Contribution ID: **388** Type: **not specified**

PCI device authentication & encryption

This presentation is to revive last year's discussion on PCIe device attestation. The first thing to understand is if last year's consensus to use netlink sockets to convey device attestation information to user space still holds. The second thing to review is the device attestation workflow itself. Given the difference between the CMA and PCI/TSM scenarios, it may be better to build an attestation workflow that fits PCI/TSM and see what can be reused for CMA rather than last year's direction to finish CMA before extending to PCI/TSM.

Primary authors: KARDASHEVSKIY, Alexey (AMD); POIRIER, Mathieu (Linaro)

Presenters: KARDASHEVSKIY, Alexey (AMD); POIRIER, Mathieu (Linaro)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC