TEEP BOF
Overview

Hannes Tschofenig

28th March 2017 -- IETF 98th, Chicago

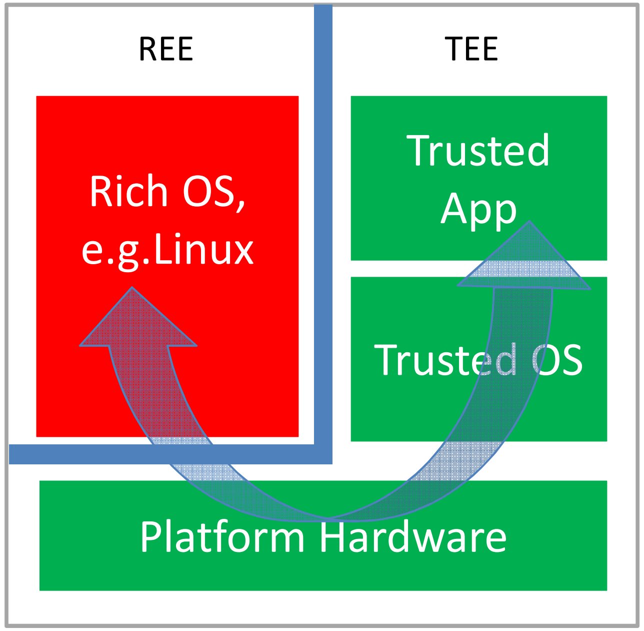
Agenda

- What is a TEE and what problem do we want to solve?
- Why should the IETF community care?

Background

- Today’s processor technology supports various isolation concepts.
- Well known are the concepts like the memory management unit, user and kernel space, and the hypervisor.
- There are, however, additional isolation concepts where a Rich Execution Environment (REE) resides alongside a Trusted Execution Environment (TEE).
- The TEE is designed to reside alongside the REE and provides a safe area of the device to protect assets and execute trusted code.

