
# OP-TEE

# Open Portable Trusted Execution Environment

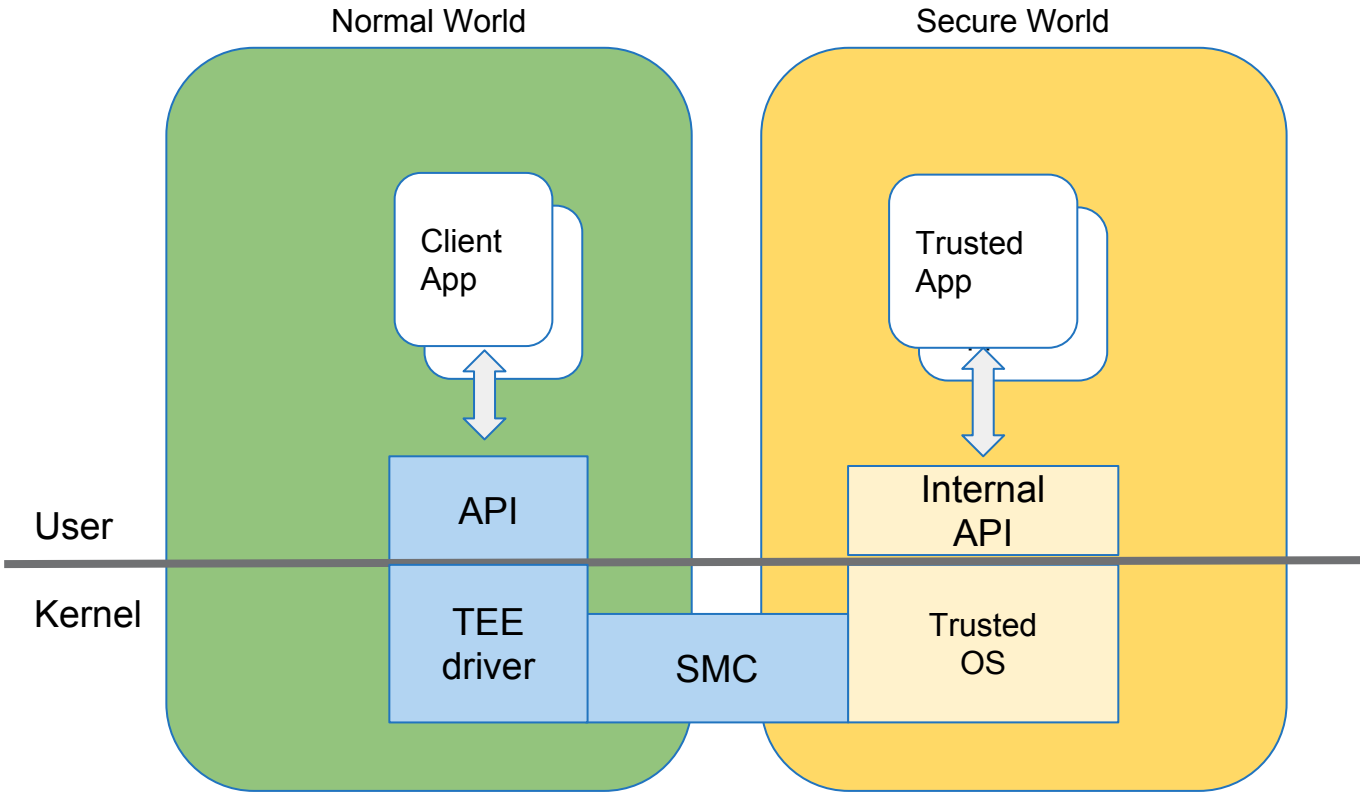
Jens Wiklander

# Why an Open Source TEE?

- Provides a shared basis for product TEE developments
  - Collaboration and consolidation not re-invention/fragmentation
  - OP-TEE has BSD 2-clause license (GPLv2 for Linux driver, test suite)
- Provides a full example for research and education
  - Historically hard to learn about Trusted Environments
- Can be included in reference platform deliveries
- More eyes on security-critical code

