

TEEP BOF
Problem Statement
draft-liu-opentrustprotocol-usecase

Hannes Tschofenig, Mingliang Pei
IETF 100th, Singapore

Background

- Hardware based security is desirable
 - 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.
 - Additional isolation concepts where a Rich Execution Environment (REE) resides alongside a Trusted Execution Environment (TEE)
- TEE already widely deployed in the payment industry
- TEE already adopted in other standard bodies (GP, OneM2M, etc.)

Benefits of TEE

- A TEE provides hardware-enforcement that
 - The device has unique security identity
 - Any code inside the TEE is authorized code
 - Reduced risk for application compromise
 - Any data inside the TEE cannot be read by code outside the TEE
 - Safe area of the device to protect assets (great for key management)
 - Compromising REE and normal apps don't affect TEE and code (called Trusted Application) running inside TEE



Background: Hardware Details

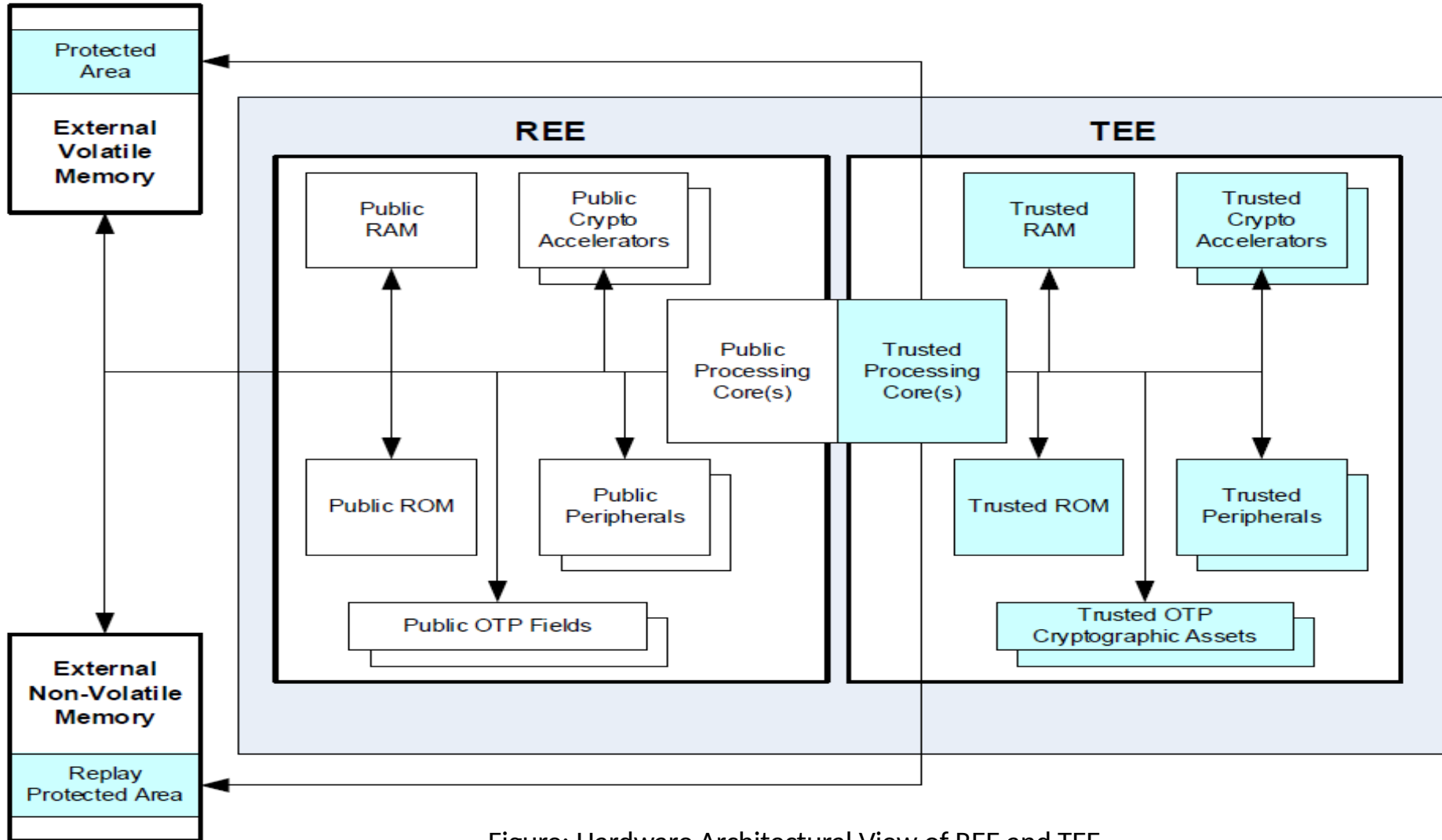


Figure: Hardware Architectural View of REE and TEE,
Global Platform, TEE System Architecture v1.1

