Designing Security & Trust into Connected Devices

ARM

Rob Coombs
Security Marketing Director

TechCon
11/10/15

Agenda

- Introduction
- Security Foundations on Cortex-M
- Security Foundations on Cortex-A
- Use cases
- Certification
- Summary

Why Security Matters

Security done well provides the foundations
For services, capabilities and user experiences:

Can I stream movies to my tablet/phone/dtv?

Can I replace my username/password with a swipe of a finger?

Can I separate my business applications from my personal ones?

Can I have a "kill switch" that makes my phone worthless if stolen?

ARM

ARM TrustZone Technology – A Security Foundation

Today

Authentication

Mobile Payment

Content Protection

Enterprise Security

ARM TRUSTZONE

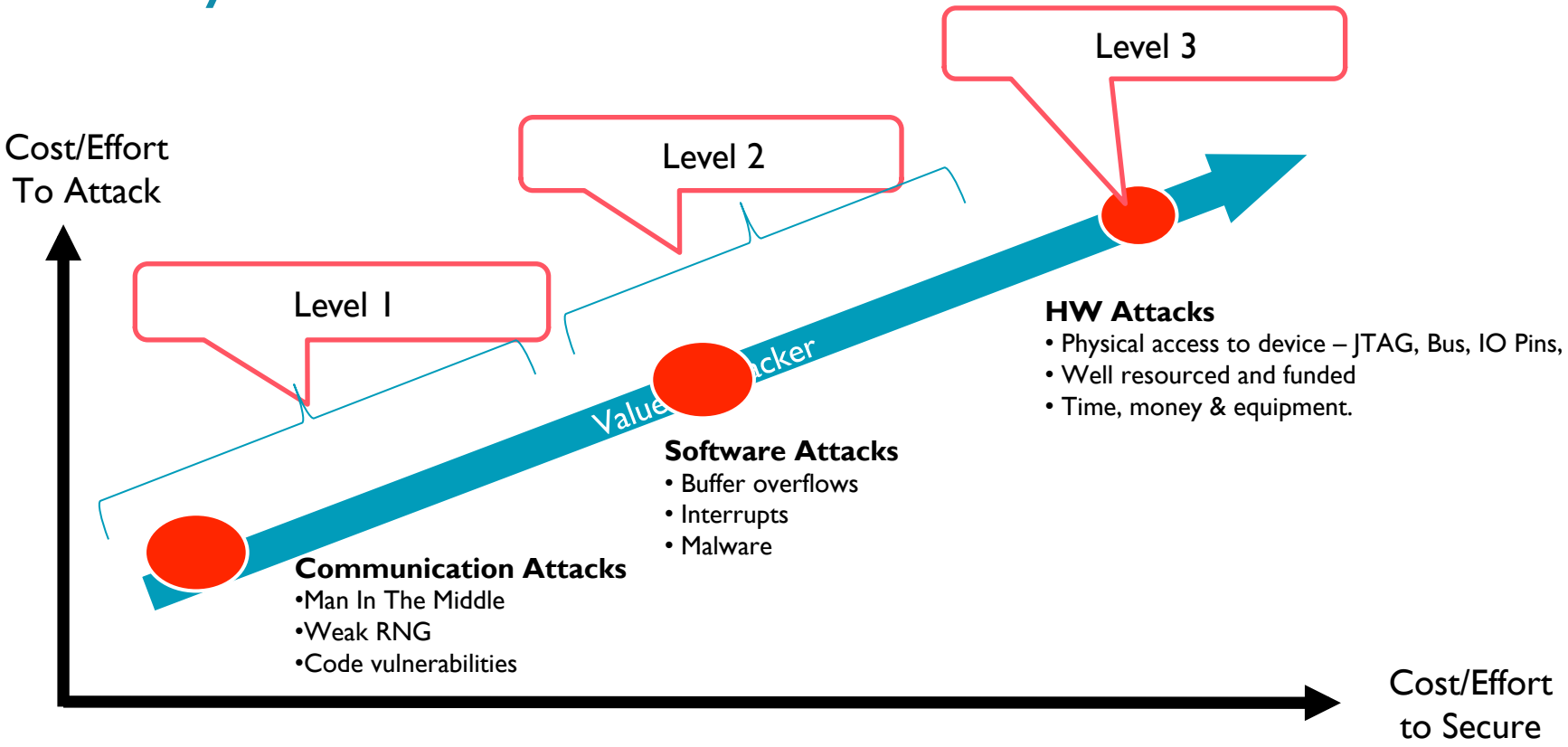
System Security

IOT Security Enables New Business Opportunities

- If you can trust devices and the little data you can transform industries
- Electricity meter example – if you can trust a remote meter reading on a consumer meter…
  - No need to send someone to the house
  - Billing costs are reduced