# High level architecture

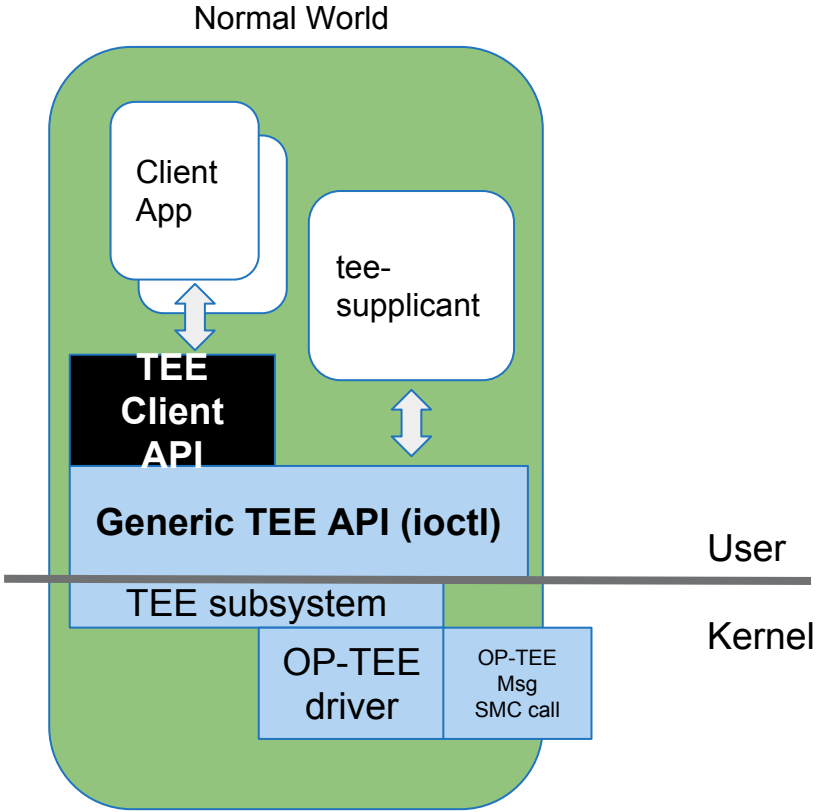
Both OP-TEE and Trusty share the same high level architecture



# Linux Kernel Subsystem (from OP-TEE point of view)

- TEE subsystem:
  - Manages Shared Memory
  - Provides generic API as ioctl
- tee-supplicant:
  - Helper process for OP-TEE
- OP-TEE driver:
  - Forwards command from the Clients to OP-TEE
  - Manages RPC requests from OP-TEE to the supplicant

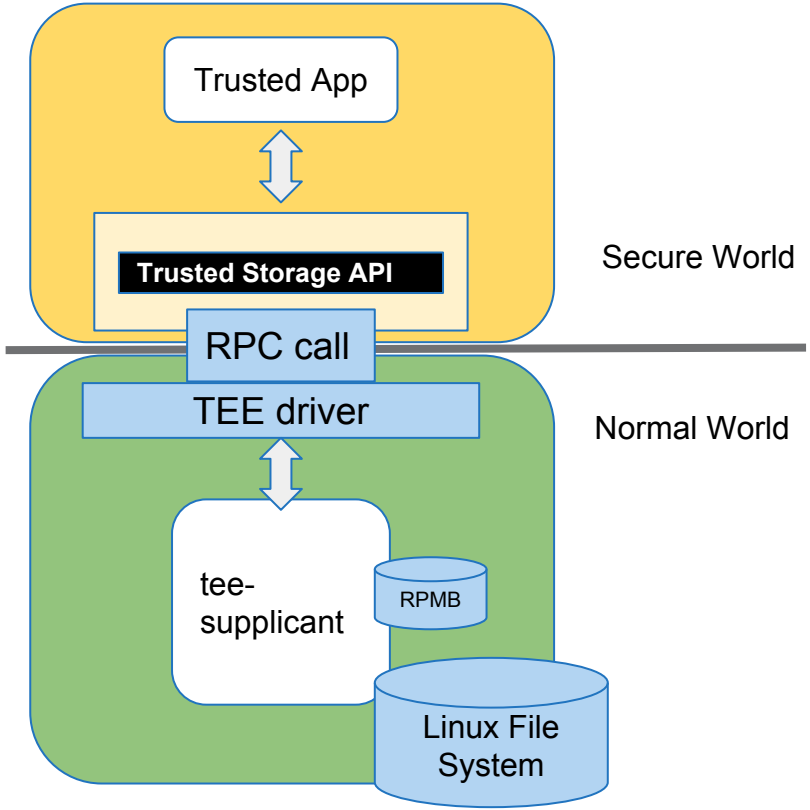
The Trusty driver is based on virtio instead



