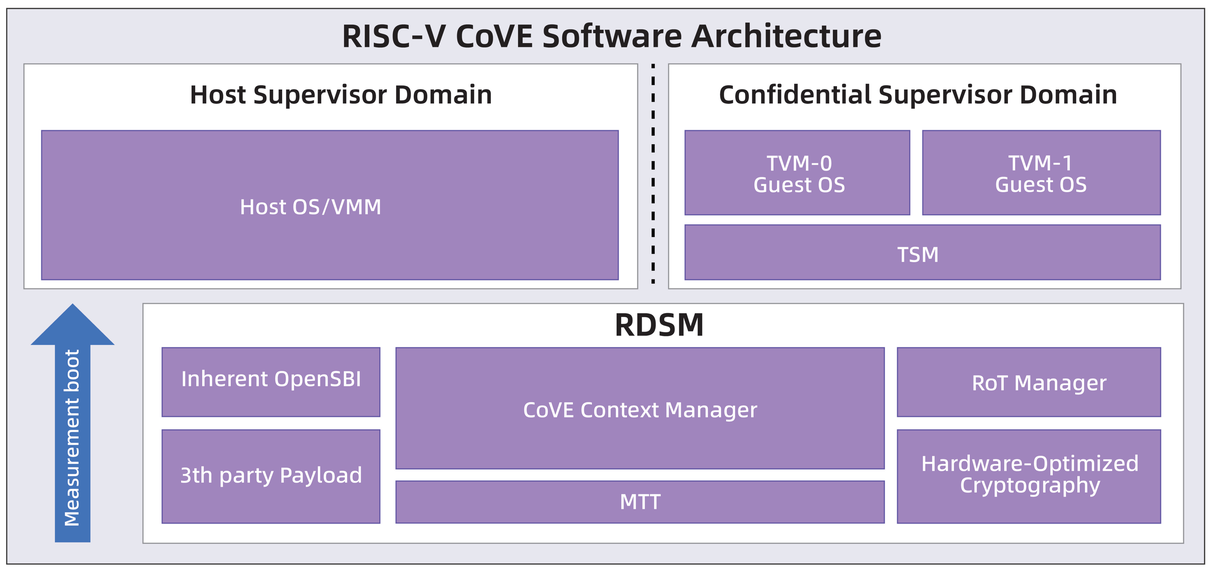
XUANTIE

RISC-V CoVE Implementation In Privileged Firmware

Author: Vincent Cui, Alibaba Damo Academy
Email: cxx194832@alibaba-inc.com

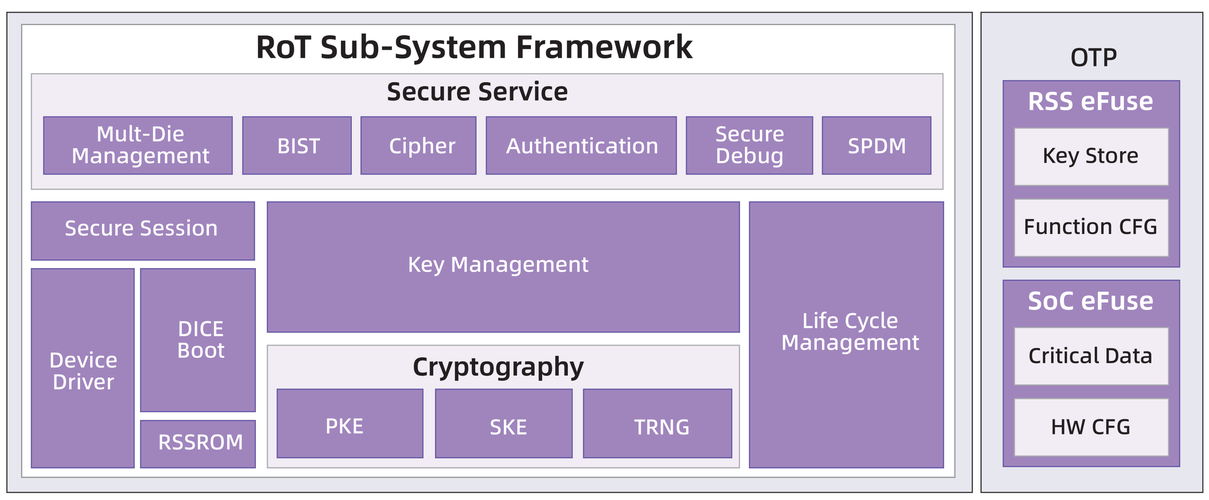
Introduction

In the confidential computing CoVE solution, RISC-V provides a classic type of privileged firmware running in machine privilege mode, as referred to RDSM (RoT domain Security Manager). This poster introduces a new suite of components designed to meet critical security requirements defined in RISC-V Server SoC specification v1.0. All new components introduced to RDSM conform to NIST SP 800-193 and ISO/IEC 20831 standards, ensuring compliance with global confidential computing requirements.



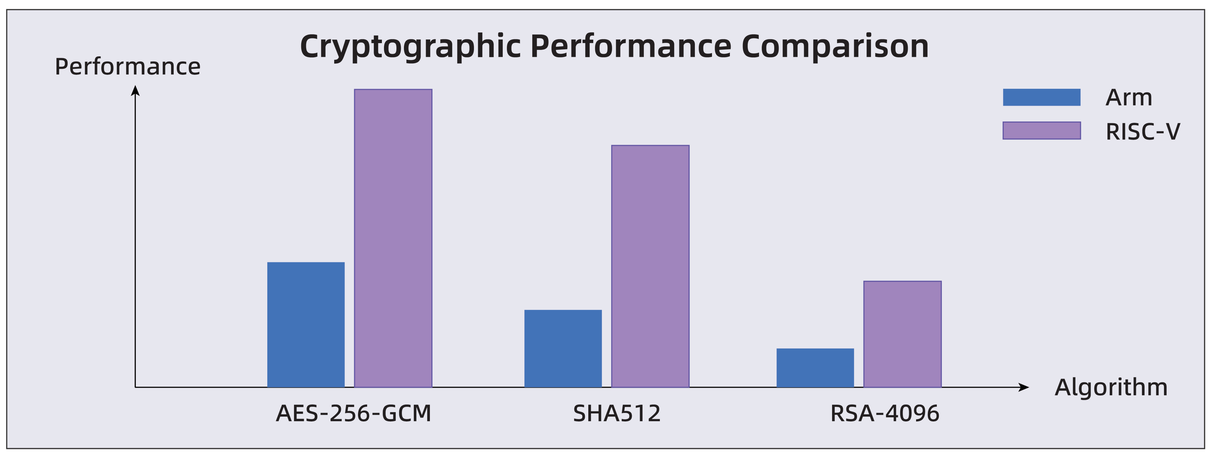
Root of Trust (RoT)

In confidential computing systems, the RoT underpins every secure operation. A hardware RoT is an isolated, deticated trusted subsystem that can provide stronger protection against both physical and logic attacks. The RoT manager is responsible for calling secure service in RoT subsystem and offering cryptographic keys and CoVE measurement in tamper-resistant memory, and validating firmware integrity via hardware-based attestation.



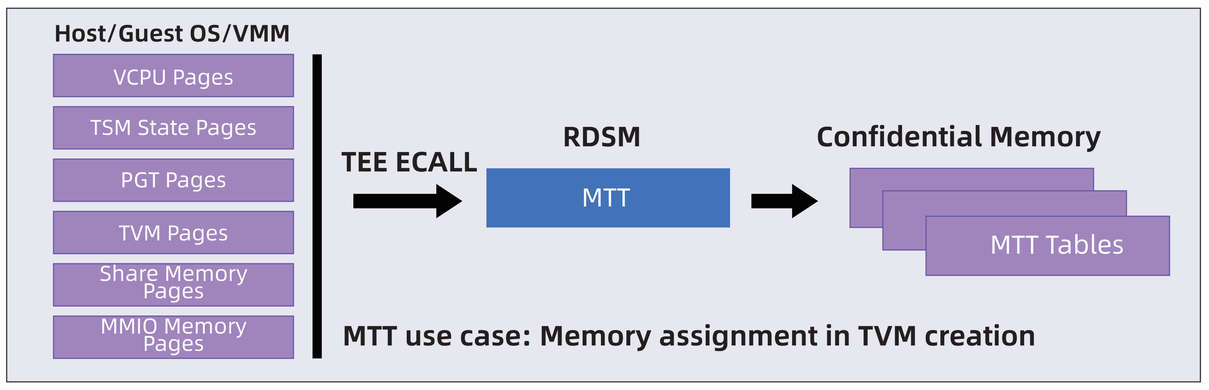
Hardware-optimized Cryptography

The new cryptographic library is a hardware-optimized cryptography using RISC-V cryptography vector extension to accelerate encryption/decryption workflow. It is used by RDSM to implement CoVE measurement and TSM decryption and authentication during bootstrap.



MTT (Memory Transaction Table)

The Rust-based MTT driver inherits robust memory management and reduces runtime vulnerability. Its primary obligation is to establish MTT table for memory regions allocation from Host/Guest OS to enforce access control polices at runtime.

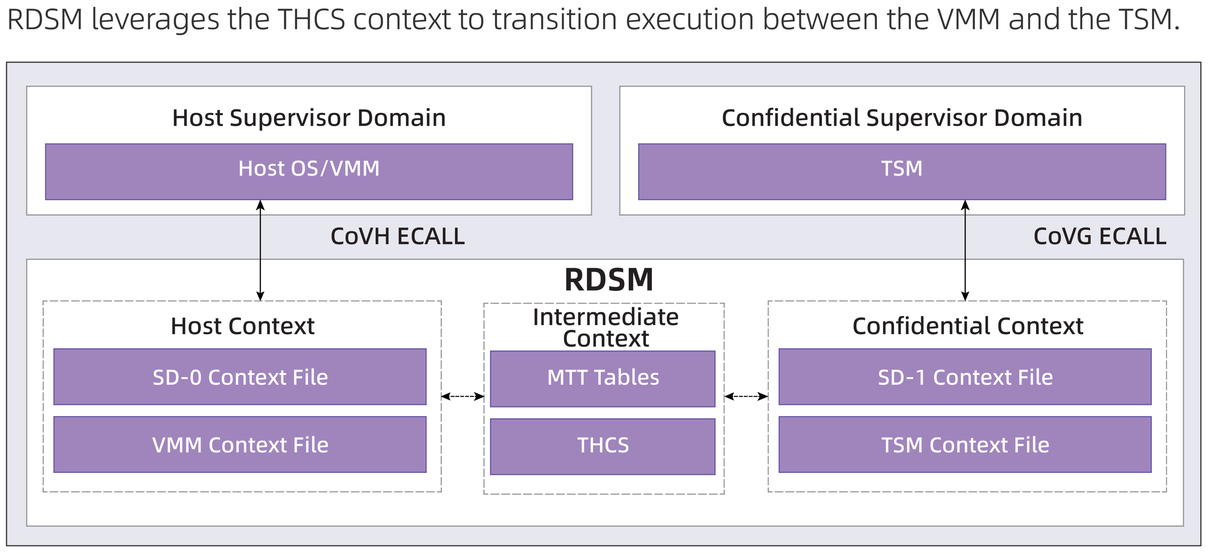


CoVE Context Manager

The CoVE Context Manager handles TEE requests and responses for both the Host OS and the Guest OS. The workflow involves two types of context switches:

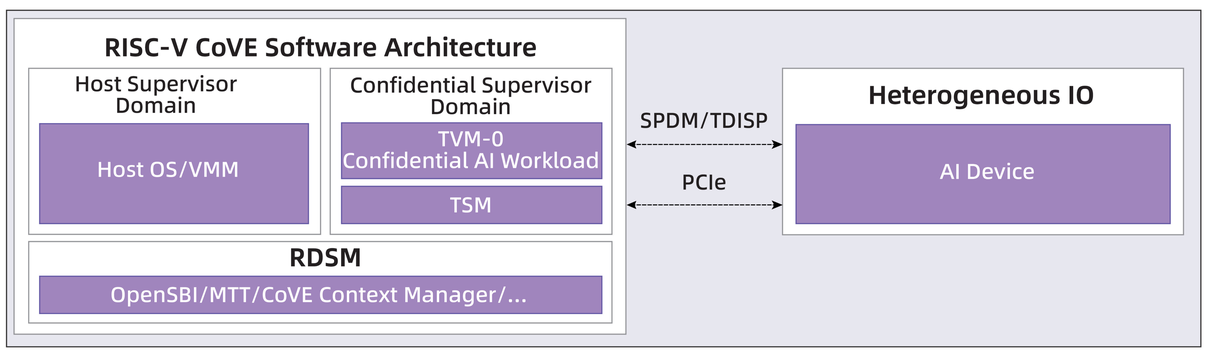
Supervisor Domain (SD) context switch
RDSM uses the MTT engine to load the appropriate MTT table for the target Supervisor Domain.

HS execution context switch
RDSM leverages the THCS context to transition execution between the VMM and the TSM.



CoVE Application Scenarios

RISC-V community currently maintains only a CoVE PoC for deployment model-2(Nested Virtualization Deployment). The new RDSM provides robust support for CoVE deployment model-1, as defined in CoVE specification, enabling volunteers to build CoVE deployment model-1 on the basis of new RDSM. Below diagram displays one application scenarios to support confidential AI business with CoVE support.



TODO List

1. Integrate CoVH, CoVG and CoVI interfaces to be part of SBI 3.0 specification
2. Deep-dive into CoVE IO scheme to summarize new enforcement in privilege firmware
3. Support AIA interrupt policy

For more information，please visit ***xrvm.com***