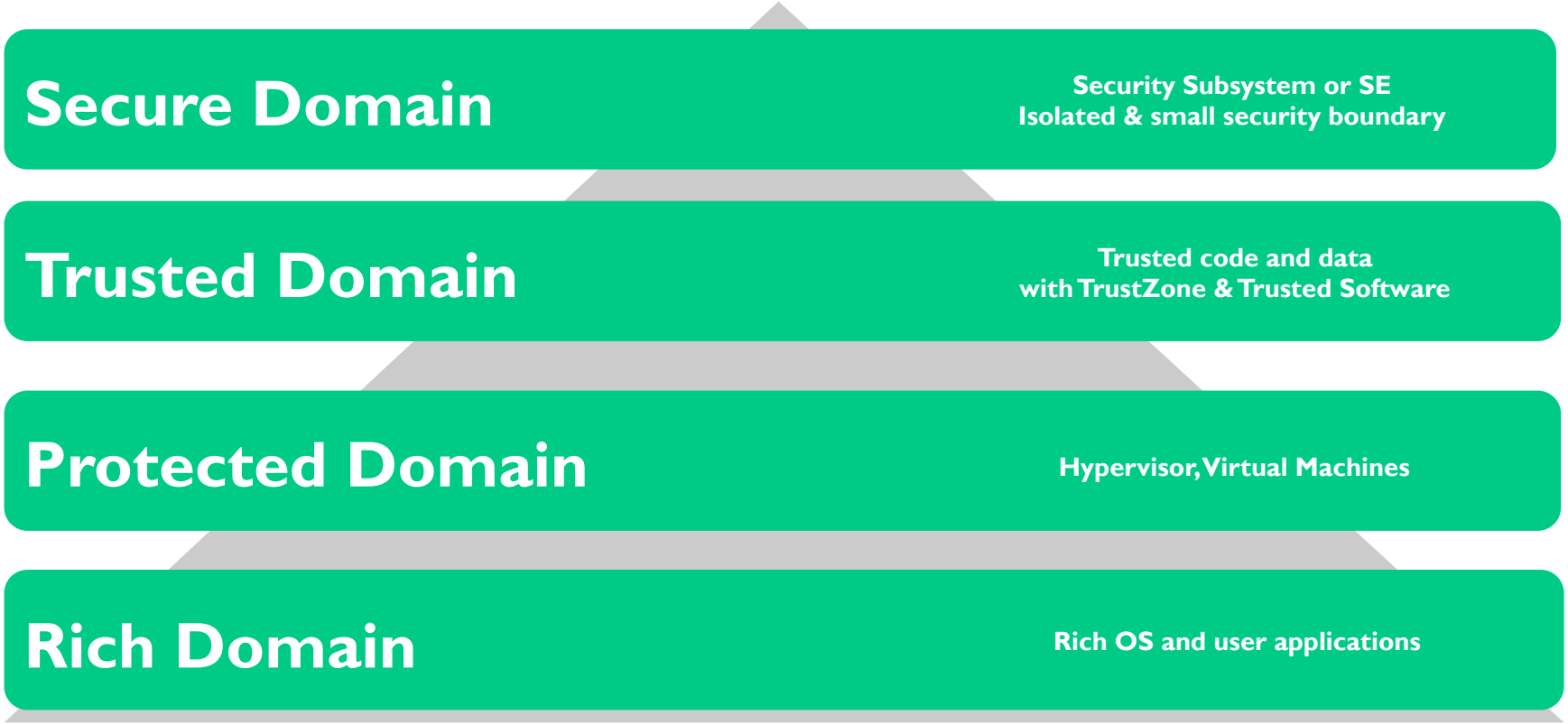
- Home security example – if you can trust a connected security system …
  - You will be more likely to purchase and enable remote monitoring

Security is a Balance



ARM

ARM Builds Layers of Hardware Security - Hierarchy of Trust



How Do We Build the Internet of Trustworthy Things?

- Make end to end security easier by providing right sized secure foundations that scale for different use cases and market needs

- Make it easier
  - Build security in or enable easy integration of subsystems
  - Trusted software that is free and easy to use

- Make it right sized
  - Security for any ARM platform
  - Provide multiple solutions

- Keep it agile

Security Foundations for Cortex-M

- Software - mbed OS, mbed uVisor, mbed TLS & 3rd party ecosystem
- TrustZone for ARMv8-M
  - New microcontroller architecture gains TrustZone

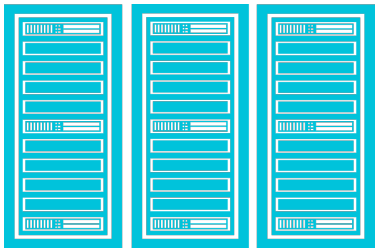
- TrustZone CryptoCell-310
  - Adds a configurable security system close to the root of trust suitable for microcontrollers

ARM mbed Device Platform for Microcontrollers

ARMmbed

IoT Device Platform

mbed OS
mbed TLS
mbed uVisor



Productivity

Security

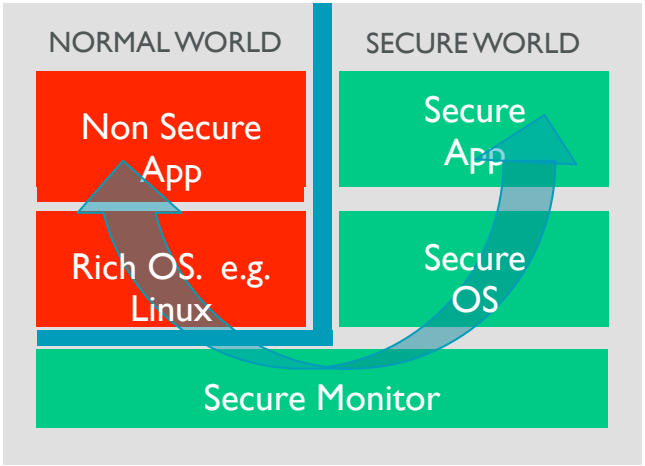
Connectivity

Management

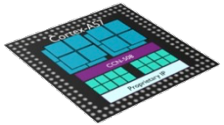
Efficiency

TrustZone for ARMv8-M

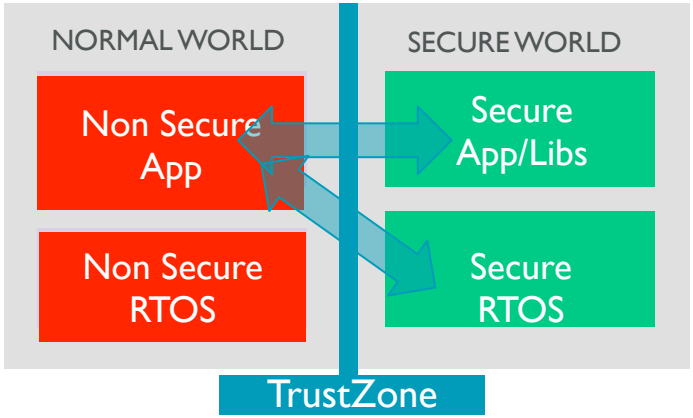
TrustZone® for ARMv8-A



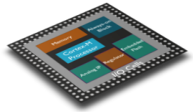
Applications Processors



TrustZone® for ARMv8-M



ARMv8-M Microcontroller



ARM

ARM TrustZone® Architecture Extensions

Feature/Architecture	TrustZone® ARMv7-A & ARMv8-A	TrustZone® for ARMv8-M
Additional Security States	SEL0* – Trusted Apps SEL1 – Trusted OS EL3 – Trusted Boot & Firmware (ARMv8-A)	Secure Thread – Trusted code/data Secure Handler – Trusted device drivers, RTOS, Library managers…
Secure Interrupts	Yes	Yes (Fast)
State Transition (Boundary crossing)	Software transition	Hardware transition (Fast)
Memory Management	Virtual Memory MMU with secure attributes	Secure Attribution Unit (SAU) & MPU memory partitions
System Interconnect Security	Yes	Yes
Secure Code, Data and Memory?	Yes	Yes
Trusted Boot	Yes	Yes
Software	ARM Trusted Firmware (+ 3rd party TEEs)	Keil CMSIS, ARM mbed OS, mbed uVisor + 3rd party software

*Secure Exception Level

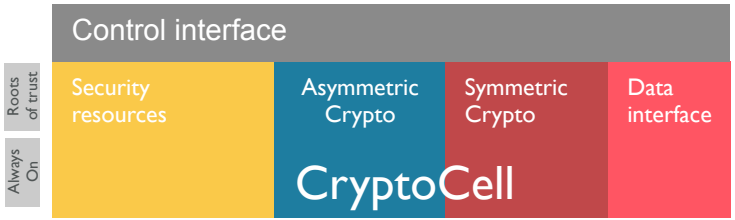
ARM

TrustZone for ARMv8-M Use Cases

- Protection from attack
  - Protect assets from scalable software attacks
  - Compartmentalization
  - Least Privilege
  - Protect assets from "shack" hardware attacks
- Preventing code theft
  - Protect valuable firmware assets
  - IP protection
- Safety critical system / system liability / multi party
  - Sandbox certified software
  - Secure peripherals and drivers

ARM TrustZone CryptoCell

- Family of security subsystems applicable to any ARM platform
- CryptoCell-700 series for Cortex-A & CryptoCell-300 series for Cortex-M – "right size"
- Enhances usability e.g. time for DTLS handshake & door lock to open
- Acts as Root of Trust / Trust Anchor for the system
- Compatible with TrustZone architecture on CPU
- Robust security solution suitable for most use cases
- Simplifies security implementations



AMBA 5 AHB5: Extending Security to the System

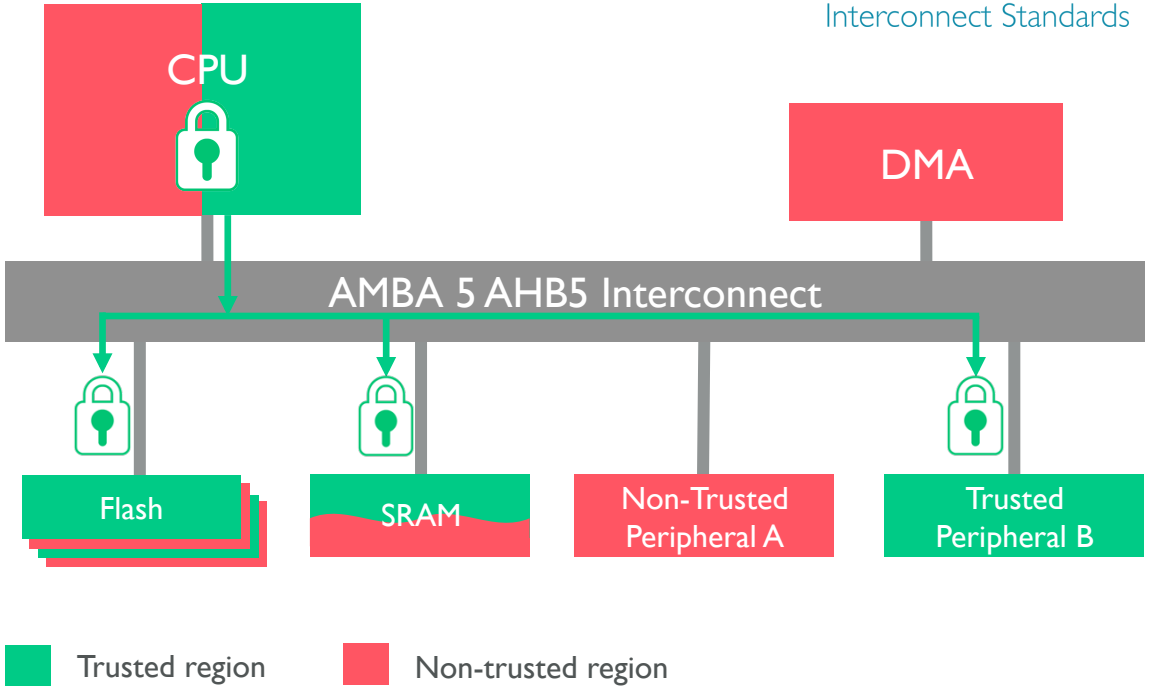
ARM AMBA
Interconnect Standards

Extends security foundation to the SoC

Efficient security control across all of the SoC

Optimized for embedded SoCs

Security state extends across Cortex-A and Cortex-M systems



ARM

AMBA 5 AHB5: Extending Security to the System

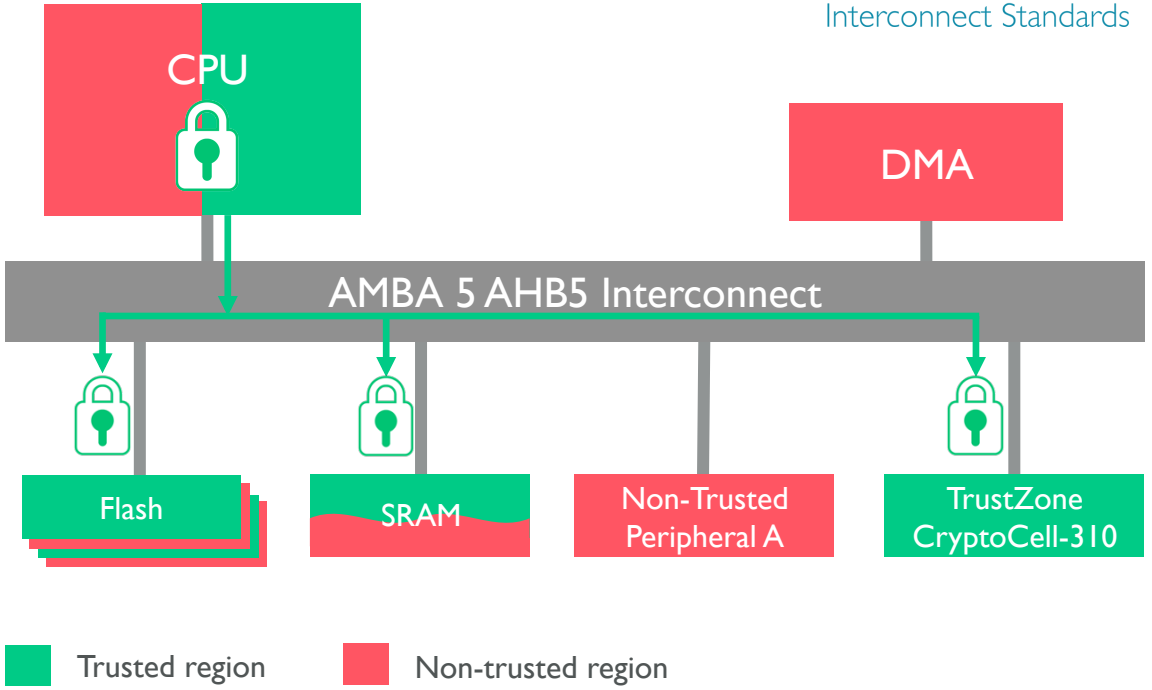
ARM AMBA
Interconnect Standards

Extends security foundation to the SoC

Efficient security control across all of the SoC

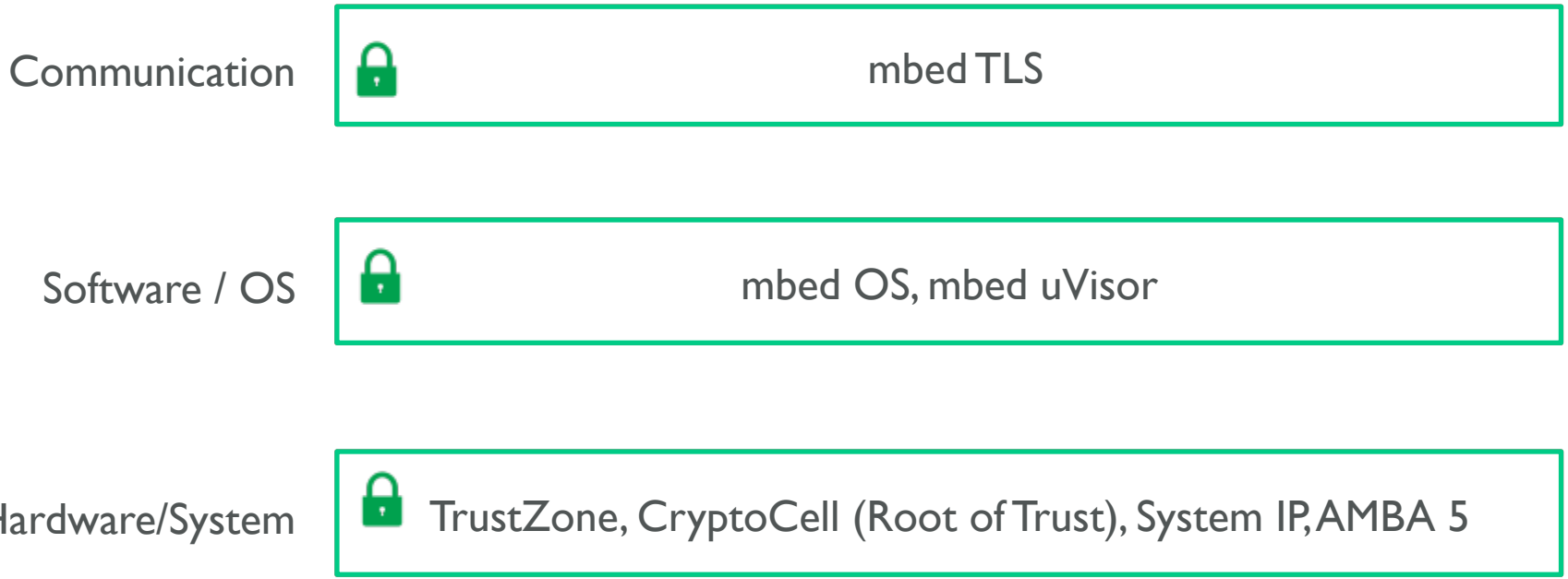
Optimized for embedded SoCs

Security state extends across Cortex-A and Cortex-M systems



ARM

Secure Foundations for Services

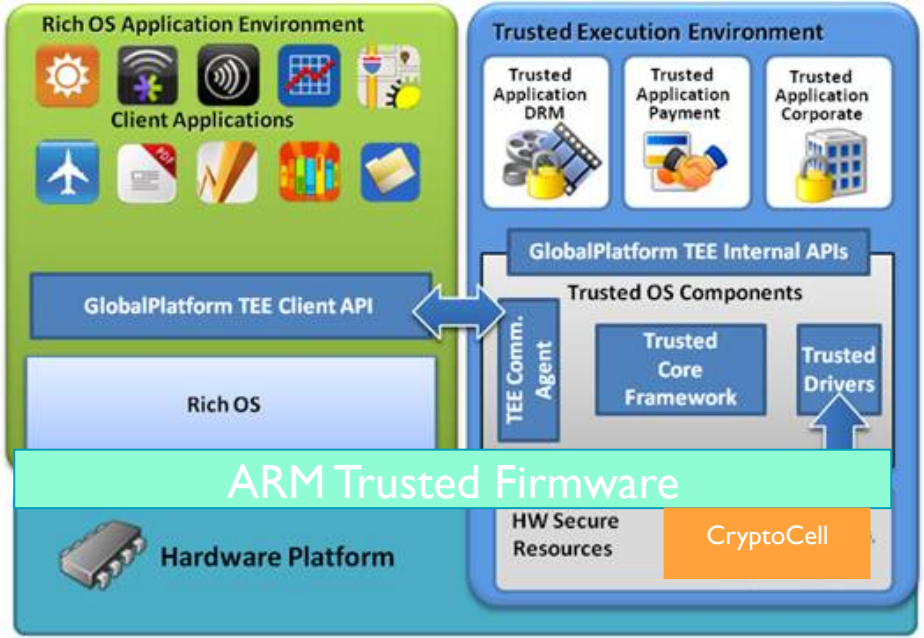


Security Foundations for Cortex-A

- Software – ARM Trusted Firmware & 3rd party TEE ecosystem
  - Security certification for TEE via GlobalPlatform
- TrustZone for ARMv8-A & ARMv7-A
  - Established architecture protecting billions of devices and services
  - TrustZone Media Protection architecture
- TrustZone CryptoCell-710
  - Configurable security subsystem adds a deep layer of hardware based security easily integrated into SoC

