IoT Device security

Ashutosh Singh

Agenda

Connected devices common use-cases

Device security challenges

Common security functions across use-cases

Introduction to Platform Security Architecture (PSA)

Introduction to Trusted Firmware M

Questions

Please feel free to interrupt during the course of this presentation!

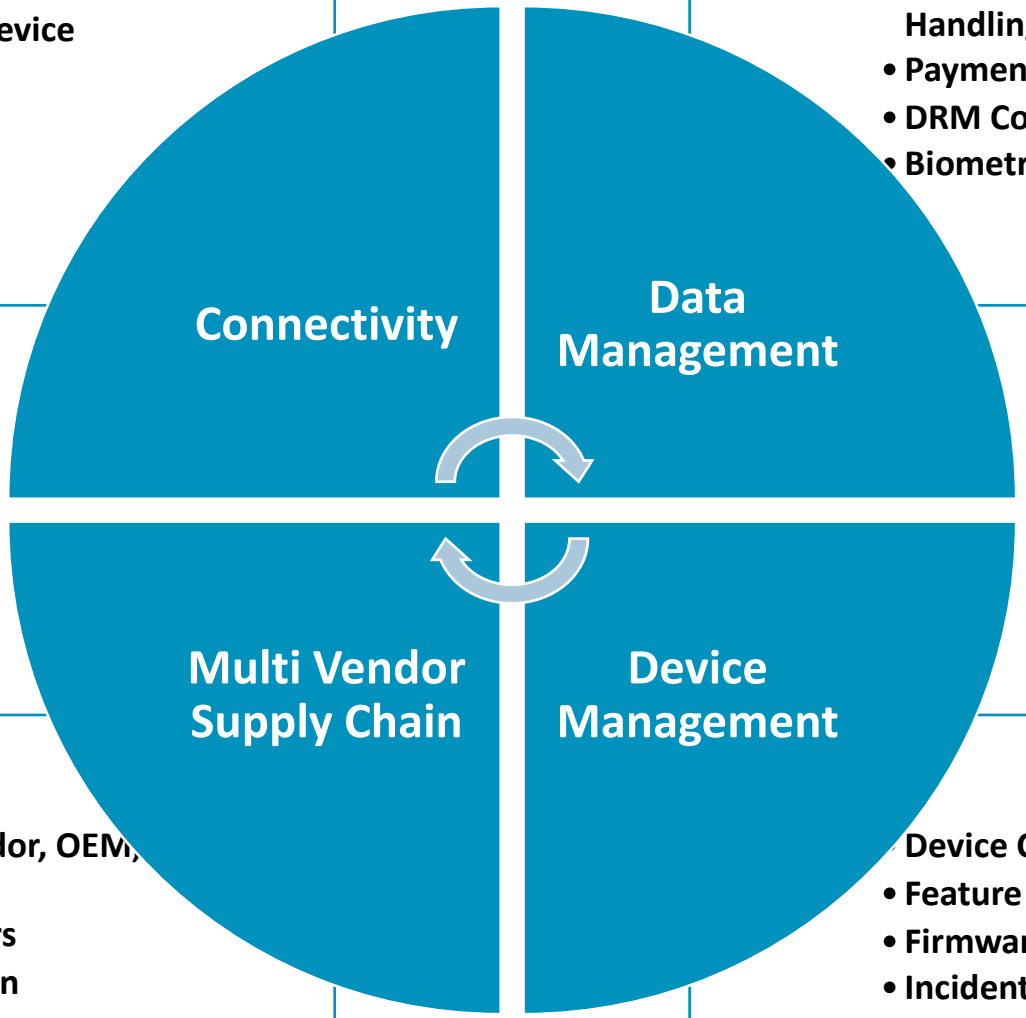
Usage Patterns & Device Security Challenges

