arm

Tech Symposia 2019

Building Trust Across IoT Devices at Scale

Samuel Chiang
Emerging Business Group, Arm

2019

Agenda

- The IoT security landscape
- Solving IoT Security Challenges
  - The Platform Security Architecture
- PSA Certified: An Overview
- PSA Certified: Developing Future-proof Security
- Summary

arm

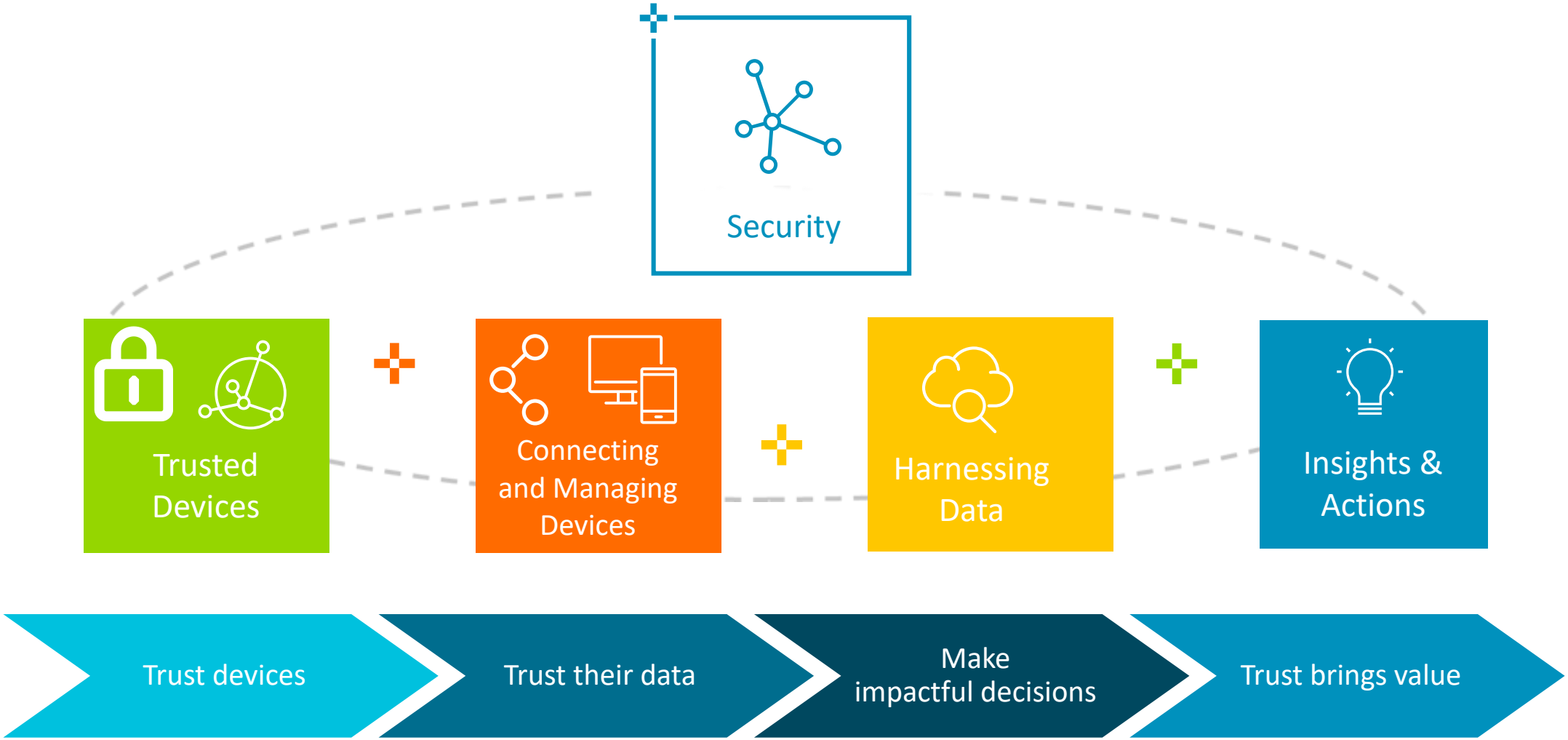
The IoT Security Landscape

IoT Devices Currently have a lot of ‘unknowns’

What I don’t know…	OEM	Security Model
Software	Chip Vendor	Root of Trust
Years of Software Updates	Robustness	Assurance/ Certification

arm

Trust is Essential for Digital Transformation



arm

The Cost of Security Inaction is Significant

There have been a number of well-documented hacks over recent years…

Eurofins Scientific: Forensic services firm paid ransom after cyber-attack

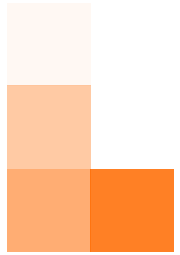
The IoT's security nightmare will never end. You can now search insecure cameras by address

Ransomware cyber-attacks are targeting large companies and demanding huge payments

Anaesthetic devices 'vulnerable to hackers'

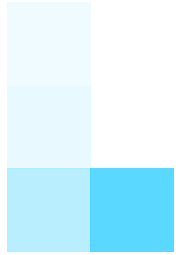
>300%

Increase in malware loaded onto IoT devices[2]



600%

Increase in IoT device attacks[1]



$6 trillion

Cost of damage related to cybercrime by 2021[3]

1 – Symantec Internet Security Threat Report 2018
2 – Kaspersky Labs, New Trends in the World of IoT Threats 2018
3 – Annual Cyber Crime Report, Cyber Security Ventures 2019

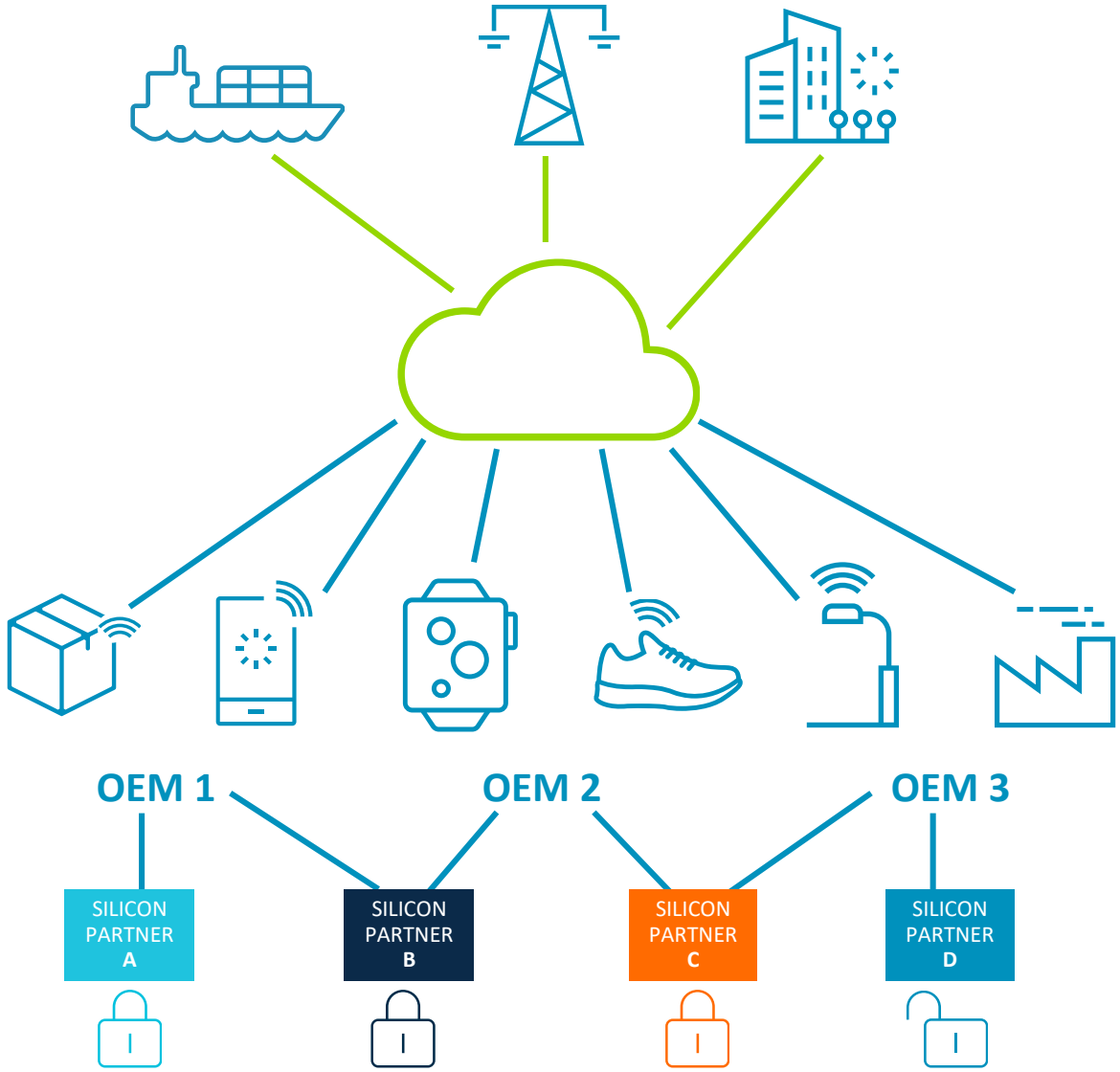
arm

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 Root of Trust

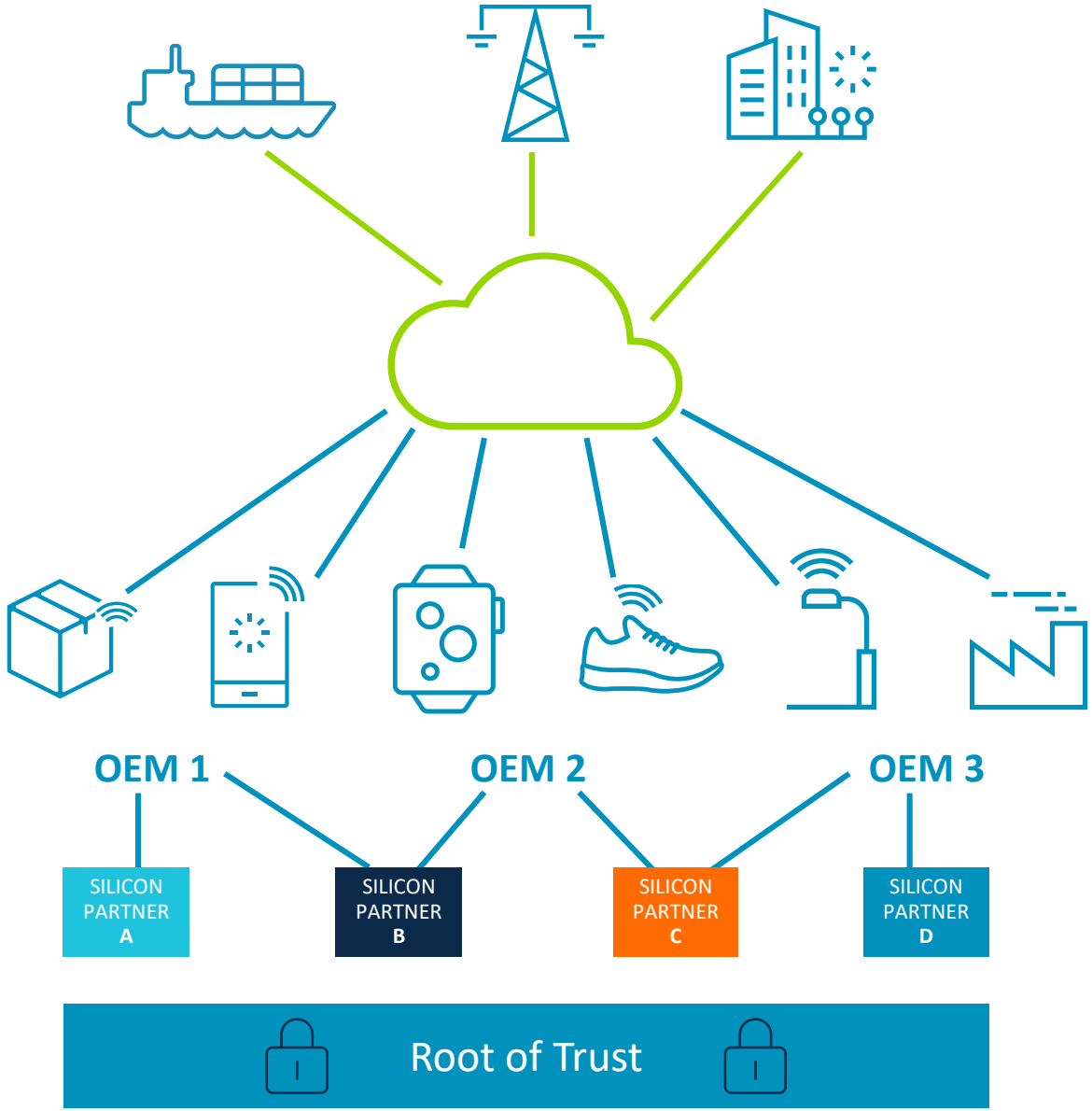


IoT Diversity Demands a Different Approach

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

10,000's OEMs

100's of chip vendors with different Root of Trust



arm

Solving IoT Security Challenges

The Platform Security Architecture

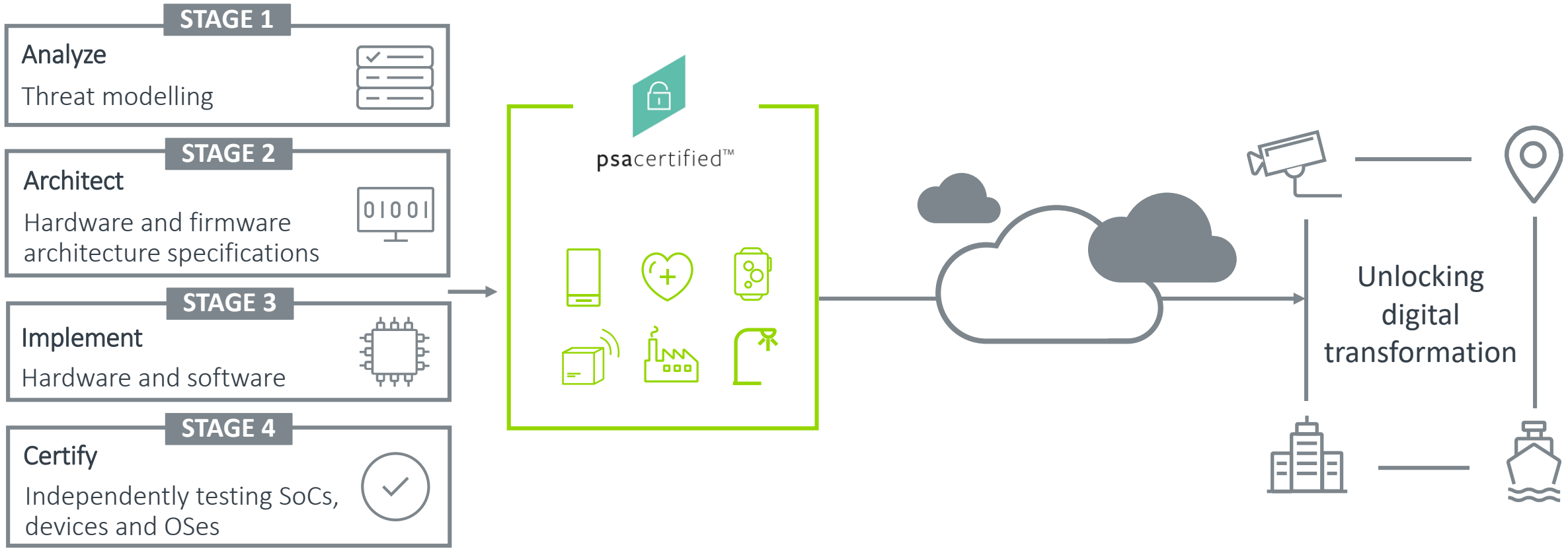
Solving the IoT Security Challenges

The Platform Security Architecture offers a number of solutions to the ecosystem

- ‘Security by design’ approach
- Removes barriers to development
- Reduces time-to-market and costs
- Industry-wide initiative on IoT security
- A baseline for security – PSA Certified
- Creating regulated device markets (most of IoT)
- Secure devices will drive IoT business
- Any architecture (not just Arm)

Platform Security Architecture (PSA)

The open device security framework, with independent testing



PSA: enabling right-sized device security

arm

Security Should Always Start with Analysis

Analyze

Threat modelling

What are the threats to my device?

What are my assets?

What is damage is done if my assets are compromised?

Security threats to be analyzed

Physical attacks

- Non-invasive; e.g. clock or power glitch or SCA
- Invasive; package removal e.g. microprobe station FIB

