
arm
Speed-up your next IoT design
Arm Secure Foundations
December 2018
Build secure IoT systems

arm

Arm's Vision For IoT Security

Making Security Easier to Implement

Key IoT security considerations

1 Security needs to built-in from the ground up

2 A collective industry responsibility

3 Security needs to be simple, with seamless integration

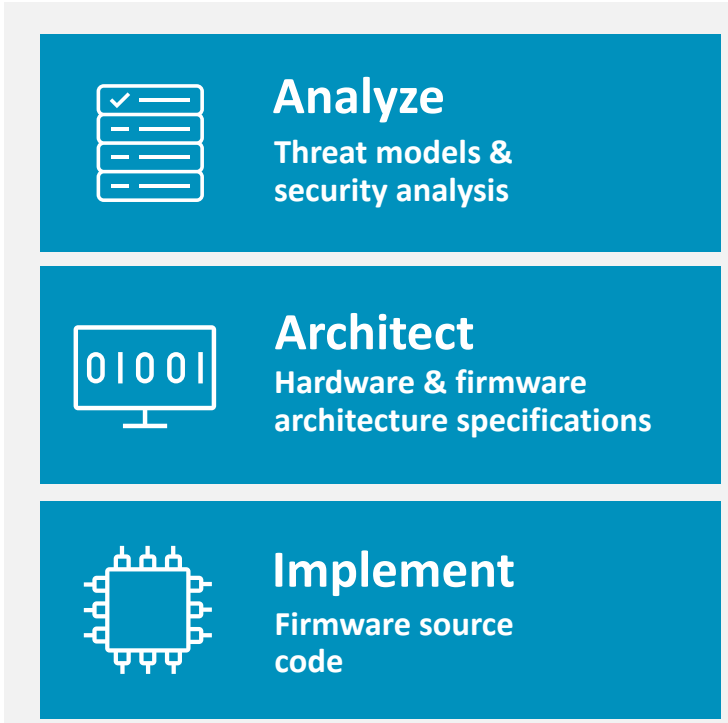
Platform Security Architecture (PSA) is the perfect starting point

Providing a framework to ensure consistent security

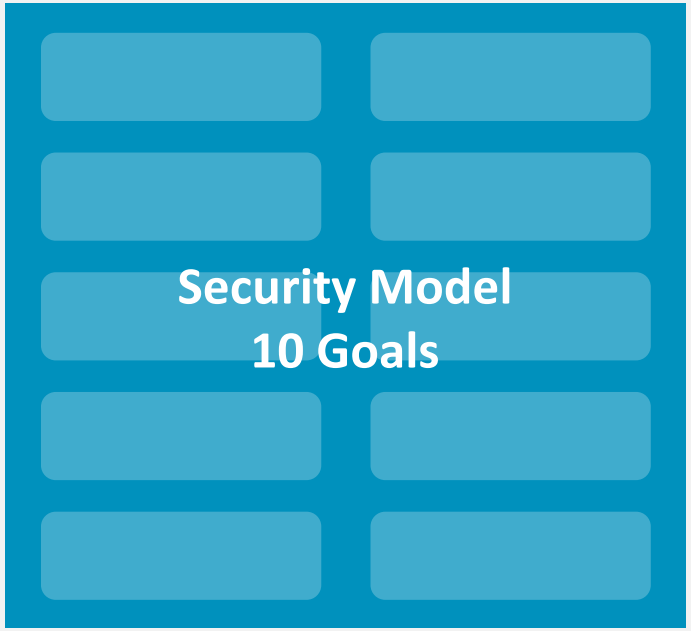
arm

Platform Security Architecture (PSA)