Despite such widely available TEE environment

- Trusted App development and distribution are hard
 - Much less than that for normal apps via App Store
 - Trust and management issues due to multiple parties involved in the scenario



Example use cases

1. Payment

- Only authorized code can make payments or see payment data, to protect against financial loss

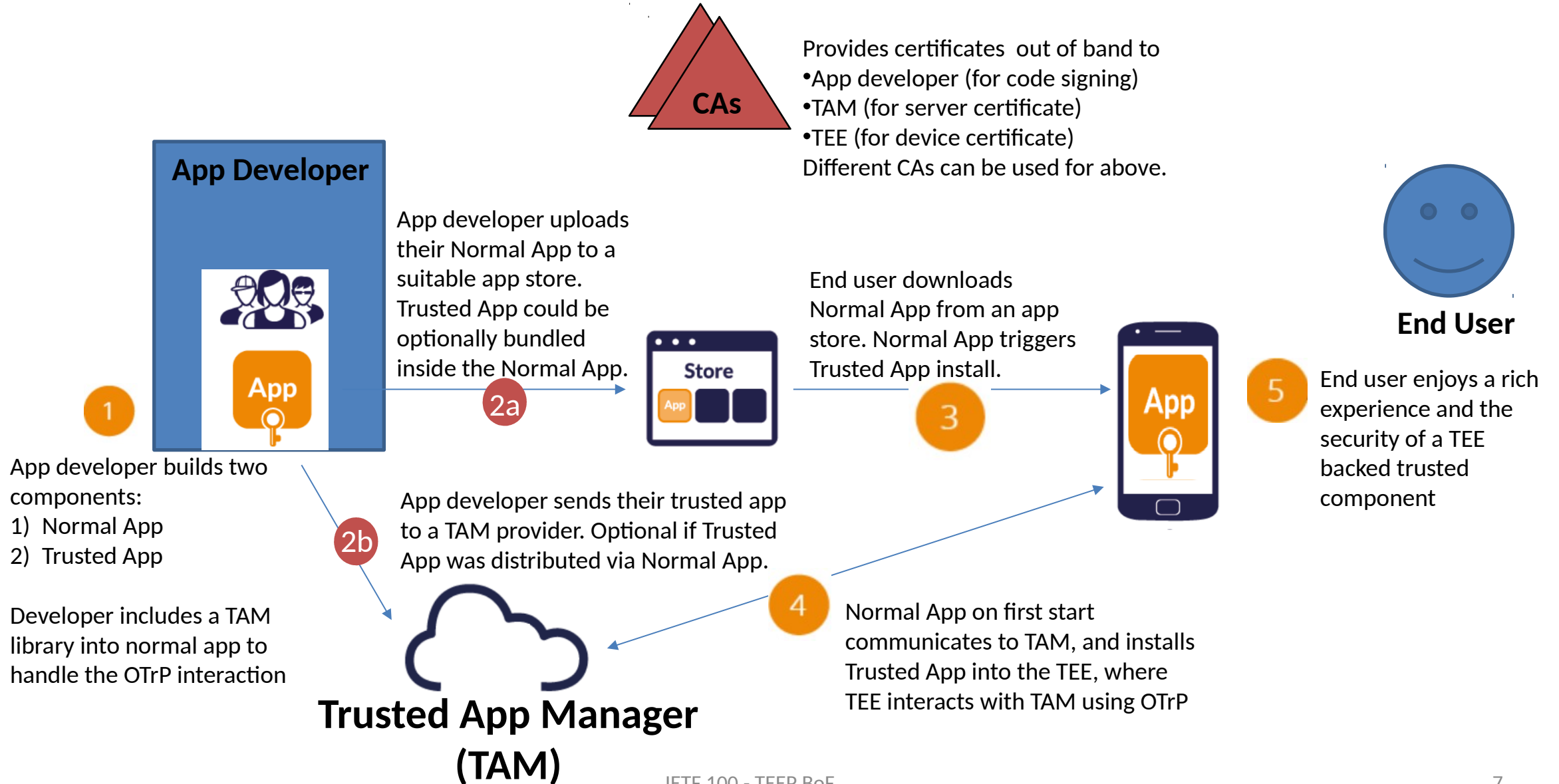
2. IoT

- Only authorized code can access physical actuator/sensor, to protect against safety issues

