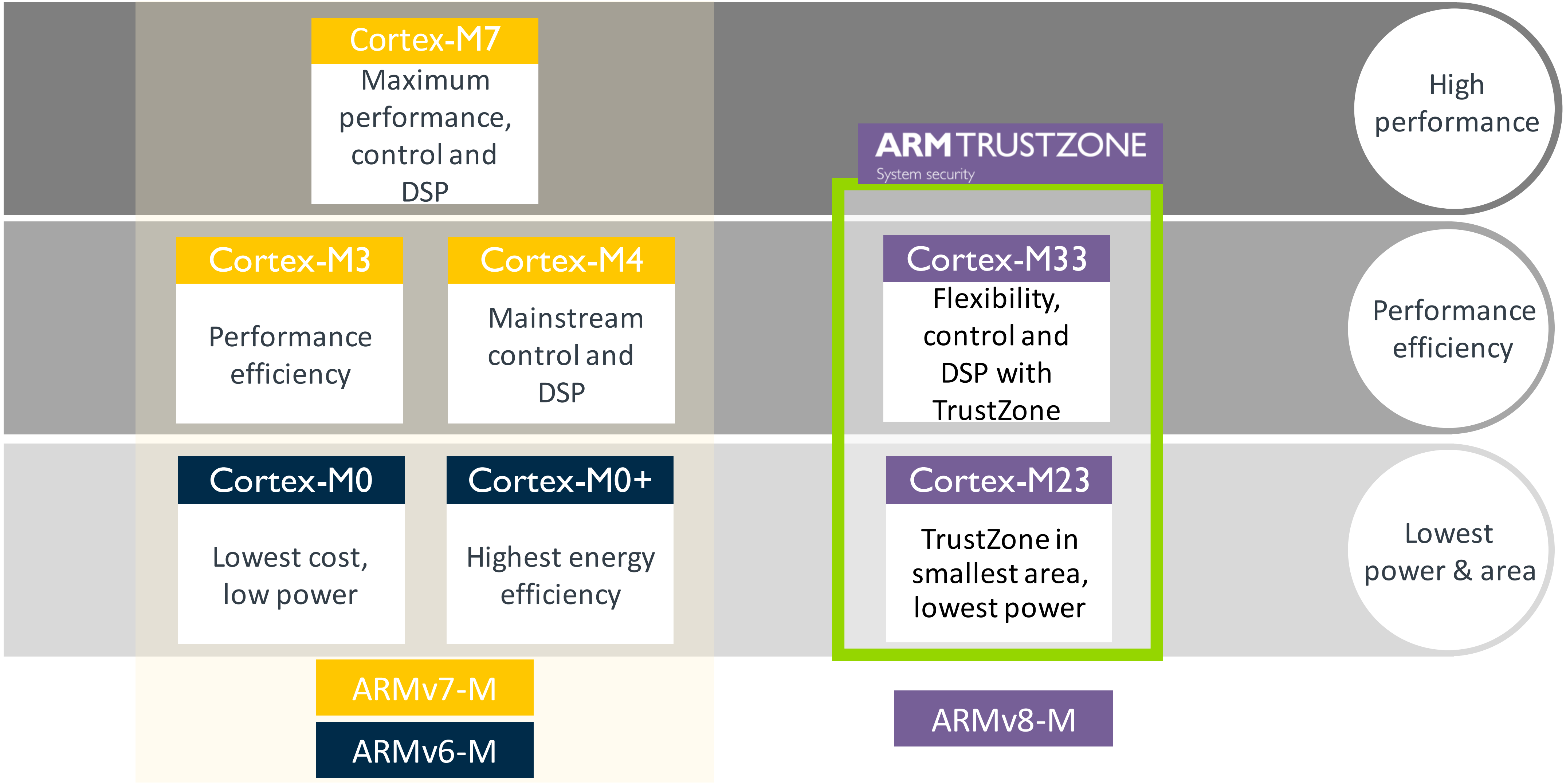


Lifecycle Security

Communications Security

Device Security

Bringing TrustZone to the Cortex-M family



Cortex-M7
Maximum performance, control and DSP

Cortex-M3
Performance efficiency

Cortex-M4
Mainstream control and DSP

Cortex-M0
Lowest cost, low power

Cortex-M0+
Highest energy efficiency

ARMv7-M

ARMv6-M

ARM TRUSTZONE
System security

Cortex-M33
