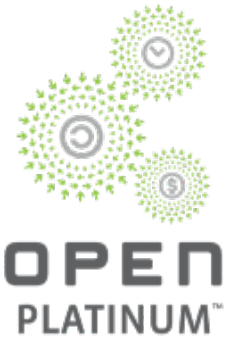
OPEN POSSIBILITIES.

Confidential Compute solutions in Arm® ecosystem

NOVEMBER 9-10, 2021

Confidential Compute solutions in Arm® ecosystem

Sridhar Valluru
Director Product Management
Arm®



OPEN POSSIBILITIES.

Confidential Compute: Threats Addressed

SECURITY

- Protect code/data from higher privileged software (eg: host, hypervisor, hardware agents) and administrators
- Strong isolation technologies to support multi-tenancy
- Encrypt memory to prevent physical access and cold boot attacks
- Encrypt multiple confidential regions with different keys
- Protect payload on IO links from interposer cards and physical probes
- Securely and uniquely bind device functions to confidential processes

Arm v8.4-A Architecture for Security

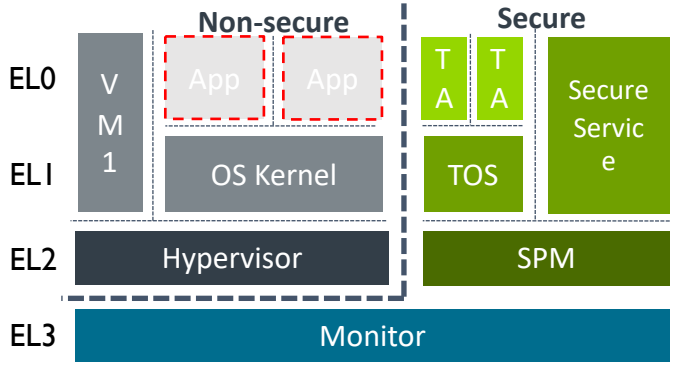
SECURITY

Architecture Features in Arm v8.4-A

TrustZone®
- Protected from Host OS/Hypervisor
- Platform security use cases for SiP + OEM
- Specific tool chains/Trusted OS
- Limited resource

Virtualization
- Can be used to protect from host primary OS kernel
- Standard OS development
- Limited only by available memory

S-EL2 Virtualization
- Complementary to first two
- Improves modularity and isolation in TrustZone®



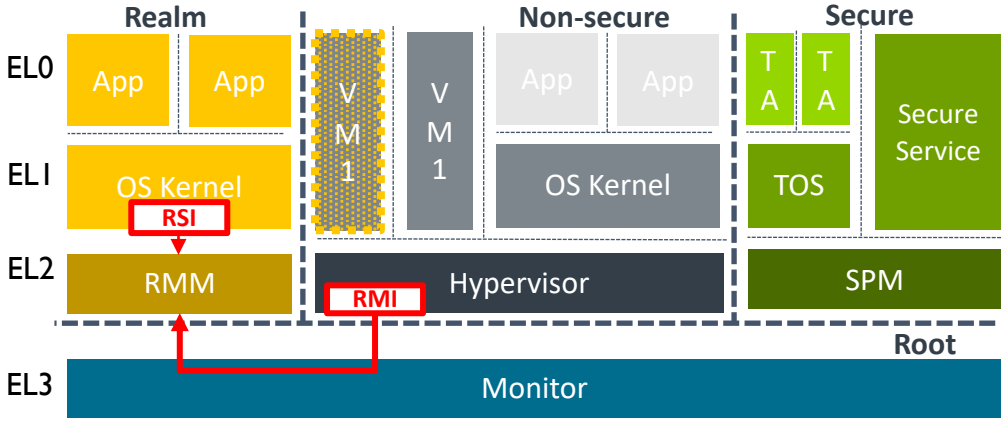
Security State / PA Space	Non-Secure PA	Secure PA
Non-Secure	Allow	Block
Secure	Allow	Allow

OPEN POSSIBILITIES.

