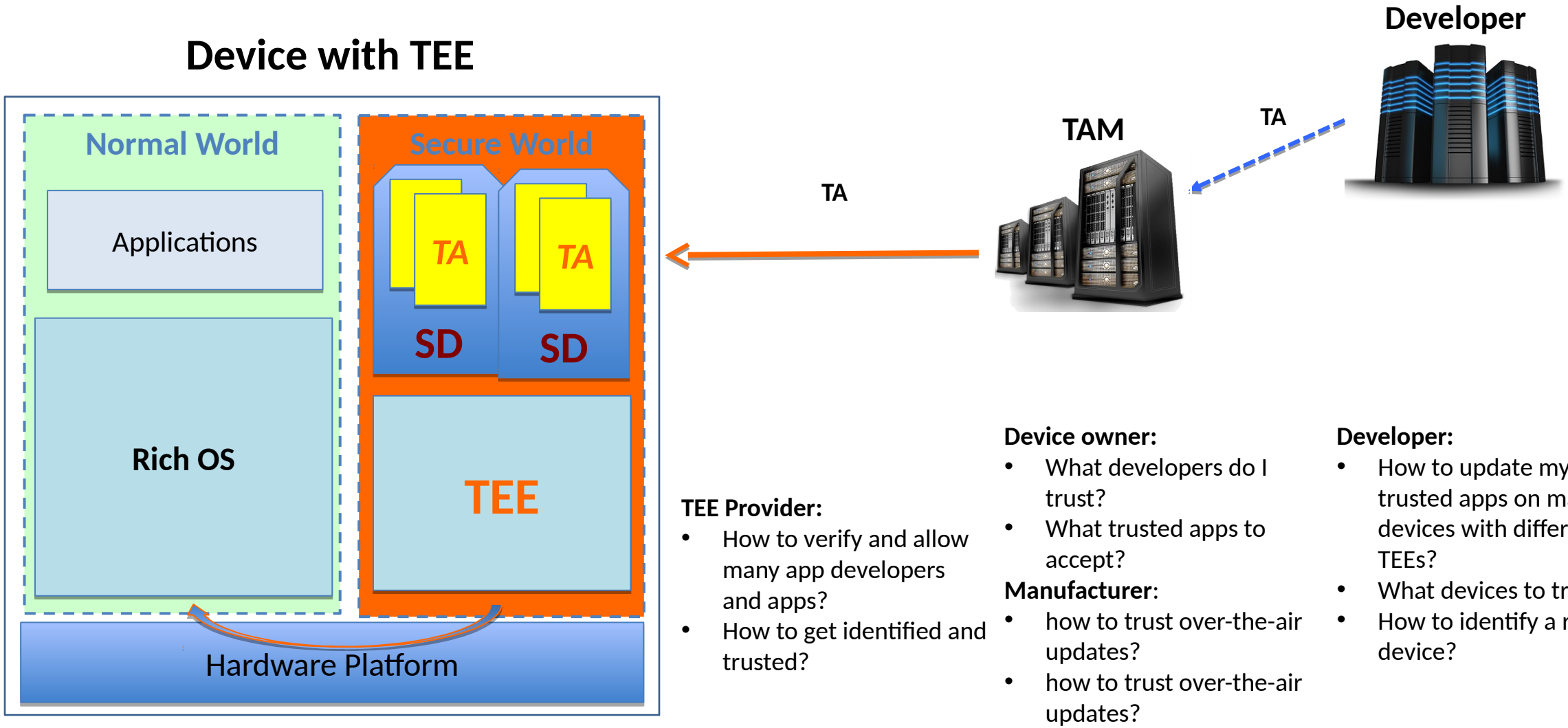
Architecture

Hannes Tschofenig

IETF#101

Demand of hardware based security with TEE and TA



TEE Provider:

- How to verify and allow many app developers and apps?
- How to get identified and trusted?

Device owner:

- What developers do I trust?
- What trusted apps to accept?