# Trusted Storage

[Note: secure world at top in picture]

- Implements GlobalPlatform Trusted Storage PersistentObject functions
- TEE File System encrypts data:
  - Secure Storage Key (per device)
  - File Encryption Key (per file)
- Data stored in Linux File System
  - Managed by tee_supplicant



# Communication & Scheduling

- Entry into secure world from SMC (or FIQ arriving), the work is done during the SMC
- Command arriving → Allocated to thread (if available), TA context set up and called
  - If normal world access is needed, the thread is suspended and an RPC is performed, for example
    - File system access
    - Sleep
    - Wait for event
    - IRQ delivery
- Return to normal world on task completion, RPC (or IRQ arriving).

In contrast with Trusty which has an integrated scheduler OP-TEE is scheduled by normal world. An OP-TEE task can be rescheduled only when CPU is normal world, which happens often, for instance when delivering a non-secure interrupt that was received while in secure world.

# Shared memory

- Shared memory between Linux user space and TEE is a must for bandwidth intensive applications
- Currently shared memory used by OP-TEE is allocated from a reserved region of physically contiguous memory
- Shared memory between secure and nonsecure world has to have compatible cache settings in both worlds
    - On ARM systems that's: Normal cached memory (write-back), shareable for SMP systems and not shareable for UP systems

# Adding a new TEE driver

- The interface to secure world defines what the driver needs to handle, for instance
  - RPC: is a new supplicant needed?
  - Shared memory: is the current model enough or does it need to be extended?
  - What happens when an IRQ is received while in secure mode?

# Selection of officially supported targets

- ARMv7-A
  - Allwinner A80
  - Freescale FSL i.MX6 UltraLite EVK Board
  - Freescale FSL ls1021a
  - QEMU
  - ST's Cannes board (b2120 / b2020)
  - Texas Instruments DRA746
- ARMv8-A
  - 96Boards HiKey (HiSilicon Kirin 620)
  - ARM Juno board
  - ARM FVP, Foundation and Base Models
  - MediaTek MT8173 EVB Board
  - QEMU
  - Xilinx Zynq UltraScale+ MPSOC

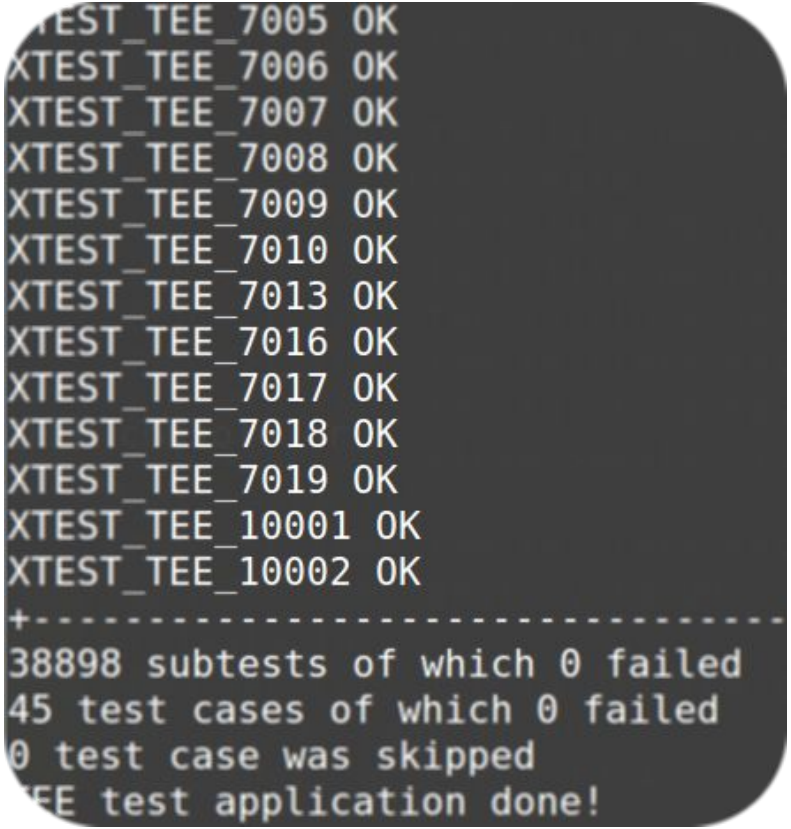
Complete list at https://github.com/OP-TEE/optee_os/#3-platforms-supported

