Contribution ID: **294** Type: **not specified**

Toward a standard device attestation token for device assignment

Friday 12 December 2025 10:30 (30 minutes)

The open-source community is hard at work on building the framework and mechanisms allowing the assignment of devices to a trusted virtual machine (TVM), a process commonly known as device assignment (DA). For the TVM to trust a device, the device must provide the TVM with Evidence claims \[RFC9334\] confirming its identity, the state of its firmware and its configuration. Since Evidence claims can be consumed by 3rd party attestation services external to the TVM, there is a need to standardise the representation of Evidence to ensure interoperability.

This session is about introducing the current proposal and an open discussion with the audience on what needs to be modified, the pieces that may be missing and the way forward for this specification.

Primary authors: POIRIER, Mathieu (Linaro); FOSSATI, Thomas (Linaro)

Presenters: POIRIER, Mathieu (Linaro); FOSSATI, Thomas (Linaro)

Session Classification: Confidential Computing MC

Track Classification: Confidential Computing MC