arm

Common Usage Patterns

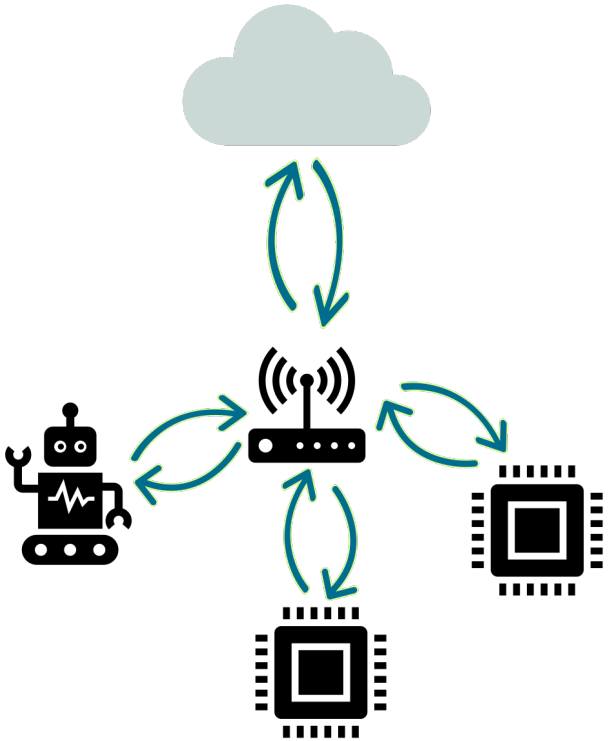
- Device to Cloud
- Device to Device

- Sensor Data Handling
- Payment Processing
- DRM Content
- Biometric data



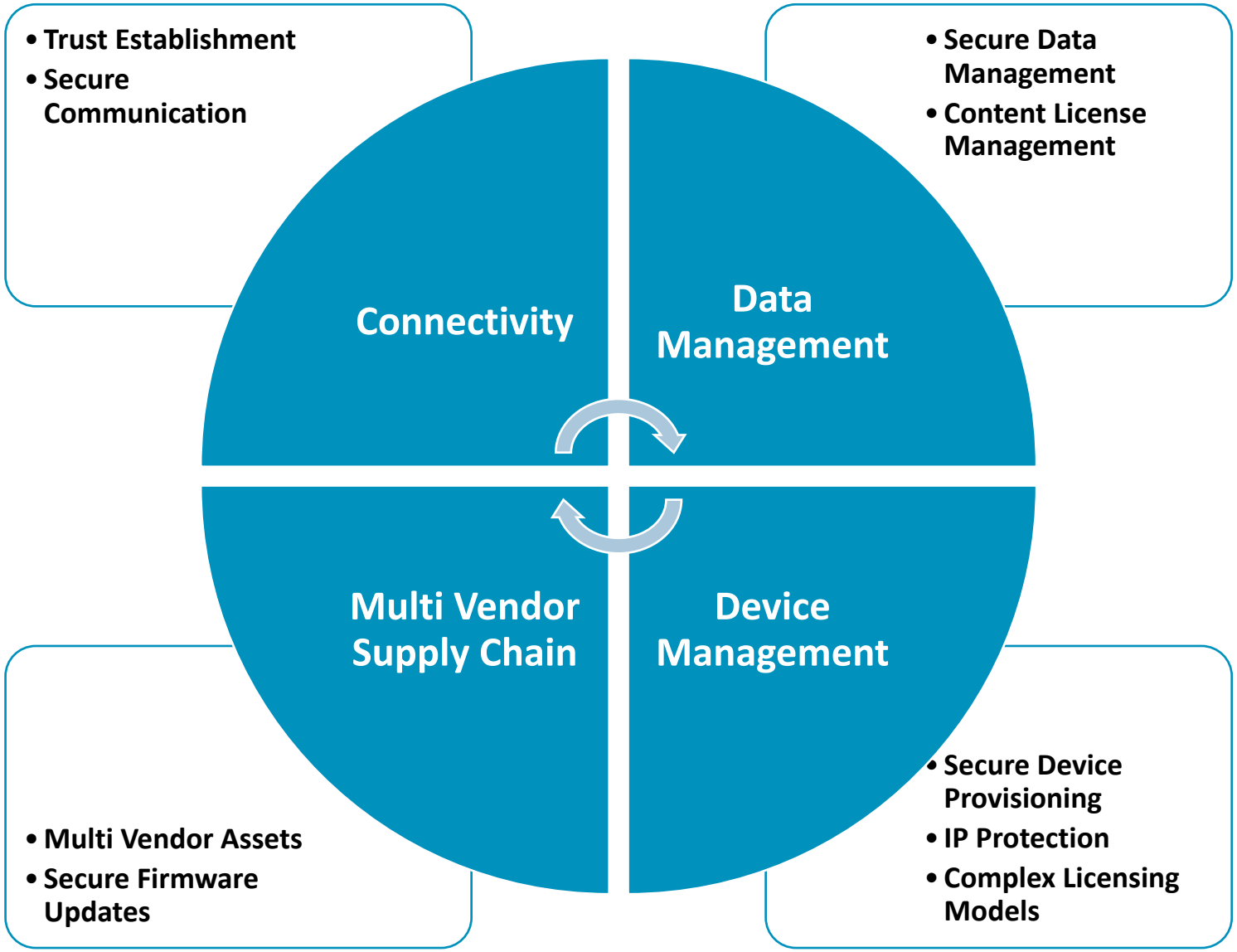
- Silicon Vendor, OEM, OS Vendors
- APP Vendors
- IP Protection