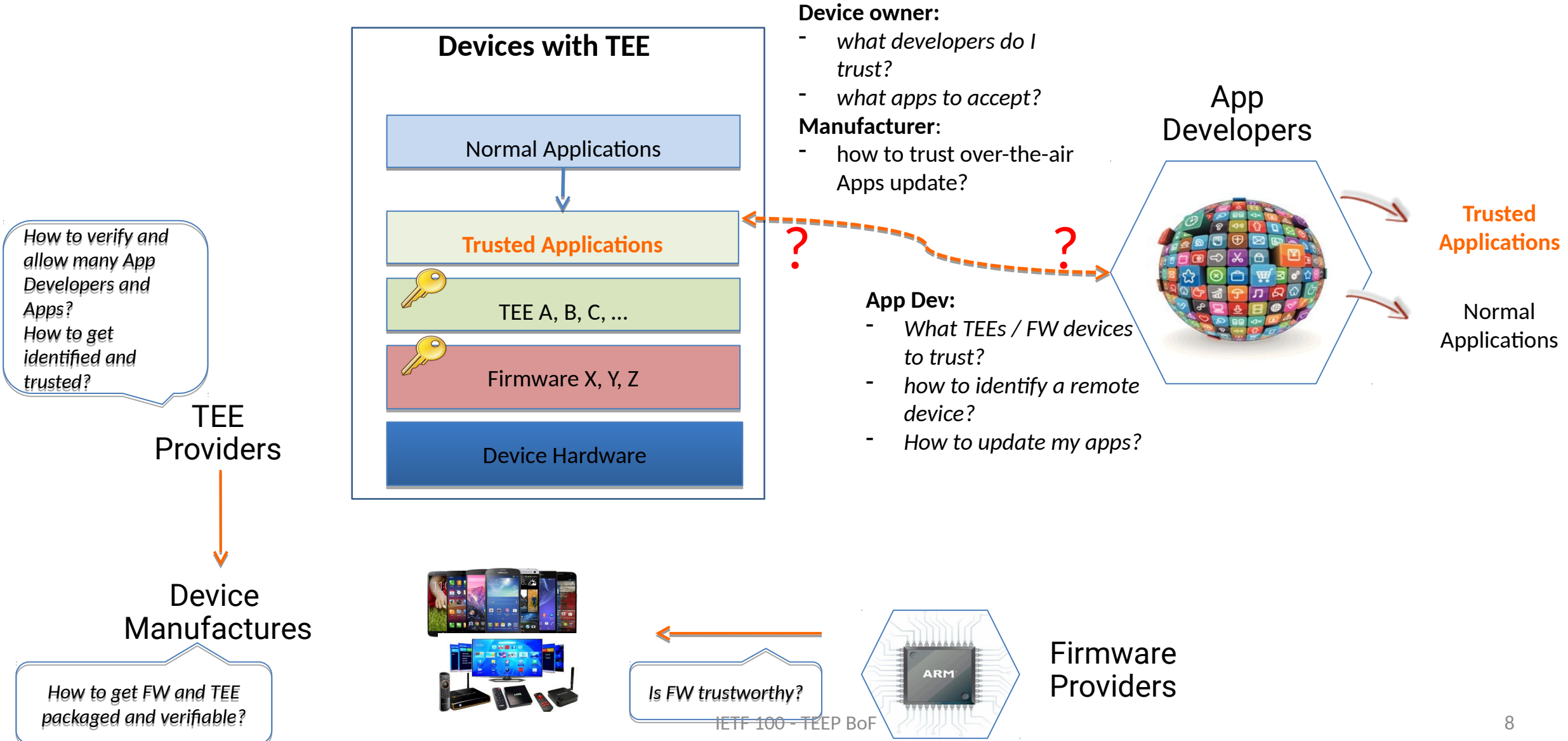
3. Confidential cloud computing

- Only tenant (not cloud hoster) can access data

Entity Roles and Experience



Gaps to utilize hardware based security



The Problems

- Adoption gap for App Developers
 - Applications have to be provisioned somehow into the TEE
 - Many device manufacturers + many device types (e.g., phones, tablets, networking equipment, servers) + multiple TEE providers
 - An application provider needs to support
- Lack of standards to manage Trusted Apps
 - Via proprietary techniques today
 - Need to answer
 - How is mutual trust based and verified
 - App Developers / TAM trusts Device's TEE / FW
 - Device trusts App Developers and Apps to be installed and updated
 - What messages for mutual communication
 - What permissions that different entities should have
- Fragmentation is growing - IoT accelerated that fragmentation

