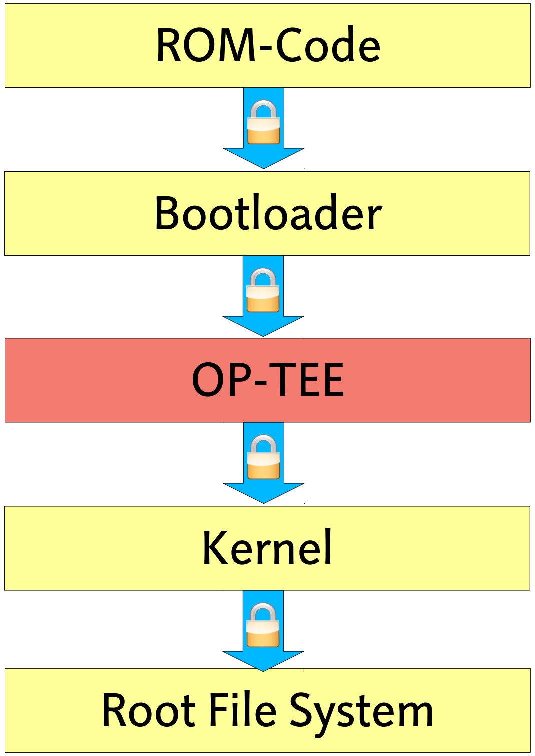
OP-TEE
Using TrustZone to Protect Our Own Secrets



ELC Europe 2017, 23.10.2017

Marc Kleine-Budde <mkl@pengutronix.de>

Overview

- ARM architecture overview
- ARM TrustZone
- Trusted Execution Environment
- Open Portable Trusted Execution Environment

What is a TEE?

- **T**rusted **E**xecution **E**nvironment
  - small OS-like environment
  - isolated from normal operating system (e.g. Linux) “rich OS”

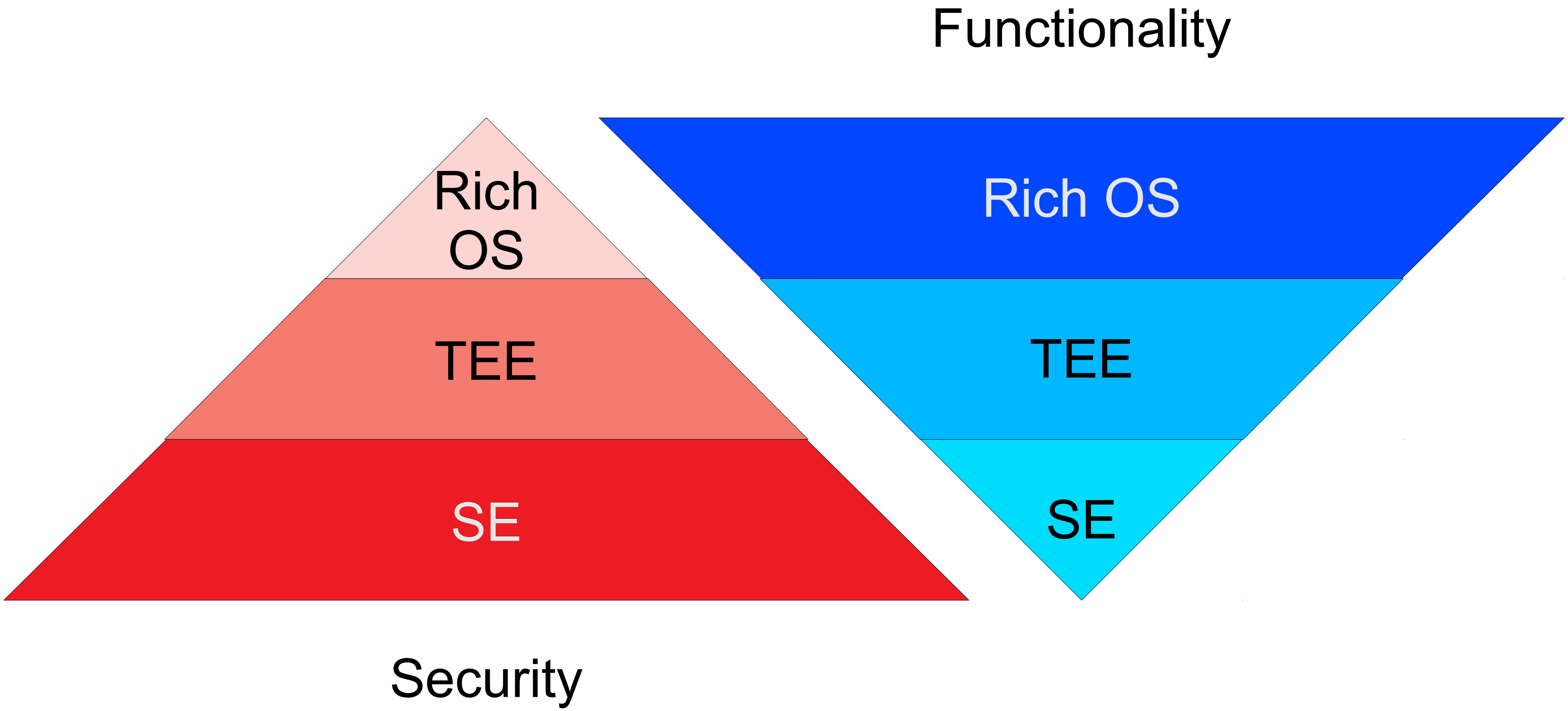
- Allows Applications to execute, process, protect and store sensitive data

- Rich OS is often target of malware and attackers

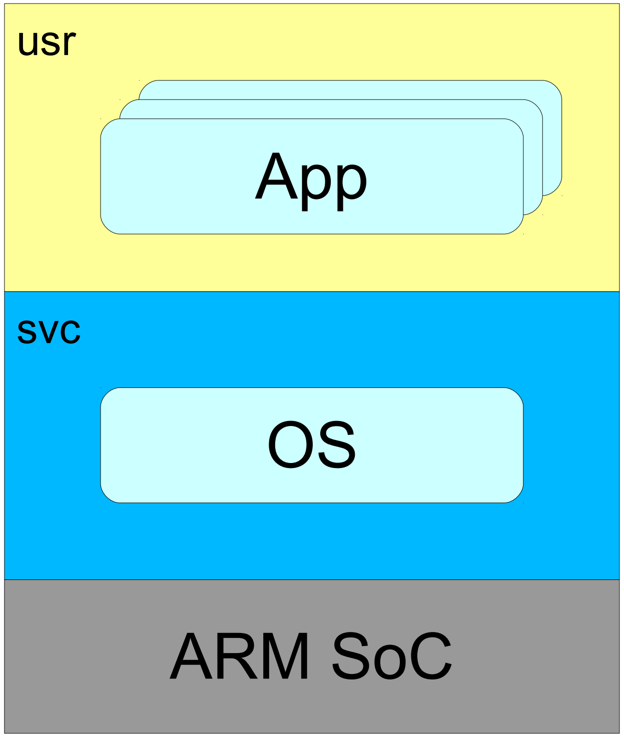
- Design applications so that sensitive functions can be offloaded to the TEE as Trusted Applications.

- API standardized by GlobalPlatform
  - TEE internal APIs for Trusted Application
  - communication interfaces between rich OS Applications and Trusted Applications