- Device Configuration
- Feature certificates
- Firmware Update
- Incident Mgmnt



arm

Security Challenges

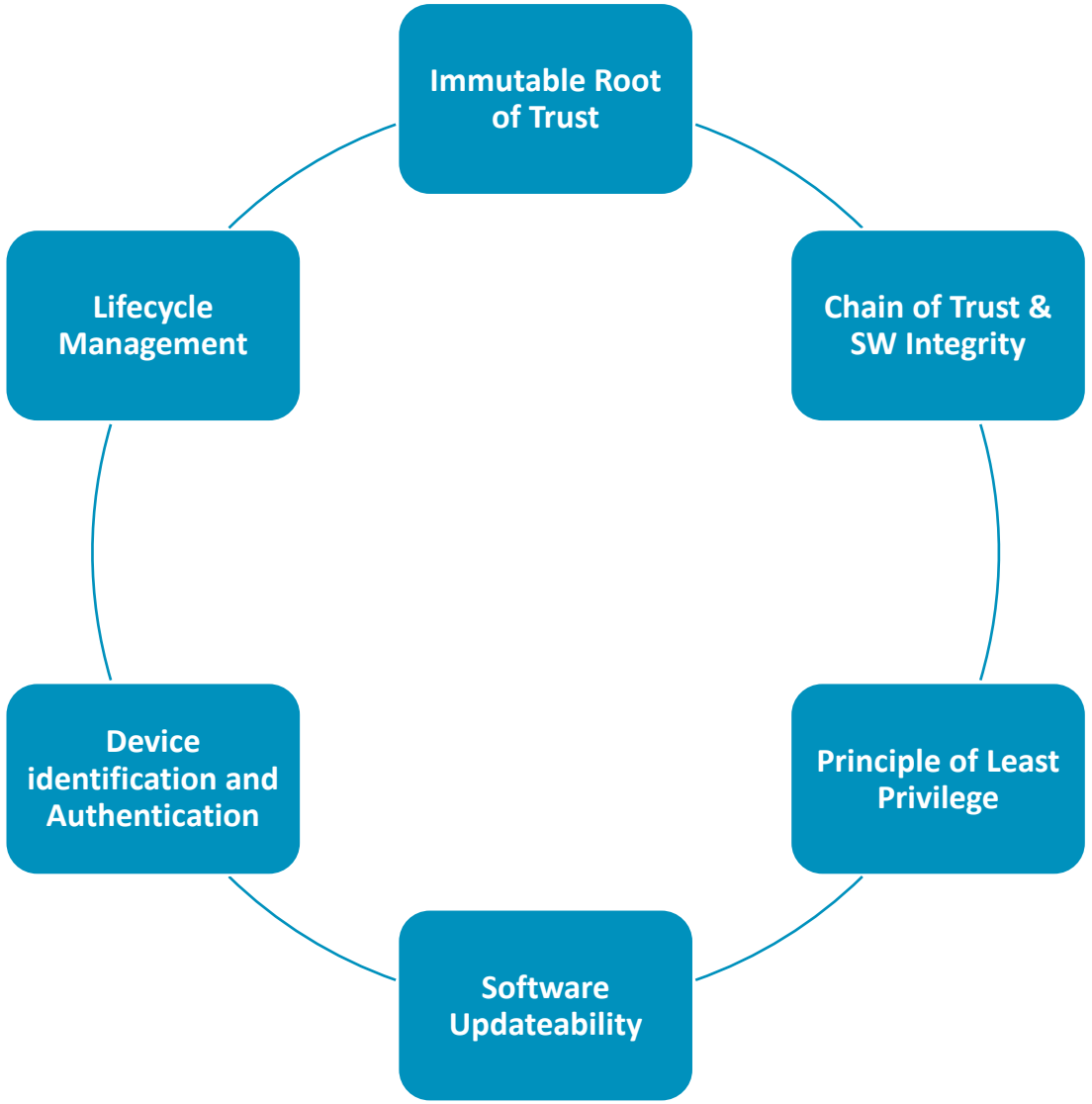


arm

Device Security Building Blocks

arm

Common Security Functions



arm

Root of Trust and Chain of Trust

LIFECYCLE STATES

Immutable RoT

ROM Code

Key signing Pub key

- Likely to be part of RTL
- Authentication of updateable bootloader
- Assist in factory floor device provisioning

Updateable Bootloader

Hardware Unique Key RNG

Image signing Pub key

Monotonic counter

- Runtime SW authentication
- Firmware update process
- Key derivation tree and boot seed
- Boot signature measurements

