TEEP Protocol

draft-ietf-teep-protocol-03

Dave Thaler <dthaler@microsoft.com>

Timeline

- -01 posted before and discussed at April virtual interim meeting
- -02 posted after April virtual interim (and 16 pull requests)
- -03 posted July 13 after SUIT hackathon (and 4 pull requests)
- Notable interop fix:
  - Fixed Success vs error message type # contradictions in spec (normative language vs CDDL was backwards)
- Currently 9 issues open in github

Issues related to teep-architecture

#2: Requested Components
#5: … when have TA binary but need metadata

Arch doc now says:

- Requested Components:
  - A list of zero or more components (TAs or other dependencies needed by a TEE) that are requested by some depending app, but which are not currently installed in the TEE.
  - The claims also need to specify for each component, whether the TA binary is needed, or whether the TA binary is already available and only permission to install is needed.

Should they be passed in:

a) attestation claims (what arch doc says now), or
b) separate QueryResponse field

#16: List of no-longer-needed TAs

- If all Untrusted Apps are deleted that depend on a given TA, can you remove the TA?
  - On some TEE architectures (like SGX), can just delete a file
  - On others, only TAM can do so
- Currently no discussion of passing list of unneeded TAs to TAM
- Should we support this scenario?
  a) Via attestation claims
  b) Via separate QueryResponse field
  c) No

Issues related to suit-manifest

#41: SUIT manifest examples?

- What would SUIT manifest look like?
  1. TA ~= TEE (no notion of SD, or ability to enumerate), e.g., SGX
  2. Install TA into a pre-existing GlobalPlatform security domain
  3. Install TA into a new GlobalPlatform security domain
     - Now that we use SUIT manifest, is it still implicit or is some separate SUIT command needed?
- And for each of the above:
  a) When TA binary comes via the TAM
  b) When TA binary is already on the device and just needs metadata
- Should they be in TEEP protocol spec or SUIT manifest spec
  - **Propose:** TEEP protocol spec (SUIT manifest is close to done)

Other issues

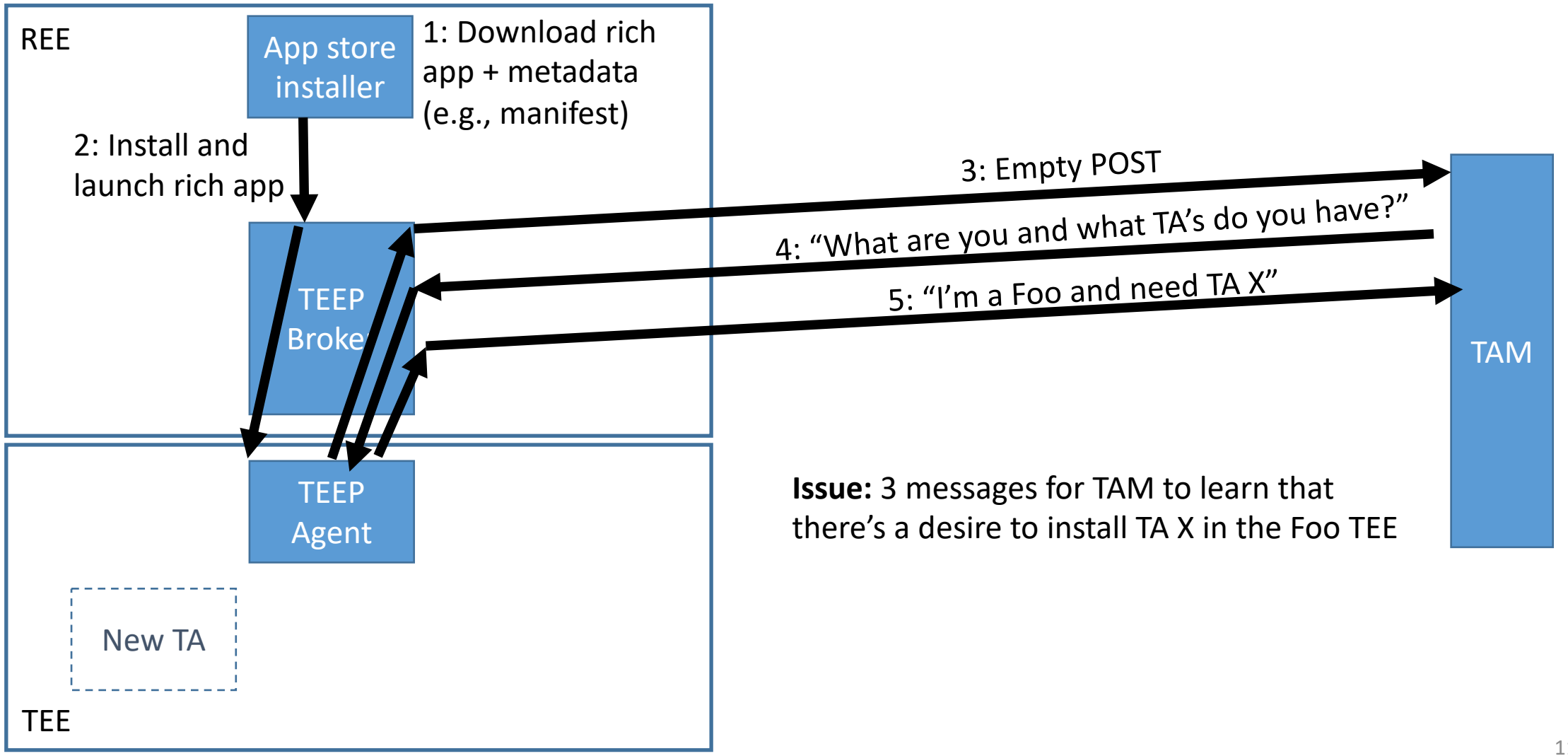
#13: Vendor-specific Attestation

- SGX already has vendor-specific evidence format (not RATS EAT) deployed
- RATS architecture discusses use of multiple evidence formats to a Verifier, e.g., to get a standard Attestation Result to Relying Party
- Should TEEP protocol:
  a) Support evidence format agility (not just EAT)
  b) Require wrapping other things in an EAT
  c) Not support existing formats