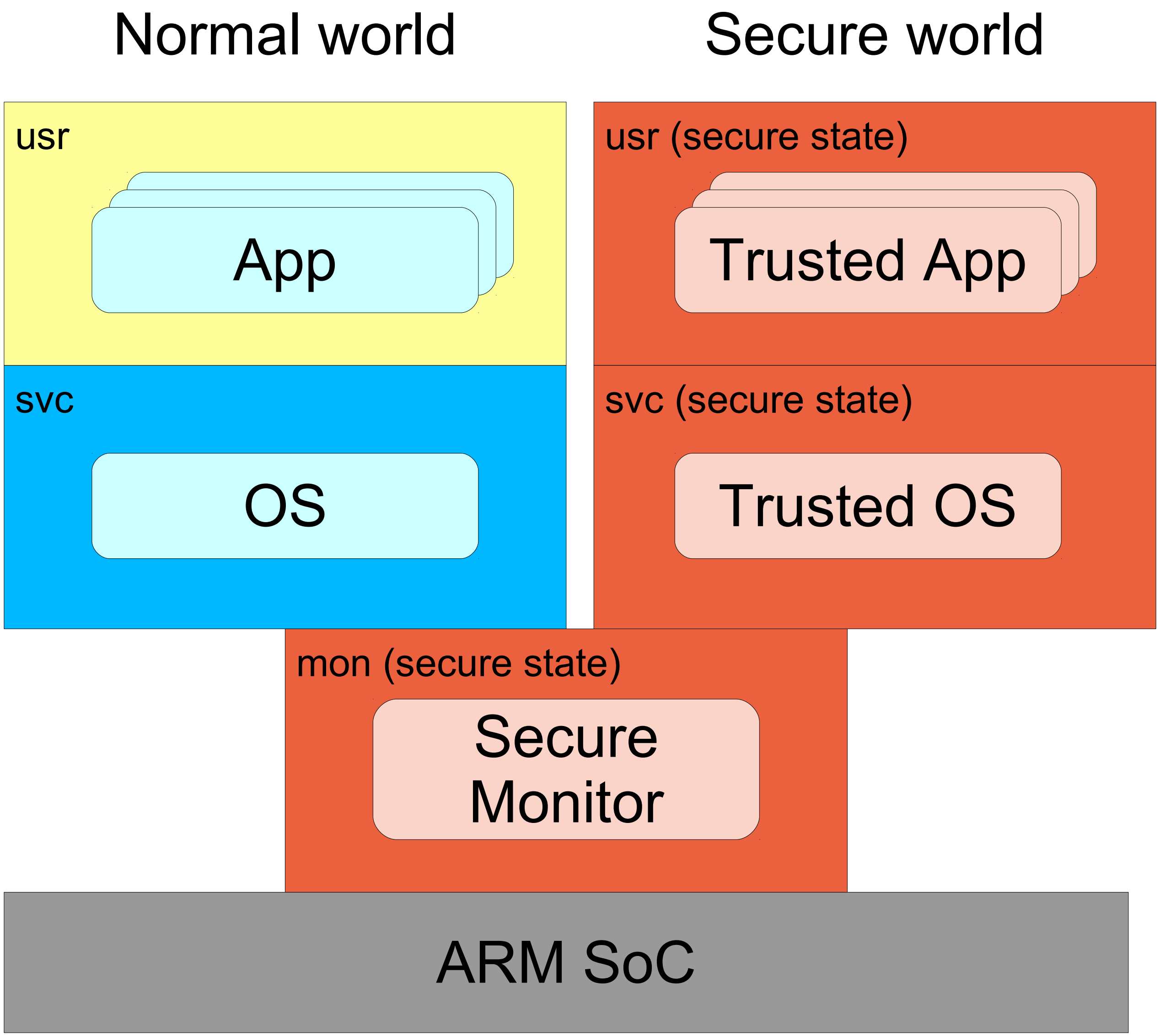
What is a TEE? (cont'd)