Arm v9+ Architecture for Security: RME

SECURITY

Architecture to protect application code and data



Security State / PA Space	Non-Secure PA	Secure PA	Realm PA	Root PA
Non-Secure	Allow	Block	Block	Block
Secure	Allow	Allow	Block	Block
Realm	Allow	Block	Allow	Block
Root	Allow	Allow	Allow	Allow

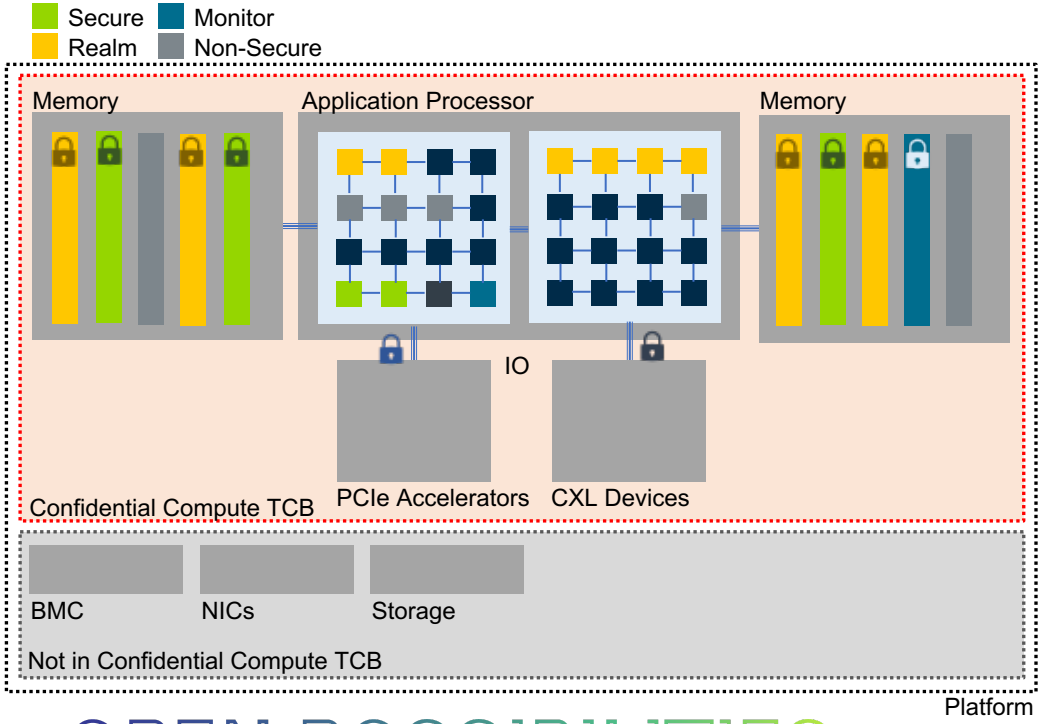
- TrustZone® 2 world to RME 4 worlds
  - Secure → Secure & Root
  - Non-Secure → Non-Secure & Realm
- Realm space is isolated from Secure & Non-Secure
  - Access violations results in page faults
- RME is implemented in hardware and firmware
  - Open source RMM and Monitor code
  - Resource allocation managed by hypervisor
  - Access management by Monitor code
- No change in programming model
  - Realm an extension of Non-Secure
  - Interrupt model remains the same

OPEN POSSIBILITIES.

RME: Realm Management Extension RMM: Realm Management Monitor RMI: Realm Management Interface RSI: Realm Services Interface

