IETF 105 during TEEP hackathon
Clarification of
the location of keys, certs, and
CA certs for prototyping

07/21/2019
Akira Tsukamoto (AIST)
Kuniyasu Suzaki (AIST)
Kohei Isobe (SECOM)
Diagram for SP/TA code signing

REE/Untrusted
- TAM
- TEEP/OTrP Broker
- APP-1

TEE/Trusted
- SP CA cert
- TA-1
  - Signed by SP priv
- TA TEEP/OTrP Agent
  - Signed by SP priv

Device Developer
- SP Developer
- SP privkey
Diagram for TEE permits what TAs to load and run

The current OP-TEE implication is expecting the TAs will be verified by TEE and not by TEEP/OTrP again. The TA-A must be signed by TEE private key. Dave idea is based on DICE model
Diagram for OTrP session

REE/Untrusted
- APP-1
- TEEP/OTrP Broker

TEE/Trusted
- TA-1
- TEEP/OTrP Agent
  - TAM CA cert
  - TEE privkey
Diagram for device attestation

TFW key concept is in TEEP/OTrP version 1 documentation as optional. May not be required in TEEP/OTrP for future versions.