#40: QueryResponse without QueryRequest

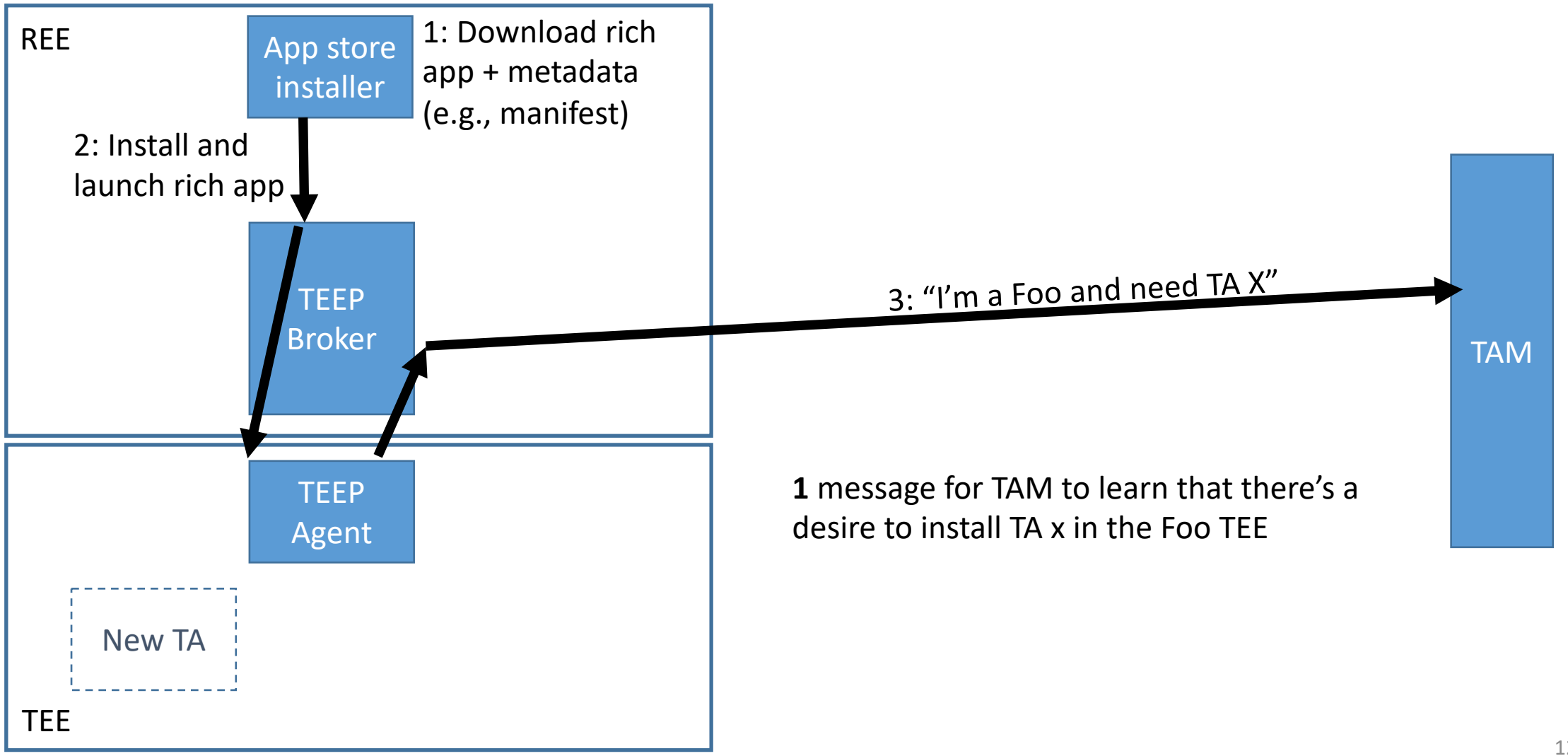
- In Hannes's review of the teep-over-http draft, he said:
  - FWIW the note that the TEEP Agent can start with a QueryResponse if it has the TAM public key is IMHO incorrect
- This came from previous OTrP text where OTrP allowed such an optimization in order to minimize RTTs and bandwidth for constrained devices.
- Shouldn't we add this optimization into the TEEP protocol?

What the TEEP protocol draft says



Issue: 3 messages for TAM to learn that there's a desire to install TA X in the Foo TEE

What OTrP allowed



1 message for TAM to learn that there's a desire to install TA x in the Foo TEE

#42: Deleting personalization data when deleting a TA

- Arch spec allows for TA binary and personalization data to be separate, and even come from different TAMs. E.g.:
  - “The TEEP protocol treats each TA, any dependencies the TA has, and personalization data as separate components with separate installation steps that are expressed in SUIT manifests, and a SUIT manifest might contain or reference multiple binaries (see [I-D.ietf-suit-manifest] for more details). The TEEP Agent is responsible for handling any installation steps that need to be performed inside the TEE, such as decryption of private TA binaries or personalization data.”
- TrustedAppDelete message does not use a SUIT manifest, and only has a list of TA's (not "components") to delete
- How can associated personalization data be deleted, especially when they were installed by different TAMs?

Other questions?