TEEP Architecture
draft-ietf-teep-architecture-15

Dave Thaler (presenting)

Ming Pei, David Wheeler, Hannes Tschofenig

Timeline

- JAN 2020: WGLC completed
- Before IETF 110: Draft -14 addressed remaining comments
- Issues raised since IETF 110, now addressed (next slides)
  - #222: Indicate the possibility to terminate TLS in the TEE
  - #224: Figure 4 - Improve readability
  - #225: Clarification regarding Data Protection
  - #226: Replace certificate chain with certificate path
- JUL 2021: Tiru did doc shepherd review and submitted to IESG

#222: Indicate the possibility to terminate TLS in the ―――

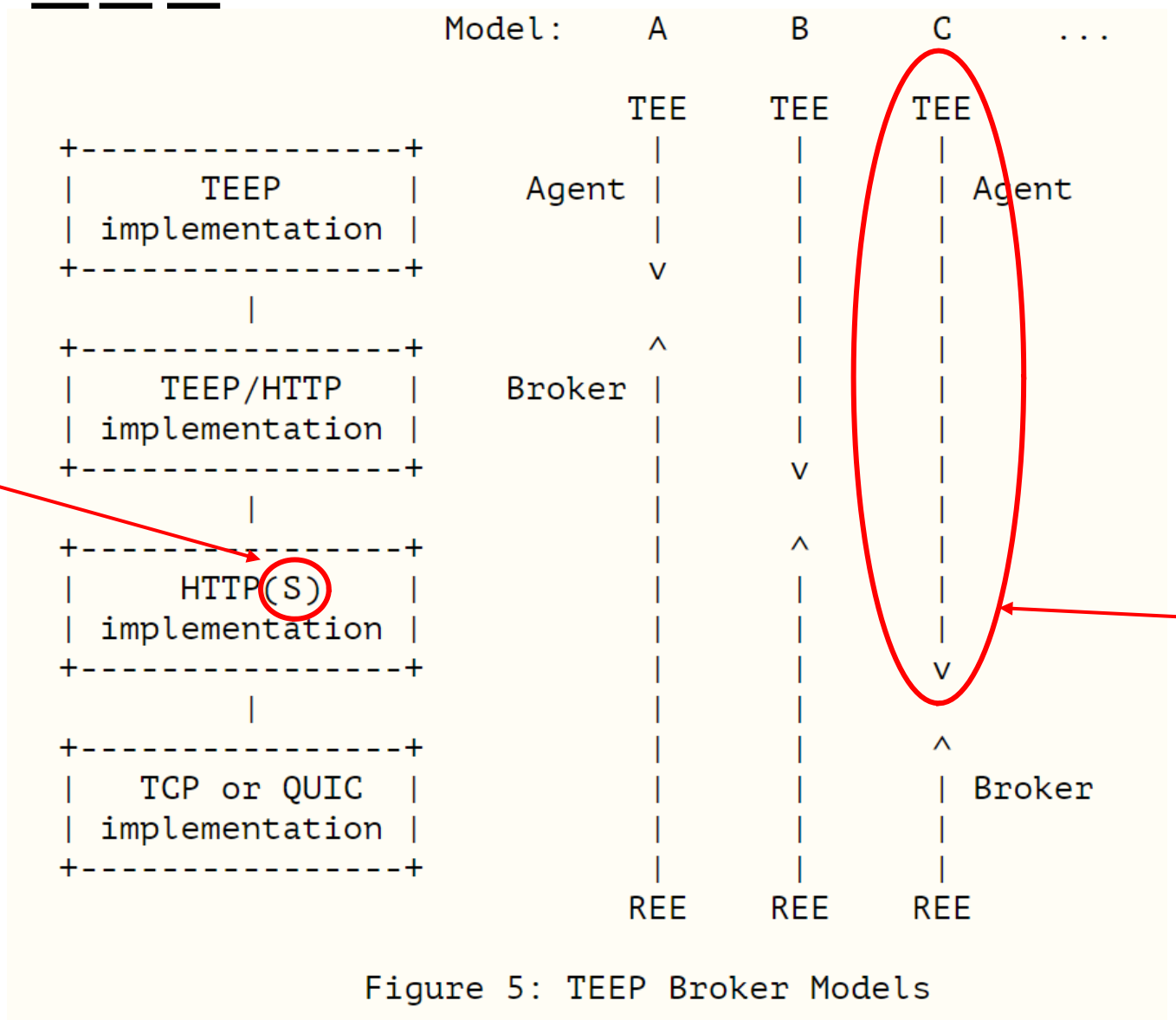

Figure 5: TEEP Broker Models

#224: Figure 4 - Improve readability

Purpose	Cardinality & Location of Private Key	Private Key Signs	Location of Trust Anchor Store
Authenticating ~~TEE~~ **TEEP Agent**	1 per TEE	TEEP responses	TAM
Authenticating TAM	1 per TAM	TEEP requests	TEEP Agent
Code Signing	1 per Trusted Component Signer	TA binary	TEE

Figure 4: Signature Keys

- TAM authenticates messages from TEEP Agent, not TEE per se

#225: Clarification regarding Data Protection

- Hannes rewrote last paragraph of Data Protection security consideration section:

The protocol between TEEP Agents and TAMs similarly is responsible for securely providing integrity and confidentiality protection against adversaries between them. ~~Since~~ **It is a design choice at what layers to best provide protection against network adversaries. As discussed in Section 6,** the transport protocol **and any security mechanism associated with it (e.g., the Transport Layer Security protocol)** under the TEEP protocol ~~might be implemented~~ **may terminate** outside a ~~TEE, as discussed in Section 6,~~ **TEE. If** it ~~cannot be relied upon for sufficient protection. The~~ **does, the** TEEP protocol ~~provides~~ **itself must provide** integrity ~~protection, but~~ **protection and** confidentiality ~~must~~ **protection to secure data end-to-end. For example, confidentiality protection for payloads may** be provided by ~~payload encryption, i.e., using~~ **utilizing** encrypted TA binaries and encrypted attestation information. See [I-D.ietf-teep-protocol] for ~~more discussion.~~ **how a specific solution addresses the design question of how to provide integrity and confidentiality protection.**

#226: Replace certificate chain with certificate path

- RFC 4949 says for certificate chain:
  - Deprecated Term: IDOCs SHOULD NOT use this term; it duplicates the meaning of a standardized term. Instead, use "certification path".
- Issue raised by RATS WG on text copied from TEEP architecture doc
- Now replaced throughout

OPEN #223: Defined what we mean by 'Software Update'

- Hannes proposed putting a definition of “Software Update” in terminology section
- But term occurs only once in the doc, way *before* terminology section
- Introduction has:
  - “To simplify the life of TA developers interacting with TAs in a TEE, an interoperable protocol for managing TAs running in different TEEs of various devices is needed. This **software update** protocol needs to make sure that compatible trusted and untrusted components (if any) of an application are installed on the correct device. In this TEE ecosystem, there often arises a need for an external trusted party to verify the identity, claims, and rights of TA developers, devices, and their TEEs. This trusted third party is the Trusted Application Manager (TAM).”
- Proposed resolution: No change