ARM architecture



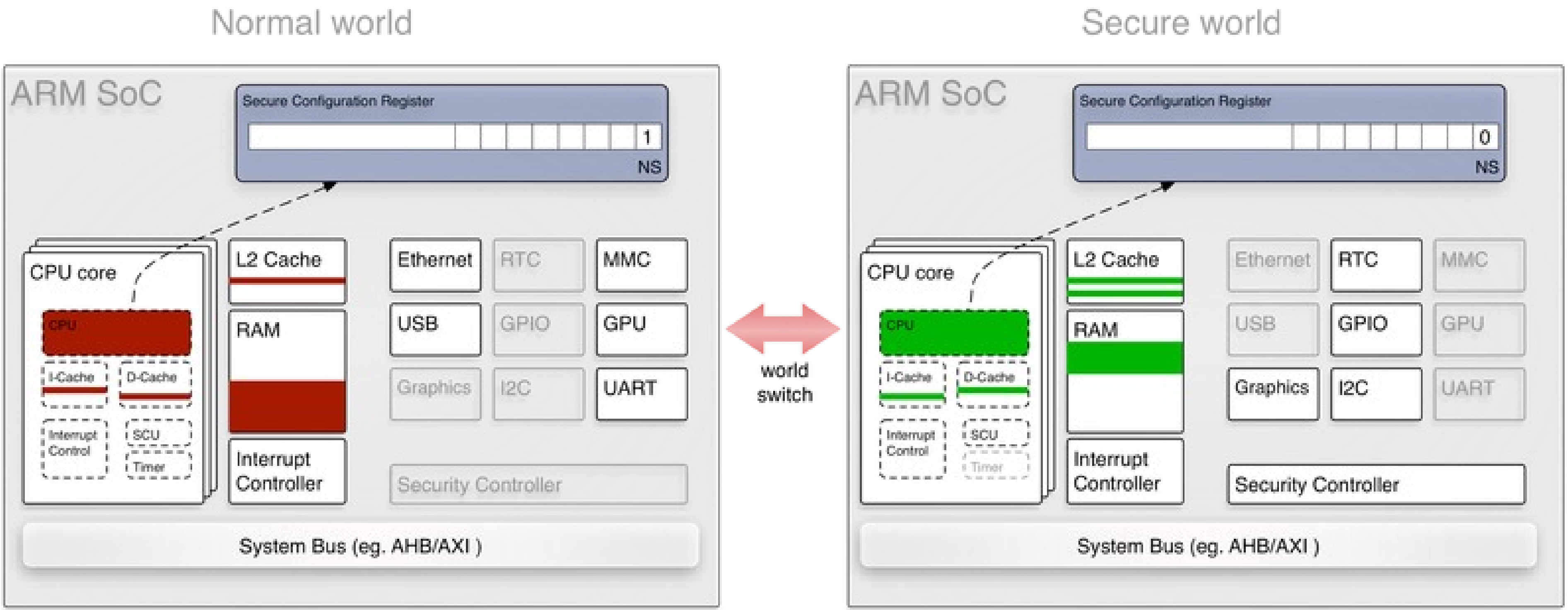
ARM architecture with TrustZone



ARM architecture with TrustZone (cont'd)

- Provides a complete “virtual system” for secure computing
- Divide hardware and software into separate partitions (“worlds”)
  - one is trusted (“secure world”)
  - the other not (“Normal world”)
- Limited and tightly defined ways to get from one world to the other
  → secure monitor

ARM TrustZone in detail



Source: http://genode.org/documentation/articles/trustzone

ARM TrustZone in detail (cont'd)

- Security Extensions to ARM processors

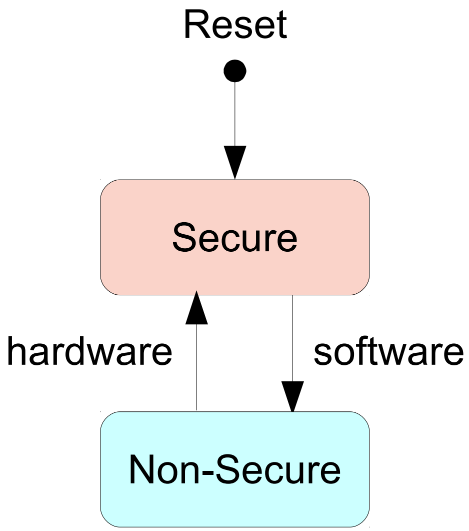
- Supported by
  - ARM1176
  - Cortex-A series (ARMv7-A, ARMv8-A)
  - ARMv8-M

- System-wide hardware isolation
  - SRAM
  - DRAM
  - CPU configuration registers
  - peripherals

