Confidential Compute for RISC-V IoT Devices

IoT TEE proposal

Dingji, Dong, and Bicheng

RISC-V TC Meeting 2022-08-30

Outline

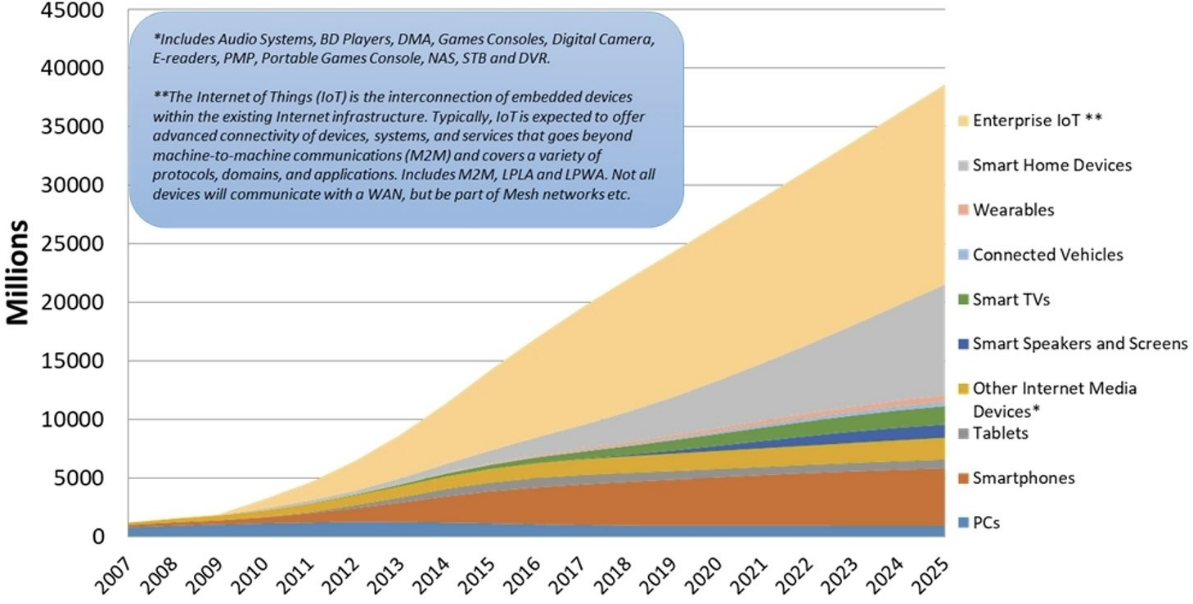
1. Background: IoT is Growing Rapidly
2. Confidential Computing and the Gap
3. IoT TEE Proposal

Emerging IoT Ecosystem

- 50 billion connected and IoT devices demand security and custom processors by 2030.

STRATEGY ANALYTICS

Global Connected and IoT Device Installed Base Forecast



*Includes Audio Systems, BD Players, DMA, Games Consoles, Digital Camera, E-readers, PMP, Portable Games Console, NAS, STB and DVR.

**The Internet of Things (IoT) is the interconnection of embedded devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. Includes M2M, LPLA and LPWA. Not all devices will communicate with a WAN, but be part of Mesh networks etc.

Source – Strategy Analytics research services, May 2019: IoT Strategies, Connected Home Devices, Connected Computing Devices, Wireless Smartphone Strategies, Wearable Device Ecosystem, Smart Home Strategies

Confidential Compute Recap

A trusted execution environment (TEE) is a secure area of a main processor. It guarantees code and data loaded inside to be protected with respect to confidentiality and integrity

—— *Wikipedia*

Confidential computing consortium

Arm, AMD, Intel, Redhat, Facebook, Google, Huawei, etc.