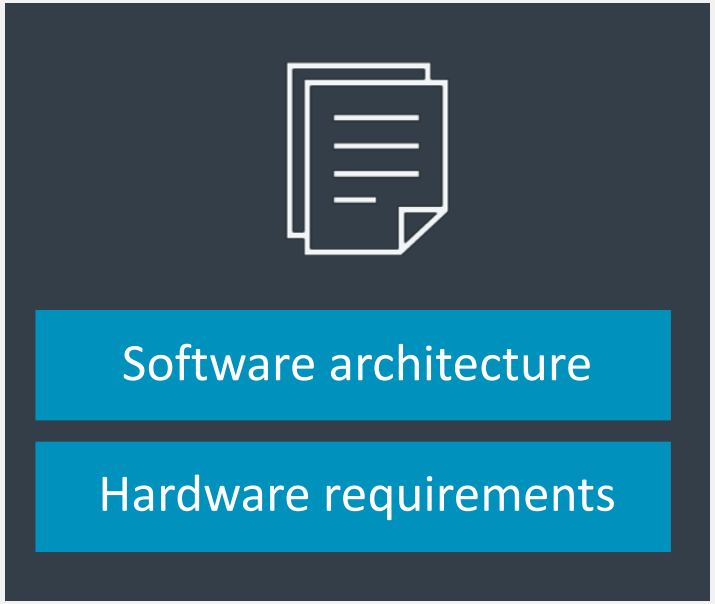
A recipe for building a secure system & a reference implementation