10, 000 foot view



Background: Hardware Details

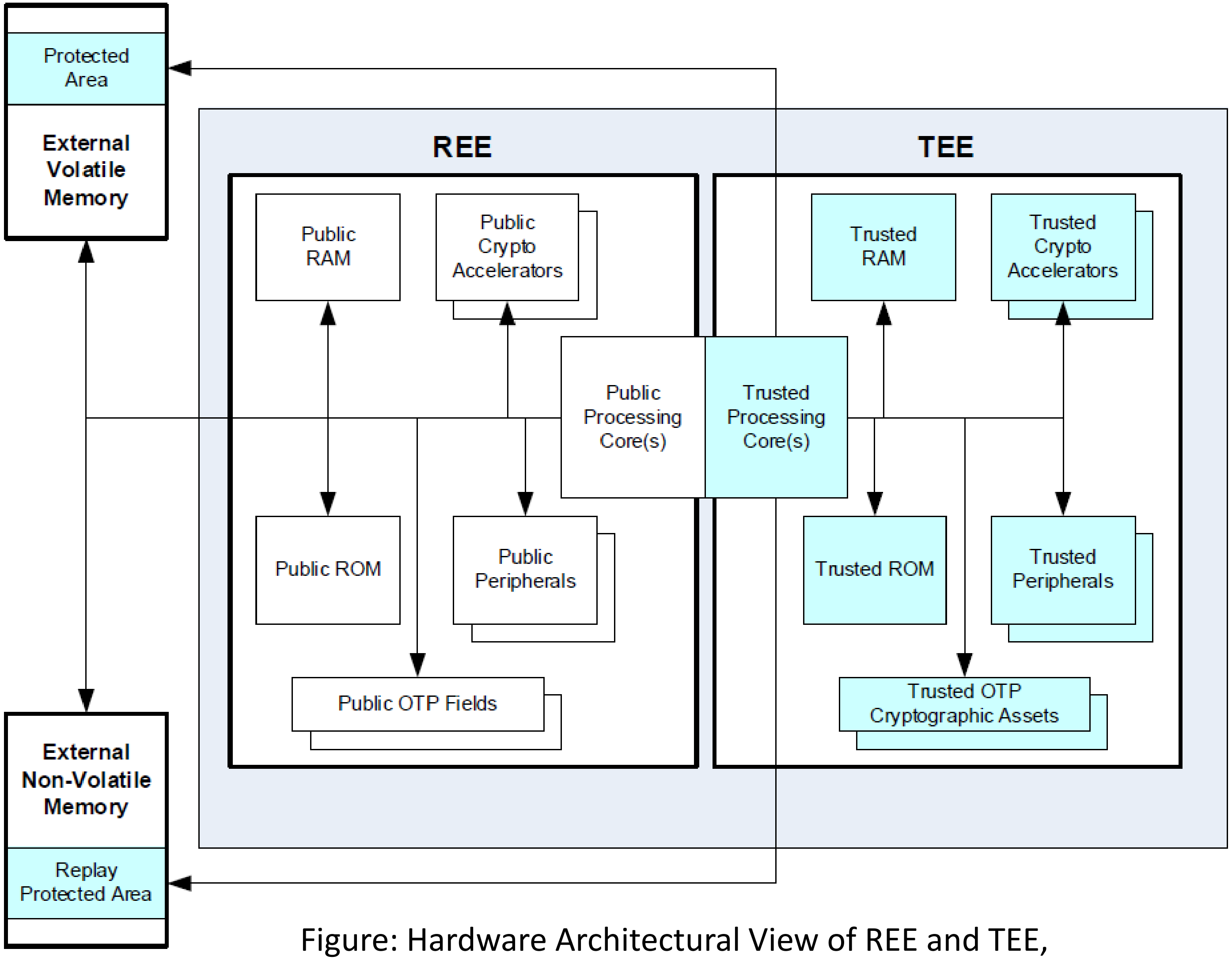

Protected Area
External Volatile Memory
REE
TEE
Public RAM
Public Crypto Accelerators
Trusted RAM
Trusted Crypto Accelerators
Public Processing Core(s)
Trusted Processing Core(s)
Public ROM
Public Peripherals
Trusted ROM
Trusted Peripherals
Public OTP Fields
Trusted OTP Cryptographic Assets
External Non-Volatile Memory
Replay Protected Area

Figure: Hardware Architectural View of REE and TEE,
Global Platform, TEE System Architecture v1.1

Background: Software Details

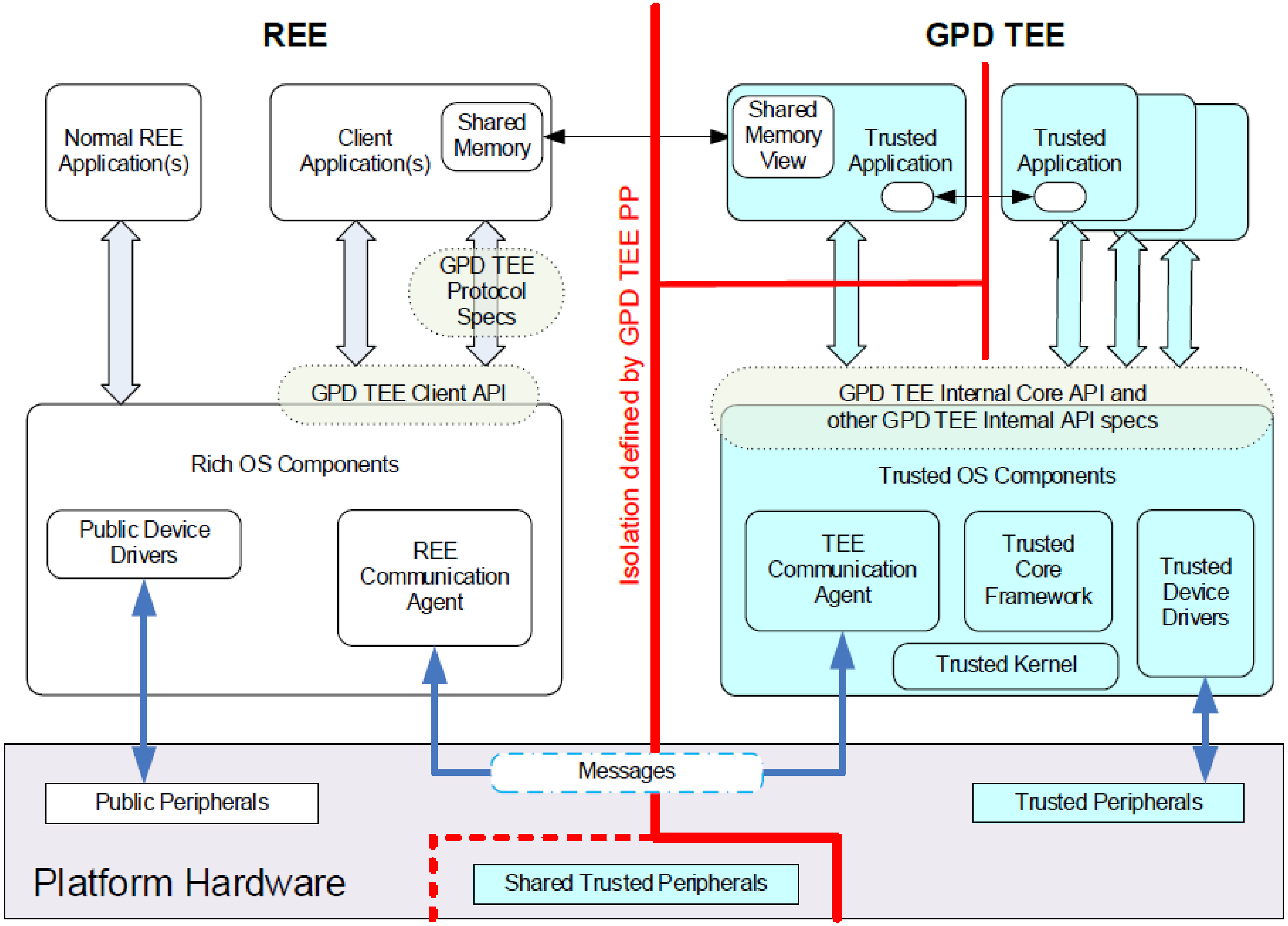


Figure: TEE Software Architecture,
Global Platform, TEE System Architecture v1.1

Problem, cont.

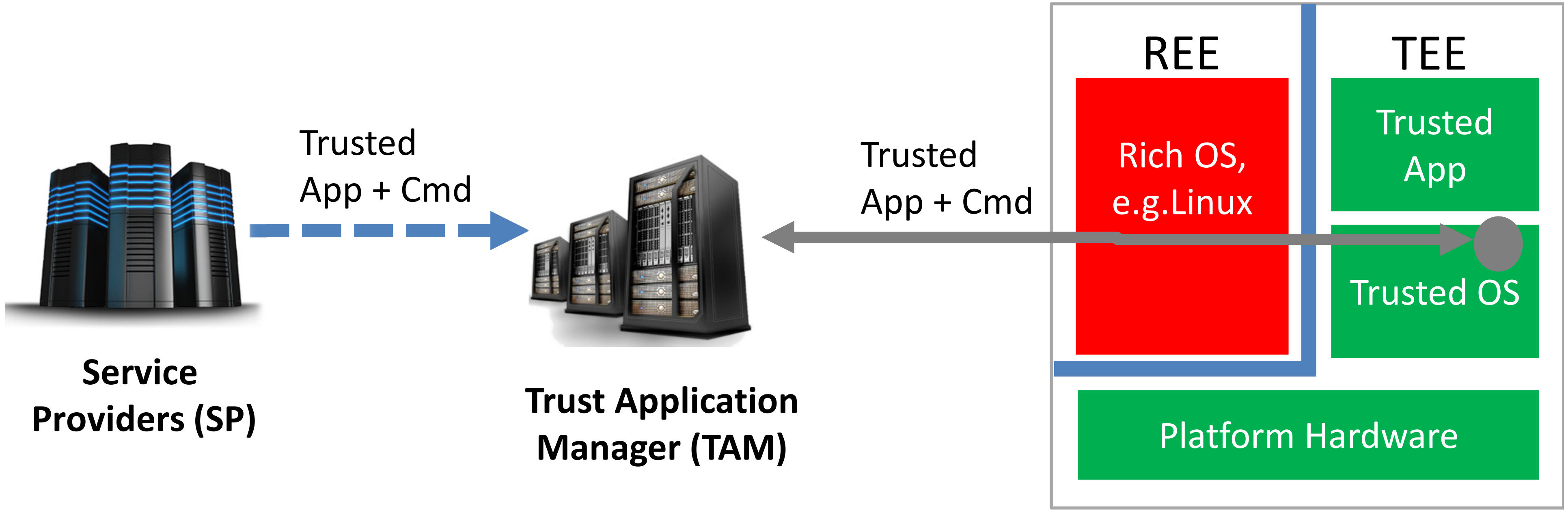
- Lots of hardware is available that offers TEE support (e.g., phones, tablets, networking equipment, servers)
- Applications have to be provisioned somehow into the TEE.
- Today, this is mostly done via proprietary techniques.
- Unfortunately, uptake (for broad range of applications) is limited.

Goal

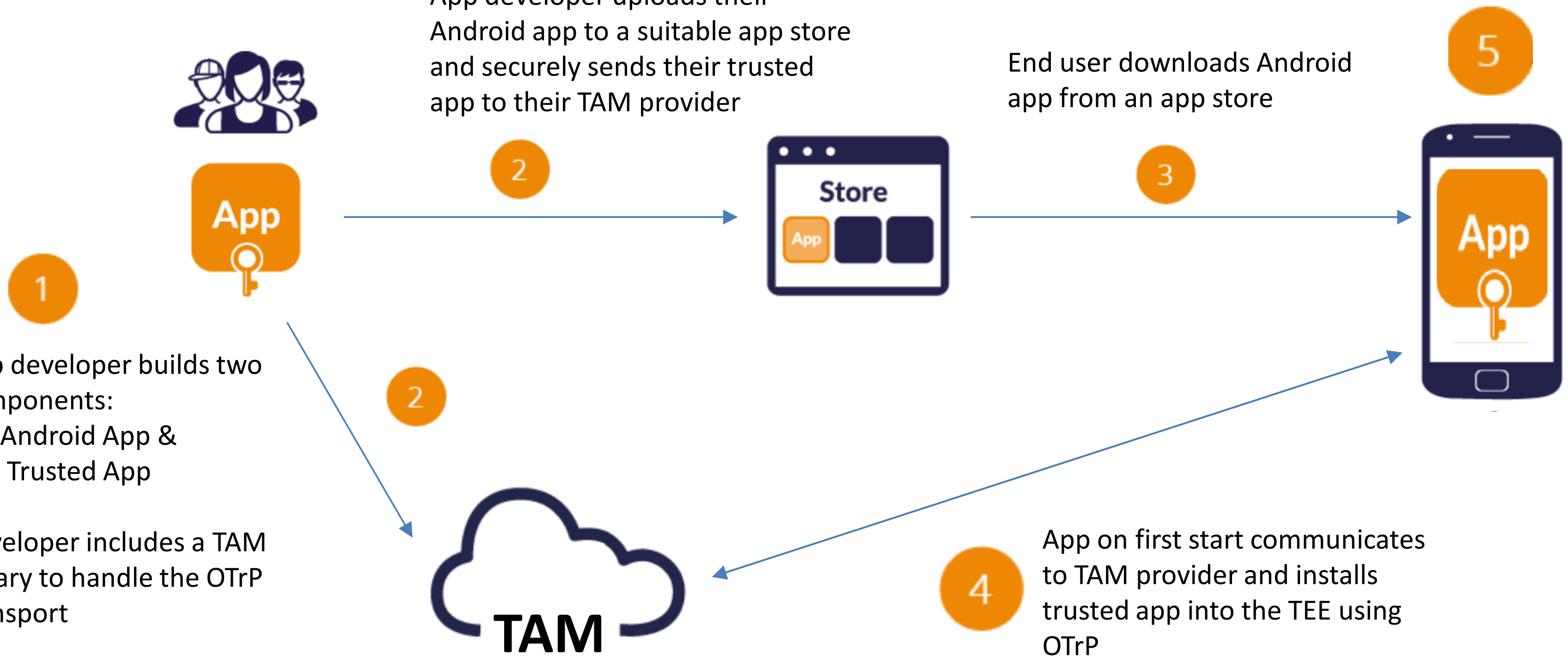
- Wouldn’t it be great if there is a standardized protocol for providing software into the TEE?
- Such a protocol should better provide security.

IETF Work TBD: A Protocol

- To illustrate the idea a proposal has been put together -- the Open Trust Protocol (OTrP)
- OTrP is a JSON/JOSE-based application layer security protocol that runs between a TAM and a component in the TEE OS.



Envisioned user experience



1

App developer builds two components:

1. Android App &
2. Trusted App

Developer includes a TAM library to handle the OTrP transport

2

App developer uploads their Android app to a suitable app store and securely sends their trusted app to their TAM provider

2

3

End user downloads Android app from an app store

4

App on first start communicates to TAM provider and installs trusted app into the TEE using OTrP

5

End user enjoys a rich Android experience and the security of a TEE backed component