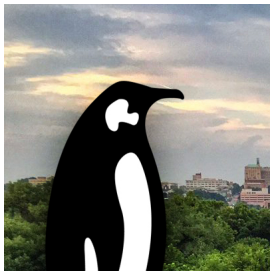

Contribution ID: **319** Type: **not specified**

# Towards unified confidential computing ABIs

*Tuesday, 14 November 2023 17:15 (15 minutes)*

The configfs-tsm proposal arose from the observation that there are several platform vendors all building similar confidential-computing functionality features into their products. It makes the assertion that the kernel has a role to play and a vested interest in aligning stakeholders behind common ABI. Going forward attestation reports are just one example of shared interfaces that the community can build to lower, or better distribute, the long term maintenance burden of confidential computing for the kernel. Another example area of collaboration is userspace ABIs for QEMU to use for managing secure device assignment to confidential VMs. Lets have an open discussion on assertions made in the configfs-tsm proposal and the future implications.

**Primary author:** WILLIAMS, Dan (Intel Open Source Technology Center)

**Presenter:** WILLIAMS, Dan (Intel Open Source Technology Center)

**Session Classification:** Confidential Computing MC

**Track Classification:** LPC Microconference: Confidential Computing MC