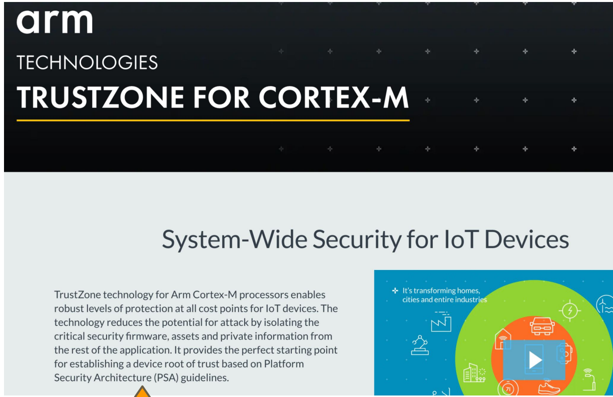
CONFIDENTIAL COMPUTING CONSORTIUM

More discussions from Security HC/TC SIG:

- *AP-TEE: https://github.com/riscv-non-isa/riscv-ap-tee/blob/main/specification/riscv-aptee-spec.pdf*
- *Security model: https://docs.google.com/document/d/1dBaDsSro6HMAmL2IEzZuanwDEQ8JKSIeICb7FxzFaqs/*
- *RISC-V TEE Architecture Goals, Assumptions, Approach, Plans: https://github.com/riscv-admin/ap-tee/blob/main/presentations/RISC-V%20TEE%20architecture.pdf*

The Gap

	Server	Desktop	IoT
Intel	TDX、SGX		
AMD	SEV-ES-SNP		
ARM	CCA、TrustZone		Trustzone-M
RISC-V	**AP-TEE**		?



arm

TECHNOLOGIES

TRUSTZONE FOR CORTEX-M

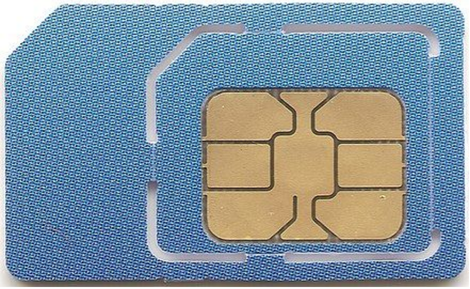
System-Wide Security for IoT Devices

TrustZone technology for Arm Cortex-M processors enables robust levels of protection at all cost points for IoT devices. The technology reduces the potential for attack by isolating the critical security firmware, assets and private information from the rest of the application. It provides the perfect starting point for establishing a device root of trust based on Platform Security Architecture (PSA) guidelines.

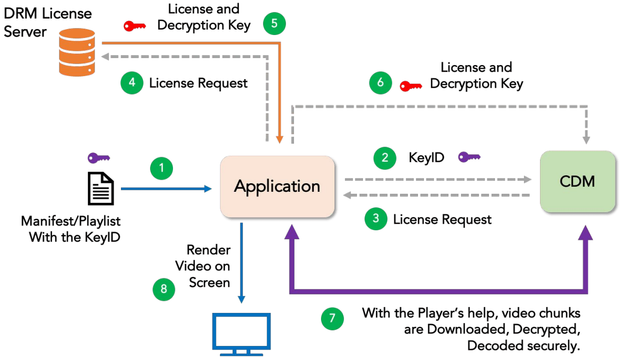
It's transforming homes, cities and entire industries

IoT TEE proposal

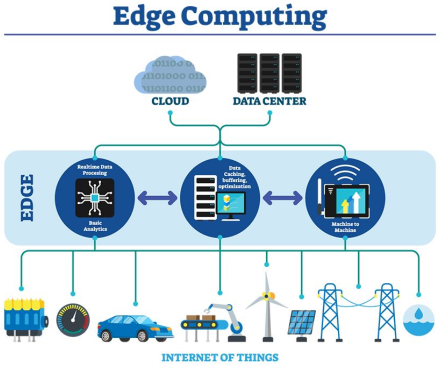
IoT TEE Scenarios



SIM card


DRM License Server
License and Decryption Key
5
4
License Request
License and Decryption Key
6
1
Manifest/Playlist With the KeyID
Application
2
KeyID
CDM
3
License Request
Render Video on Screen
8
7
With the Player's help, video chunks are Downloaded, Decrypted, Decoded securely.