# xtest

This is the main test suite for OP-TEE

Possible to extend the test suite to also make use of the GP TEE Compliance test suite

Uses TA-dev-kit from optee_os and TEE client API from optee_client




# Thank You

For further information:

www.linaro.org

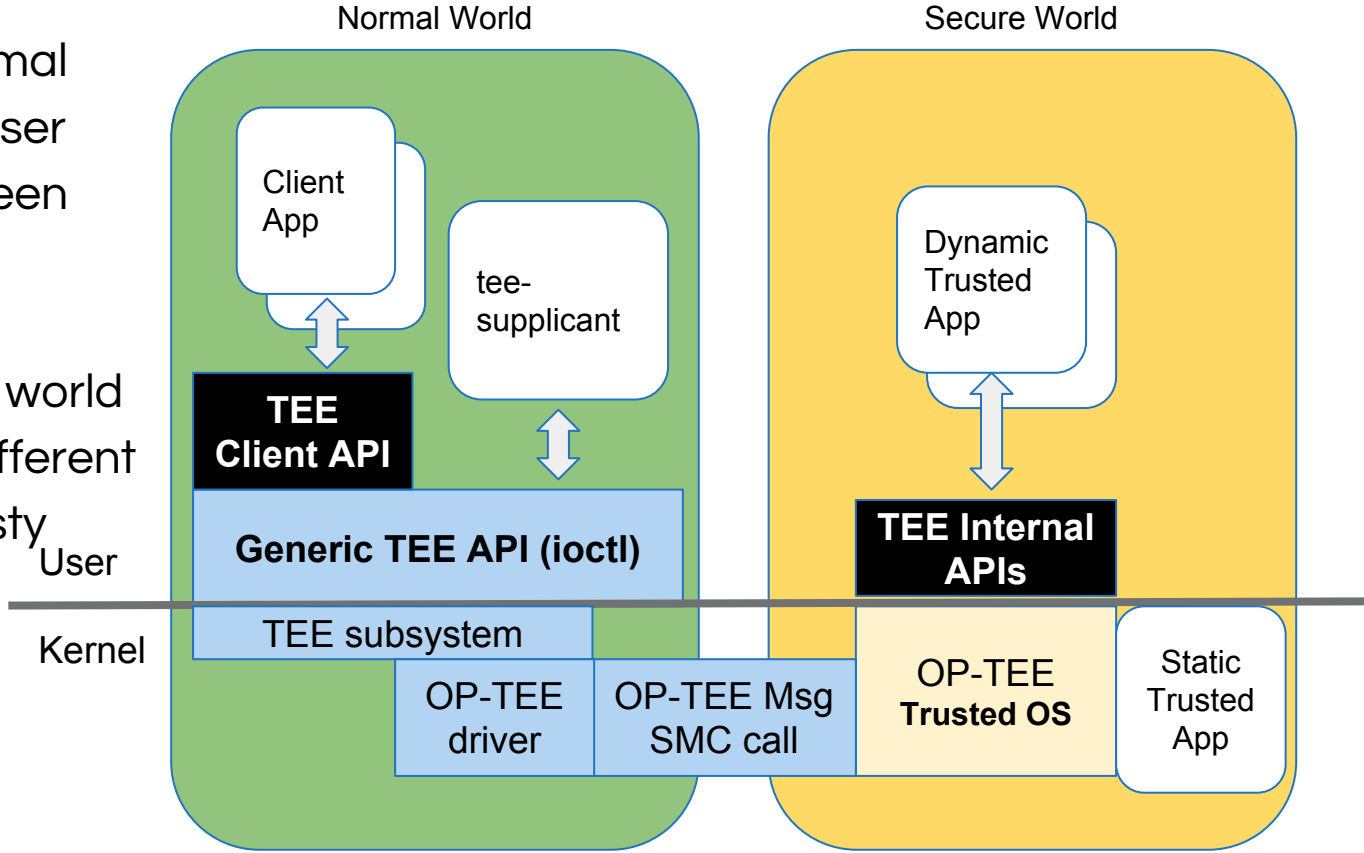
www.op-tee.org

OP-TEE

