TEEP Use Case for Confidential Computing in Network 04

IETF 117
TEEP Meeting
update1: packaging model

Simplify Packaging model to 4 types, which includes all the possibilities of packaging

4.1. UA, TA and PD are bundled as a package
4.2. PD is a separate package, TA and UA are separate or integrated
4.3. TA and PD are bundled as a package, and UA is a separate package
4.4. TA and PD as a package, no UA
4.5. TA and PD are separate packages, no UA
Update2: use case figure

Use “Confidential Process”, “Confidential Container”, “Confidential VM” to replace “Process”, “Container”, “VM”.

Use () in Load Sequence to represent package model.
Update3: introduction improvement

Comments: the introduction can improved by describing early on what the users represent in this scenario, and where the TEEs are located in the network fabric. Similar to the abstract - what is the motivation for doing this? Simply having it possible is not enough of a reason.

Using MEC to explain when to use this document:

For example in MEC, the autonomous vehicles could deploy private applications and data on confidential computing device to calculate on-vehicle and destination road information without knowing by MEC platform.
Update 4: Using Nist standard to specify secure channel

After verification, Network User works as Relying Party to receive the attestation result. If positive, Network User establishes secure channel [NIST-Special-Publication-800-133-V2] with TEEP Agent, and transfers this package to TEEP Agent.

Definition of “secure channel” in NIST-Special-Publication-800-133:

| Secure channel | A path for transferring data between two entities or components that ensures confidentiality, integrity, and replay protection as well as mutual authentication between the entities or components. The secure channel may be provided using cryptographic, physical, or procedural methods or a combination thereof. |
Thanks