Architecture

Hannes Tschofenig
IETF#101
Demand of hardware based security with TEE and TA

Device with TEE

Normal World
- Applications

Secure World
- SD
- TA
- TA

Rich OS

TEE

Hardware Platform

Developer

Device owner:
- What developers do I trust?
- What trusted apps to accept?

Manufacturer:
- how to trust over-the-air updates?
- how to trust over-the-air updates?

Developer:
- How to update my trusted apps on many devices with different TEEs?
- What devices to trust?
- How to identify a remote device?

TEE Provider:
- How to verify and allow many app developers and apps?
- How to get identified and trusted?
Scope

PKI

Certification Authority

Device Software

Agent

App

OTrP

TEE

TAs

Service Provider

TAM

Device

Hardware Platform

Messages

Agent API

Certificate Enrollment API

Implementation specific API
Entity Relationships
Security Domain

• Idea: TAs in one SD shouldn’t access TAs in other SDs

• Up to TEE’s implementation of isolation and access control

• Should there be a restriction for having a one-to-one relationship between security domains and TAs?

\[
\begin{align*}
\text{TAs in one SD} & \quad \text{TAs in other SDs} \\
\text{TEE's implementation} & \quad \text{Access control} \\
\text{One-to-one relationship} & \quad \text{Security domains and TAs?}
\end{align*}
\]
**Keys**

- **Certification Authority**
  - CA Certificate
  - Used to issue certificates

- **Service Provider**
  - SP Key pair and Certificate
  - Used to sign TAs

- **TAM**
  - TAM Key pair and Certificate
  - Used to sign OTrP requests

- **TEE**
  - TEE Key pair and Certificate
  - Device attestation