- SoC design has impact on practical usefulness of security features

ARM TrustZone switching worlds

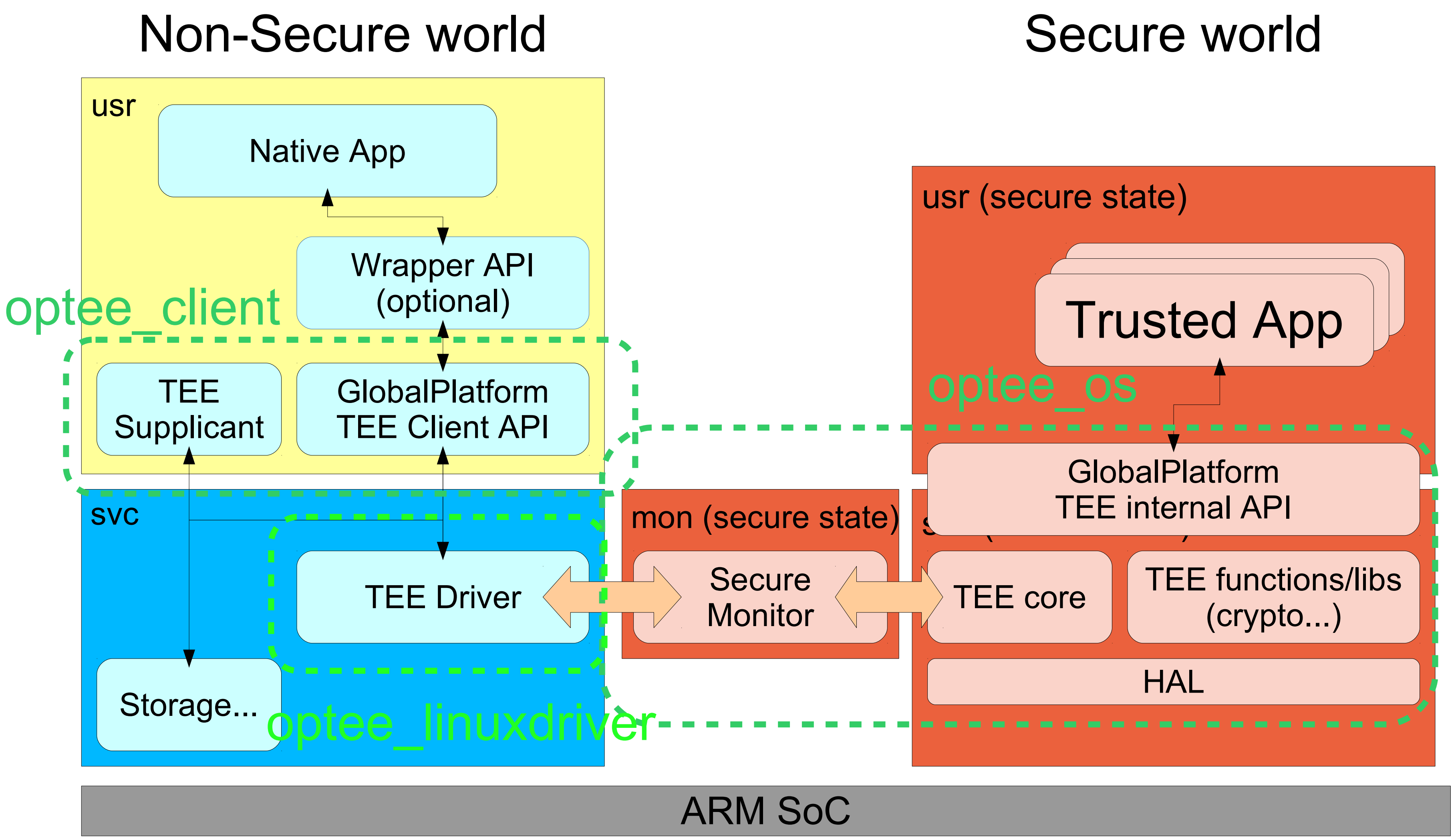
- Secure World entry
  - Hardware-controlled
    - automatic
    - partly configurable
  - By exception
    - Reset
      - CPU always starts secure
    - Secure Monitor Call
      - SMC #n instruction
      - analogous to Supervisor Call (SVC)
      - always handled in Secure World
    - IRQ, FIQ, Data abort
      - configurable (by secure software)
- Non-Secure World entry
  - Software-controlled
  - Typically
    - set SCR.NS
    - return from execption



What is OP-TEE?

- Started as closed source implementation by some mobile, telco and chip vendors
- Since 2015 Open Source (BSD license), owned and maintained by Linaro
- In 2017 the TEE driver went mainline with v4.12
- Small and simple TEE
- Relies on rich OS to schedule TEE
- Based on ARM TrustZone to provide isolation of the TEE from the rich OS in hardware
- Runs on ~20 platforms
  - 32 bit: ARMv7-A
  - 64 bit: ARMv8-A

OP-TEE architecture



Source: https://www.linaro.org/blog/core-dump/op-tee-open-source-security-mass-market/

Pengutronix.

