Contribution ID: **102** Type: **not specified**

Kernel TEE subsystem BoF

A Trusted Execution Environment (TEE) is an isolated execution environment running alongside the rich operating system. It provides the capability to isolate security-critical or trusted code and corresponding resources like memory, devices, etc. The isolation is backed by hardware security features such as Arm TrustZone, AMD Secure Processor, RISC-V TEE, etc.

This BoF will provide a platform to discuss topics related to the ongoing evolution of the kernel TEE subsystem with support for new drivers coming up like Trusted Services TEE, Qualcomm TEE, or any other future TEE drivers. Along with that, we will see how the recently merged RPMB subsystem in the kernel helped the easier enablement of OP-TEE based fTPM in-kernel use cases. The next big feature up for discussion is protected DMA-Bufs managed by a TEE looking for real-world upstream user-space use cases like DRM protected media pipelines, TEE protected crypto accelerator keys, secure user interfaces, etc.

Primary author: GARG, Sumit

Co-author: WIKLANDER, Jens

Presenters: WIKLANDER, Jens; GARG, Sumit

Session Classification: Birds of a Feather (BoF)

Track Classification: Birds of a Feather (BoF)