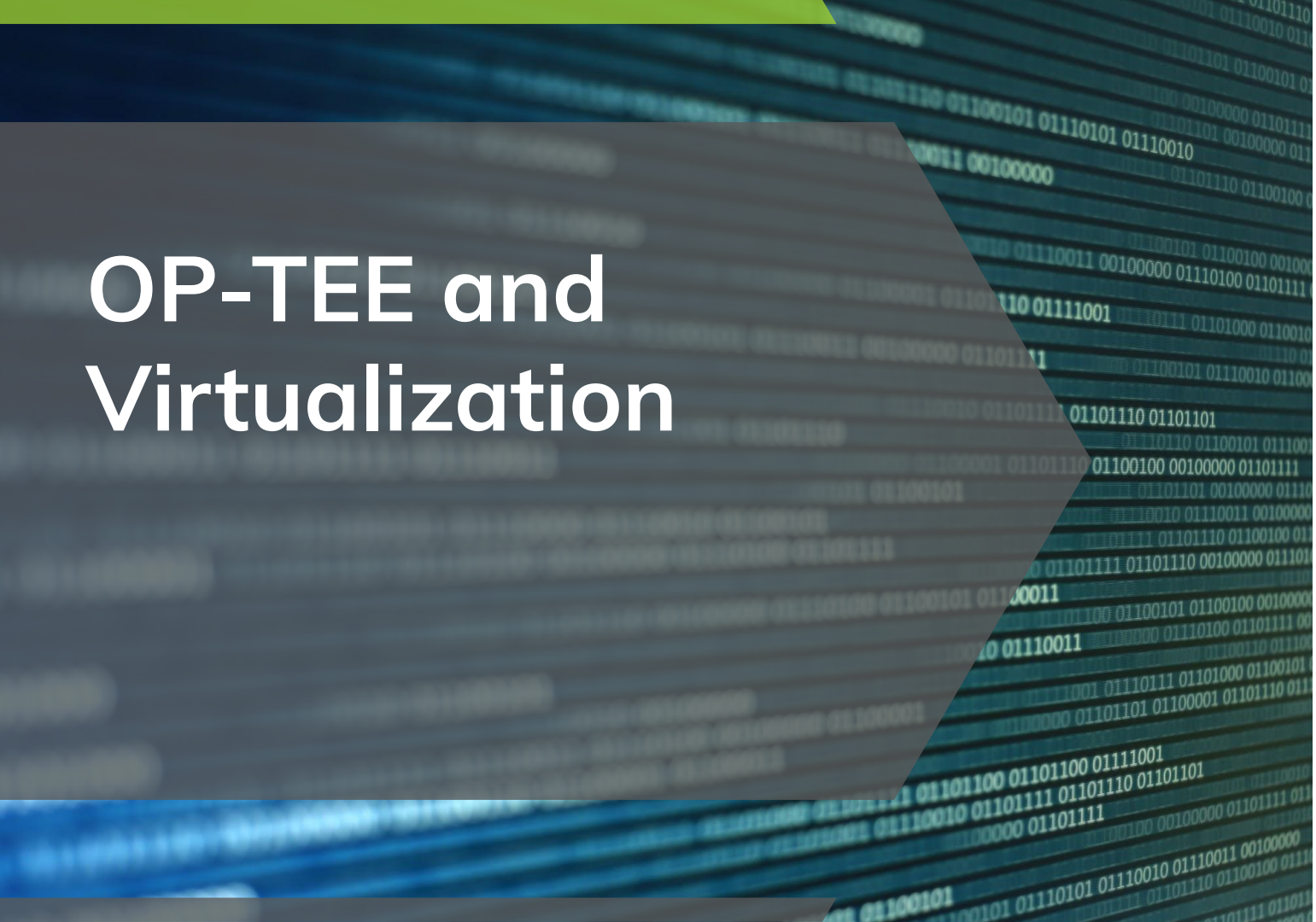
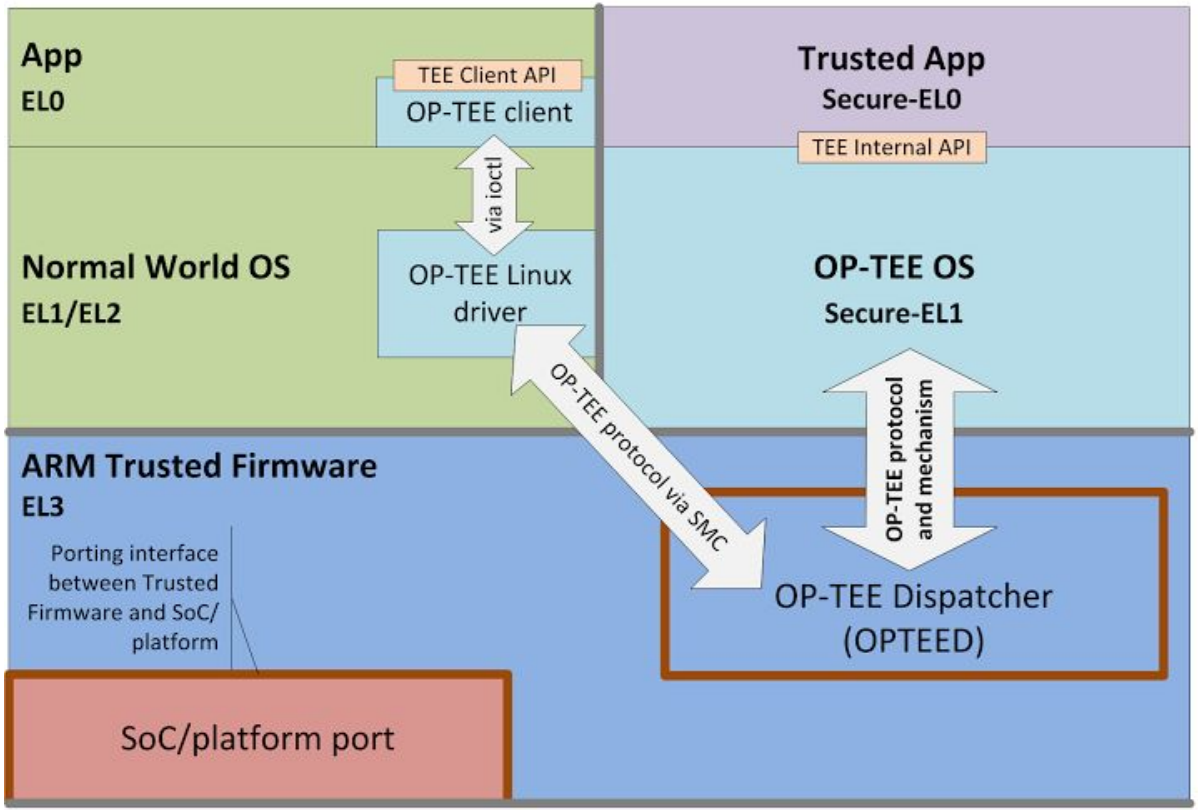
OP-TEE and Virtualization