Software attacks

- Buffer overflows
- Interrupts
- Malware
- Code vulnerabilities

Communication attacks

- Man-in-the-middle
- Weak RNG
- Weak protocols

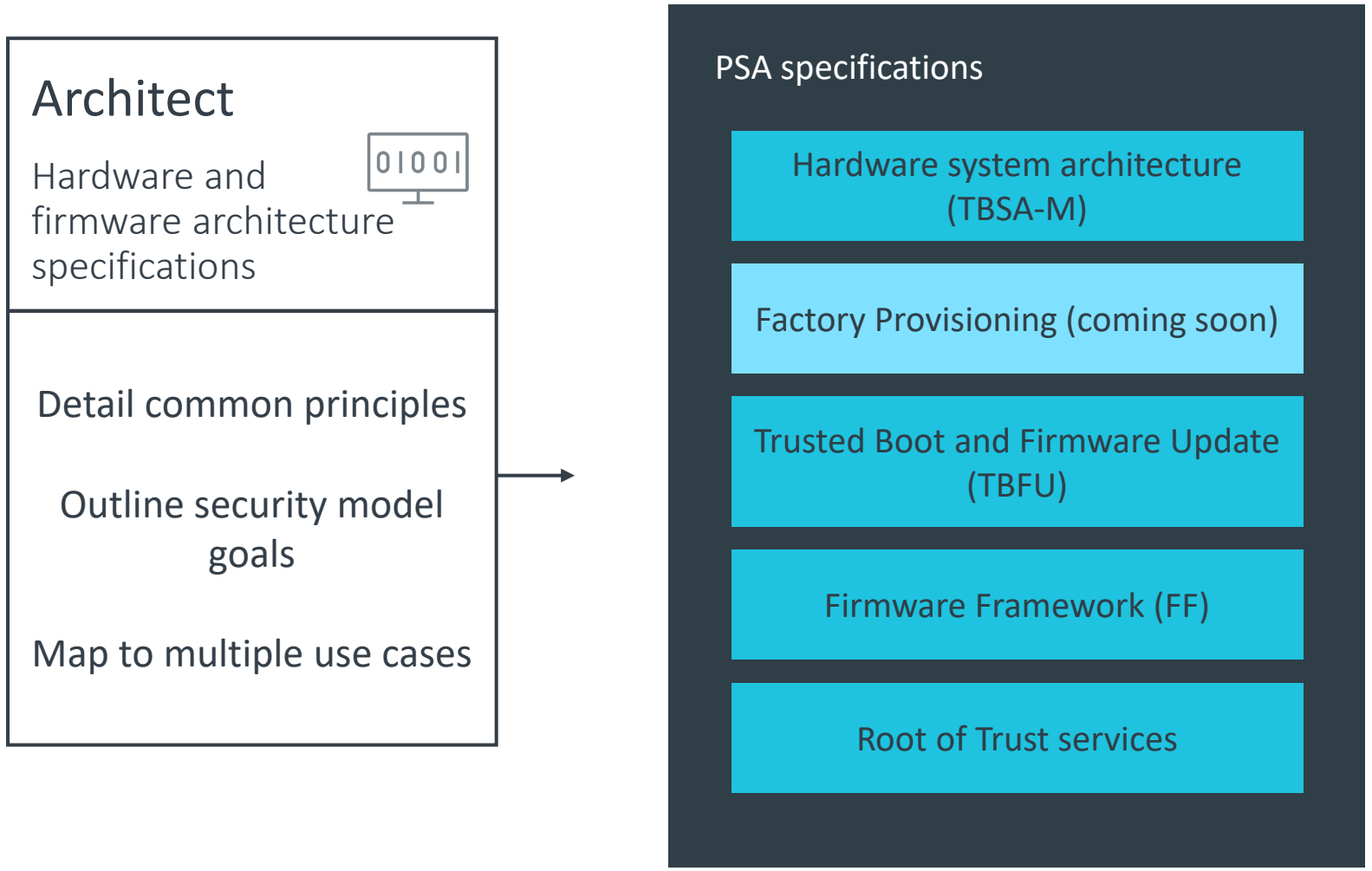
Lifecycle attacks

- Code downgrade
- Ownership changes
- Unauthorized overproduction
- Debug

Define security objectives

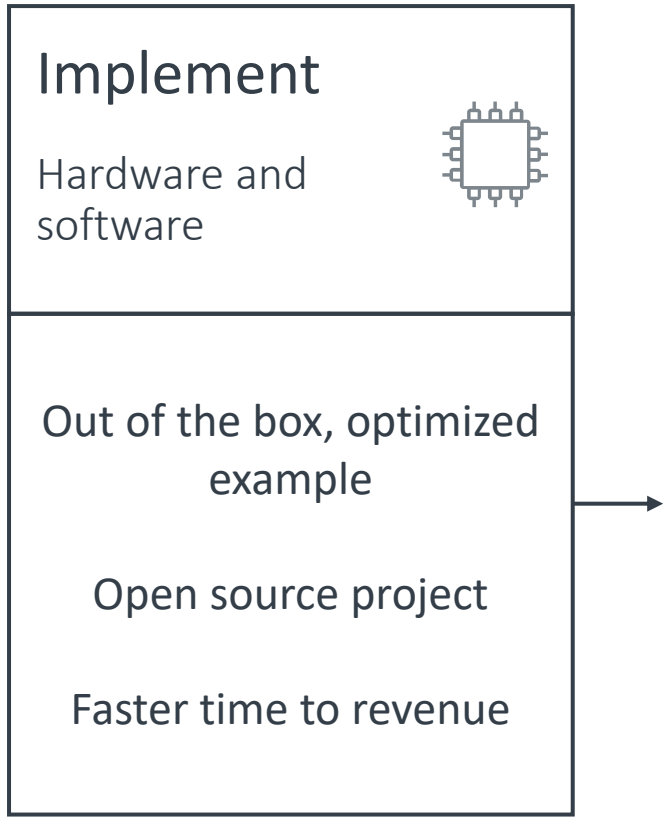
arm

Architecture Blueprints for Building Platforms based on Secure IP



arm

Accelerating the Journey to Security



PSA Developer APIs

PSA developer APIs ensure a consistent developer experience for different hardware implementations of the Root of Trust.

Trusted Firmware-M

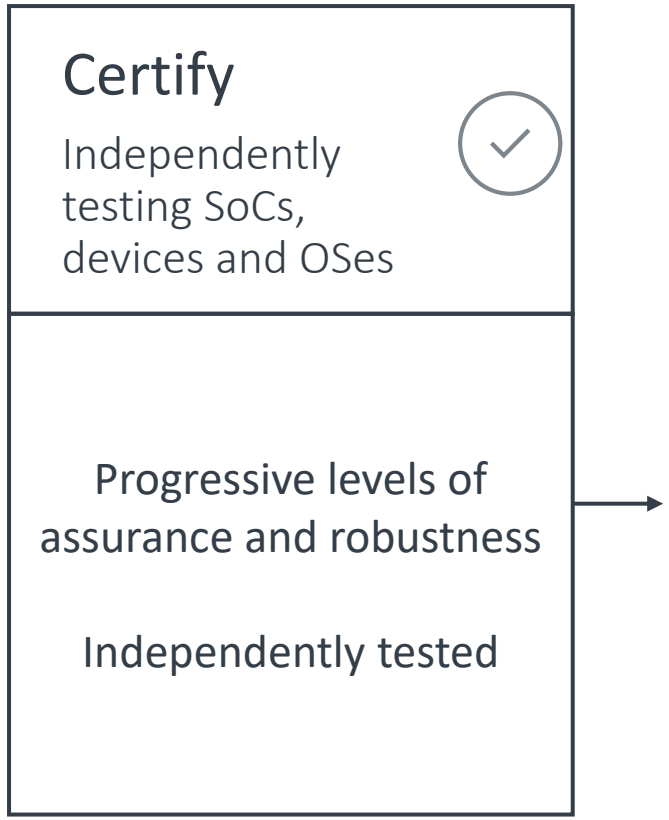
A reference implementation of secure world software. It provides SoC developers and OEMs with a reference trusted code base that complies with the PSA specifications.

arm

arm

PSA Certified: An Overview

Building an Ecosystem of Trust



psacertified™

A multi-level security evaluation scheme for chip vendors, OS providers and IoT device makers.