TrustZone Based Trusted Execution Environment

Mobile devices with integrated HW security



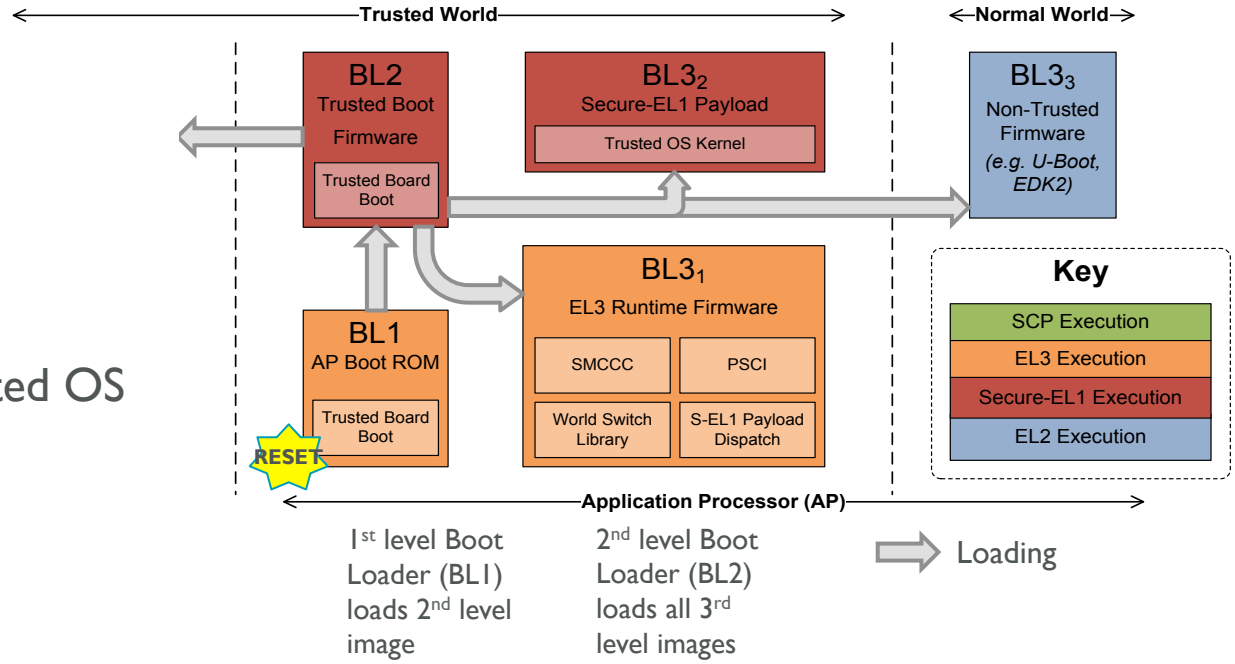
- Hardware root of trust
  - A basis for system integrity
- Integrity through Trusted Boot
- Secure peripheral access
  - Screen, keypad , fingerprint sensor etc.
- Secure application execution
- Technology called TrustZone®
- Trust established outwards
  - With normal world apps
  - With internet/cloud apps

ARM

ARM Trusted Firmware for Cortex-A Processors

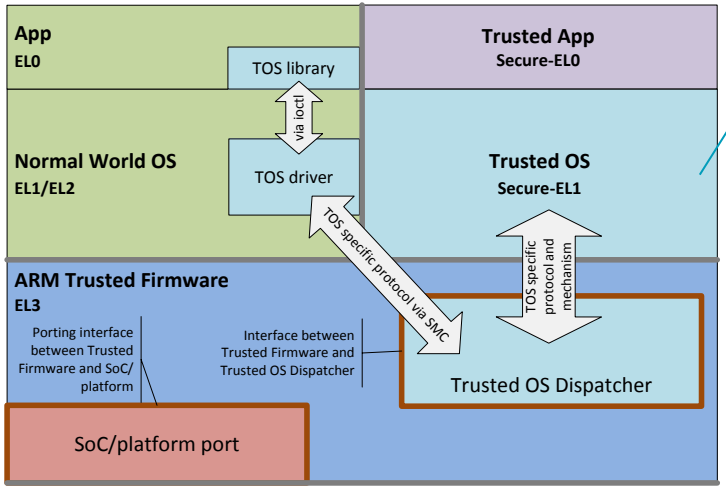
Authenticated Trusted Boot & Runtime

- Reference implementation:
  - Authenticated Trusted Boot
  - Runtime Firmware
- Provides basis for integrity
- Provides foundation for Trusted OS
- Open Source at GitHub
  - BSD License



Cortex-A: Putting it All Together

TrustZone Media Protection 1 (TZMP1)
System Hardware on ARM®
Document number: ARM DEN 0036 Version 1.0
Copyright ARM Limited 2014



OSS or
TEE Vendor

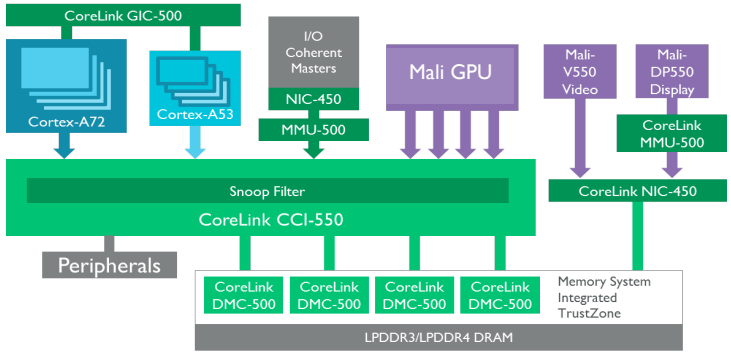
Trusted Base System Architecture CLIENT2
(TBSA-CLIENT2)
System Hardware on ARM®
Document number: ARM DEN 0021A-9
Copyright ARM Limited 2011-2014