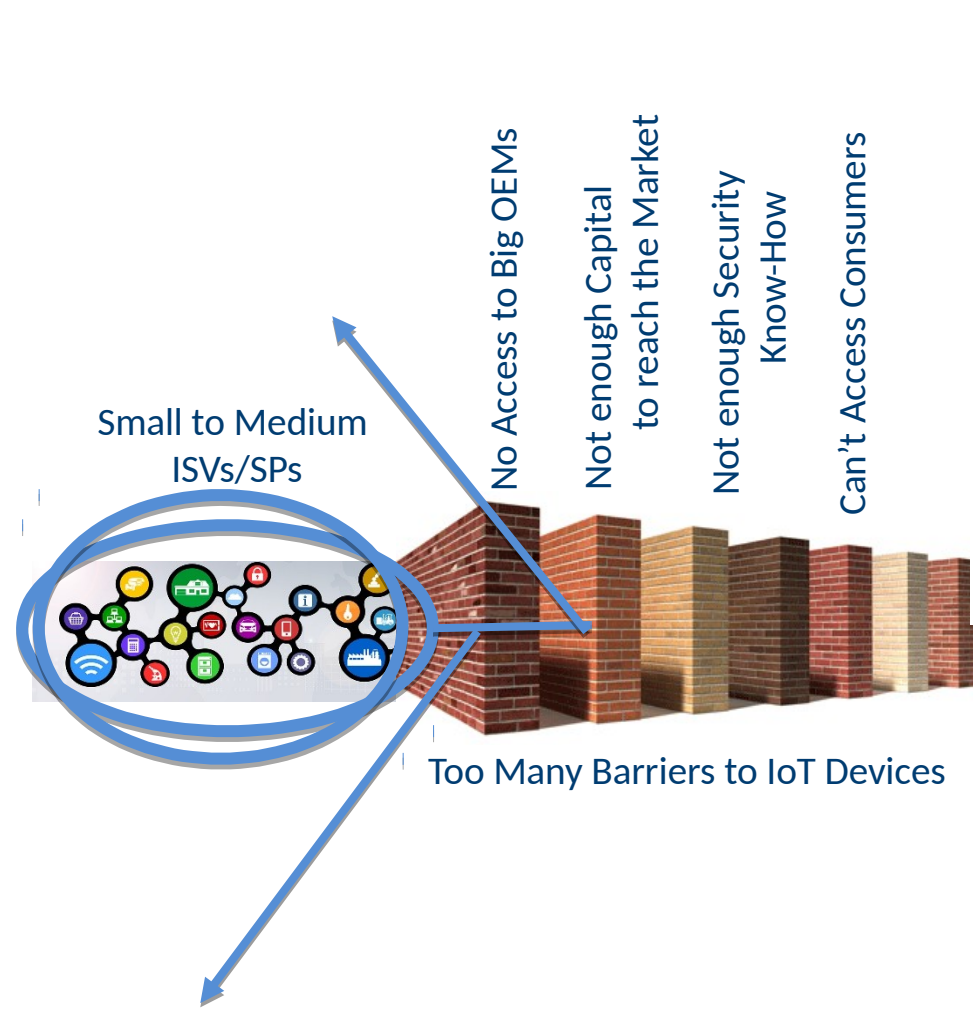
Goal

- Define a standardized protocol for providing and managing trusted applications in various devices with TEE
 - Grow the adoption of trusted applications to reduce the inherent security weakness with rich OS
 - Non-lock in for broad device types and providers
 - E.g., allow a TAM to work with multiple TEE & device vendors and flavors
 - Such a protocol better provides security

