

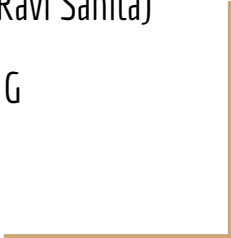


Confidential Compute for RISC-V Platforms

AP-TEE TG proposal (presented by Ravi Sahita)

For Trusted Computing SIG

Assignee - Security HC



Confidential Computing

Confidential Computing is the protection of data in use by performing computation in a Hardware-based Trusted Execution Environment.

This definition is independent of topological location, which processor does it, and whether encryption or some other isolation technique is used.

The protection of data in use is against a well-defined adversary.

Key properties of a HW-based TEE for Conf. Comp.

A Trusted Execution Environment (TEE) is an environment that provides a level of assurance of three key properties:

- Data confidentiality
- Data integrity
- Code integrity

Additional desirable characteristics:

- Code confidentiality
- Authenticated Launch
- Programmability
- Attestability -- This is a required from the Trusted Computing SIG perspective
- Recoverability

Confidential Compute Threat Model

User/System Software attacks

Protocol attacks

Cryptographic attacks

Basic hardware attacks

Basic upstream supply-chain attacks

Advanced hardware attacks

Upstream hardware supply-chain attacks

uArch and Arch Side-channel attacks*

Detailed threat model has been defined and documented [here](#).

We note that different implementations will have varying degrees of resistance to attacks

The TC SIG (or proposed TG) does not aim to specify any threats as out of scope.

RVI Gaps → AP-TEE TG Charter

Why should we do this? And why now?

- Confidential Computing is at an inflection point and all compute domains (Data Center/Servers to Embedded) require support for it - alternate architectures have solutions in place

Intel SGX, TDX
AMD SEV-ES-SNP
ARM Trustzone, CCA
RISC-V ?

What are the key gap areas? [TG components proposed below described on next slide]

- **AP-TEE TG to cover Reference Architecture, Interfaces, Uncover potential ISA gaps**
 - Interfaces must be designed to be extensible to future ISA (via gap analysis) --normative.
 - ISA proposals -- request FT/TG as needed -- normative.
 - Security Arch for CC -- *Separate living doc* - also use as an Implementers Guide.

RISC-V AP-TEE TG addresses this gap

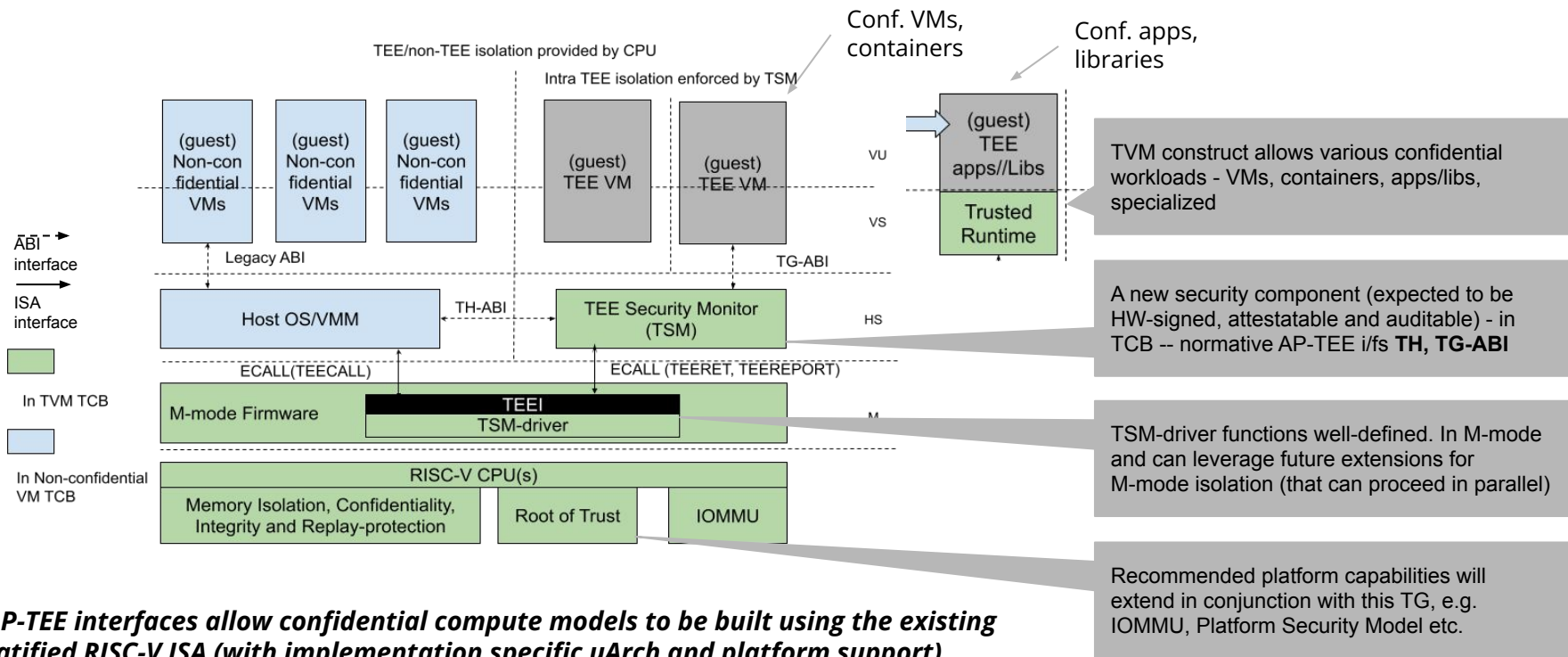
Who else do /should we work with?

- **Within RVI** - Security HC/Trusted Computing SIG, TEE TG, CFI SIG, Software HC (Hypervisor SIG), SOC infrastructure SIG (IOMMU, QoS, RAS ...), DataCenter SIG
- **Outside RVI** - Confidential Computing Consortium (CCC), Trusted Computing Group (TCG), Internet Engineering Task Force (IETF), Distributed Management Task Force (DMTF), PCIe, CXL

CCC
Open Enclave SDK
Keystone
Project Veraison

IETF RATS
TCG DICE
DMTF SPDM
PCIe IDE, TDISP

AP-TEE TG Charter: Reference Arch



AP-TEE interfaces allow confidential compute models to be built using the existing ratified RISC-V ISA (with implementation specific uArch and platform support)

AP-TEE TG Charter: Interfaces

Specs



Area	Function	Resources
AP-TEE TH-ABI	SBI Extension Interface implemented by the TSM via TEECALL for use by OS/VMM to manage TVMs	TG WG members
AP-TEE TG-ABI	SBI Extension Interface implemented by the TSM via ECALL for use by TVM guest workloads	
TEE Security Manager (TSM)	TSM is a RISC-V 64 bit SW module that uses RISC-V H-extension and implements TH and TG-ABI. It is in the TCB for all TVM workloads (Expected to be HW-vendor signed and may be HW-operator signed)	Rivos contributes to start
M-mode FW	Minimal SBI extensions (TCB component) to support TSM initialization, TEECALL, TEERET implementation. It is in the TCB for all TVM workloads (Expected to be HW-vendor signed and may be HW-operator signed) - Collab with OpenSBI	Expecting collaborators on these existing projects from SW HC
Linux, KVM (Host OS/VMM)	<i>Untrusted</i> (enlightened) host OS/VMM that manage resources for TVM-based confidential workloads [TSM enforces security properties] - Collab with Hypervisor SIG	
Linux (TVM Guest OS), Guest Firmware	Enlightened guest OS/runtime (in TCB of TVM workload) - Collab with SW HC	

POCs



AP-TEE TG Charter: Platform specific & ISA (Scope)

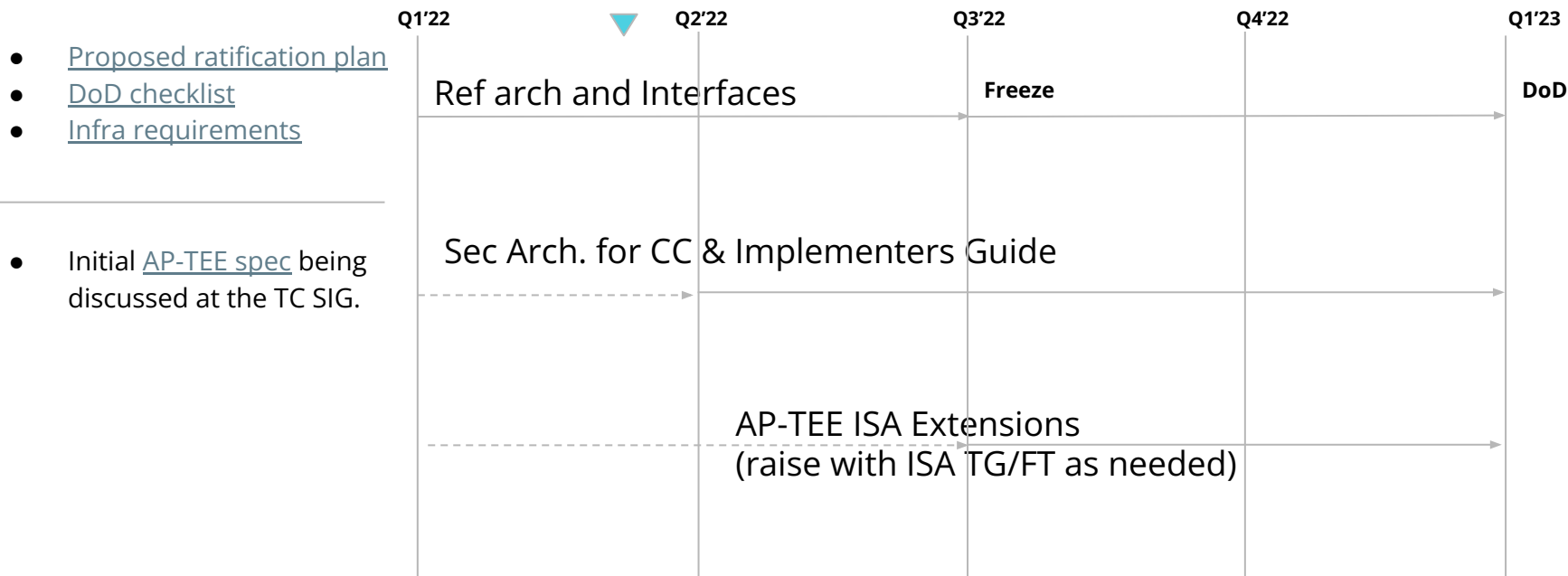
Area	Function	Resources
CPU	AP-TEE mode qualifier ; Memory page access-control isolation properties	TG members
IOMMU	AP-TEE mode qualifier; Memory page access-control isolation properties	+ IOMMU TG
TLB, Caches	AP-TEE mode qualifier	TG members
Interconnect, Fabrics	Platform-specific cryptographic memory isolation and mode qualifier	AP-TEE TG members to document + Implementation feedback
Memory (volatile and persistent)	Platform-specific cryptographic memory isolation and mode qualifier	
HW Root-of-trust	Platform-specific subsystem to support HW Attestation, Sealing interfaces	
Devices	Device-specific subsystem to support Device attestation, link security	

Security Arch for CC and Implementers Guide covers these as recommendations:

- Mapping of mitigations to threat model
- Recommendations for crypto modes
- Attestation protocols, formats



Proposed AP-TEE TG workstreams



Seeking TSC Approval to form AP-TEE TG with this charter