3 parts to PSA



Common principles across multiple use cases



Architecture & Specifications

Designing Secure IoT Systems

arm

Designing Secure IoT Systems with Arm Secure Foundation

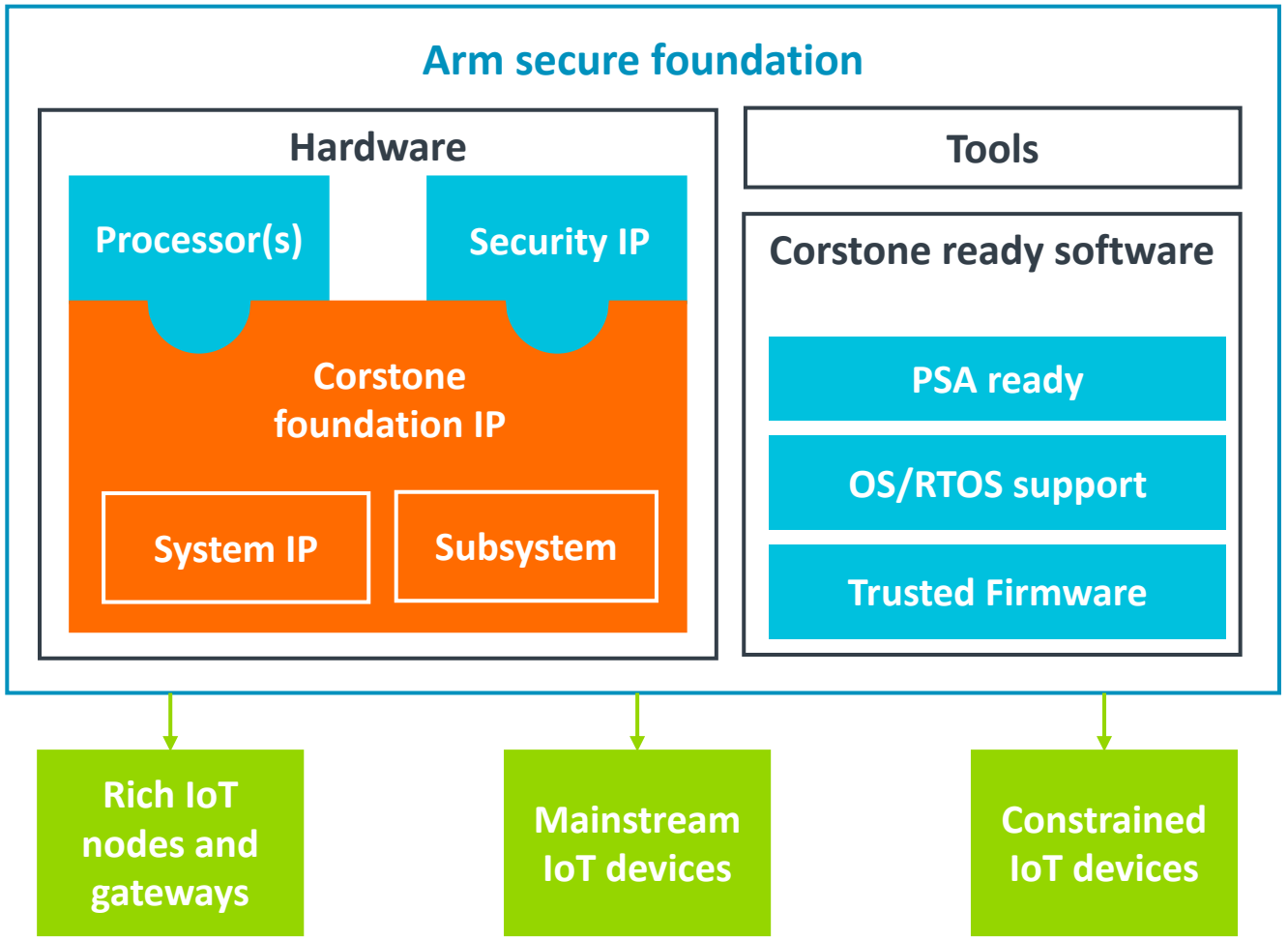
arm

Arm Secure Foundation Solutions

Arm secure foundation solutions

Extendable for differentiation & diversity

- Corstone foundation IP
  - Pre-integrated processor & security IP
  - Pre-verified, modifiable subsystems
- Corstone ready software
  - Standardized interfaces and architecture
  - Mbed OS and Mbed Linux
- Tools
  - Arm and 3rd party development tools
  - FPGA, fast models, test chip boards



Note: Arm Corstone replaces Arm System Design Kits (SDK)

Different Classes of Devices have Different Requirements

Rich IoT nodes & gateways

Data processing at the edge

Decision making

Machine learning

Gateway to cloud

Mainstream

Balancing performance and cost

Moderate data / audio processing

High power efficiency

Constrained

Ultra-low-cost, sensors or beacons

Often battery powered

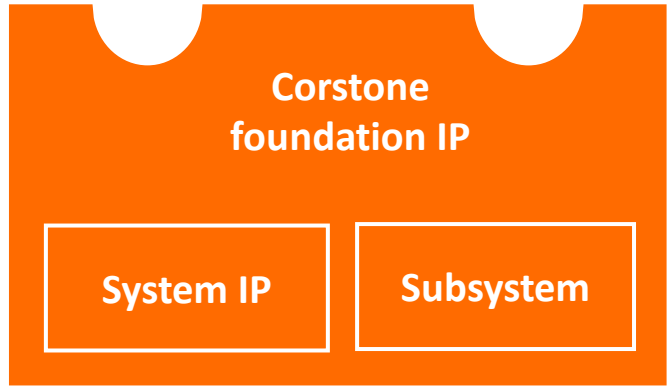
Connecting to gateway or cloud

Corstone Foundation IP

Definition

- Corstone foundation IP
  - A Licensable package that gives access to
    - Example Subsystems
    - System IP
    - Scripts
    - Basic Testbench
    - Supporting Documentation