Security Platform Design Documents

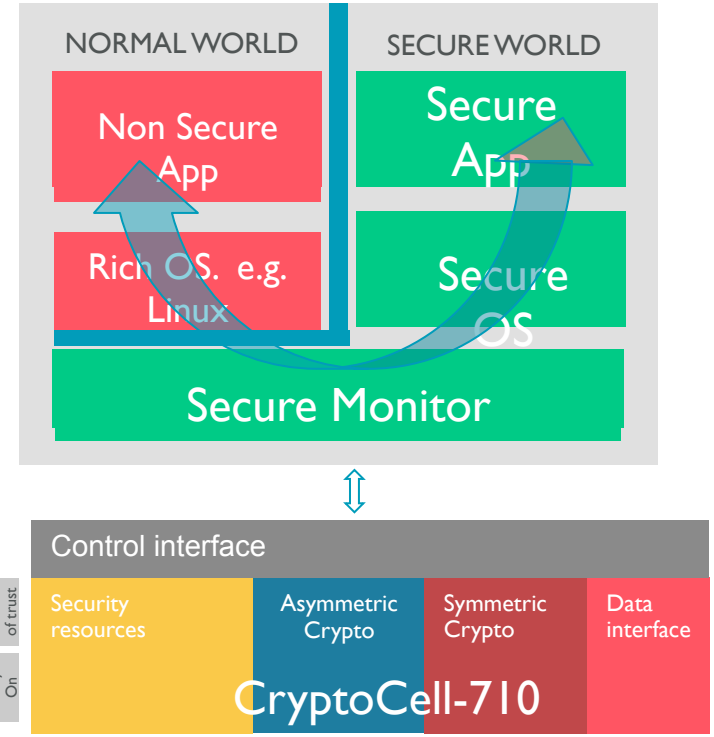
HDMI
HDCP

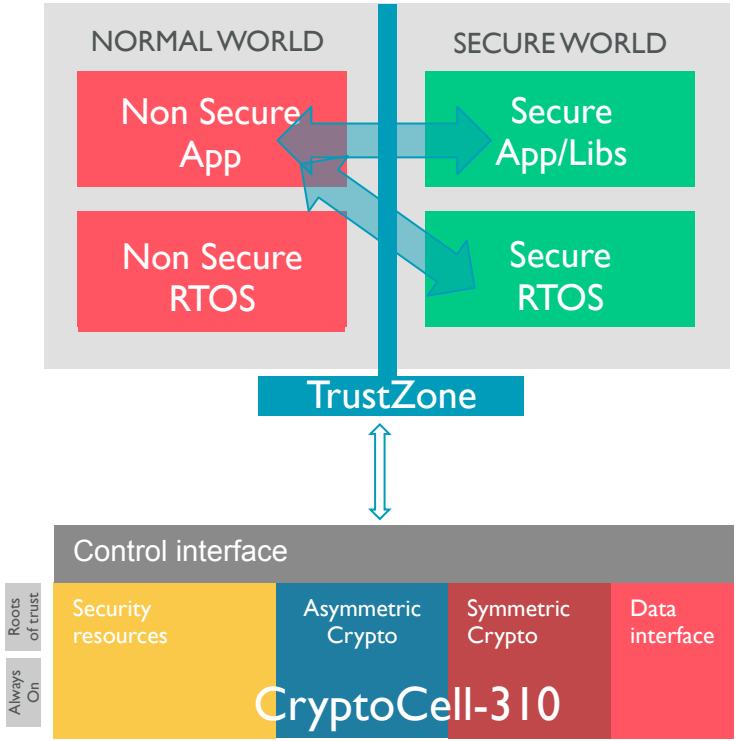
TrustZone
CryptoCell

Trusted
Peripherals



TrustZone CryptoCell for Every Platform

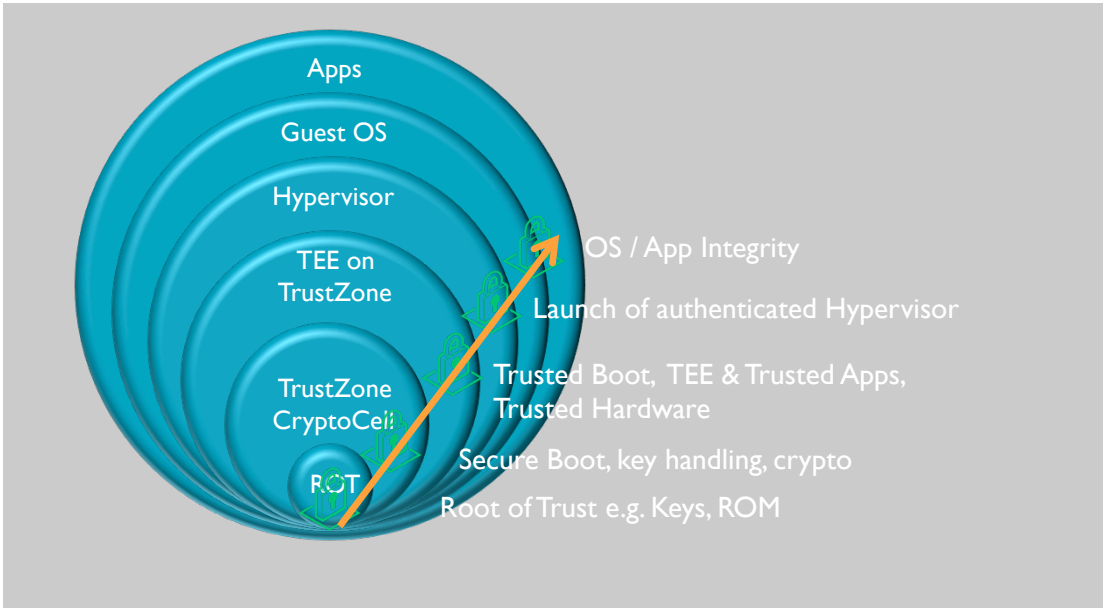




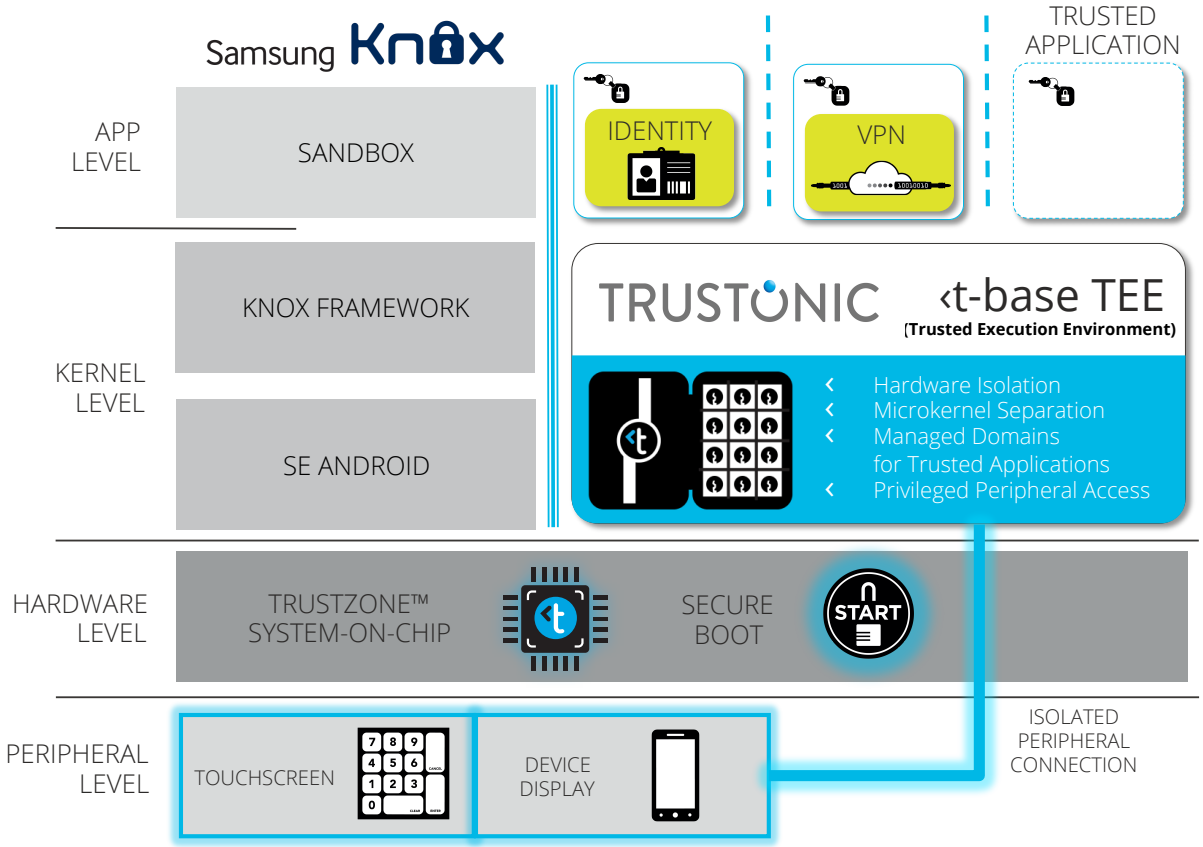
- CryptoCell acts as a trust anchor and security subsystem for the platform