Three progressive levels of **assurance and robustness.**

Functional API Certification testing that PSA-based solutions have a **consistent set of APIs for essential security functions**

arm

Building Trust Through Independent Testing

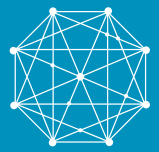
psacertified™

Dedicated to PSA Root of Trust (PSA-RoT) enabled chips, devices and platforms

Builds on IoT threat models, PSA docs, government best practice & protection profiles

Simple three-level scheme

Scalable to IoT ecosystem



Backed by reputable experts

Supporting complementary vertical evaluations

arm

PSA Certified – chips and devices

Building trust through independent security assessment

psacertified™
level one

- Based on security model goals and IoT threat models
- 40 critical security questions with lab interview
- For chip vendors, OS vendors and device makers
- Working to align next version with government regulations

psacertified™
level two

- Lab-based evaluation of the PSA-RoT
- Mid assurance & mid robustness
- Software attacks and lightweight hardware attacks
- For chip vendors

psacertified™
level three

- Under development
- Lab-based evaluation of the PSA-RoT
- Substantial protection from software and hardware attacks
- Aligned with Mobile TEE used to protect smartphones

www.psacertified.org/

arm

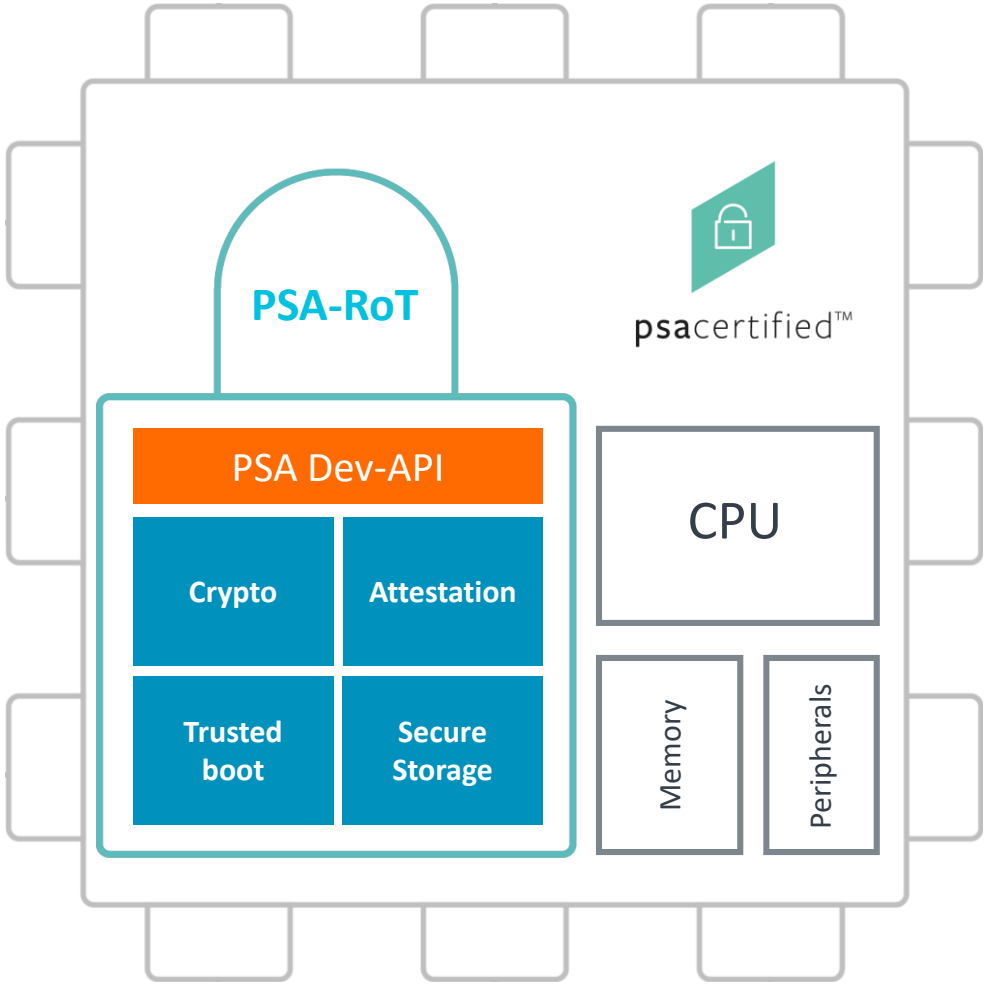
Remind Me… PSA Root of Trust (PSA-RoT)

Source of integrity and confidentiality

Separates critical security functions in a Secure Processing Environment (SPE) from rest of system

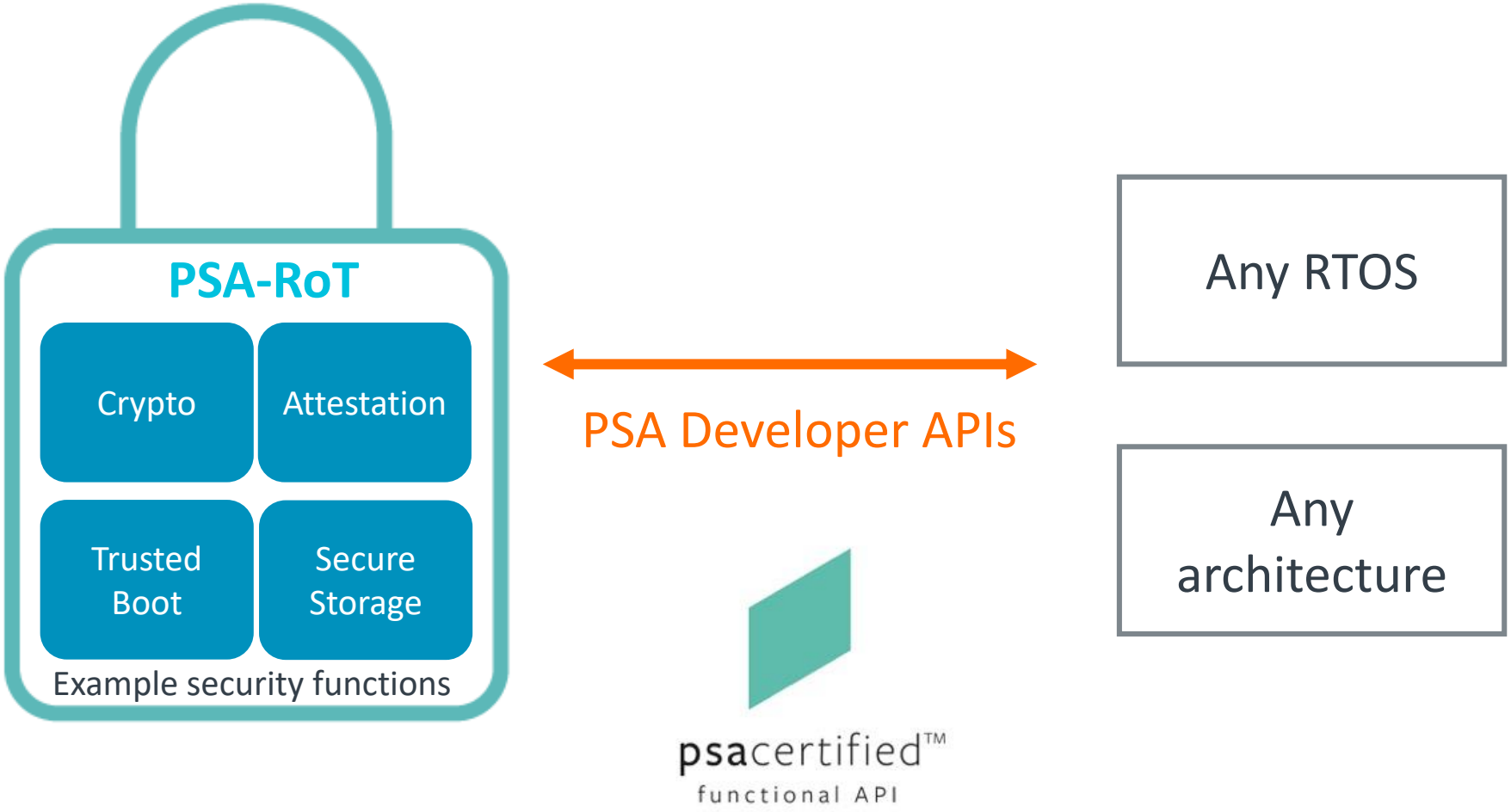
Typically used for secure boot, storing secrets, crypto, attestation, audit logs…

Developed by chip vendors
(for example, by porting Trusted Firmware-M open source software to secure hardware)



arm

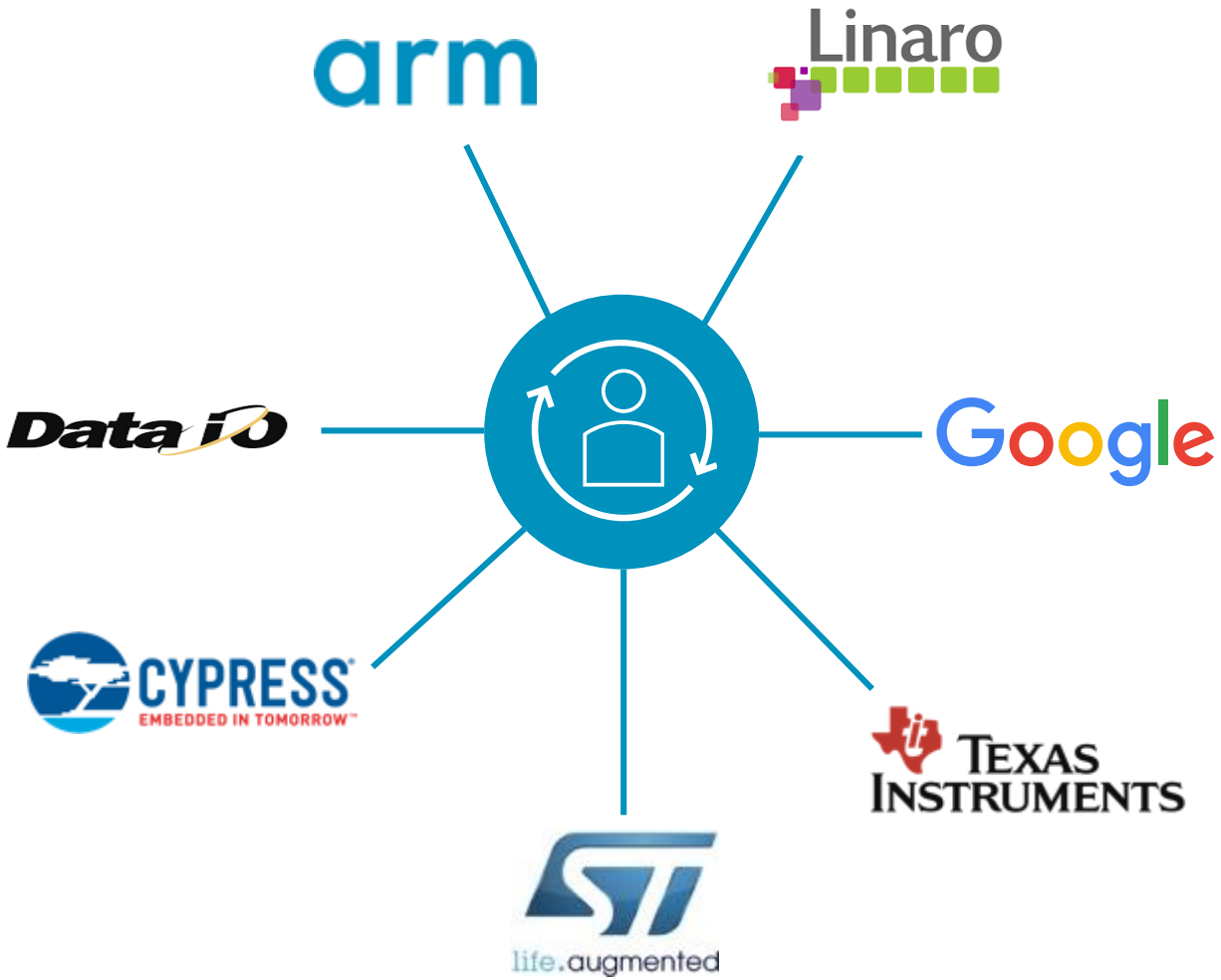
PSA APIs: An Interface between PSA-RoT and Architecture