DRM



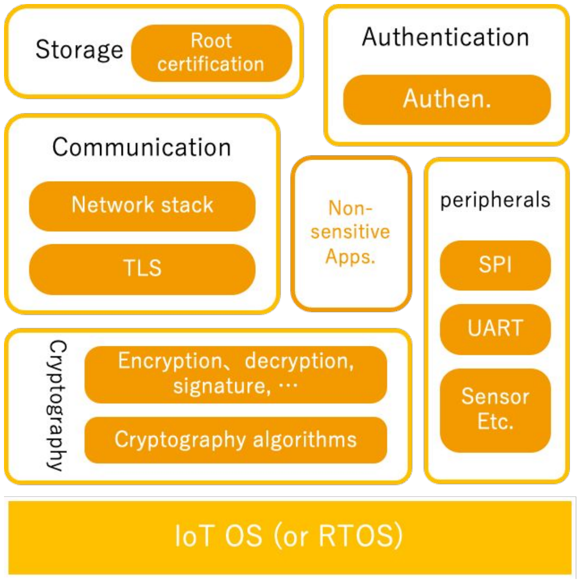
Car

Pic refs: (1) SIM card: https://en.wikipedia.org/wiki/SIM_card (2) DRM: https://ottverse.com/eme-cenc-cdm-aes-keys-drm-digital-rights-management/ (3) edge computing: https://en.wikipedia.org/wiki/Edge_computing (4) Car: https://www.huaweicentral.com/huawei-does-not-build-cars-confirmed-wang-jun-huawei-smart-car-bu-coo/

IoT TEE: Benefits

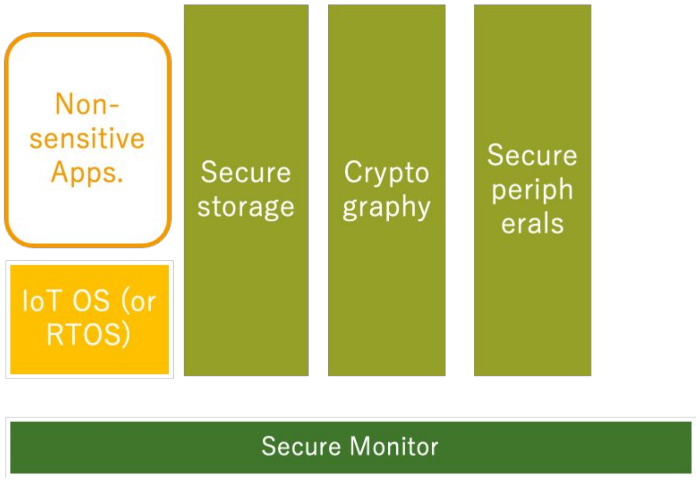
Traditional IoT Arch

Security-sensitive and non-sensitive applications are co-located. The system is compromised if any component is attacked.



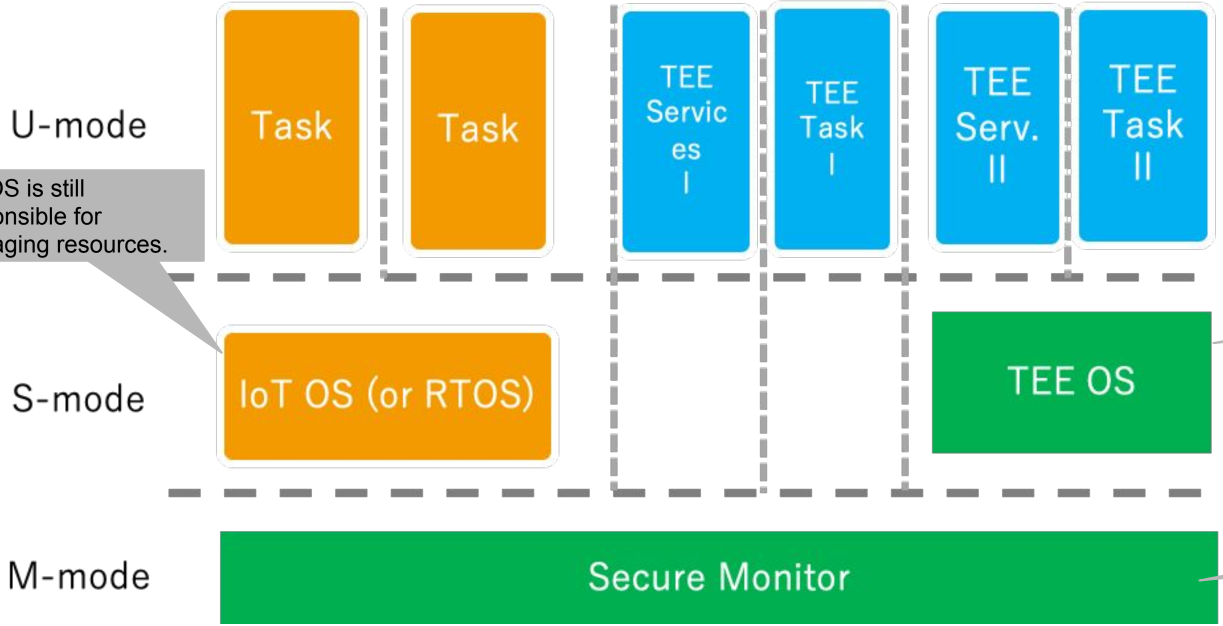
With RISC-V IoT TEE

Applications/components are isolated into different domains. Communication is only allowed through standard interfaces. Attack surface is reduced.



IoT TEE: Reference Arch (for M-S-U devices)

Overview



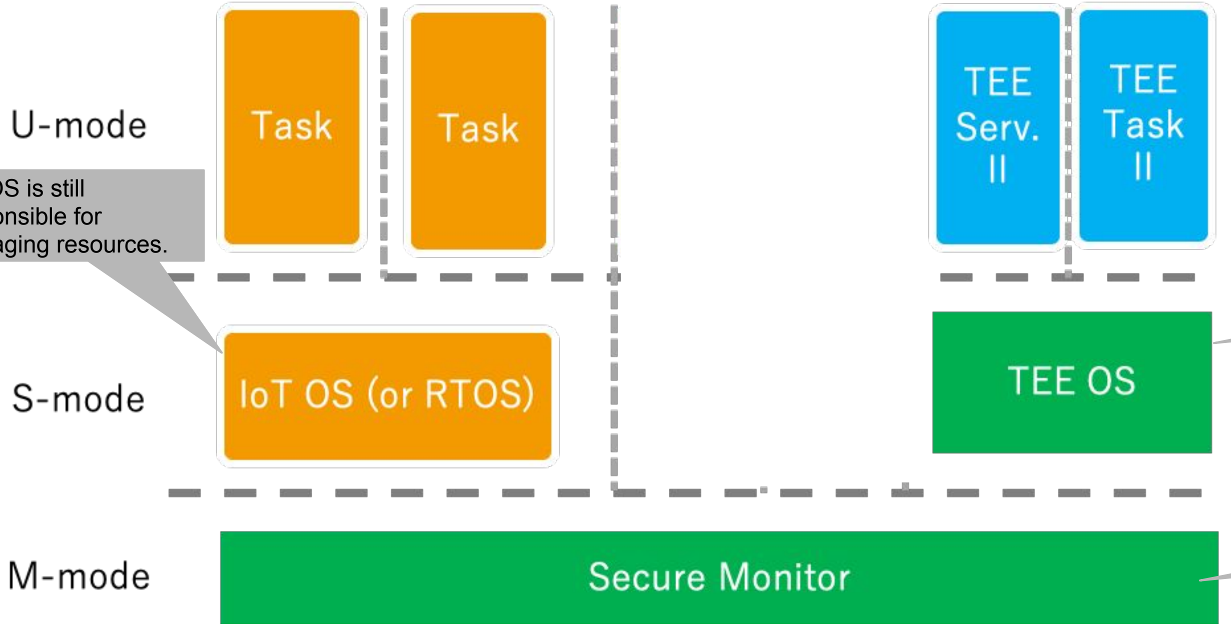
IoT OS is still responsible for managing resources.

(optional) A domain with TEE OS can launch TEE services/tasks, and the TEE OS is responsible to isolate those services and tasks.

Secure monitor runs in M-mode to provide isolation among domains. IoT TEE's secure monitor should co-design with AP-TEE's TSM-driver and will follow the interfaces of AP-TEE.

IoT TEE: Reference Arch (for M-S-U devices)

Use case #1: Secure and non-secure domains: *running all security-sensitive applications in the secure domain (with TEE OS)*



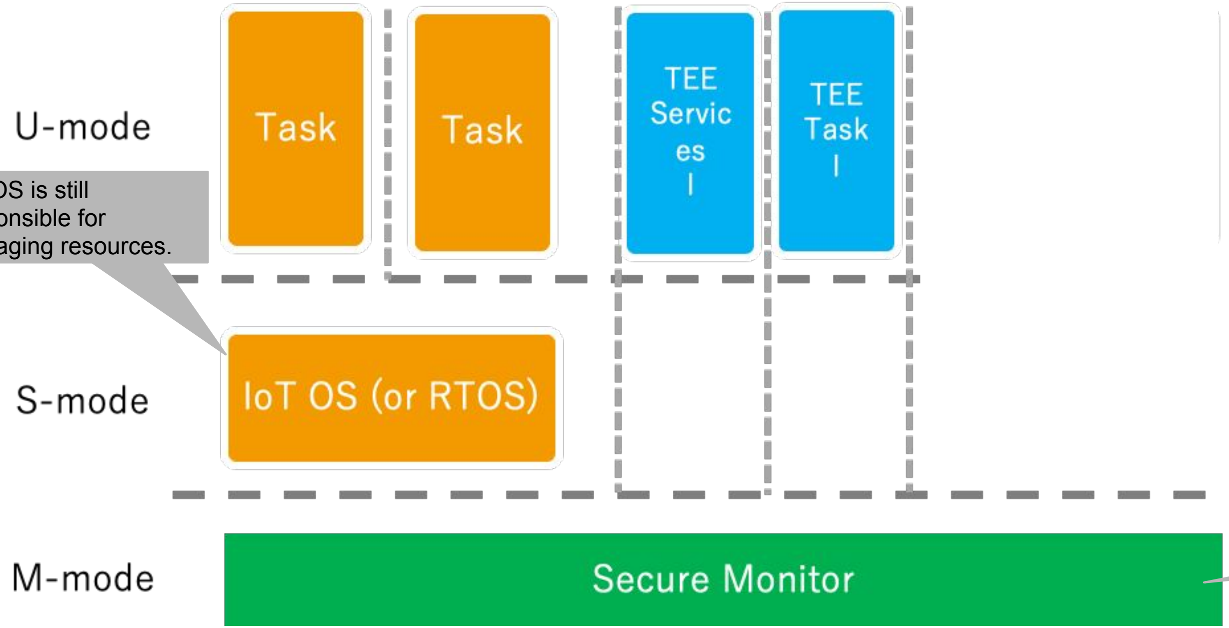
IoT OS is still responsible for managing resources.

(optional) A domain with TEE OS can launch TEE services/tasks, and the TEE OS is responsible to isolate those services and tasks.

Secure monitor runs in M-mode to provide isolation among domains. IoT TEE's secure monitor should co-design with AP-TEE's TSM-driver and will follow the interfaces of AP-TEE.

IoT TEE: Reference Arch (for M-S-U devices)

Use case #2: Isolated services/tasks: *isolating security-sensitive services/tasks into different domains, still relying on the IoT OS for system services*.

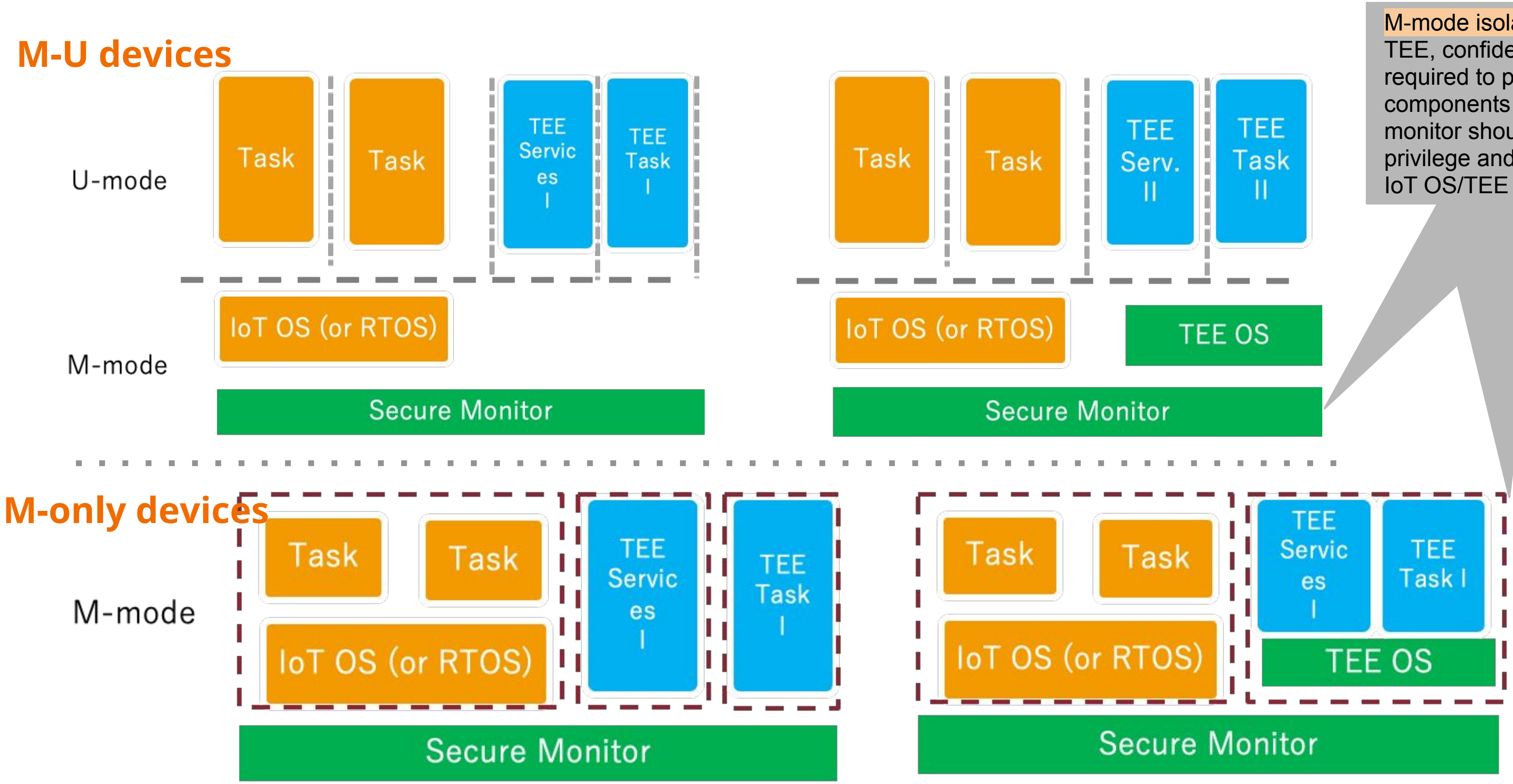


IoT OS is still responsible for managing resources.

Secure monitor runs in M-mode to provide isolation among domains. IoT TEE’s secure monitor should co-design with AP-TEE’s TSM-driver and will follow the interfaces of AP-TEE.

IoT TEE: Reference Arch (for M-U/M-only devices)

M-mode isolation (e.g., lightweight TEE, confidential M-mode, etc.) is required to provide isolation between components in the M-mode. Secure monitor should have the highest privilege and can not be accessed by IoT OS/TEE OS/tasks directly.



IoT TEE: Scope and Relation with AP-TEE

	Area	Function	Relation with AP-TEE	Resources
Specs	IoT-TEE Host-ABI	SBI Extension Interface implemented by the secure monitor (or TEE OS when available) via ECALL for use by IoT OS to manage TEE tasks/services	Co-design with AP-TEE TG, based on AP-TEE's TH-ABI	A new TG under TC SIG? Collaborations with AP-TEE TG and others.
	IoT-TEE TEE-ABI	SBI Extension Interface implemented by the secure monitor (or TEE OS when available) via ECALL for use by TEE tasks/services	Co-design with AP-TEE TG, based on AP-TEE's TG-ABI	
Platform	Hardware requirements	Support M-only, M-U, and M-S-U IoT devices. Support both 32 and 64 bit devices. PMP/ePMP is required for M-only/M-U devices, and paged virtual memory or sPMP/sMPU is required for M-S-U devices. No need to support H-extensions. IOPMP is required for secure I/O.	Targeting different scenarios (IoT) compared with AP-TEE.	
POCs	Security monitor (M-mode FW)	Minimal SBI extensions to support IoT TEE functionalities. Part of TCB (expected to be HW-vendor signed and may be HW-operator signed). Implement Host-ABI/TEE-ABI or relies on a TEE OS to implement Host-ABI/TEE-ABI (when TEE OS available)	Co-design with AP-TEE's M-mode FW and TSM. Collab with OpenSBI.	
	IoT OS	*Untrusted* IoT OS (RTOS) that manages resources for both untrusted or TEE tasks/services.		
	TEE OS	Software module that implements Host-ABI/TEE-ABI and (optional) system services.		