ARM

Technology Model



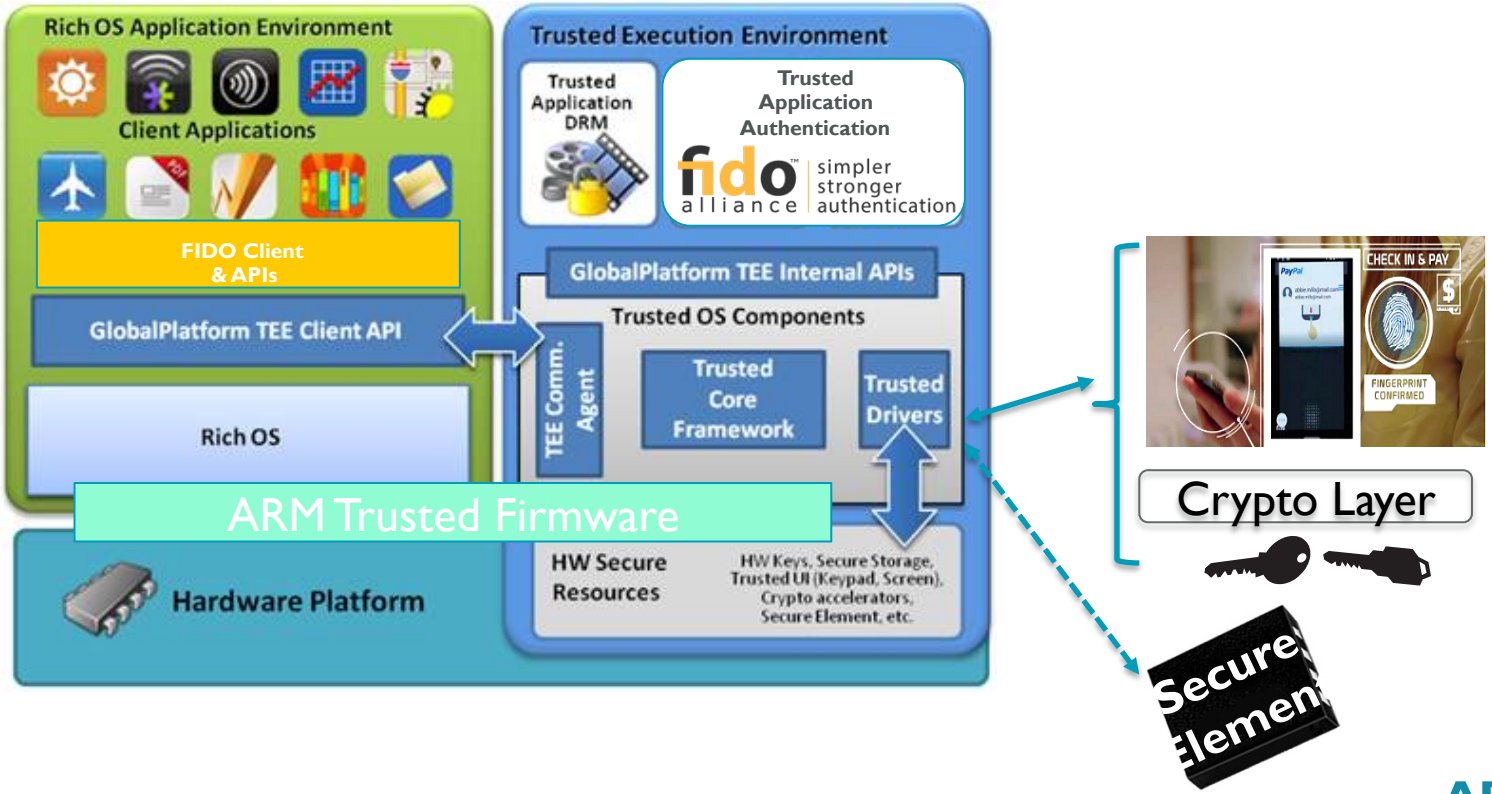
Use Cases: MDM & Enterprise



Trusted Boot
Integrity Management (TIMA)
MDM
Business Apps…

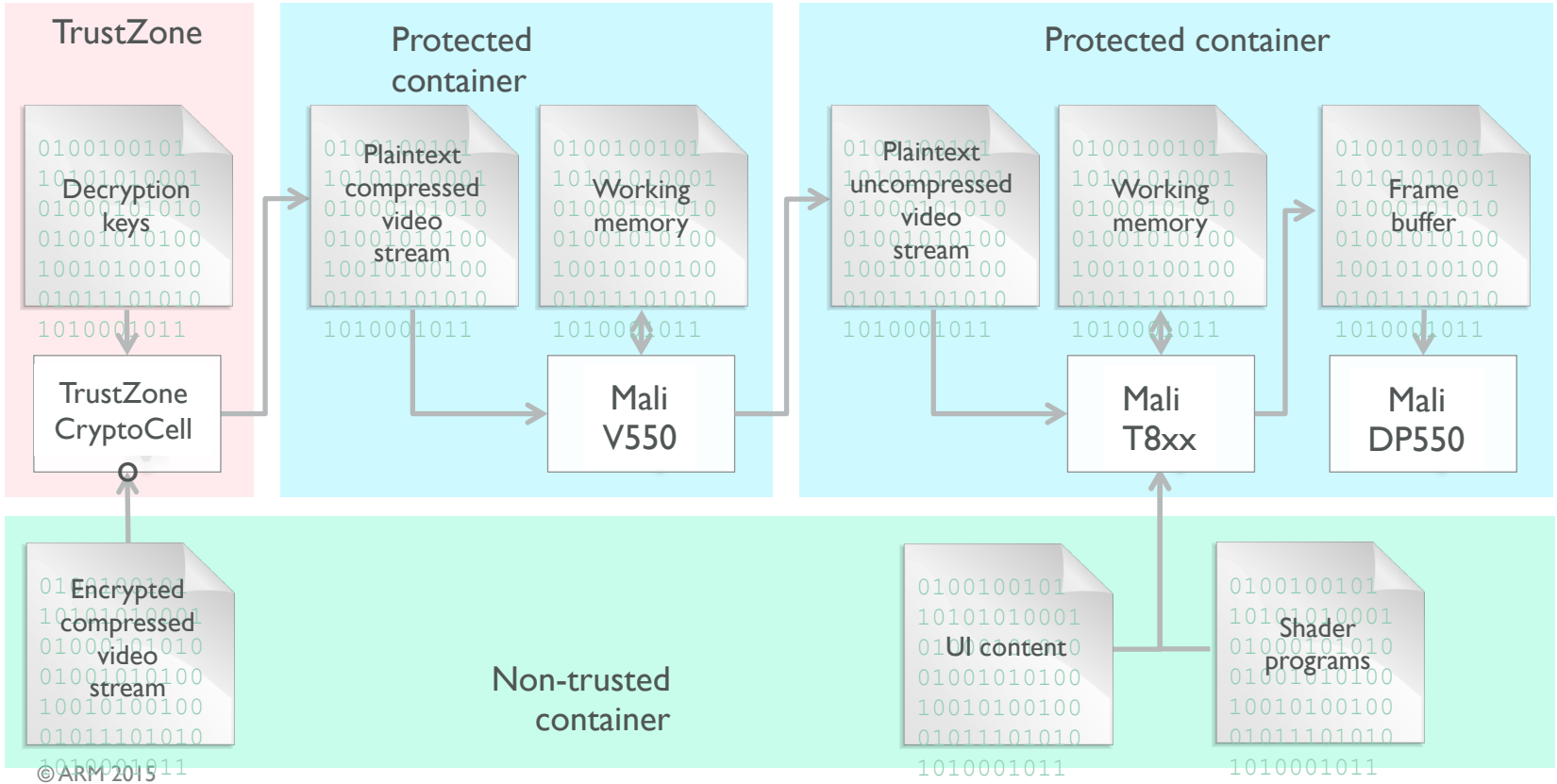
ARM

FIDO Implementation Using TrustZone based TEE



ARM

Use Case: TrustZone Media Protection



ARM

Typical Content Protection Requirements

- Secure Boot, Hardware Root of Trust
- Certified Trusted Execution Environment
- Strong Crypto
  - Secure Key Storage
- Decompressed Frame Buffer Encryption (or) Scrambling
- Protected/Secure Media Pipeline
- Protected/Secure (HDCP 2.2) Output Control
- Forensic Marking
- Detection and Traitor Tracing
- Secure Manufacturing (or) Secure Remote Key Provisioning
- Trusted Implementer (or) Third Party Security Evaluation

Note:
Common HD requirements shown in BLACK
Advanced requirements shown in GREEN

Proving It: GlobalPlatform TEE Certification

- GlobalPlatform has developed a TEE certification program
- 3 Month Evaluation
- Enables independent evaluation of partner solutions
- Builds confidence for users
- Enables Silicon Partners to differentiate on security

The GlobalPlatform Trusted Execution Environment Protection Profile is Officially Certified Against Common Criteria

Infrastructure | Insurance Systems | Risk Management Systems

4 February 2015 Like 0 Share Tweet 0 +1 0

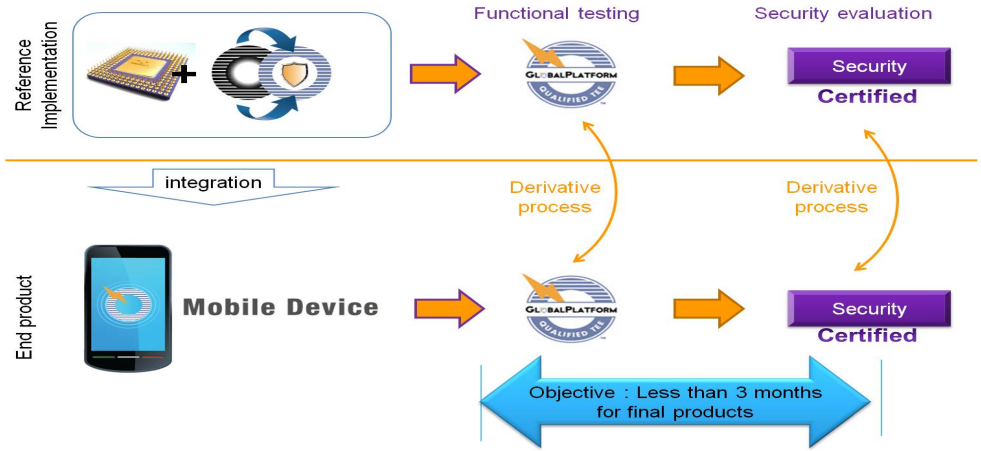