- Supported by Corstone Ready Software



arm CORSTONE

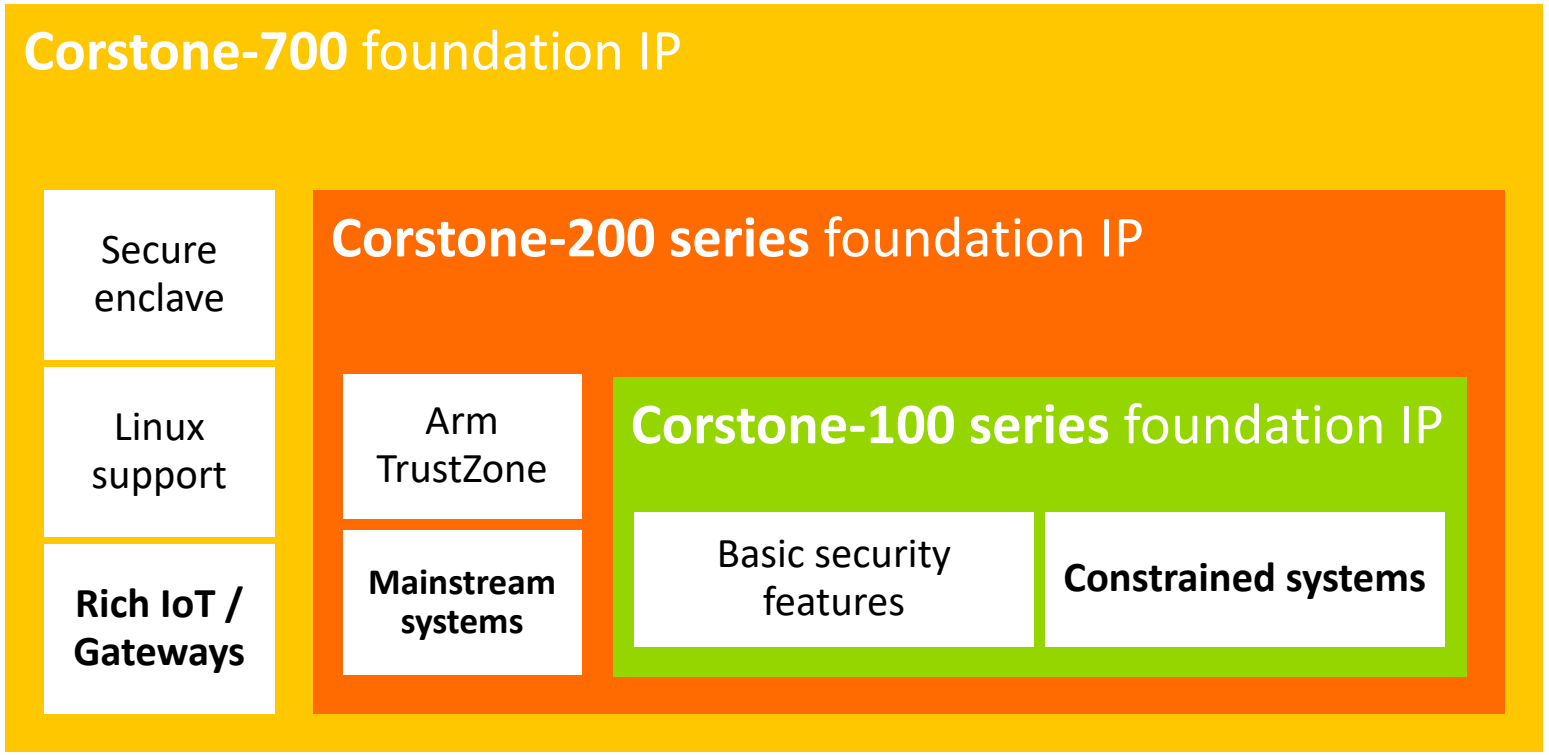
*Corstone is the new brand name that replaces System Design Kit (SDK)

arm

A Family of Solutions

Nested Doll Principle

- Corstone-700 includes Corstone-100 & 200 components
- Corstone-200 includes Corstone-100 components



Corstone foundation IP – Subsystem for Embedded (SSE)

A range of subsystems available with security

Rich nodes / gateways

SSE-700 + Media / AI

- Cortex-A + Cortex-M

SSE-700

- Cortex-A + Cortex-M
- TrustZone
- Secure enclave
- Firewalls
- Protected multi-domains debug support
- Isolated domains