OP-TEE in detail

- The OP-TEE consists of three parts

- Normal World, User Mode
  - TEE client library
  - tee-supplicant
    - file system access
    - access to shared resources

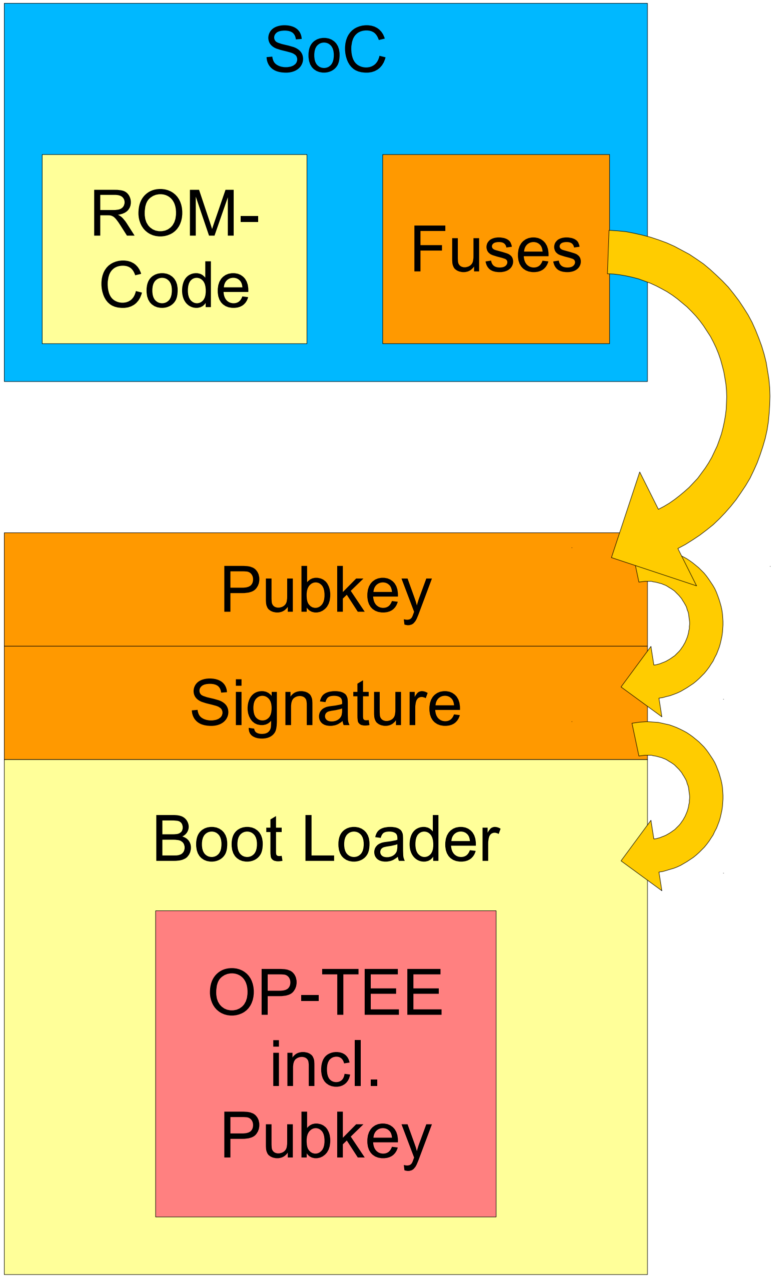
- Normal World, Priviledged Mode
  - Linux kernel TEE subsystem
  - Linux kernel TEE device driver

- Secure world, Priviledged Mode
  - Trusted OS (optee_os)