Flexibility, control and DSP with TrustZone

Cortex-M23
TrustZone in smallest area, lowest power

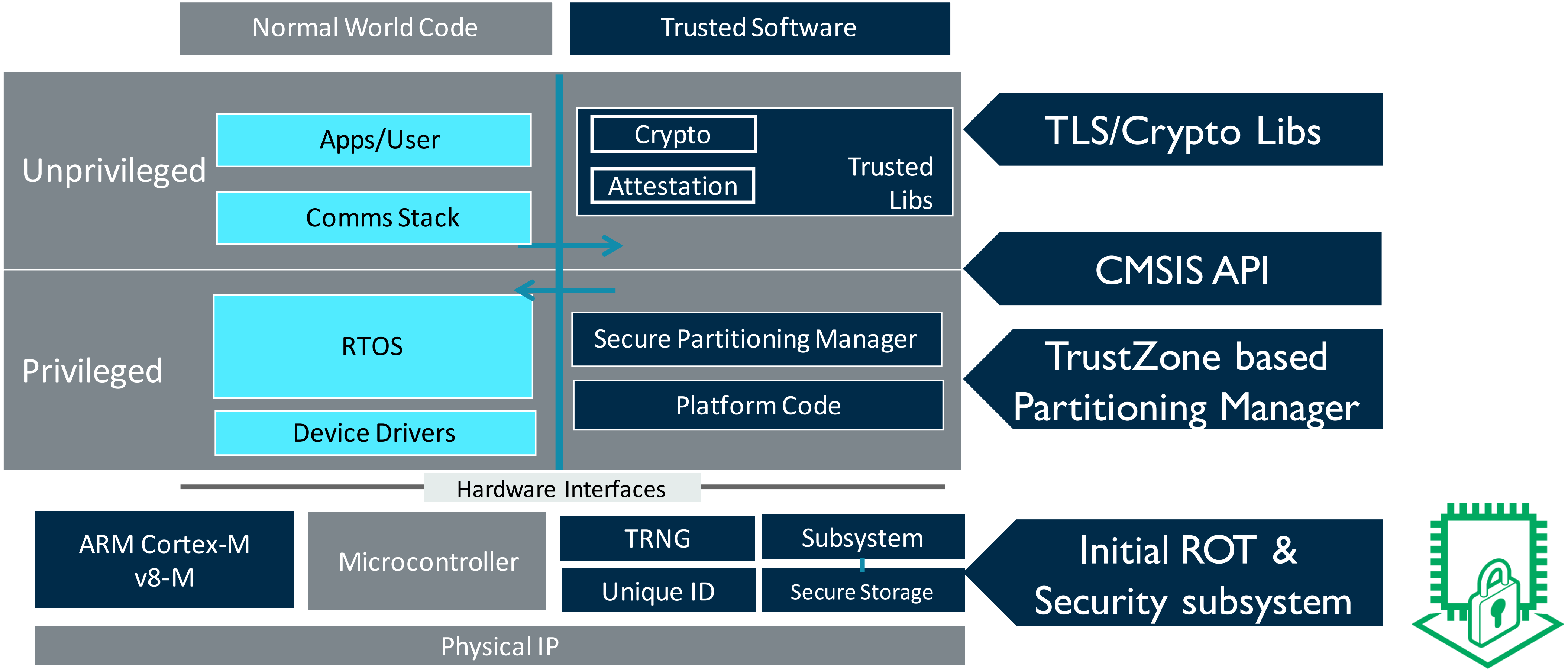
ARMv8-M

High performance

Performance efficiency

Lowest power & area

MCU architecture becoming similar to mobile



Normal World Code

Trusted Software

Unprivileged

Apps/User

Comms Stack

Crypto

Attestation

Trusted Libs

Privileged

RTOS

Device Drivers

Secure Partitioning Manager