Product vendors are now able to undertake formal security evaluations for TEE products

The Common Criteria portal has officially listed the GlobalPlatform® Trusted Execution Environment (TEE) Protection Profile (PP) on its website, under the Trusted Computing category. This important milestone means that industries using TEE technology to deliver services such as premium content and mobile wallets, or enterprises and governments establishing secure mobility solutions, can now formally request that TEE products are certified against this security framework.

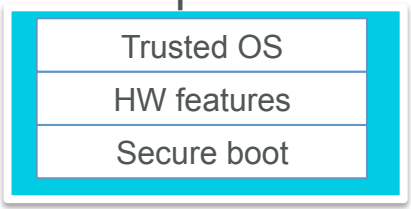
ARM

GlobalPlatform TEE Certification Initiative

- Multi market recognized certification scheme
  - Adapted to a mixed set of market requirements
  - Facilitate procurement rules (e.g. Common Criteria based)
- Two phased process
  - Certification of the TEE in a reference board implementing the complete architecture
  - Second phase on the final device



Evaluation scope



ARM

Summary

- ARM is making end to end security easier by providing right sized secure foundations that scale for different use cases and market needs
- All platforms, including the tiniest IOT devices, will be able to benefit from new TrustZone technology
- ARM TrustZone CryptoCell brings easy to implement security systems to all platforms
- Together we can make the Internet of Trustworthy Things