- TEE contains public key

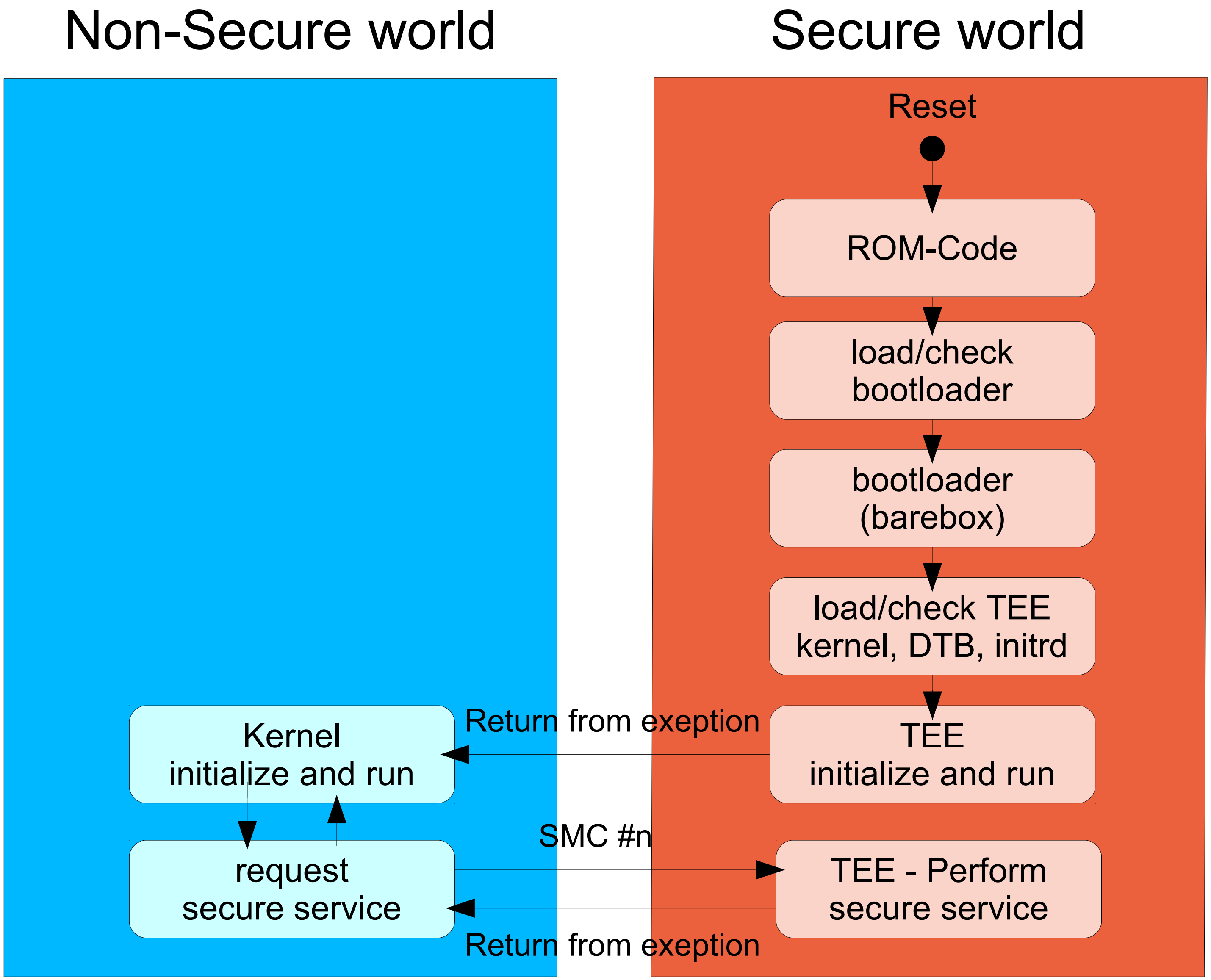
- Trusted Applications are singed and can be loaded from the Normal World into the TEE

OP-TEE - Trusted Boot ARMv7-A: i.MX6



For details on trusted boot see my talk from ELCE 2016.

OP-TEE - Boot sequence in ARMv7-A: i.MX6



Observations & What's Missing?

- Better SoC support
  - more SRAM
  - TrustZone support missing in some peripherals

- TrustZone: From my (limited) point of view:
  - The concept of moving peripherals into Secure World is “complicated” on todays SoCs.
  - Think about turning off the clock of the Secure World's I2C, PWM or Ethernet Controller.