Runtime Software

RNG

Use-case keys

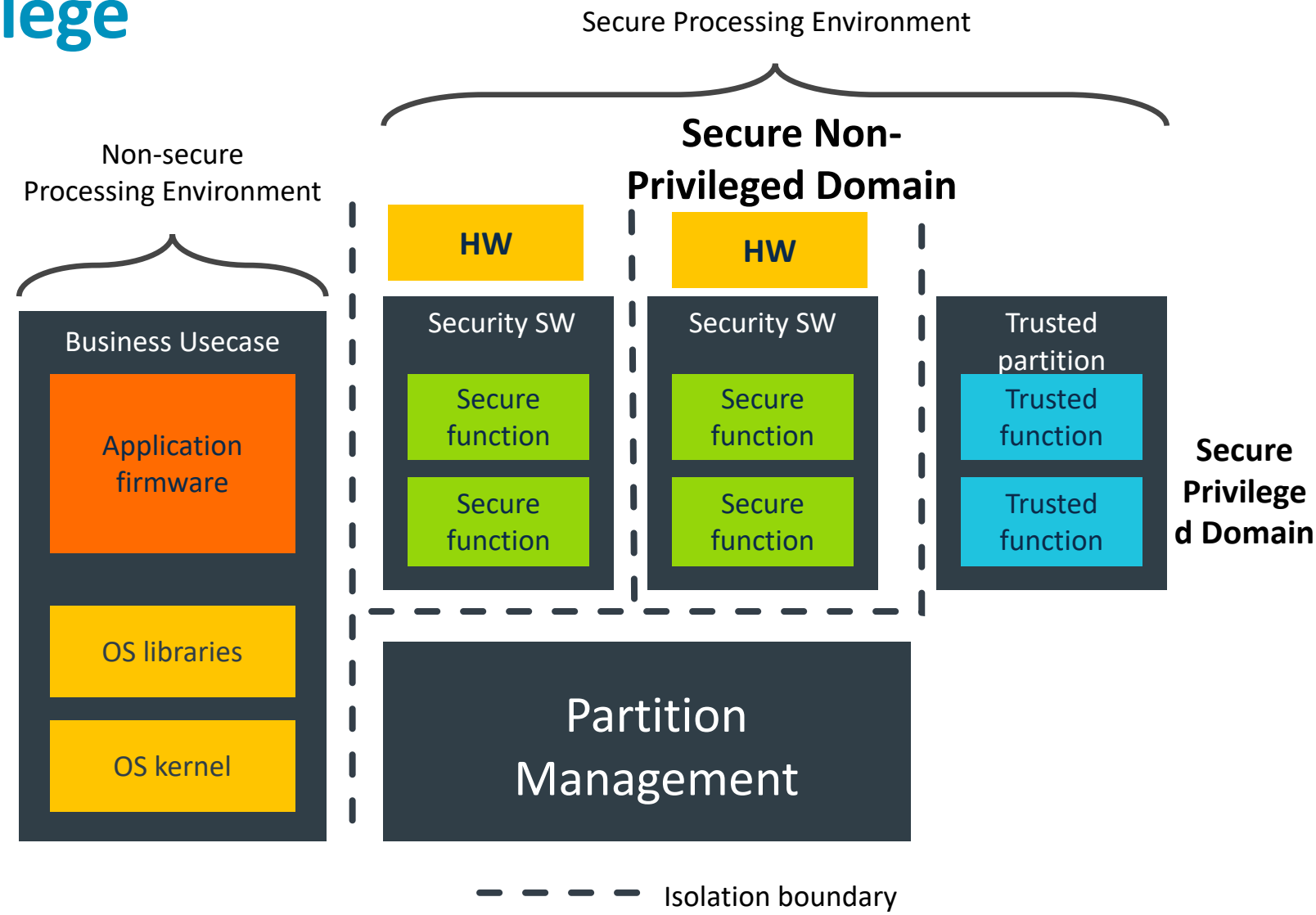
Crypto accelerator

- Business use-case
- Secure communication
- Firmware update support
- Compartmentalization

arm

Principle of Least Privilege

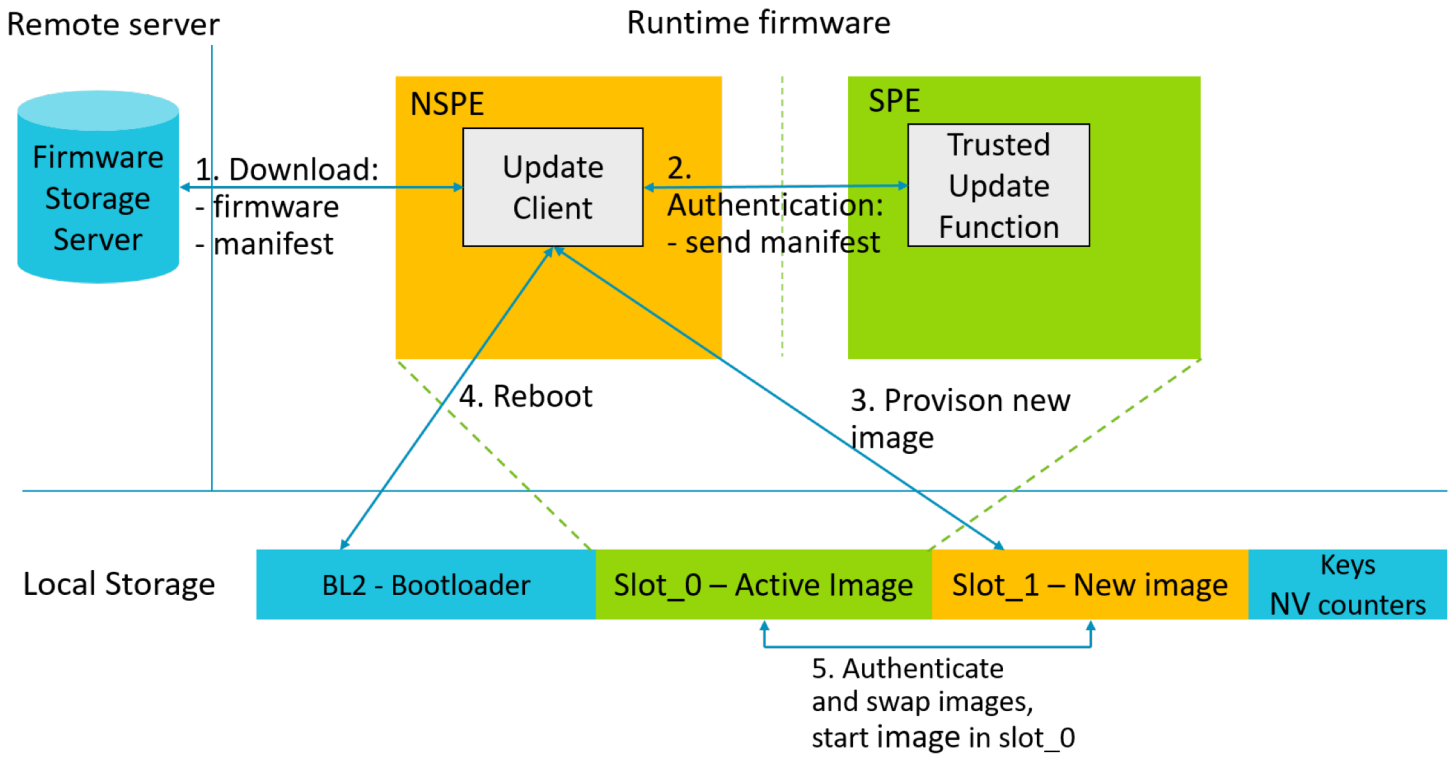
- SW and HW compartmentalization
- Cryptographic key hygiene
- Multivendor scenarios with mutual distrust