Mainstream

SSE-200

- Cortex-M33
- TrustZone
- CryptoCell pre-integrated
- Secure debug

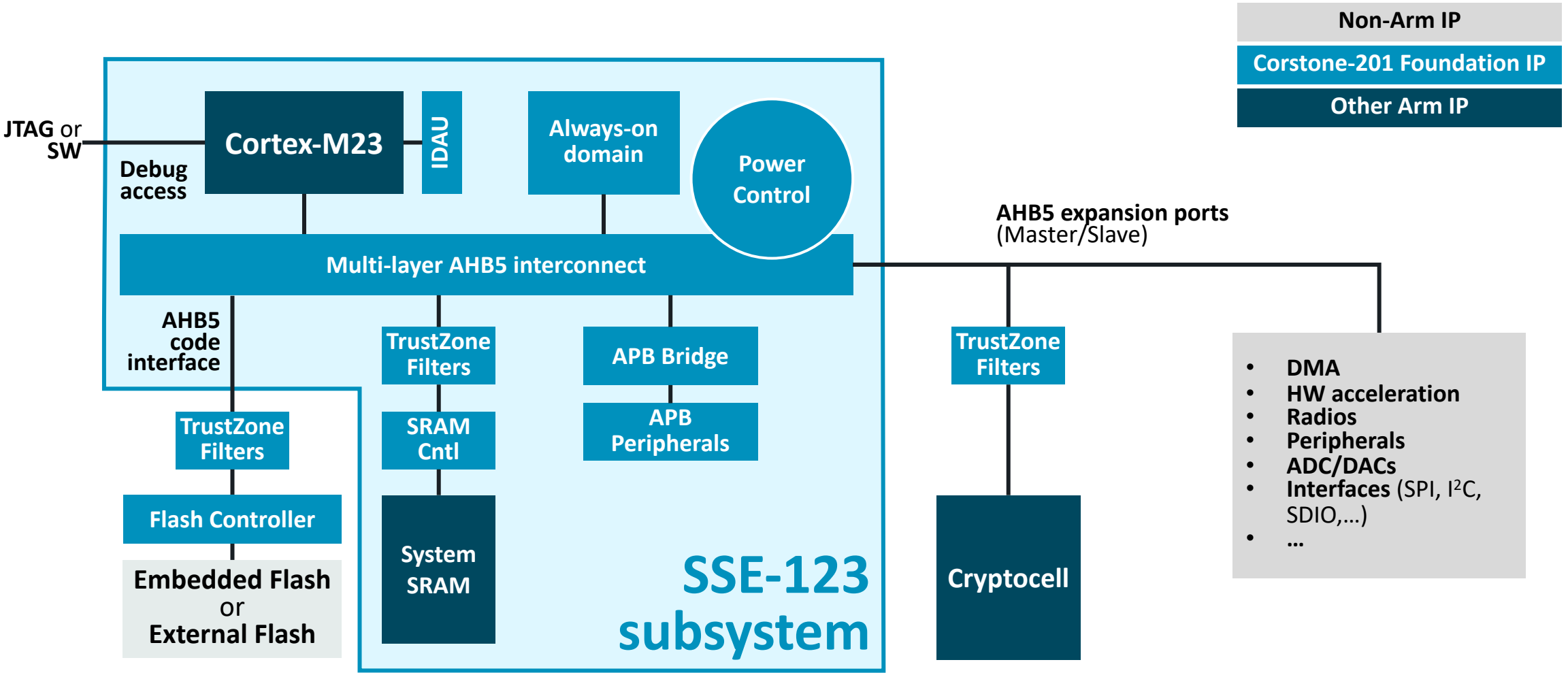
Constrained

SSE-123

- Cortex-M23
- TrustZone

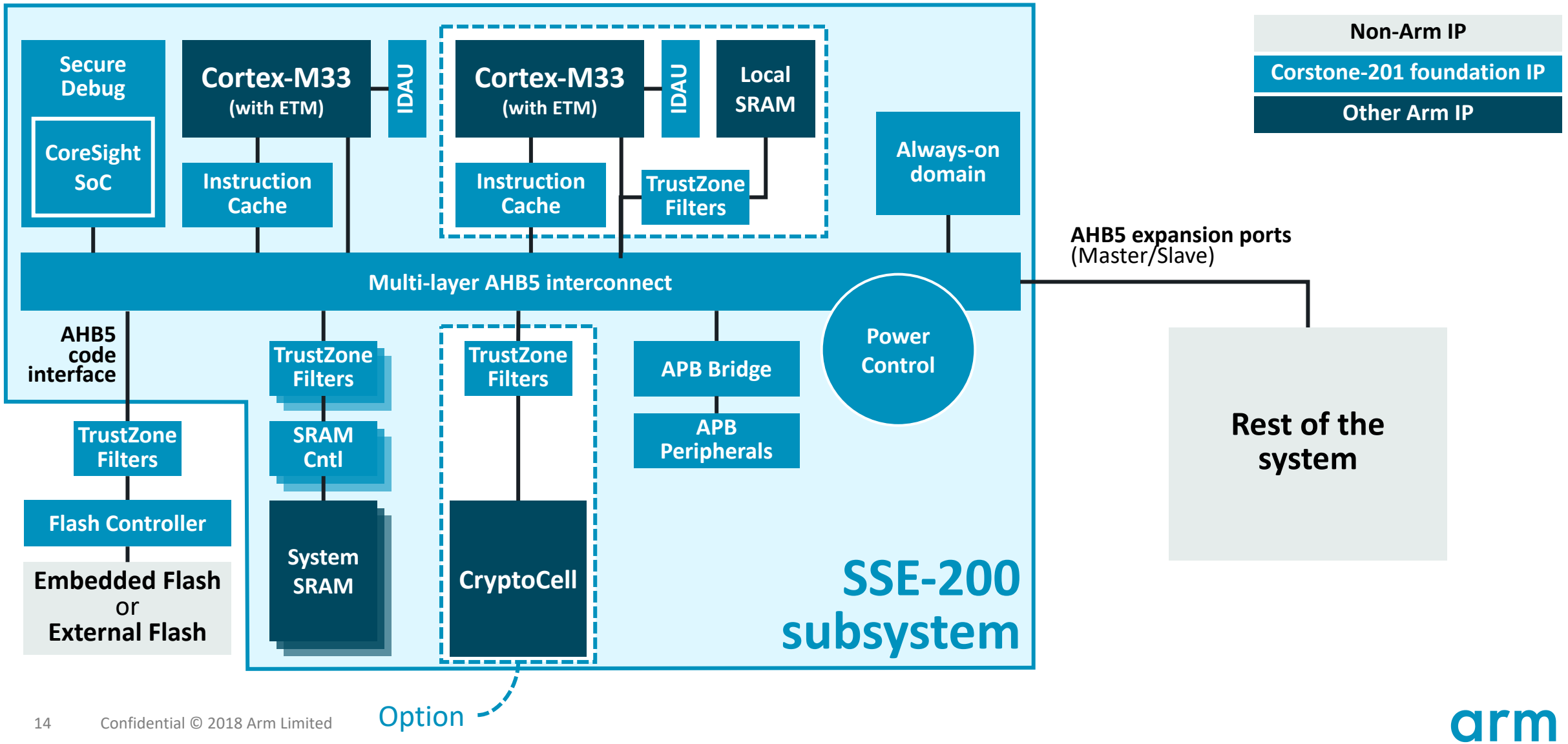
arm

Constrained Subsystem - SSE-123 example subsystem



arm

SSE-200 Subsystem



Corstone-Ready Software for 100 and 200 Series

Essential elements

- Keil MDK pack supports any RTOS
  - Largest RTOS choice
- Trusted Firmware (TF-M)
  - Implementation of PSA APIs

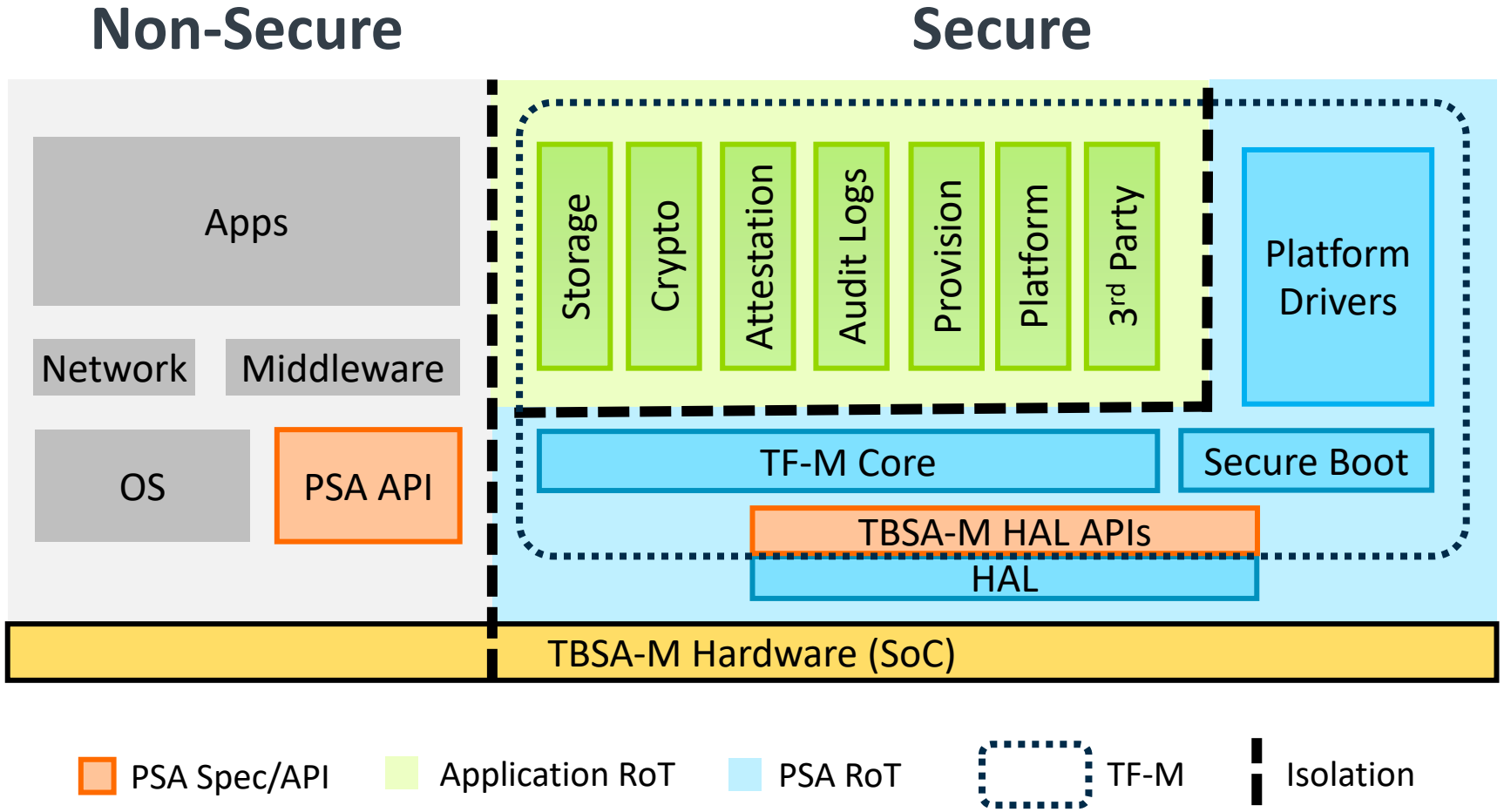
Application and RTOS support

- Mbed OS
  - Support out of the box
  - Integrated with TF-M in Mbed OS 5.12 (December)
- Other RTOS support
  - E.g. Zephyr, FreeRTOS
- Example applications

arm

Trusted Firmware-M (TF-M)