- Support for existing private key storages
  - inside the Linux kernel
  - opengpg/ssh
  - TPM

- build system feels Android centric
- make use more use of DT
- convert config #ifdef to kconfig

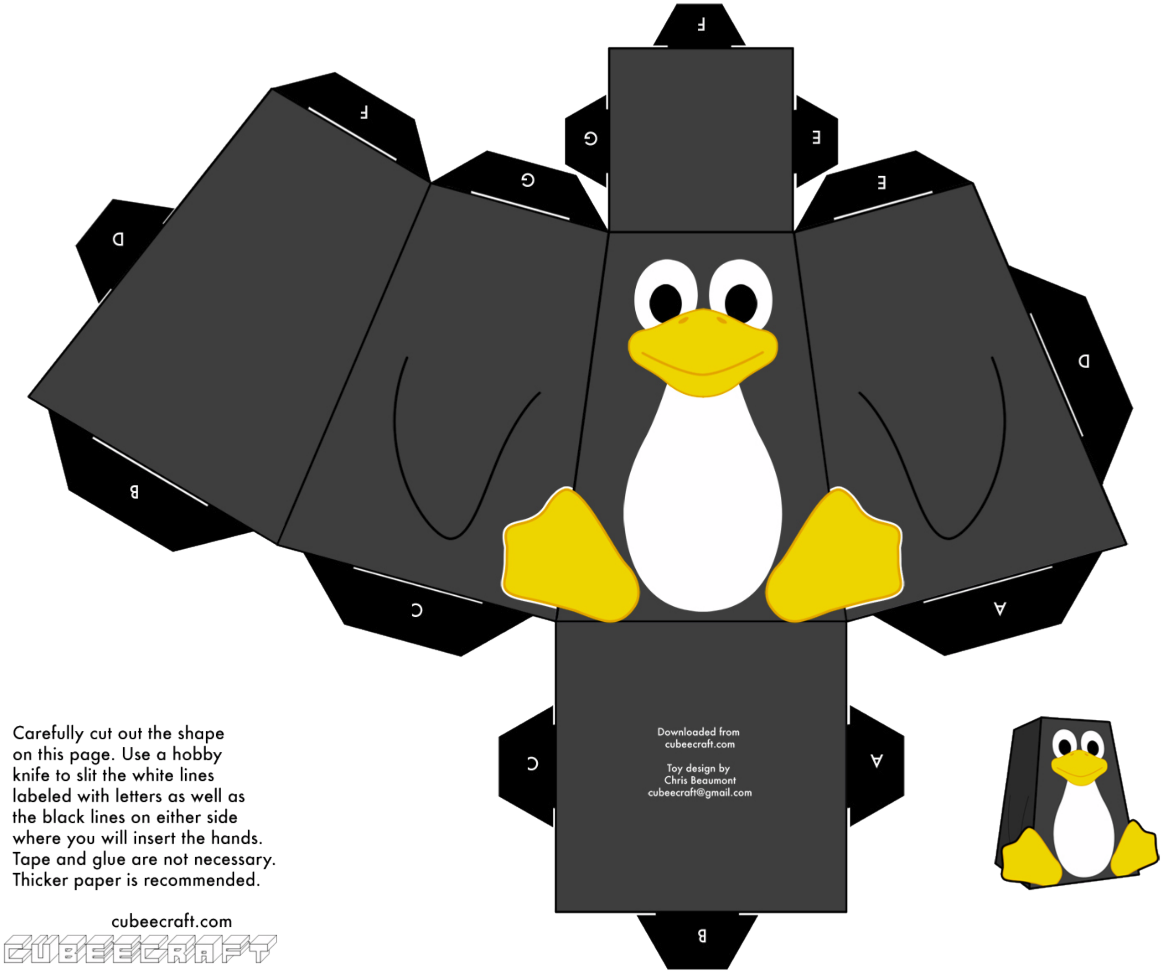
Summary

- TEE – Trusted Execution Environment
  - Set of APIs to split applications into normal and secure part

- TrustZone
  - Security extension for ARM processors to partition one SoC into Normal and Secure World
  - Practical usefulness depends on SoC design

- OP-TEE – Open Platform TEE
  - Implements TEE on ARM using TrustZone

Q & A



Downloaded from
cubeecraft.com

Toy design by
Chris Beaumont
cubeecraft@gmail.com

Carefully cut out the shape on this page. Use a hobby knife to slit the white lines labeled with letters as well as the black lines on either side where you will insert the hands. Tape and glue are not necessary. Thicker paper is recommended.

cubeecraft.com
CUBEECRAFT

@marckleinebudde