arm

Trusted Firmware-M: Building Security Collaboratively

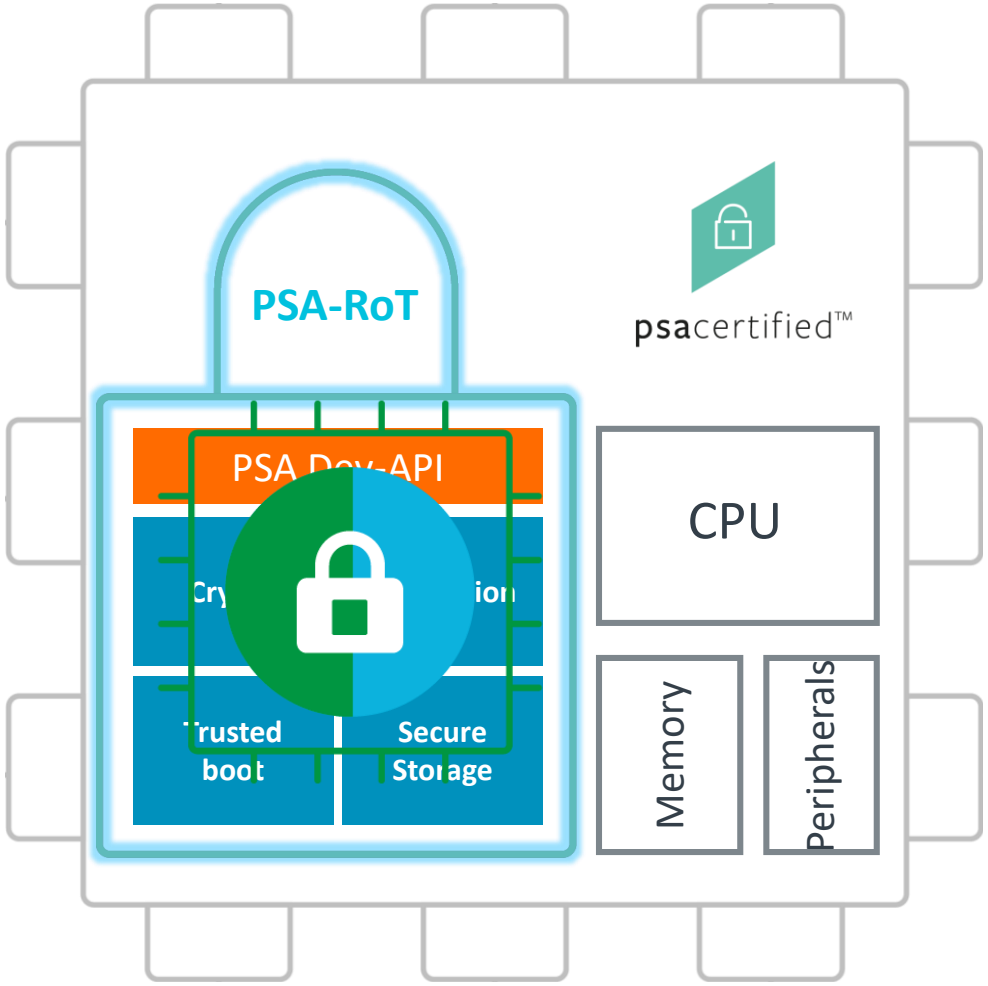
- Part of Trustedfirmware.org
  - Open Governance Community Project
- Membership open to all
- Governance overseen by a board of member representatives
- Technical direction overseen by TSC



arm

PSA Certification and Trusted Firmware-M (TF-M)

- PSA Certification
  - Evaluation of PSA-RoT
  - Compliance to PSA Developer APIs
- TF-M
  - Provides updatable PSA-RoT
  - Implements PSA developer APIs
  - Meets PSA security goals
  - HAL for easy porting to different platforms
  - Example port and certification available for Armv8-M reference platform Musca-A and Musca-B1

