TEEP Use Cases

Goal: determine which are in/out of scope

Entities with potential requirements

- Device/TEE admin
- Trusted Application author
- Rich Application author
- TEE chip vendor
- Device OEM

These may or may not all be different entities

Device/TEE admin #1: check allow list

- Admin of device/TEE wants to manage what TA's are allowed in its TEE (e.g., because of limited secure storage capacity).
  - Not necessarily any trust relationship between device and author of TA.
  - Owner validates TA and authorizes it for use on their devices.
  - If allowed list == installed list, then don't need an exchange.
  - If allowed list can be pre-provisioned in TEE, then don’t need an exchange.
  - If allowed list >> installed list AND allowed list doesn't fit on device due to space or dynamism reasons, then need a check at installation time.

Device/TEE admin #2: private data

- Admin of device/TEE wants to keep a given TA and/or its config encrypted (independent of anything the author does) so needs to be in the loop when the TA is installed.
- Purpose of protocol exchange is to get the secret info or decryption key from the admin's agent.

TA author: private data

- TA author wants to keep the TA code and/or its config encrypted (independent of anything the device/TEE admin does) and only let it be decryptable within a kind of TEE that it trusts to keep the info private, so needs to somehow be in the loop when the TA is installed.
- Purpose of protocol exchange is to get the secret info or decryption key from the author’s agent.

Rich app author: use a TA

- (REE) Client app author wants to depend on a TA from another vendor, and expresses a dependency either at install time or at run time.
- TAM protocol exchange seems mostly orthogonal to this use case

TEE chip vendor: vet TAs

- A TEE chip vendor wants to only allow authorized TA's to run in its chip.
  - E.g., first vet the code as being safe under the assumptions that TEE chip makes
  - E.g., have trusted authors rather than vetting each TA

Device OEM: vet TAs

- A device OEM wants to only allow authorized TA's to run in the TEE on its devices.
  - E.g., first vet the code as being safe under the assumptions that TEE chip makes
  - E.g., have trusted authors rather than vetting each TA