Platform Code

Hardware Interfaces

ARM Cortex-M v8-M

Microcontroller

TRNG

Unique ID

Subsystem

Secure Storage

Physical IP

TLS/Crypto Libs

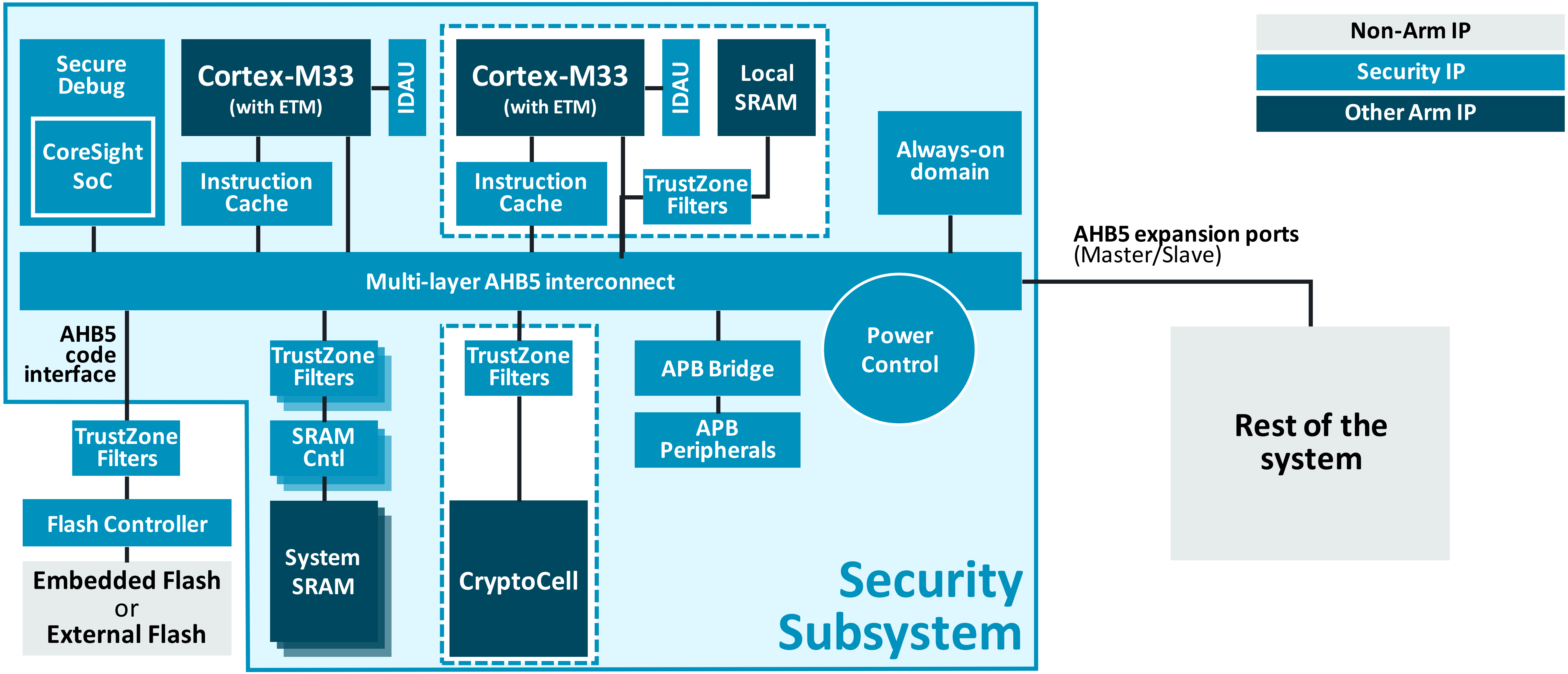
CMSIS API

TrustZone based Partitioning Manager

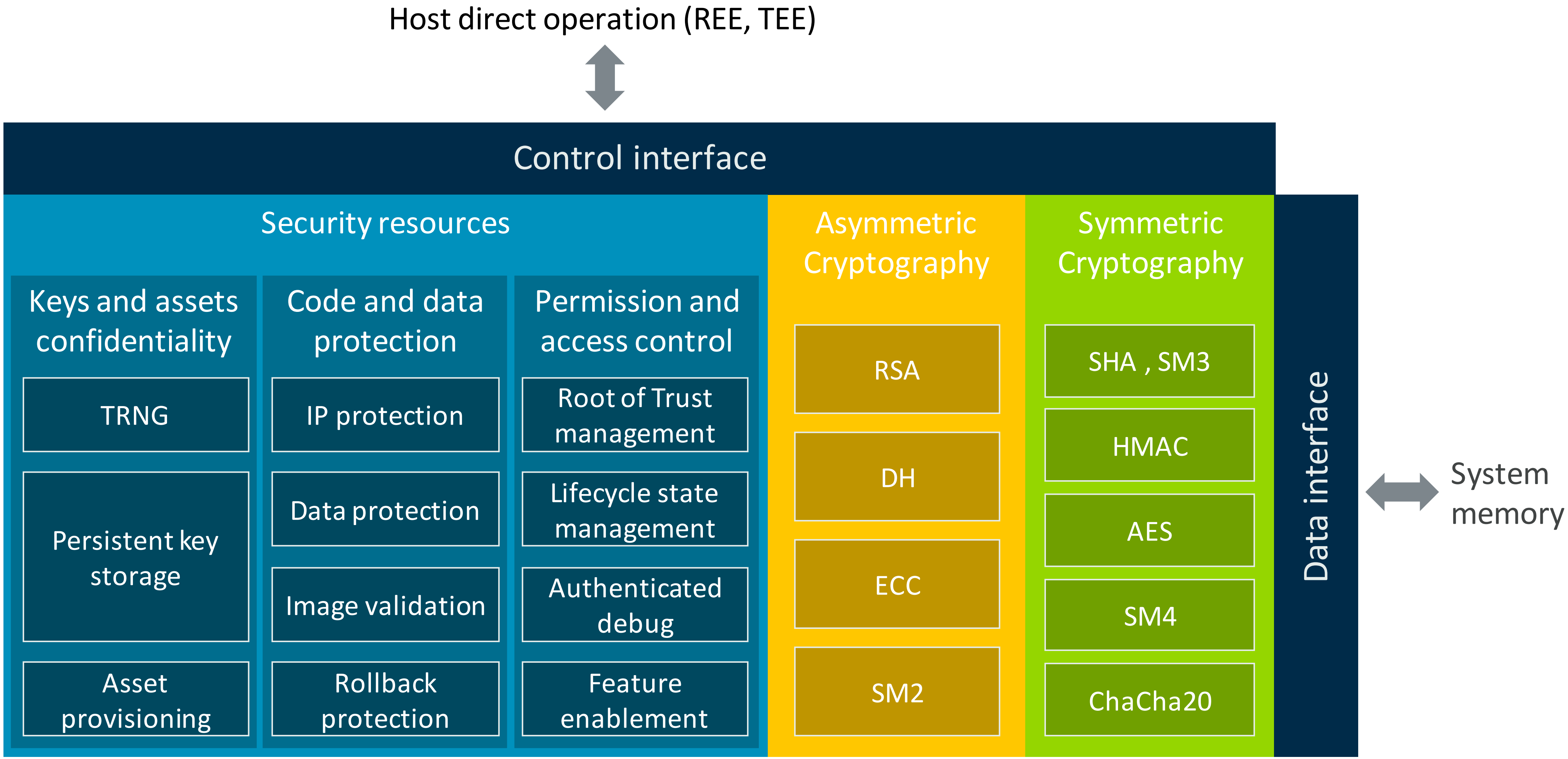
Initial ROT & Security subsystem

TrustZone enabled MCU

Security Subsystem Example



TrustZone CryptoCell



Host direct operation (REE, TEE)