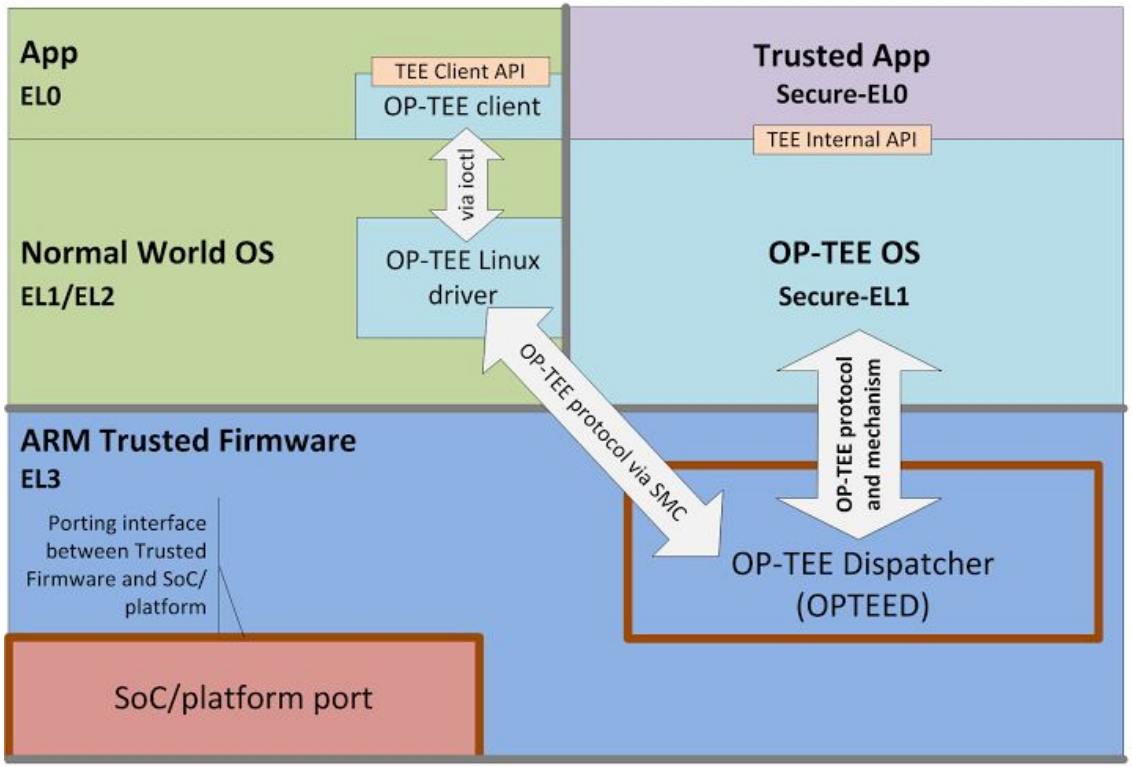
.org

# OP-TEE architecture

- All APIs both in normal and secure world user space differs between OP-TEE and Trusty
- Interface between secure and normal world is fundamentally different in OP-TEE and Trusty



# 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



Linaro

OP-TEE .org