Q&A

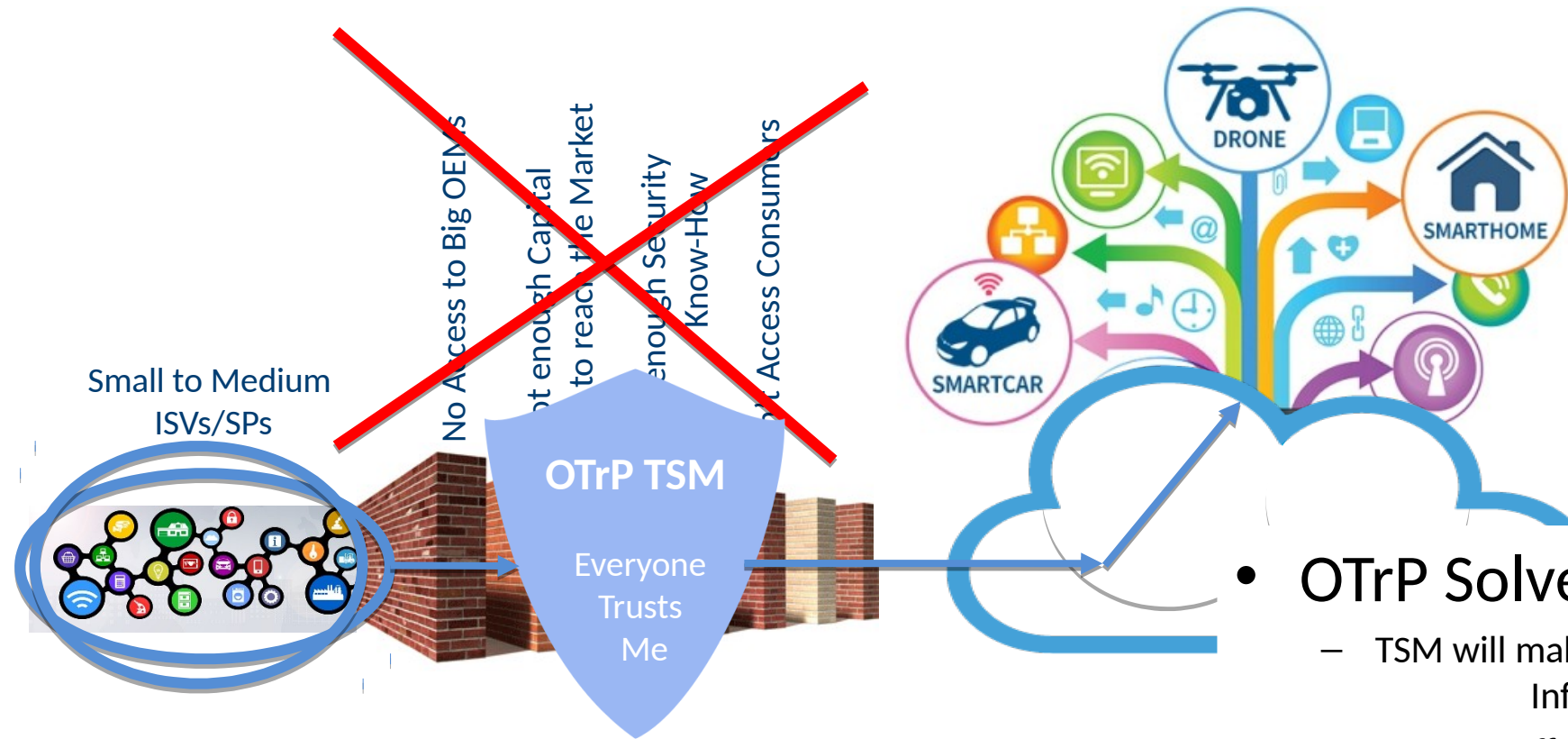
Backup

Small to Medium ISV's & SPs have a Problem



- Small ISV's and Service Providers
 - Don't have the clout to talk to big OEMs
 - Don't have the capital to build large infrastructure
 - Don't have the Brains & Brawn to tackle security on the devices

OTrP is Striking a Market Need



OTrP TSM Punctures the Barriers
For Small to Medium Sized ISV's & SP's

Large SP's can benefit from OTrP because
they can scale their infrastructure investment
to their available market easily at lower cost