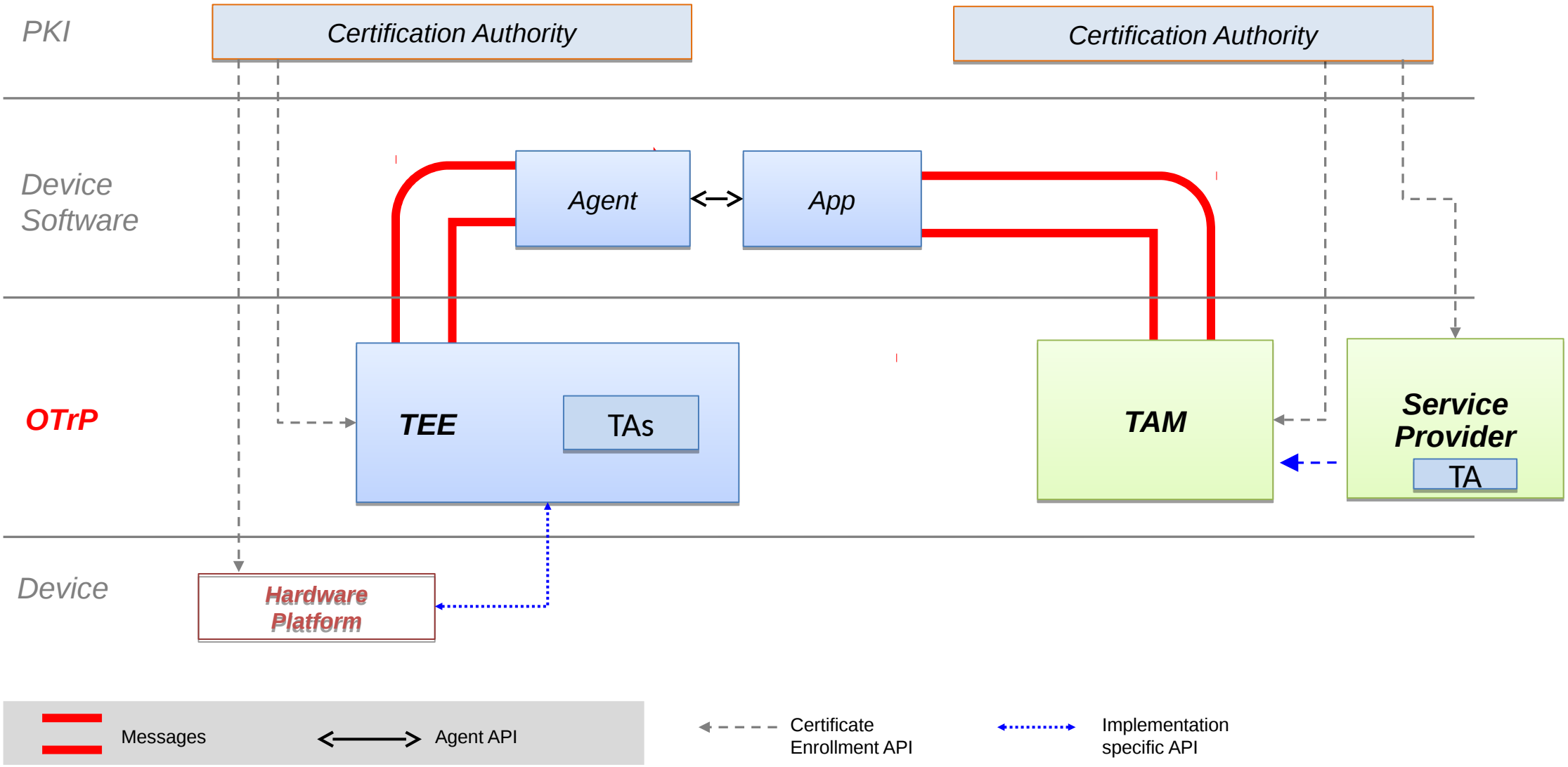
Manufacturer:

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

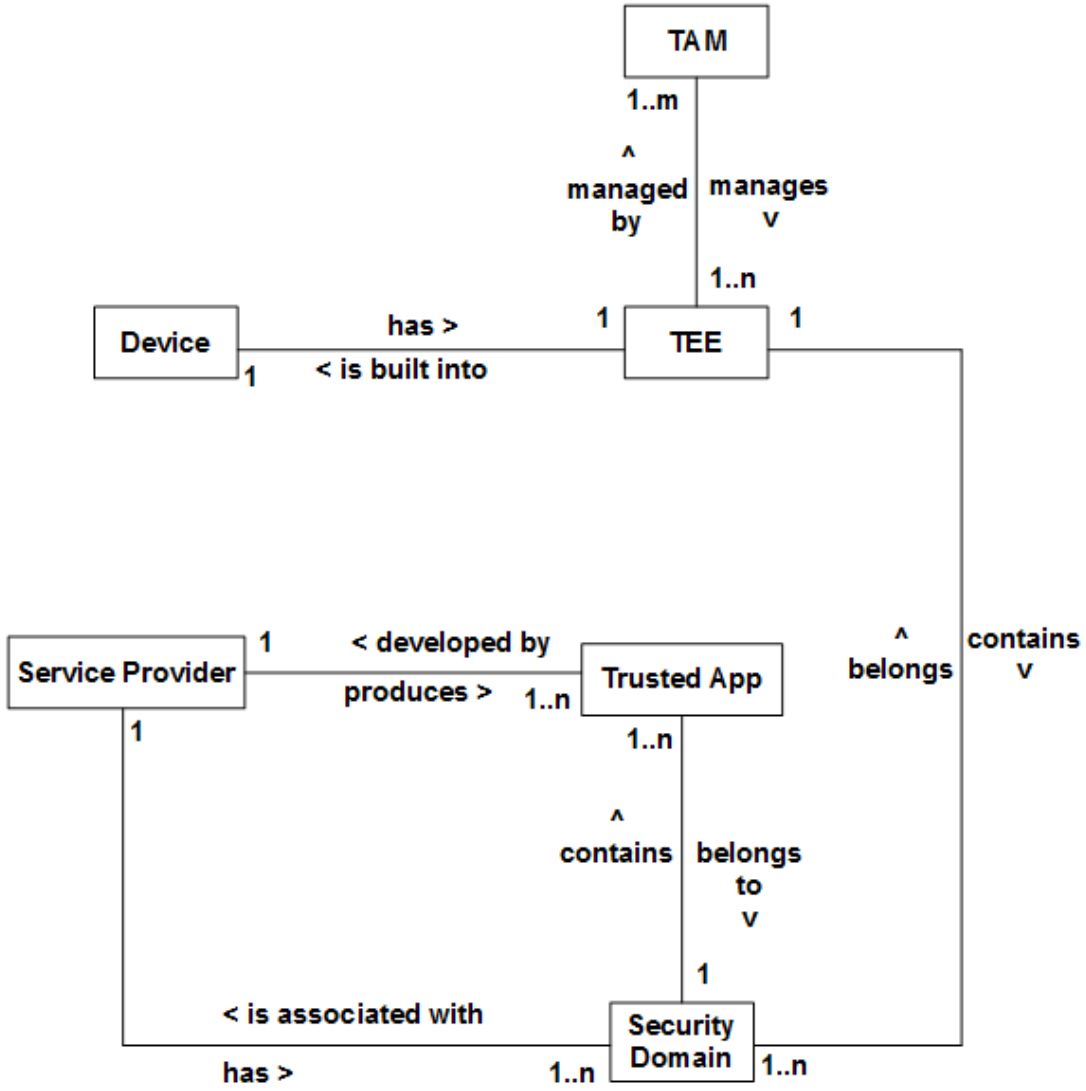
Developer:

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

Scope

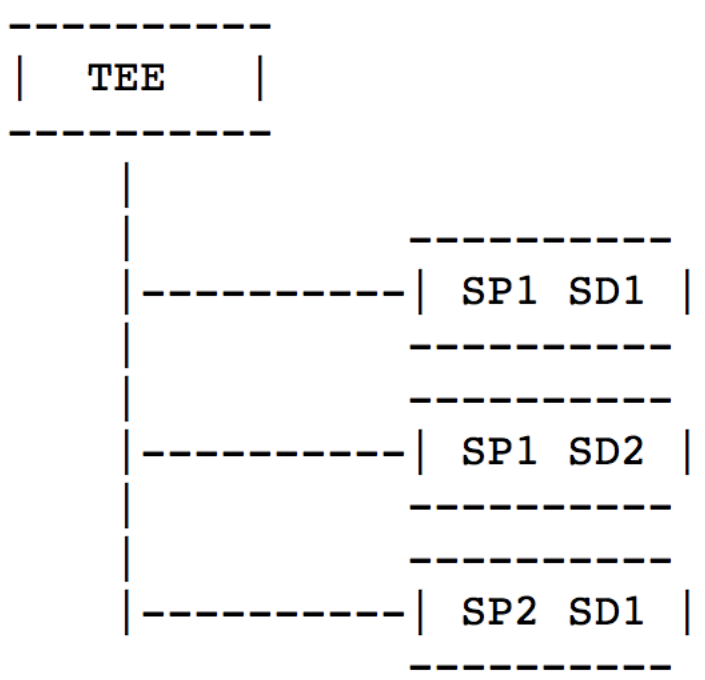

PKI
Certification Authority
Certification Authority
Device Software
Agent
App
OTrP
TEE
TAs
TAM
Service Provider
TA
Device
Hardware Platform
Messages
Agent API
Certificate Enrollment API
Implementation specific API

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?



Keys

	Certification Authority	*Service Provider*	*TAM*	*TEE*
Keys	 **CA Certificate**	 SP Key pair and Certificate	 TAM Key pair and Certificate	 TEE Key pair and Certificate
Usage	Used to issue certificates	Used to sign TAs	Used to sign OTrP requests	Device attestation