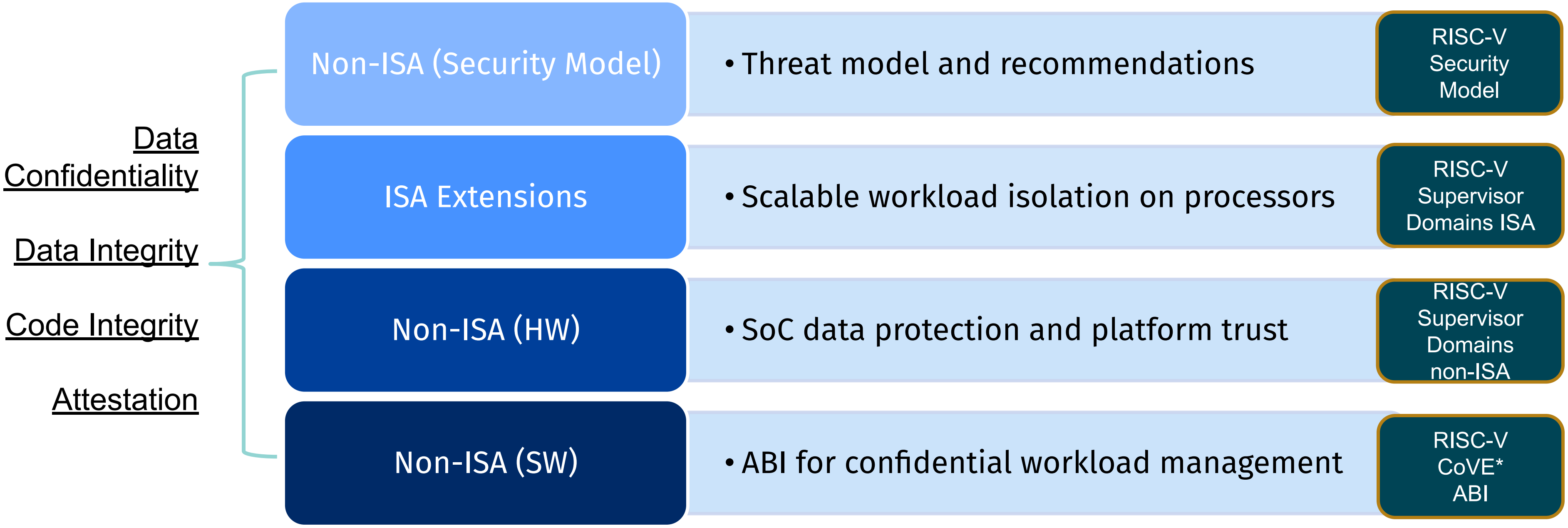
Confidential Computing on RISC-V platforms (update)

