**# Title**: RISC-V AP-TEE Confidential Computing Extension for UEFI

**# Status**: Submitted to industry standard forum

**# Document**: UEFI Specification

**# License**: SPDX-License-Identifier: CC-BY-4.0

**# Submitter**: Ravi Sahita [ravi@rivosinc.com](mailto:ravi@rivosinc.com) (RISC-V AP-TEE TG Chair), Samuel Ortiz [sameo@rivosinc.com](mailto:sameo@rivosinc.com) (RISC-V AP-TEE-IO TG Chair), Jiewen Yao [jiewen.yao@intel.com](mailto:jiewen.yao@intel.com) (RISC-V AP-TEE-IO TG Vice-Chair)

**# Summary of the change**

**[Background]**

UEFI spec chapter 38 defined confidential computing extension.

Current 38.4 (<https://uefi.org/specs/UEFI/2.10/38_Confidential_Computing.html#vendor-specific-information>) adds vendor extension for CC vendor, such as Intel TDX.

RISC-V AP-TEE has similar requirement and need to define CC event log extension. (<https://github.com/riscv-non-isa/riscv-ap-tee/issues/29>)

RISC-V AP-TEE specification described CC event log in UEFI firmware at <https://github.com/riscv-non-isa/riscv-ap-tee/blob/main/specification/attestation.adoc>.

**[Proposal]**

This proposal adds RISC-V AP-TEE extension for CC event log.

Reference:

1. UEFI Specification 2.10 - [www.uefi.org](http://www.uefi.org)
2. RISC-V AP-TEE Specification - <https://github.com/riscv-non-isa/riscv-ap-tee>

**# Benefits of the change**

The OS kernel can get standardized RISC-V AP-TEE CC event log.

**# Impact of the change**

No compatibility impacts. It is a RISC-V AP-TEE specific feature.

# Detailed description of the change [normative updates]

### 38.4.2. RISC-V AP-TEE

The following table shows the TPM PCR index mapping and CC event log measurement register index interpretation for RISC-V AP-TEE.

*Table 38.2****Mapping for RISC-V AP-TEE***

|  |  |  |
| --- | --- | --- |
| **TPM PCR Index** | **CC Event Log Measurement Register Index** | **RISC-V AP-TEE Measurement Register** |
| [0~16,23] | [0~16,23] | Runtime Measurement [0~16,23] |

**Related Definitions**

*#define EFI\_CC\_TYPE\_RISCV\_APTEE 3*

**# Special Instructions**

NO