Confidential Compute TCB

Trust needs to extend to any component where code/data reside

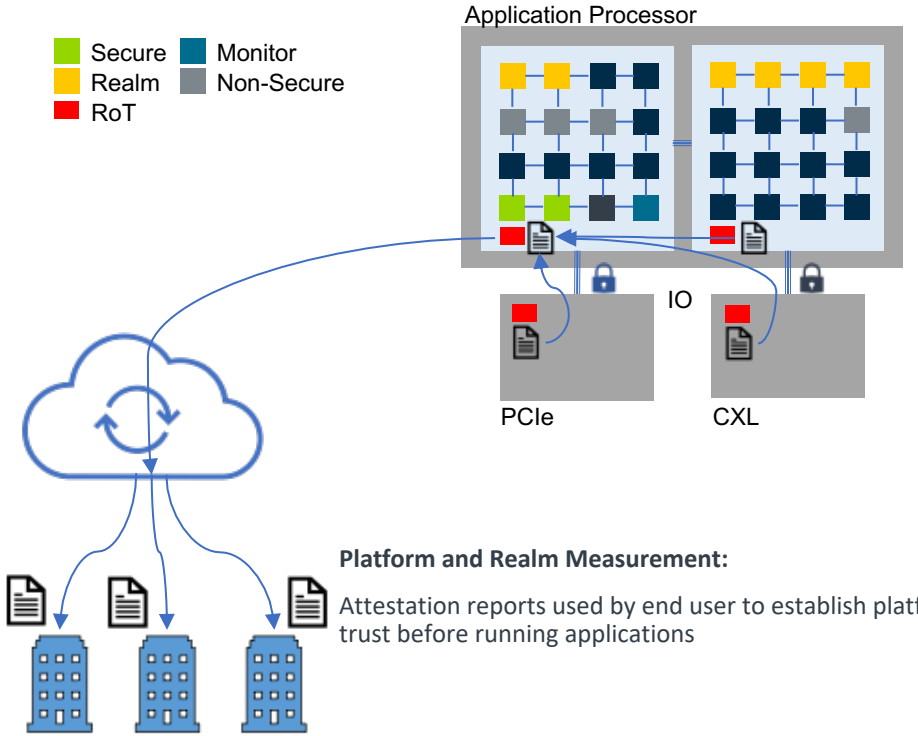


Confidential Compute needs Trust extended beyond CPU's

- Memory controllers
  - Separate keys for worlds
  - Fresh Keys for individual Realms
- IO (CXL and PCIe) Controllers
  - Enable device assignment
  - Security support defined by SIG/Consortium

Attestation

For end user confidence in platform



Platform and Realm Measurement:

Attestation reports used by end user to establish platform trust before running applications

- Hardware Enforced Security (HES) for Arm Confidential Compute Architecture
  - Initiates and measures AP Boot
  - Key generation and management
  - Collect measurements for the system
- Provides on-demand Attestation reports
  - Separate from cloud provider attestation

SECURITY

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Arm Confidential Compute Resources

SECURITY

https://www.arm.com/armcca

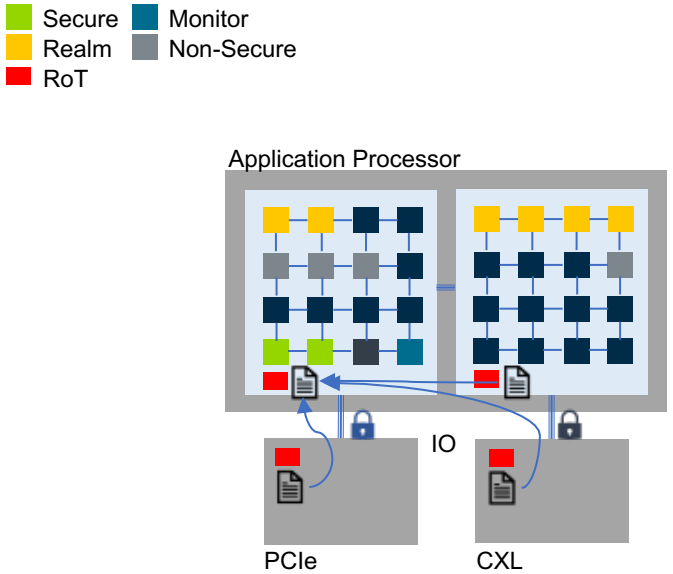
https://developer.arm.com/armcca

Contact: armcca@arm.com

Call to Action

Need for a subgroup to address common industry Confidential Compute issues

SECURITY



Need for OCP Security sub-group to address common industry confidential compute issues

- Device attestation report standardization and verification
- Standardization of device isolation granularity
  Security context is same or smaller than Virtualization context
- Life cycle and supply chain management
- Independent device security certification

Visit Arm @ OCP 2021

Booth (B11)

- **Demos: Arm SystemReady Certified Hardware**
  - Arm SystemReady, SR – ServerReady:
    - **Ampere Altra 'Mt Jade' Platform (Wiwynn)**
  - Arm SystemReady, ES – Embedded Server:
    - **Hawkeye Tech HK-6010**
    - **SolidRun Macchiatobin**
  - Arm SystemReady, IR – IoT:
    - **Raspberry Pi**

Talks

- Wed, Nov 10 @ 8:35am Room 211A-D
  Cost Modeling Analysis for Heterogeneous Integration of Chiplets, Javier DeLaCruz (Arm), Mudasir Ahmad (Google), Anu Ramamurthy (Microchip Technology)
- Wed, Nov 10 @ 10:00am Room 220C
  Confidential Compute Solutions in Arm Ecosystem, Sridhar Valluru (Arm)
- Wed, Nov 10 @ 1:00pm Room 210C
  Introduction to Open System Firmware (OSF) at OCP, Dong Wei (Arm), Ryan O'Leary (Google), Anjaneya "Reddy" Chagam (Intel)
- Wed, Nov 10 @ 2:30pm Room 210BF
  Arm and Ampere support for Standards-based OpenSource Firmware, Samer El-Haj-Mahmoud (Arm), Peter Pouliot (Ampere)

OPEN POSSIBILITIES.

OCP GLOBAL SUMMIT
NOVEMBER 9-10, 2021

Thank you!