Open-source reference implementation of PSA

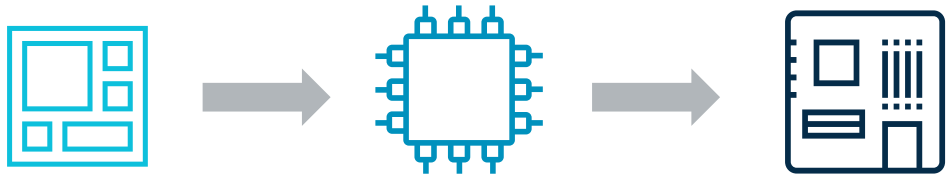


www.trustedfirmware.org

arm

Some Ways Arm is Promoting Security

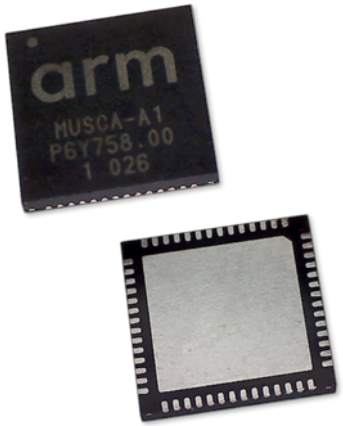
Thought-leadership & education	→	Security manifesto, surveys and events
Platform Security Architecture	→	Offering an industry best practice framework
Providing security elements	→	TF-M, PSA ready systems, security IP
Develop the ecosystem	→	Musca test chip program

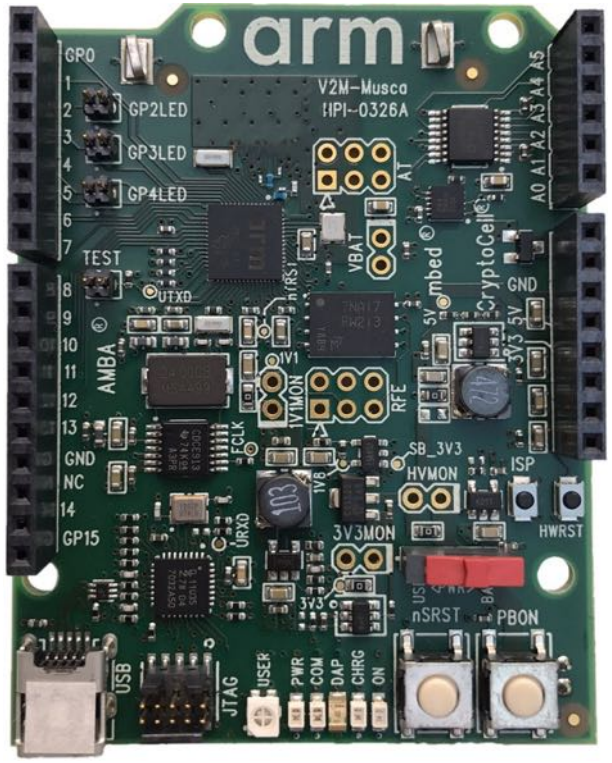


Musca-A Test Chip

SSE-200 Proven In Silicon

- SSE-200
- Cortex-M33





Distributed to the ecosystem

- SW developers
  - Target for TF-M
  - Develop secure software
- SoC developers
  - Evaluate the IP
  - Understand security architecture

100s of companies already use a Musca board

Ask for a free loan!

Conclusion

- Arm invests in secure IoT solutions
  - For all IoT segments (constrained, mainstream, rich nodes / gateways)
  - System approach – HW, SW, services, tools
  - Corstone foundation IP

- Benefit for users
  - Reduced cost, faster TTM, focusing on differentiation
  - Security in line with PSA principles
  - Architecture alignment ➔ Ecosystem