Linaro

ARM Trusted Firmware and OP-TEE



ARM Trusted Firmware
github.com/OP-TEE
SoC supplier
OS/hypervisor supplier
Trusted App supplier
Global Platforms spec.
Internal OP-TEE interface

SMC Calls to EL3 are specified by the SMC Calling Convention PDD (ARM DEN 0028A)

OP-TEE is an open source Trusted OS implementing the Global Platform TEE specifications

AVPS (Automotive Virtual Platform Specification) v1.01 on TEE

- Access to TrustZone and equivalent Trusted Execution Environments (TEE) should not require modification of the software. This is a feature that is frequently requested from the guest and when legacy systems are ported from native hardware to a virtual platform, there should be minimal impact on the software. Accessing the trusted execution environment should work in the exact same way as for a native system.

- The rationale for this is that implementations that have been carefully crafted for security (e.g. Multimedia DRM) are unlikely to be rewritten only to support virtualization

TEE and Virtualization

For Cortex A pre v8.4 without Secure EL2

- One Secure OS and multiple Secure Apps
  - Secure Apps accessed by multiple guests
  - 1:1 mapping of some Secure Apps with Guest/VM

For Cortex A post v8.4 with Secure EL2 and secure hypervisor

- Multiple Secure partitions and Secure Hypervisor with a per guest/VM secure partition
  - 1:1 mapping between secure partition and guest/VM

What exists today ?

- Since a while ago there has been experimental support to run virtualization in OP-TEE - Added by Volodymyr Babchuk, Senior Embedded Engineer at EPAM Systems

- Ongoing work in OP-TEE with adding support for secure EL-2 that is coming in newer Armv8-A versions - usage of FFA and secure world hypervisor Hafnium.

Experimental support in XEN and OP-TEE - What is available ?

- One OP-TEE instance can run TAs from multiple virtual machines. OP-TEE isolates all VM-related states, so one VM can't affect another in any way.
- With virtualization support enabled, OP-TEE will rely on a hypervisor, because only the hypervisor knows which VM is calling OP-TEE.
- Hypervisor enables two-stage MMU translation, so VMs does not see real physical address of memory, instead they work with intermediate physical addresses (IPAs). On other hand OP-TEE can't translate IPA to PA, so this is a hypervisor's responsibility to do this kind of translation. So, hypervisor should include a component that knows about OP-TEE protocol internals and can do this translation. We call this component "TEE mediator" and right now only XEN hypervisor have OP-TEE mediator.

Proposed work

- Evaluate and run the existing XEN mediator and OP-TEE with AGL/Linux with xtest.
  - Platform to be used - QEMU ARMv8
- Improvements/Architectural changes if required in existing mediator on XEN
  - Mature the experimental support
  - Add missing features
- Addition of similar support in other hypervisors -> KVM ??
- Shift to usage of FFA in the Mediator for easy migration to architecture post v8.4 where we can have multiple secure partitions in secure world.
- Sharing of hardware resources
  - Integration of tee-supplicant with virtio-rpmb.
  - Virtio-crypto ??
- Running OEM Crypto library (Widevine DRM) from multiple VM's

Thank you