arm

Firmware Update

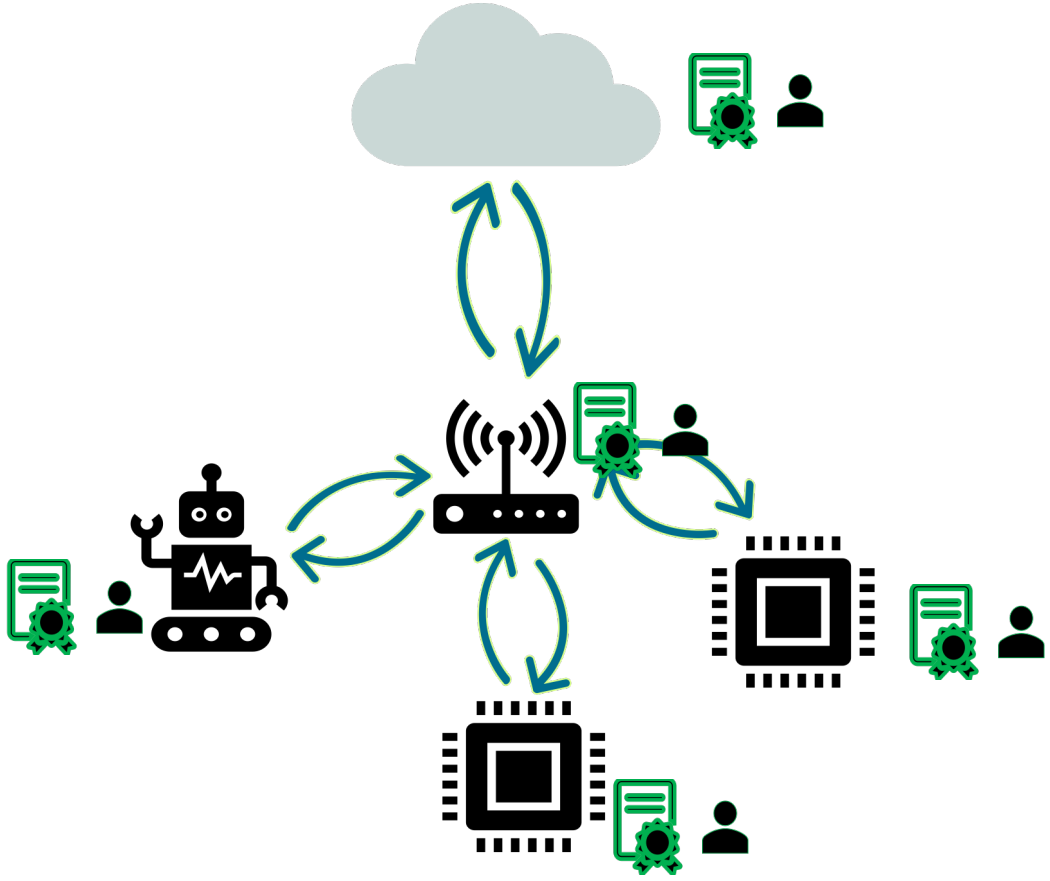
- SW/HW vulnerability fixes
- Multivendor software updates
- Public key based image authentication
- Rollback Protection



arm

Device Identification and Authentication

- Immutable Unique Identity
- Certificate based authentication
- Device attestation



Lifecycle Management

Silicon Manufacturing

- RTL Key
- Feature control

- Secure device provisioning
- Feature subscription licensing models

OEM/OS Vendors/ APP Vendors

- Key provisioning
- Firmware Provisioning

- Secure device provisioning
- SW Integration

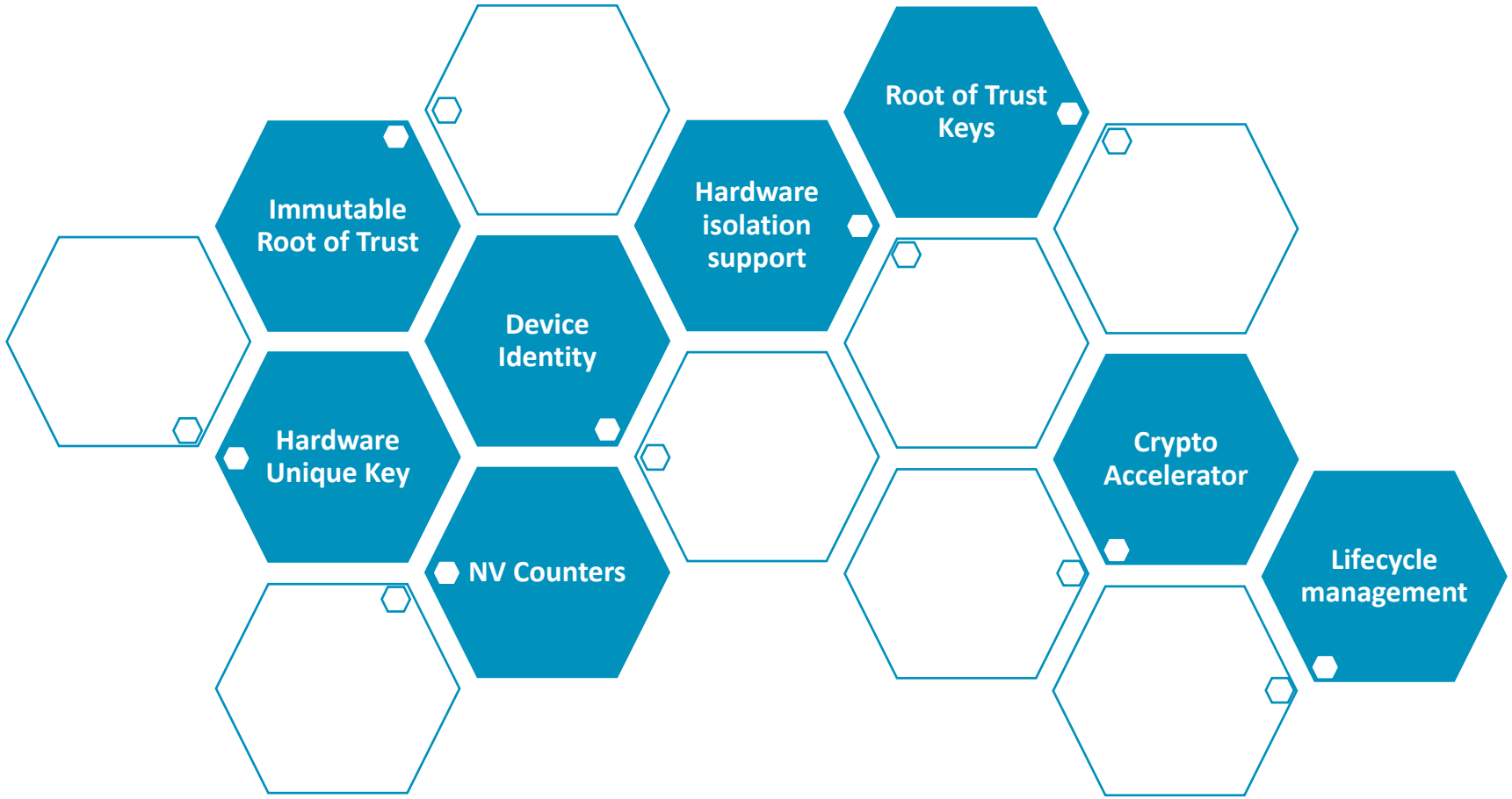
Field Deployment

- Keys
- Subscription Certs
- HUK

- Multiple vendor (apps, firmware fragments) management
- Device Recall

arm

Hardware Building Blocks

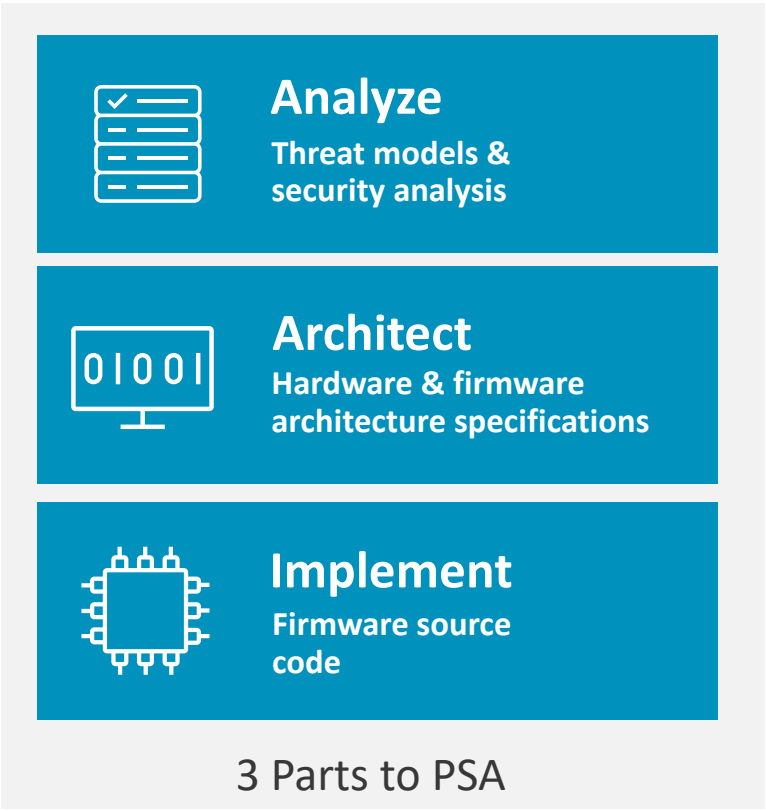