Ravi Sahita

August 8, 2025

Rivos

Confidential Computing on RISC-V



Data Confidentiality

Data Integrity

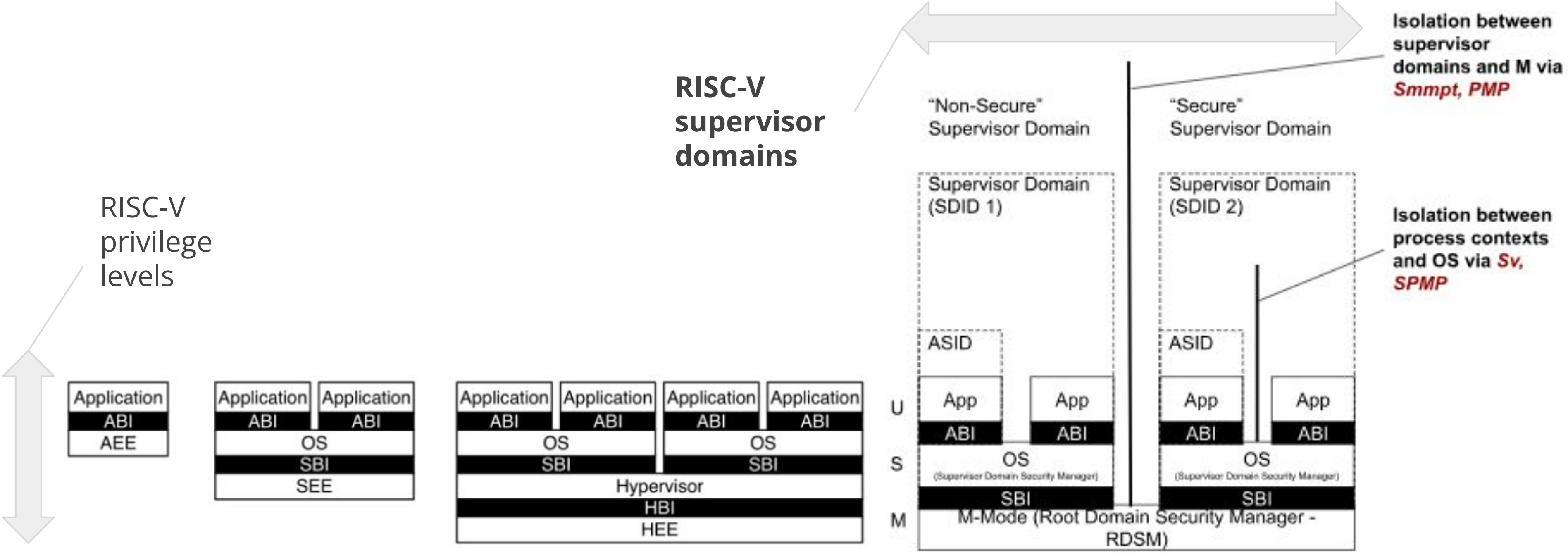
Code Integrity

Attestation

Non-ISA (Security Model)	• Threat model and recommendations	RISC-V Security Model
ISA Extensions	• Scalable workload isolation on processors	RISC-V Supervisor Domains ISA
Non-ISA (HW)	• SoC data protection and platform trust	RISC-V Supervisor Domains non-ISA
Non-ISA (SW)	• ABI for confidential workload management	RISC-V CoVE* ABI

*Confidential VM Extension

RISC-V Priv. ISA and Supervisor Domains ISA Extension



RISC-V privilege levels

RISC-V supervisor domains

Isolation between supervisor domains and M via *Smmpt, PMP*

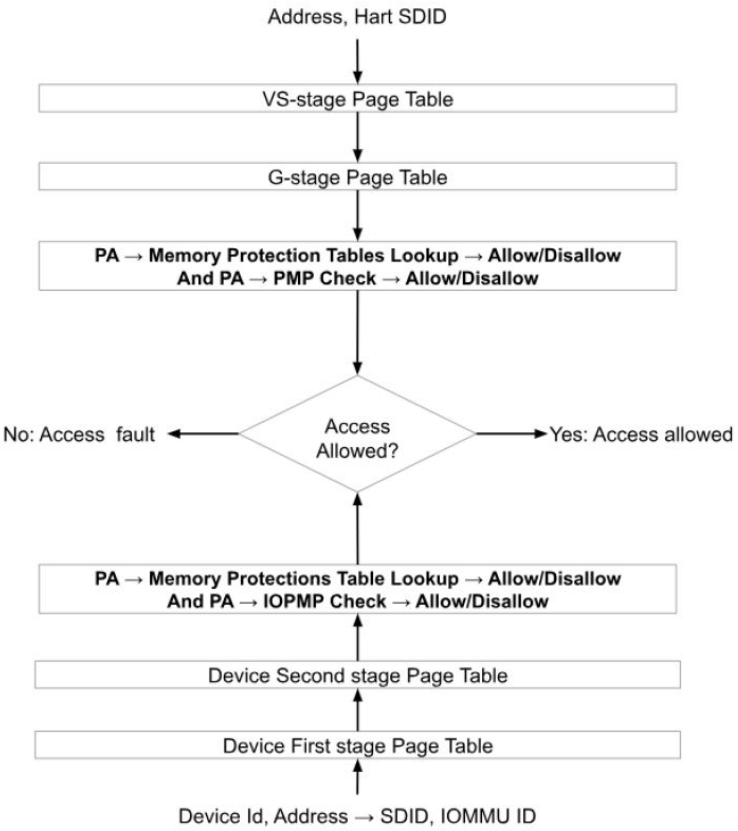
Isolation between process contexts and OS via *Sv, SPMP*

Application
ABI
AEE
Application
Application
ABI
ABI
OS
SBI
SEE
Application
Application
Application
Application
ABI
ABI
ABI
ABI
OS
OS
SBI
SBI
Hypervisor
HBI
HEE
"Non-Secure" Supervisor Domain
"Secure" Supervisor Domain
Supervisor Domain (SDID 1)
Supervisor Domain (SDID 2)
ASID
ASID
U
S
M
App
App
App
App
ABI
ABI
ABI
ABI
OS (Supervisor Domain Security Manager)
OS (Supervisor Domain Security Manager)
SBI
SBI
M-Mode (Root Domain Security Manager - RDSM)

Supervisor domains extends RISC-V priv. ISA to enable isolated supervisor contexts

https://github.com/riscv/riscv-smmtt/releases

Memory Isolation Model (Smmpt)



Address, Hart SDID

VS-stage Page Table

G-stage Page Table

PA → Memory Protection Tables Lookup → Allow/Disallow
And PA → PMP Check → Allow/Disallow

No: Access fault

Access Allowed?