Control interface

Security resources

Keys and assets confidentiality

TRNG

Persistent key storage

Asset provisioning

Code and data protection

IP protection

Data protection

Image validation

Rollback protection

Permission and access control

Root of Trust management

Lifecycle state management

Authenticated debug

Feature enablement

Asymmetric Cryptography

RSA

DH

ECC

SM2

Symmetric Cryptography

SHA , SM3

HMAC

AES

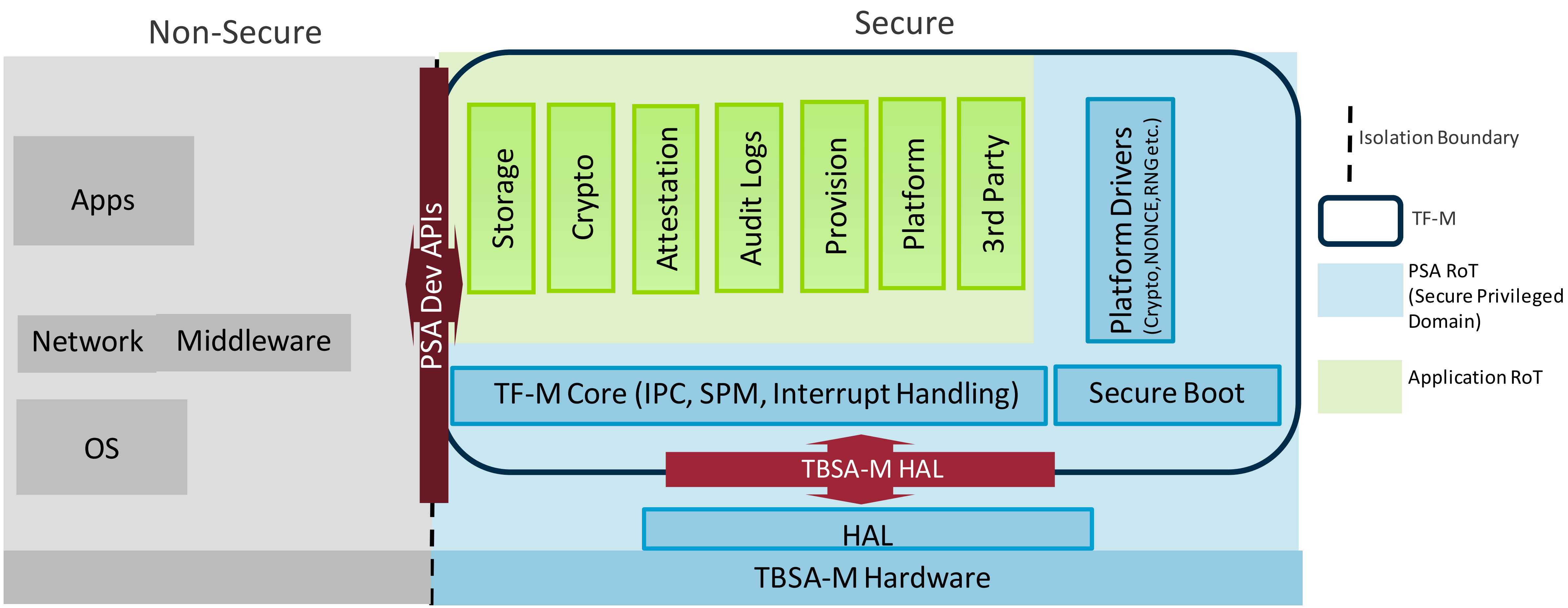
SM4

ChaCha20

Data interface

System memory

Trusted Firmware-M

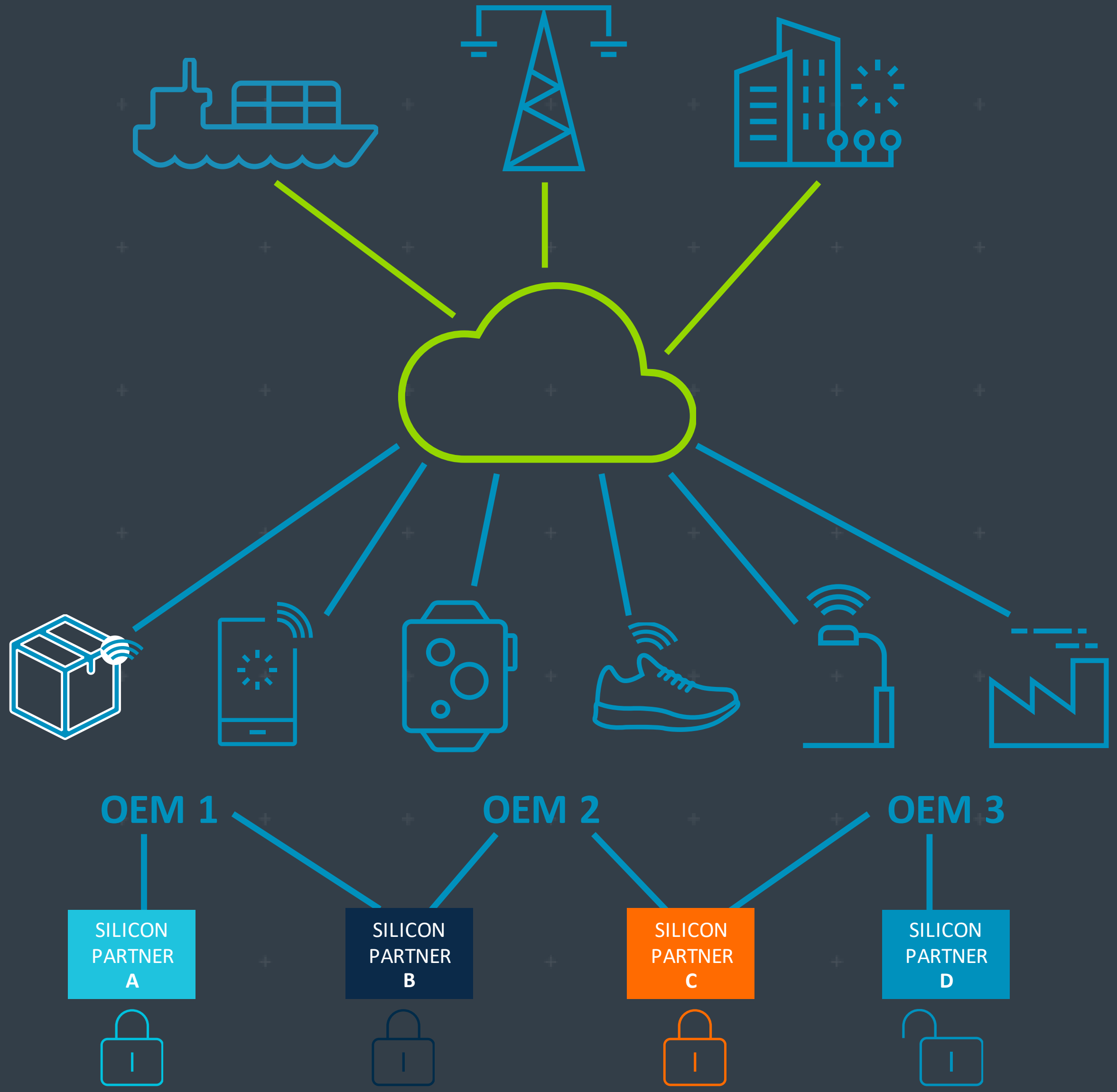


IoT Diversity Demands a Different Approach