arm

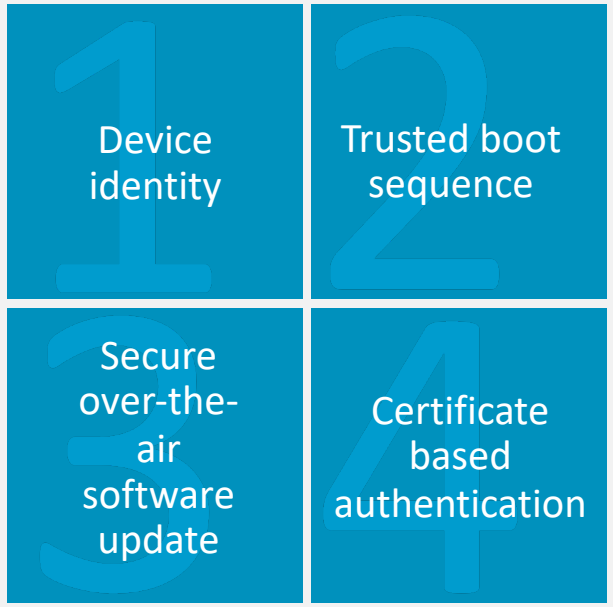
Platform Security Architecture

arm

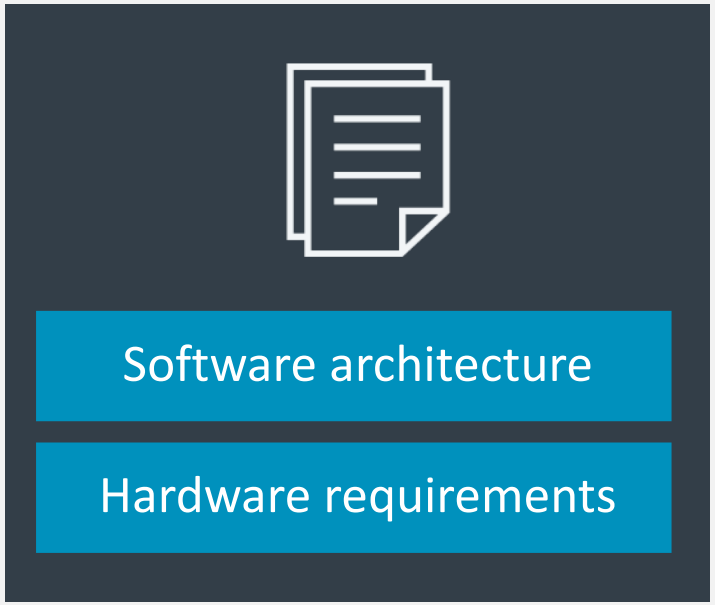
Platform Security Architecture



3 Parts to PSA



Common principles across multiple use cases



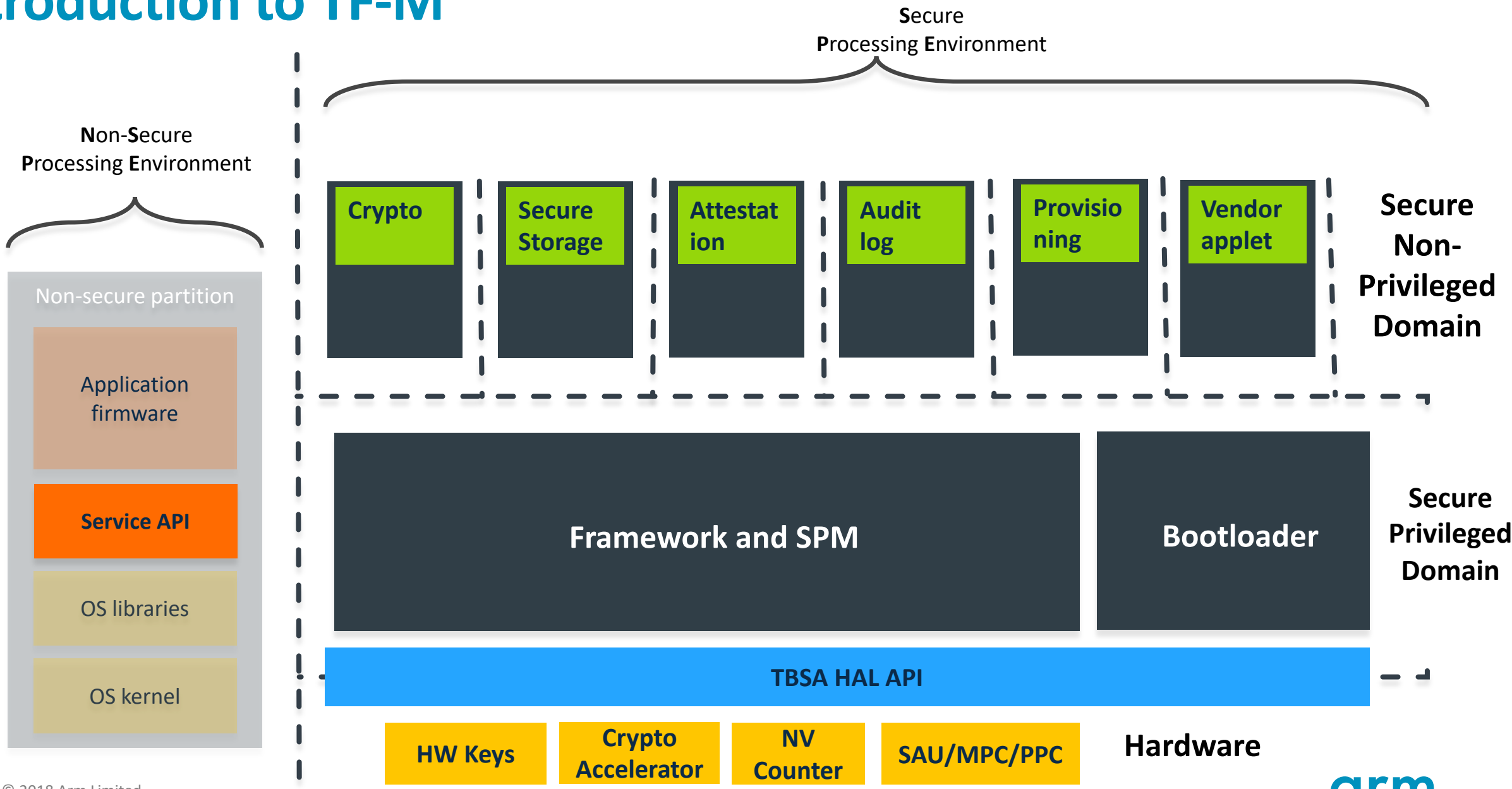
Architecture & Specifications

arm

Trusted Firmware M

arm

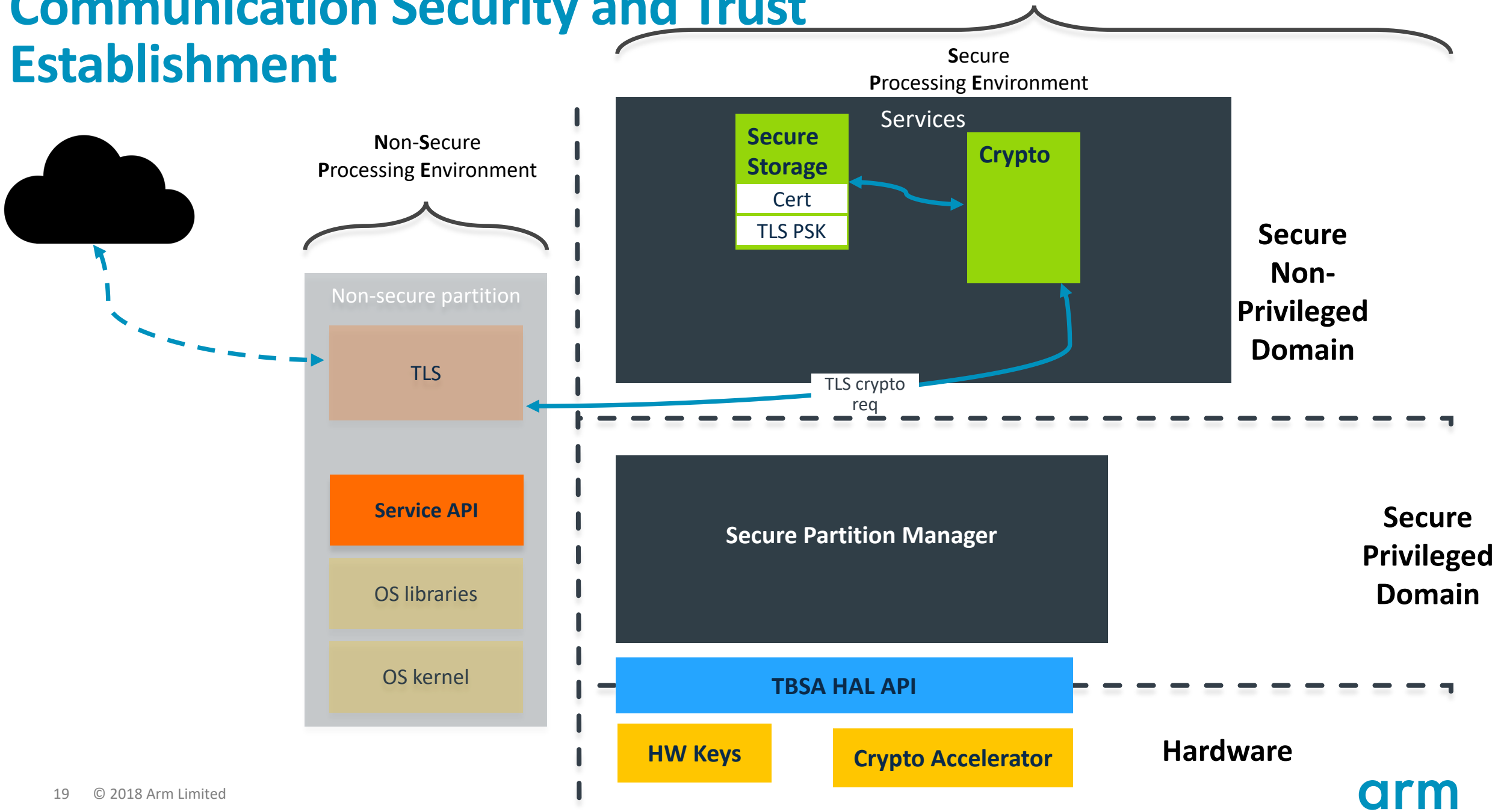
Introduction to TF-M



Securing Use-cases with TF-M

arm

Communication Security and Trust Establishment



How to get involved

TF-A and TF-M master codebases

- https://git.trustedfirmware.org/

TF-M Team @ OpenIoT Summit Europe 2018

- Shebu Varghese Kuriakose
- Ken Liu
- Miklos Balint
- Ashutosh Singh

Get in touch

- Come round to the Arm booth during the summit
- Contact TF-M team at support-trustedfirmware@arm.com

TF-M Secure Partitioning Talk – Wednesday, October 24 • 14:15 - 14:55

More info on developer.arm.com and trustedfirmware.org

arm

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