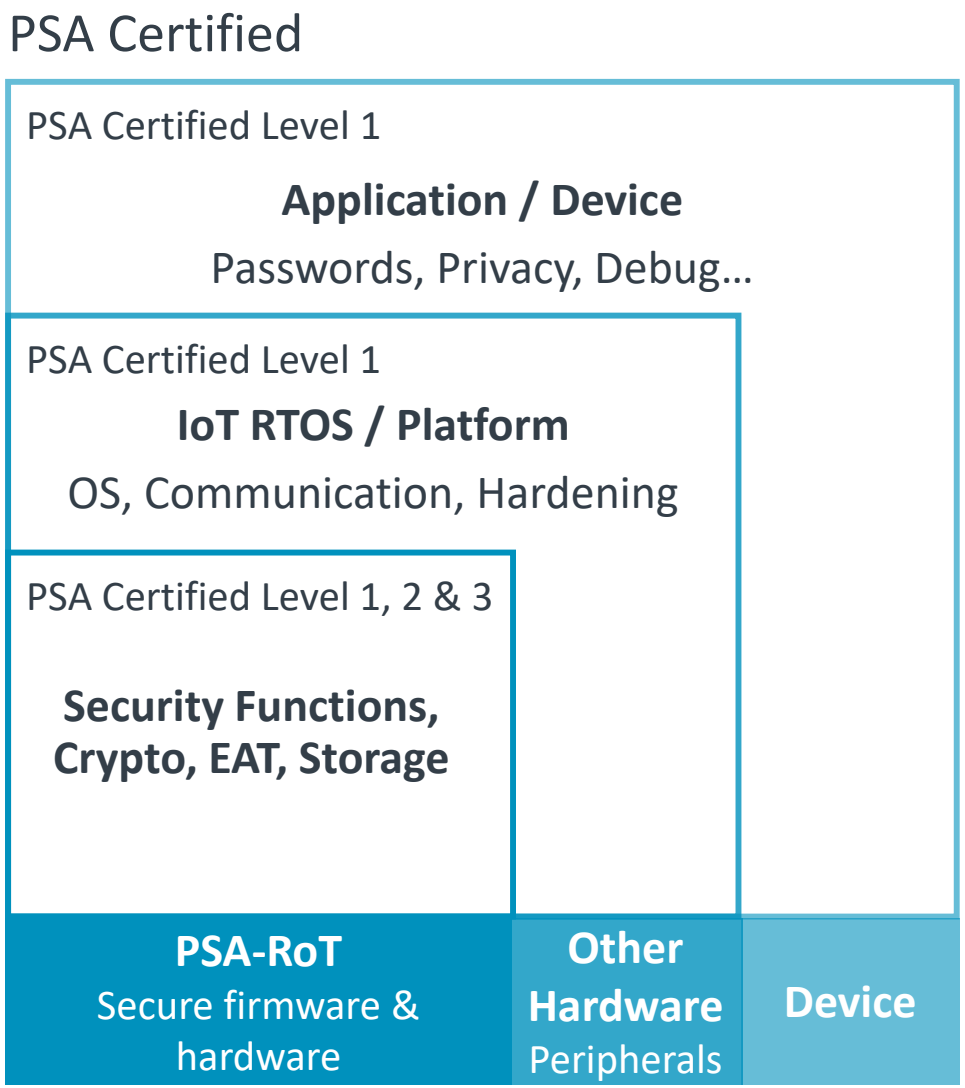


arm

arm

PSA Certified: Developing Future-proof Security

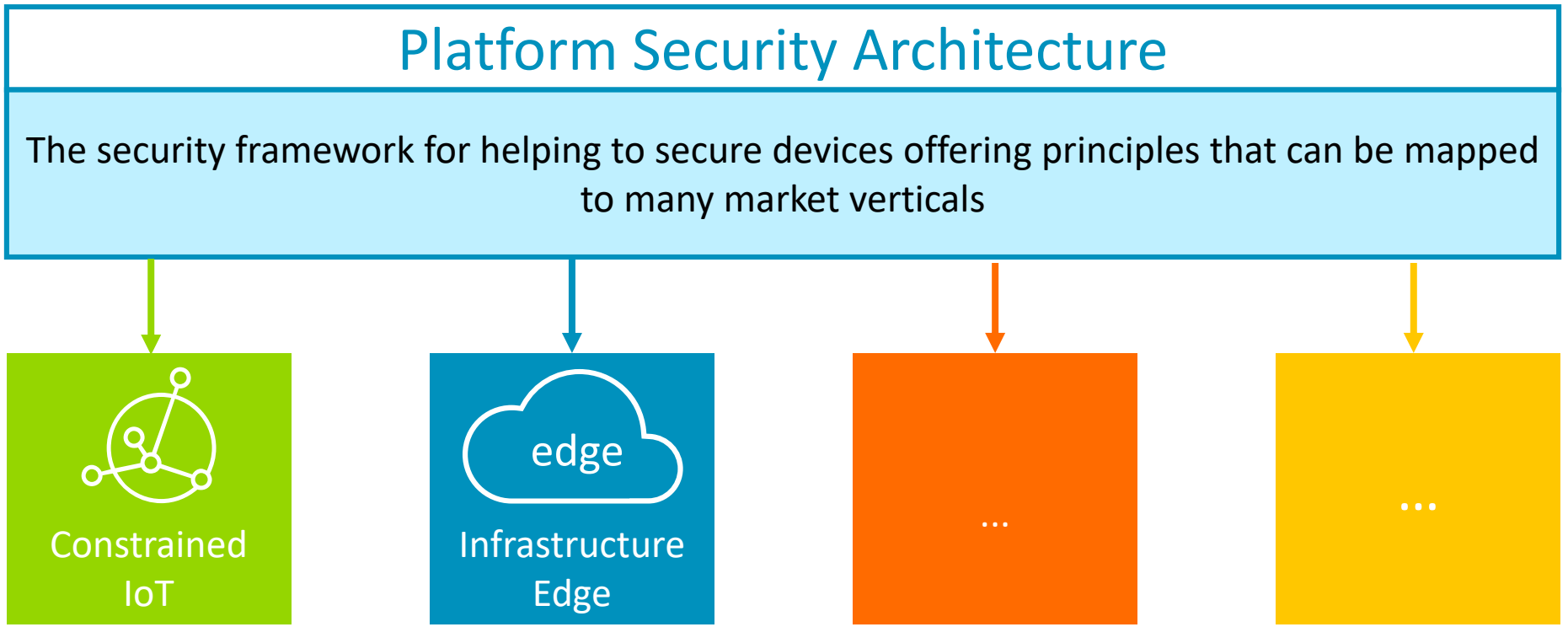
PSA Certified Provides a Baseline for Other Schemes



Comparison between NIST Core IoT Cybersecurity Capabilities Baseline and PSA Certified Level 1		
NIST Core IoT Cybersecurity Capabilities Baseline		**L1 D&D v1.0**
1	The IoT device can be identified both logically and physically.	R2.1 Device ID R4.1 Attestation
2	The IoT device's software and firmware can be updated using a secure, controlled, and configurable mechanism.	R1.1 Firmware Update
3	Authorized users can securely change the IoT device's configuration, including restoration to a secure "default". Unauthorized changes to the IoT device's configuration can be prevented.	Can be controlled by password/user authentication features of PSA L1
4	Local and remote access to the IoT device and its interfaces can be controlled.	R3.4 Malformed input D2.1 No unnecessary network port
5	The IoT device can use cryptography to secure its stored and transmitted data.	R2.4 Cryptography
6	The IoT device can use industry-accepted, standardized protocols for all layers of the device's transmissions.	R3.3 TLS
7	The IoT device can log the pertinent details of its cybersecurity events and make them accessible to authorized users and systems.	R4.3 Logging

PSA Applicability to Other Markets

Flexibility and scalability to address data challenges from multiple markets



arm

arm

Summary

Key Takeaways

PSA and PSA Certified Builds Trust in Devices and Data

PSA is a framework for security, enabling the right amount of security to be designed into devices through the PSA Root of Trust, **unlocking innovation opportunities and digital transformation**.

arm.com/psa

PSA Certified assesses the framework through

Testing solutions have **consistent developer APIs** for fundamental security functions

Providing **multi-level assurance and robustness testing** of the PSA-RoT

psacertified.org

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה