



Contribution ID: 75

Type: **not specified**

Update on RISC-V Confidential VM Extension (CoVE)

Tuesday, 14 November 2023 17:30 (10 minutes)

This session aims to cover the ongoing development of the RISC-V architecture for Confidential VM Environment (CoVE) using ratified RISC-V privileged ISA extensions and proposed new ISA extensions (SmMTT). This session will describe the ongoing specifications for proposed ABI, ISA and SoC requirements that enable Confidential Computing on RISC-V-based platforms. The common/abstract aspects that are cross-architectural for Linux/KVM will be discussed to enable inter-operability across different RISC-V as well as non-RISC-V platforms. The discussion is to cover RFC patches for ABI in development stage and target for public review by Q4'23.

Primary author: SAHITA, RAVI (Rivos)

Co-author: PATRA, ATISH (Rivos)

Presenters: PATRA, ATISH (Rivos); SAHITA, RAVI (Rivos)

Session Classification: Confidential Computing MC

Track Classification: LPC Microconference: Confidential Computing MC