Many cloud services needing to trust the data & therefore trust the devices

10,000’s OEMs

100’s of chip vendors with different RoT

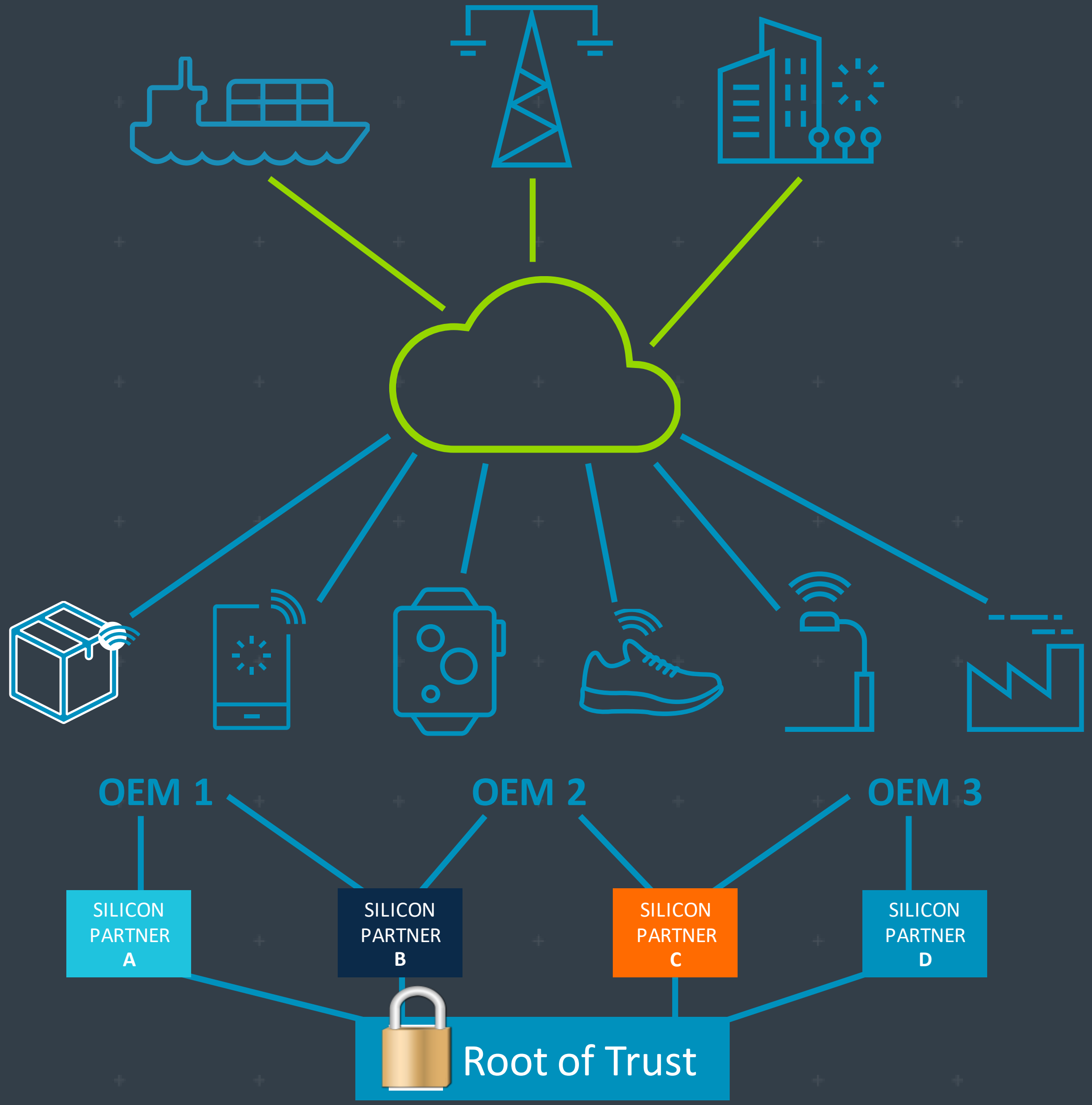


IoT Diversity Demands a Different Approach

Many cloud services needing to trust the data & therefore trust the devices

10,000’s OEMs

100’s of chip vendors with different RoT



Platform Security Architecture

The open device security framework, with independent testing

Analyze

Threat models
& security analyses

Architect

Hardware & firmware
architect specifications

Implement

Firmware
source code

Certify

psacertified™

PSA Certified – An Overview

Building trust through independent testing

Builds on IoT threat models, PSA docs, Government IoT security best practice

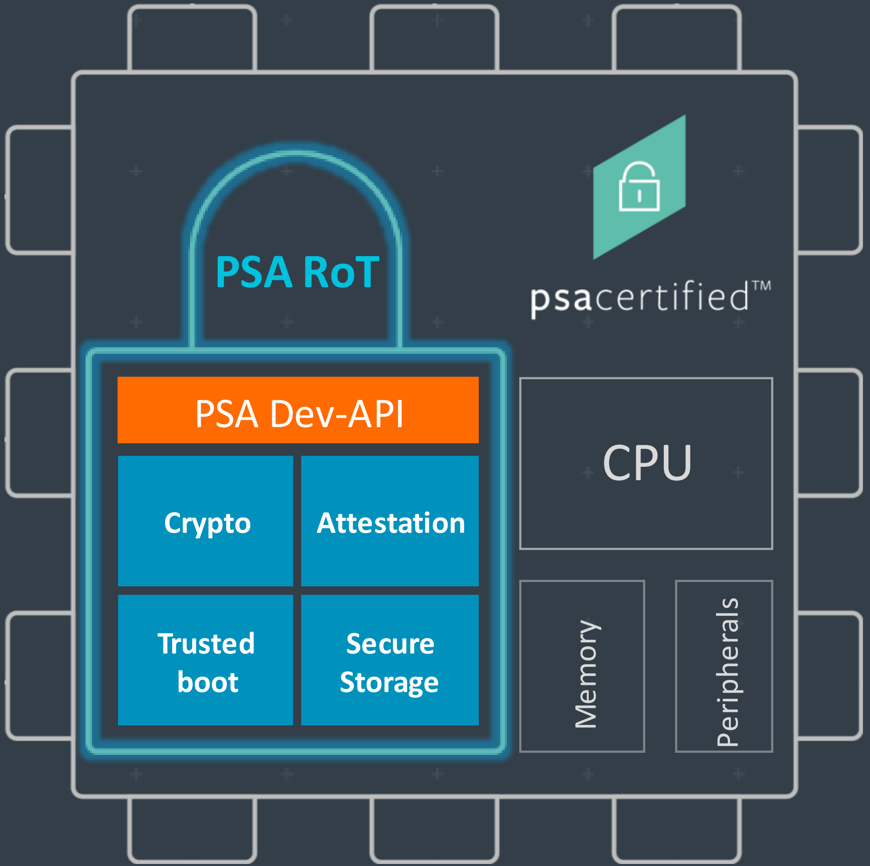
Backed by reputable experts

Supporting complementary vertical evaluations

Devices Need a Source of Trust

PSA Root of Trust (PSA-RoT)

- The source of integrity and confidentiality
- Provides **hardware isolation** of the critical security functions from the rest of the system
- Typically used for security functions such as boot, storing keys, cryptography, attestation, audit logs
- Defines PSA developer APIs to simplify access to secure services



PSA Security Model- 10 Goals

Fundamental security requirements

Secure Storage

Secure Boot

Isolation of Root of Trust

Secure update process

Validation of updates

Attestation

Unique instance ID

TRNG services

Security lifecycle

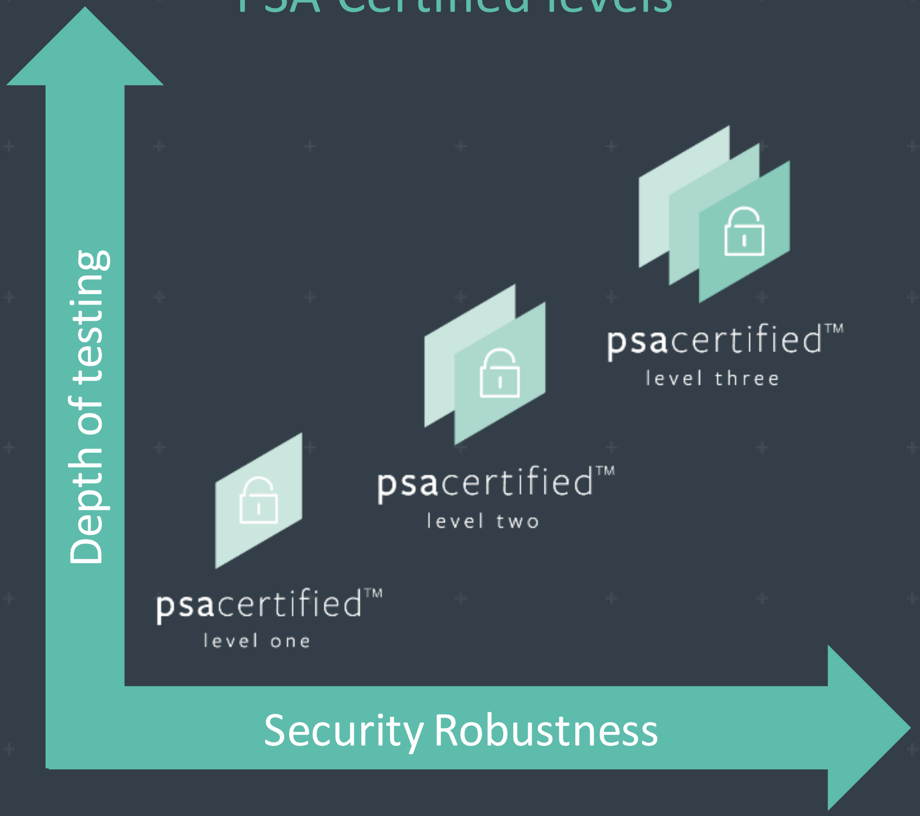
Anti-rollback feature

How it Works

- PSA Certified provides three progressive levels of security assurance/robustness: PSA Certified Level 1, 2 and 3

- PSA functional API enables software scalability

PSA Certified levels



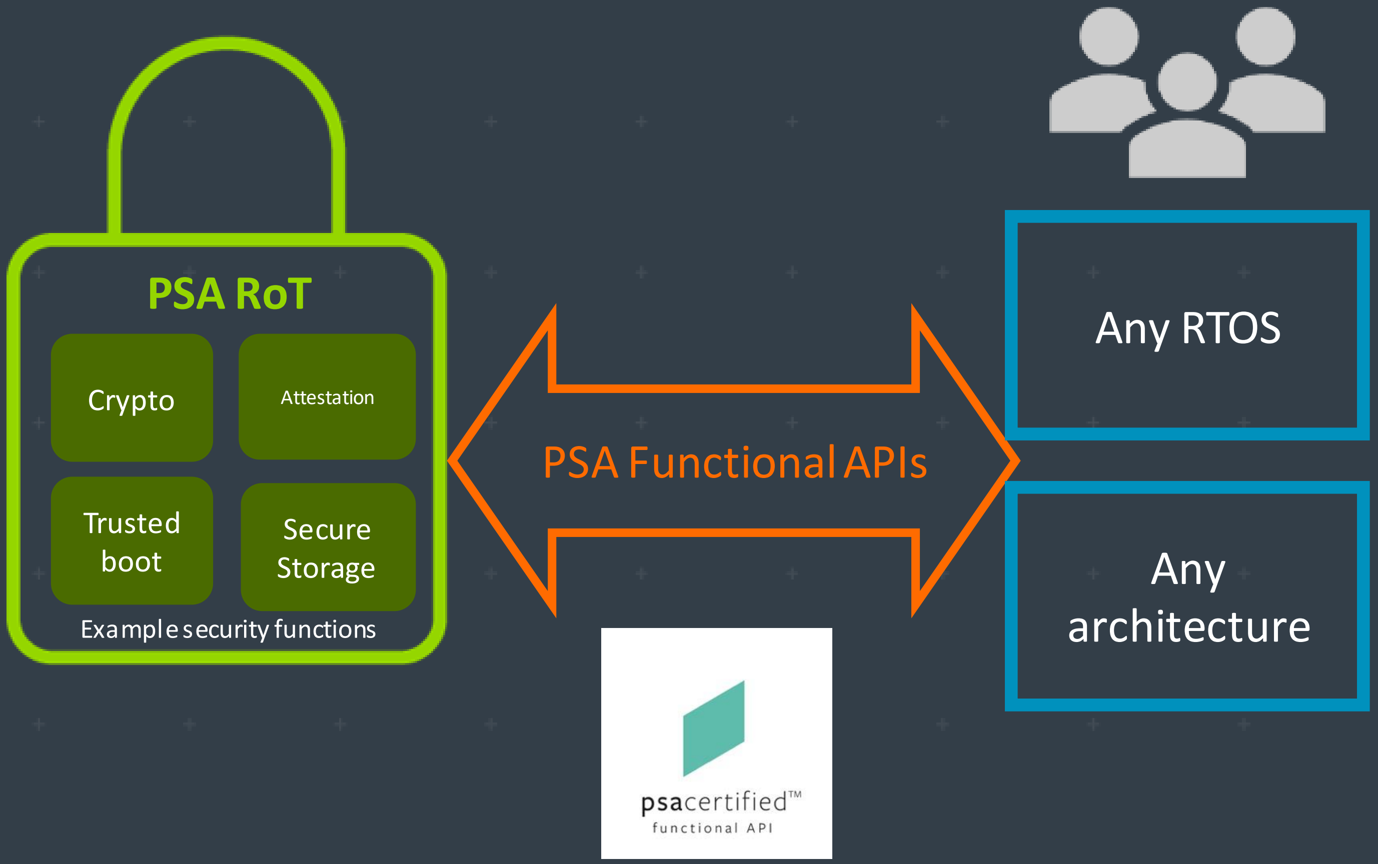
Who it targets

- Level 1 targets silicon, OS, and OEM
- Level 2 & Level 3 focus on silicon companies PSA RoT implementations

PSA Certification level & test time	Silicon	OS	OEM
Level 3 *Months*	✓	3rd party evaluation schemes	
Level 2 *1 month*	✓		
Level 1 *1 day*	✓	✓	✓

www.psacertified.org

PSA Functional API Certification



PSA RoT

Crypto

Attestation

Trusted boot

Secure Storage

Example security functions

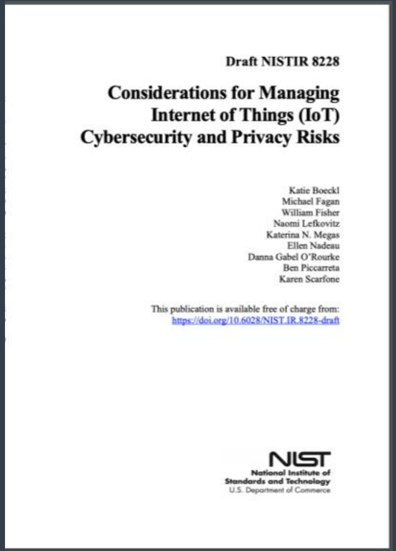
PSA Functional APIs

Any RTOS

Any architecture

Governments are creating IoT security requirements

PSA & PSA certified help address common IoT security



Draft NISTIR 8228

Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

Katie Boeckl
Michael Fagan
William Fisher
Naomi Lefkovitz
Katerina N. Megas
Ellen Nadeau
Danna Gabel O'Rourke
Ben Piccarreta
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8228-draft

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

US: NIST

ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 36951—2018

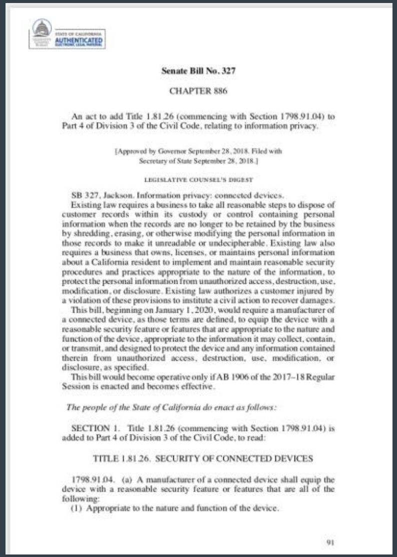
信息安全技术
物联网感知终端应用安全技术要求

Information security technology—Security technical requirements for application of sensing terminals in internet of things

2018-12-28 发布　　2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

China



STATE OF CALIFORNIA
AUTHENTICATED
ELECTRONIC LEGAL MATERIAL

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

The people of the State of California do enact as follows:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. SECURITY OF CONNECTED DEVICES

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

91

US: California

enisa

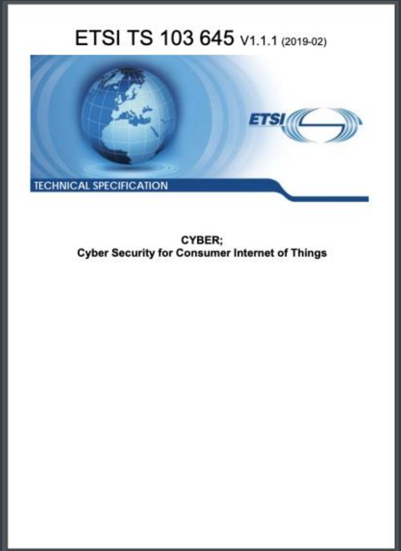
Baseline Security Recommendations for IoT

in the context of Critical Information Infrastructures

NOVEMBER 2017

www.enisa.europa.eu　European Union Agency For Network And Information Security

EU: ENISA



ETSI TS 103 645 V1.1.1 (2019-02)

ETSI

TECHNICAL SPECIFICATION

CYBER;
Cyber Security for Consumer Internet of Things

UK: ETSI

IoT security is an issue that affects citizens lives, crime reduction & counter terrorism

Visit psacertified.org

Download the documents and get started

Supported by the world’s leading chip vendors

Easy process for OEMs and software platforms to build on this momentum and demonstrate they are getting basic security principles correct

PSA Certified:
building trust in IoT

Building trust through independent security assessment

PSA Partners

Chip Vendor, RTOS, OEM

arm CHINA

arm MBED

CYPRESS EMBEDDED IN TOMORROW™

ECO LUX IoT Lifecycle Security

expresslogic

lierda 利尔达科技集团

Zephyr™ Project

MICROCHIP

NORDIC SEMICONDUCTOR

NXM

NXP

RENESAS

security platform connecting trusted

SILICON LABS

ST

紫光展锐™ UNISOC

winbond

ZAYA

ATS 摩联科技

INGEEK 银基

RT-Thread 小而美的物联网操作系统

青莲云

……

Summary

PSA Certified™ builds trust in devices and data

Security certification
A multi-level scheme testing the security assurance/robustness of IoT chips, platforms & devices designed for systems that contain a PSA-RoT

psacertified™

Functional API certification (API Compliance)
Uses test kits to prove that PSA based solutions have a consistent set of APIs for essential security functions, ensuring a consistent developer experience

psacertified™
functional API