Yes: Access allowed

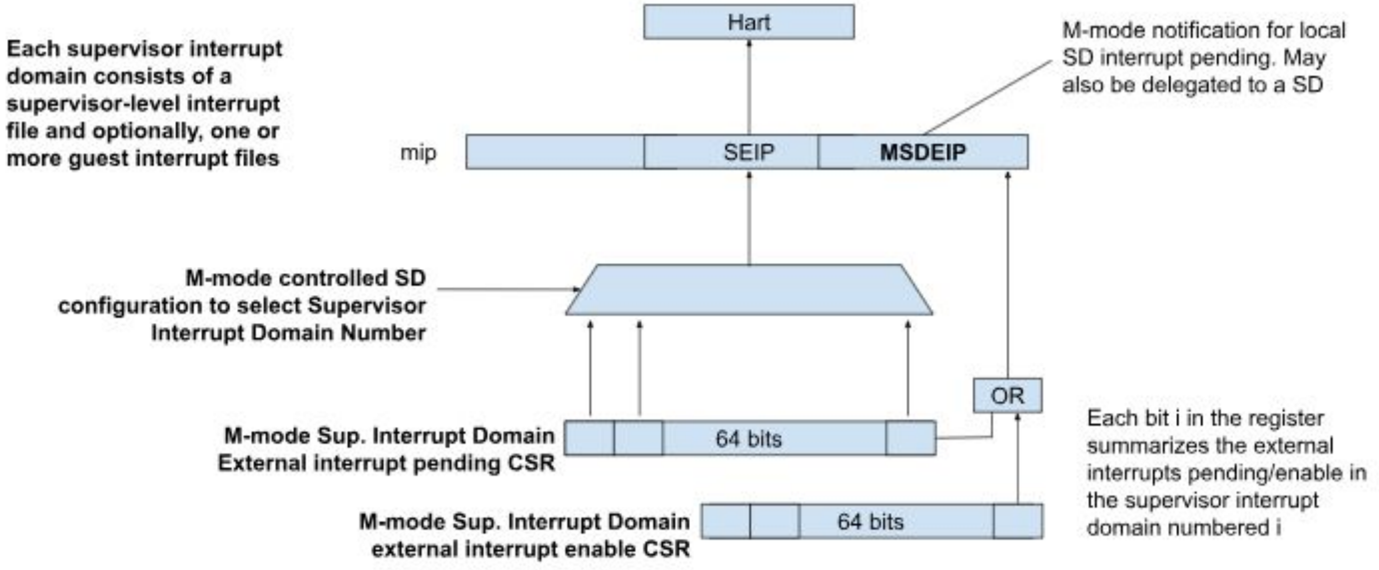
PA → Memory Protections Table Lookup → Allow/Disallow
And PA → IOPMP Check → Allow/Disallow

Device Second stage Page Table

Device First stage Page Table

Device Id, Address → SDID, IOMMU ID

Secure Interrupts (Smsdia - extends RISC-V Advanced Interrupt Arch.)



Each supervisor interrupt domain consists of a supervisor-level interrupt file and optionally, one or more guest interrupt files

M-mode notification for local SD interrupt pending. May also be delegated to a SD

M-mode controlled SD configuration to select Supervisor Interrupt Domain Number

M-mode Sup. Interrupt Domain External interrupt pending CSR

M-mode Sup. Interrupt Domain external interrupt enable CSR

Each bit i in the register summarizes the external interrupts pending/enable in the supervisor interrupt domain numbered i

Figure: Smsdia-defined CSRs and controls in bold

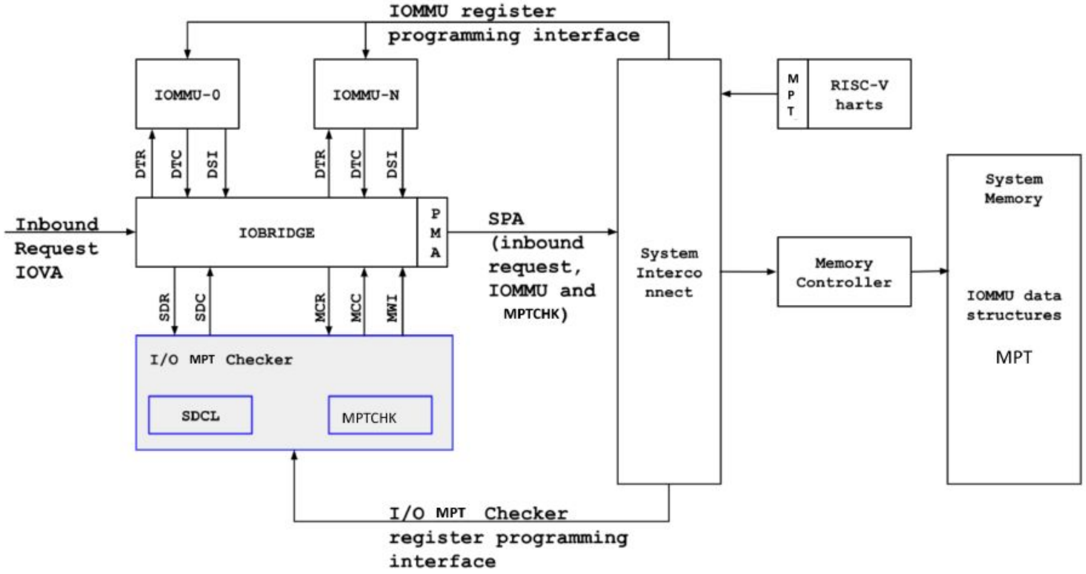
Via a sub-extension Smgeien, a subset of Guest interrupt files within a Sup. Interrupt domain may be made accessible to another supervisor domain

Non-ISA: Platform IO and Data Protection

Devices may be assigned to supervisor domains

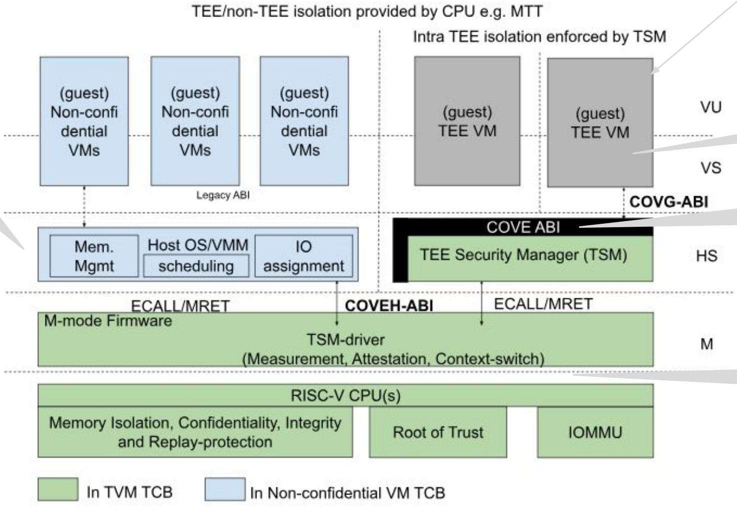
IOMPT composes with RISC-V IOPMP, IOMMU, Smmpt for direct device assignment to supervisor domains

Enables compatibility with PCIe & CXL standard interfaces for TEE-IO



Non-ISA: SW - CoVE ABI and Ref. Arch

OS/VMM retains resource management role


TEE/non-TEE isolation provided by CPU e.g. MTT
Intra TEE isolation enforced by TSM
(guest) Non-confidential VMs
(guest) Non-confidential VMs
(guest) Non-confidential VMs
(guest) TEE VM
(guest) TEE VM
VU
VS
Legacy ABI
COVG-ABI
COVE ABI
Mem. Mgmt
Host OS/VMM scheduling
IO assignment
TEE Security Manager (TSM)
HS
ECALL/MRET
COVEH-ABI
ECALL/MRET
M-mode Firmware
TSM-driver
(Measurement, Attestation, Context-switch)
M
RISC-V CPU(s)
Memory Isolation, Confidentiality, Integrity and Replay-protection
Root of Trust
IOMMU
In TVM TCB
In Non-confidential VM TCB

Confidential VMs

Architecture for Confidential VMs also enables containers, apps/libs => avoid app changes

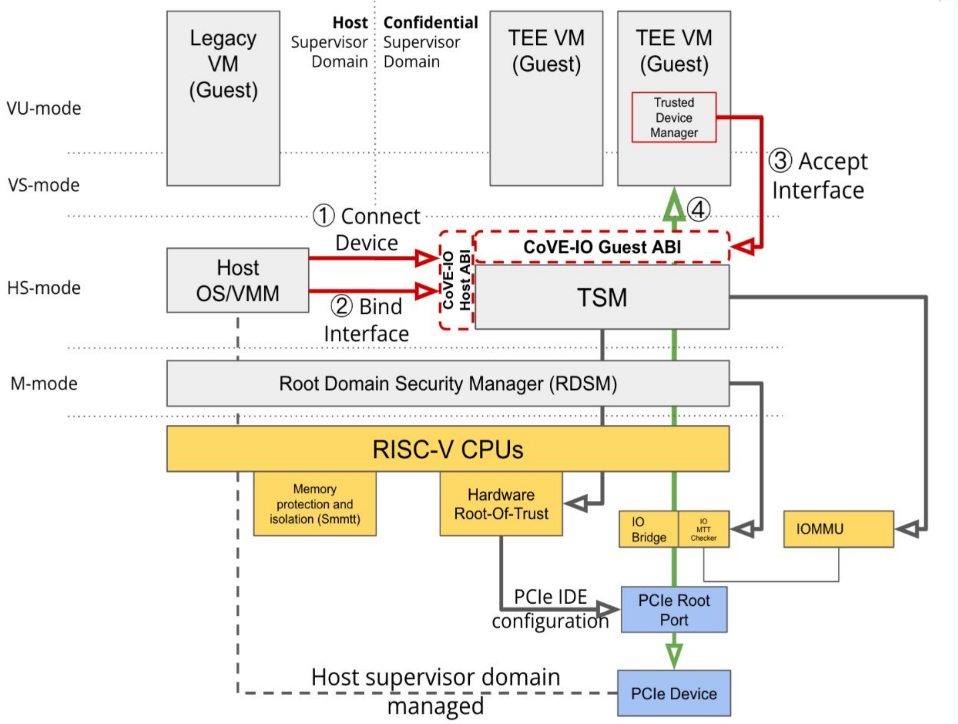
TEE Security Manager (TSM) - TCB component that *enforces security properties*. Expected to be auditable - signed, attested by the RoT - *supports proposed CoVE ABI.*

TSM-driver functions are minimal - bootstrap, attestation and context-switching to isolate the TSM.

Spec in reviews towards STABLE

https://github.com/riscv-non-isa/riscv-ap-tee/releases

CoVE-IO

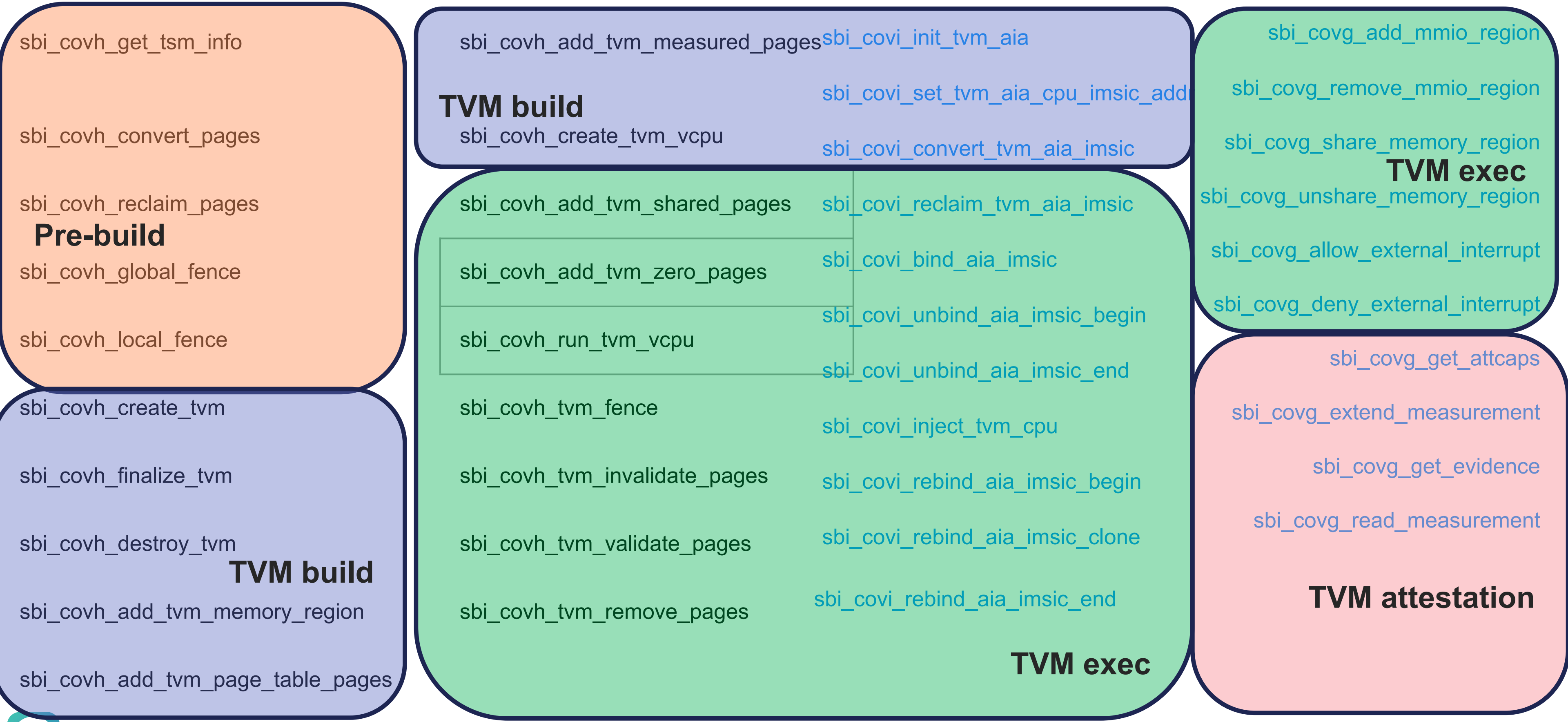


Spec in reviews towards STABLE

https://github.com/riscv-non-isa/riscv-ap-tee-io/releases/download/v0.2.0/riscv-cove-io-v0.2.0.pdf

CoVE ABI

https://github.com/riscv-non-isa/riscv-ap-tee/releases



Pre-build

sbi_covh_get_tsm_info

sbi_covh_convert_pages

sbi_covh_reclaim_pages

sbi_covh_global_fence

sbi_covh_local_fence

TVM build

sbi_covh_create_tvm

sbi_covh_finalize_tvm

sbi_covh_destroy_tvm

sbi_covh_add_tvm_memory_region

sbi_covh_add_tvm_page_table_pages

TVM build

sbi_covh_add_tvm_measured_pages

sbi_covh_create_tvm_vcpu

sbi_covi_init_tvm_aia

sbi_covi_set_tvm_aia_cpu_imsic_addr

sbi_covi_convert_tvm_aia_imsic

TVM exec

sbi_covh_add_tvm_shared_pages

sbi_covh_add_tvm_zero_pages

sbi_covh_run_tvm_vcpu

sbi_covh_tvm_fence

sbi_covh_tvm_invalidate_pages

sbi_covh_tvm_validate_pages

sbi_covh_tvm_remove_pages

sbi_covi_reclaim_tvm_aia_imsic

sbi_covi_bind_aia_imsic

sbi_covi_unbind_aia_imsic_begin

sbi_covi_unbind_aia_imsic_end

sbi_covi_inject_tvm_cpu

sbi_covi_rebind_aia_imsic_begin

sbi_covi_rebind_aia_imsic_clone

sbi_covi_rebind_aia_imsic_end

TVM exec

sbi_covg_add_mmio_region

sbi_covg_remove_mmio_region

sbi_covg_share_memory_region

sbi_covg_unshare_memory_region

sbi_covg_allow_external_interrupt

sbi_covg_deny_external_interrupt

TVM attestation

sbi_covg_get_attcaps

sbi_covg_extend_measurement

sbi_covg_get_evidence

sbi_covg_read_measurement

ISA, non-ISA *emulation* work items

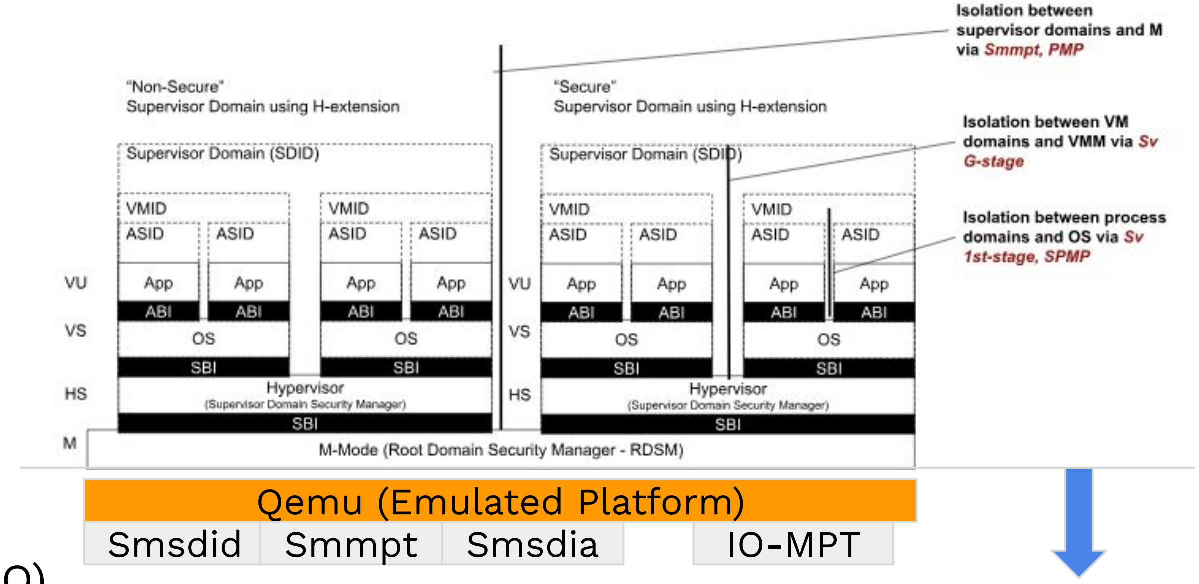
Supervisor domains spec is at v0.4 - stable with ARC review updates incorporated for baseline ISA

ISA Emulation

- ○ Memory & State Isolation (Smsdid, Smmpt)
- ○ AIA and Interrupt Isolation (Smsdia)
- ○ QoS (Smqosid CSR emulation)

Non-ISA HW Emulation (IO)

- ○ IO-MPT (use existing IOMMU model)



Isolation between supervisor domains and M via *Smmpt, PMP*

Isolation between VM domains and VMM via *Sv G-stage*

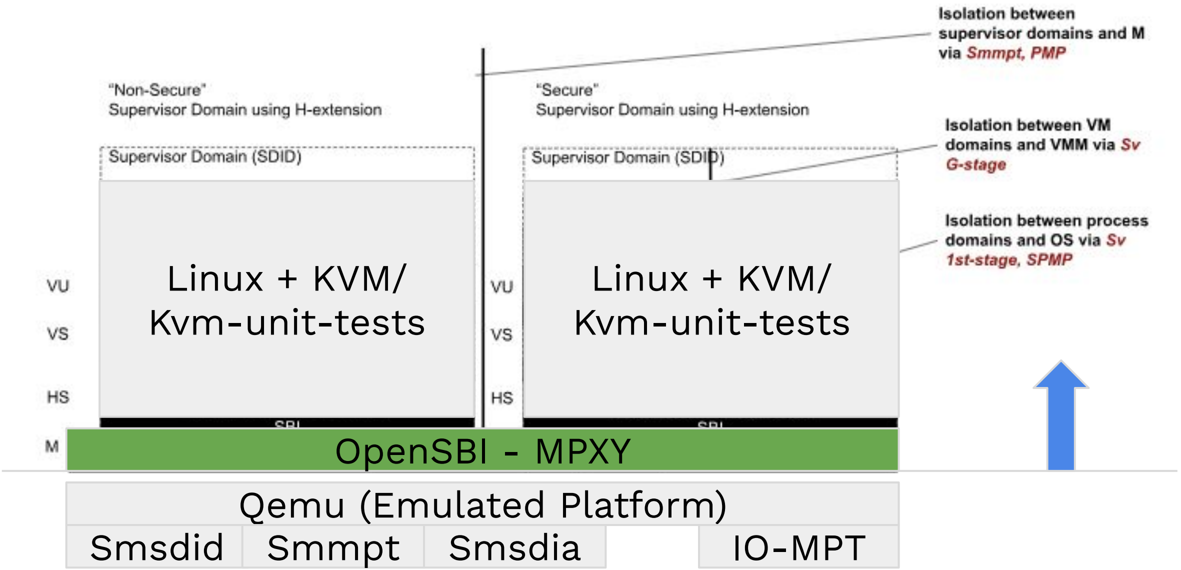
Isolation between process domains and OS via *Sv 1st-stage, SPMP*

Qemu (Emulated Platform)

Smsdid | Smmpt | Smsdia | IO-MPT

ISA, non-ISA *SW* work items to test emul.

- **Extending prior work on Smmpt emulation in QEMU - work started by Gregor Haas (link)**
  - Support all deployment models 1 (TSM as HS-peer), 2 (TSM as HS) and 3 (TSM in M-mode)
- **Supporting code for OpenSBI, kvm-unit-tests to test the QEMU changes**
  - Tests create two domains
  - Tests memory access control for different page sizes
  - Invalidation of permissions



Isolation between supervisor domains and M via *Smmpt, PMP*

Isolation between VM domains and VMM via *Sv G-stage*

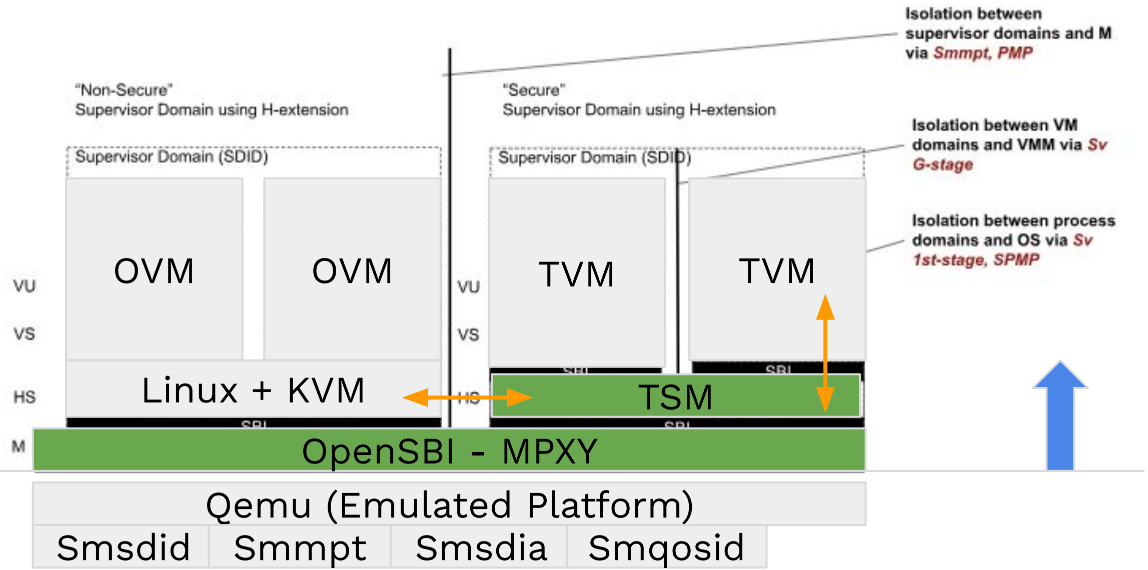
Isolation between process domains and OS via *Sv 1st-stage, SPMP*

CoVE ABI (SBI Ext) work items.

- Linux KVM Host, KVMtool
  - TVM creation, runtime and teardown
  - Future - TEE-IO updates for TVM direct-IO

TEE Security Manager (TSM) updates

- COVH, COVG, COVI
- Coordinate with pKVM



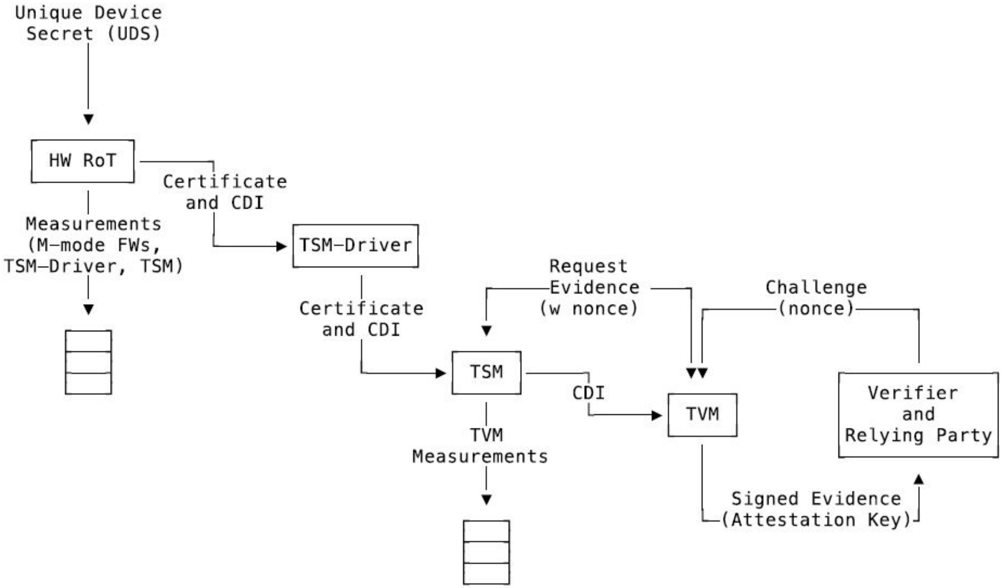
Isolation between supervisor domains and M via *Smmpt, PMP*

Isolation between VM domains and VMM via *Sv G-stage*

Isolation between process domains and OS via *Sv 1st-stage, SPMP*

Attestation

- **RoT (Platform specific)**
  - Security model recommends DICE measurement interfaces for Secure boot, TSM measurement
  - TSM implements COVG TVM measurement and COVG for fetching attestation payload
- **Format of remote attestation payload documented in CoVE spec.**
  - The CoVE Attestation Evidence uses the IETF Entity Attestation Token, formatted as CWT
  - Attestation certificate can be either CBOR-formatted or X.509.



PoCs & open tasks

Updates to Qemu, kvm-unit-tests, OpenSBI (link)

Start effort on Spike, SAIL, ACT

2 RVI/RISE Workstreams - pKVM (Client) and TSM as HS-peer (Data-center) for CoVE & CoVE-IO

OpenSBI changes for MPT mgmt, Context switching (message format for MPXY), KVM tests

Linux TEE-IO interfaces

TSM dynamic updates.