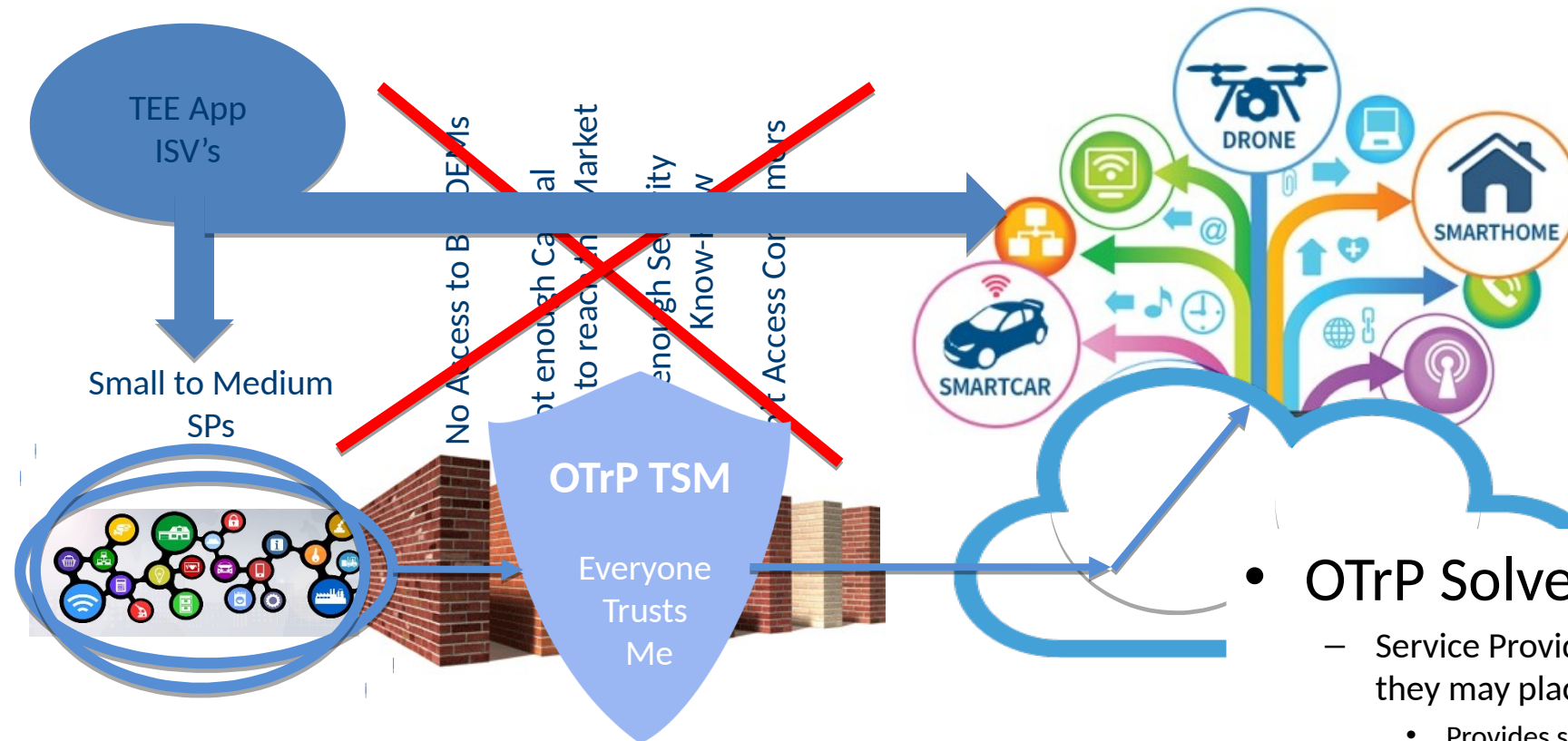
- **OTrP Solves Their Problems**

- TSM will make deals with big OEMs & Infrastructure players
- TSM can afford to build out infrastructure, because costs are leveraged across many ISVs and SPs
- TSM will hire the Brains & Brawn and manage the security (ISVs/SPs only need a single certificate)
- OTrP TSM is a ready-to-go Cloud solution

OTrP Addresses Security Know-

Secure App Problem

Even with access to the TEE, a Service Provider may not really have the **Security Expertise** to create their own Trusted Applications to run inside the TEE, or re-sign someone else's apps



The Service Provider does not have the knowledge to build trusted apps for different platforms and TEEs. The Security Domain in OTrP allows the service provider to just buy trusted apps from ISVs, not have to even re-sign those apps or manage their attestation, and install them into their own TEE

• OTrP Solves Their Problems

- Service Provider is given a Security Domain into which they may place their applications
 - Provides separation between different SP's applications
- Allows Security Domain to host off-the-shelf/common trusted applications which are bound specifically to the Service Provider
 - Common Secure Key Manager
 - Common Cloud Agent

IETF Work TBD: A Protocol

- To illustrate the idea a proposal has been put together -- the Open Trust Protocol (OTrP)
- OTrP is currently a JSON/JOSE-based application layer security protocol that runs between a TAM and a component in the TEE OS
 - Open for draft update in WG (e.g. JSON vs. CBOR, mandatory transport protocol support etc.)

