Trusted Execution Environment Provisioning (TEEP) Activity at IETF

Akira Tsukamoto

April 2023

Objective of TEEP, SUIT, RATS

Acronyms

Trusted Execution Environment Provisioning (TEEP)
Software Updates for Internet of Things (SUIT)
Remote ATtestation ProcedureS (RATS)

- Target Audience

  Vendors who develop products with CPU or SoC require Secure Update of software and data

- Lifecycle Management for Trusted Applications (Software) and Personalization data (Data)

- Main objective is to manage Software and data in IoT devices to have latest version

  Before updates of the Software and Personalization data in IoT , the server check the trustworthiness of the IoT devices remotely whether it is compromised or not

- Confidential Computing usage which technically assure the Host CPU can not read inside Guest VMs, it allows Cloud vendors provide confidentiality to customers using Guest VMs

Key features of TEEP, SUIT, RATS

- TEEP

Responsible of managing Software and Data on IoT devices

Check the version of Software and Data in devices, and updates them if necessary

- SUIT

Describes Software/Data in SUIT manifest

- RATS

Check trustworthiness of the IoT devices

Used to verity the target IoT devices are compromised or not

Key technical features of TEEP

Acronyms

Concise Binary Object Representation (CBOR)
CBOR Object Signing and Encryption (COSE)

- CBOR
  - Next generation Binary representation format for the Internet
  - Compatibility with JSON
  - Small binary size and low overhead of encoding and decoding
- COSE
  - Method of Signature Verification and Encryption on CBOR
- TEEP was the first protocol draft to adopt CBOR and COSE
  - Suitable for constrained devices and IoT while keeping similarity of JSON
- Agnostic protocol standard to difference of CPU or hardware design

Typical Trusted App and Personalization Data

- Trusted Application (Software)

  Payment App (Credit cards)

  DRM for video streaming (NetFlix)

  Firmware update (OTA)

- Personalization Data (Data)

  Device Authentication (eSIM)

  Unlock key of hardware feature (Quick Charge for Automotive)

  Personalization ID (SSN, Japanese My Number)

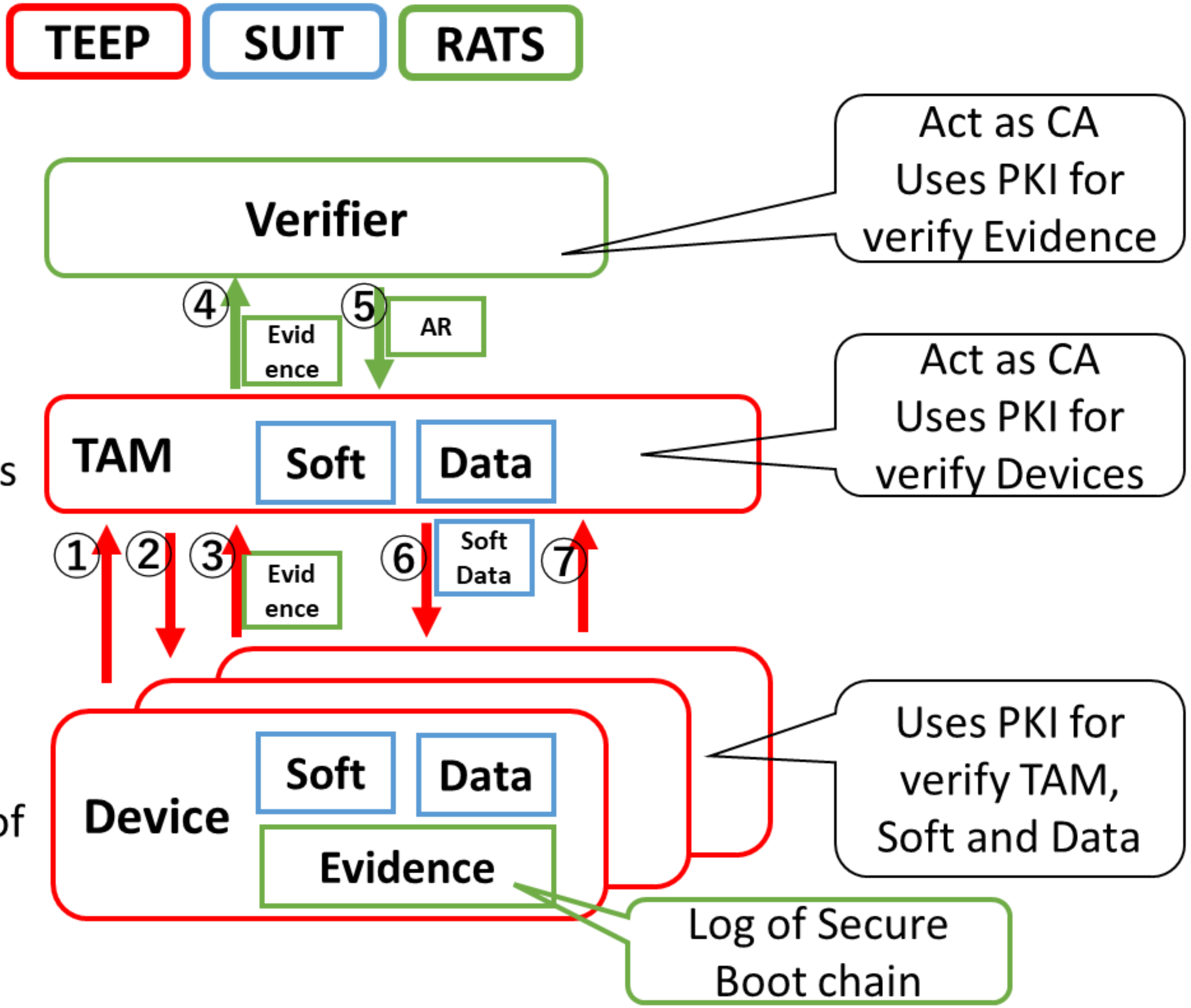
TEEP, SUIT, RATS in one chart

- Responsible areas in colors

Verifier verifies the trustworthiness of Hardware/Firmware of devices

Trusted Application Manager (TAM) maintains Software/Data in the devices
Software/Data are in SUIT manifest

Devices provide installed Software/Data information to TAM and receive updates if necessary
Devices provide integrity information of Hardware/Firmware in Evidence format (RATS) to Verifier



Operation of TEEP, SUIT, RATS

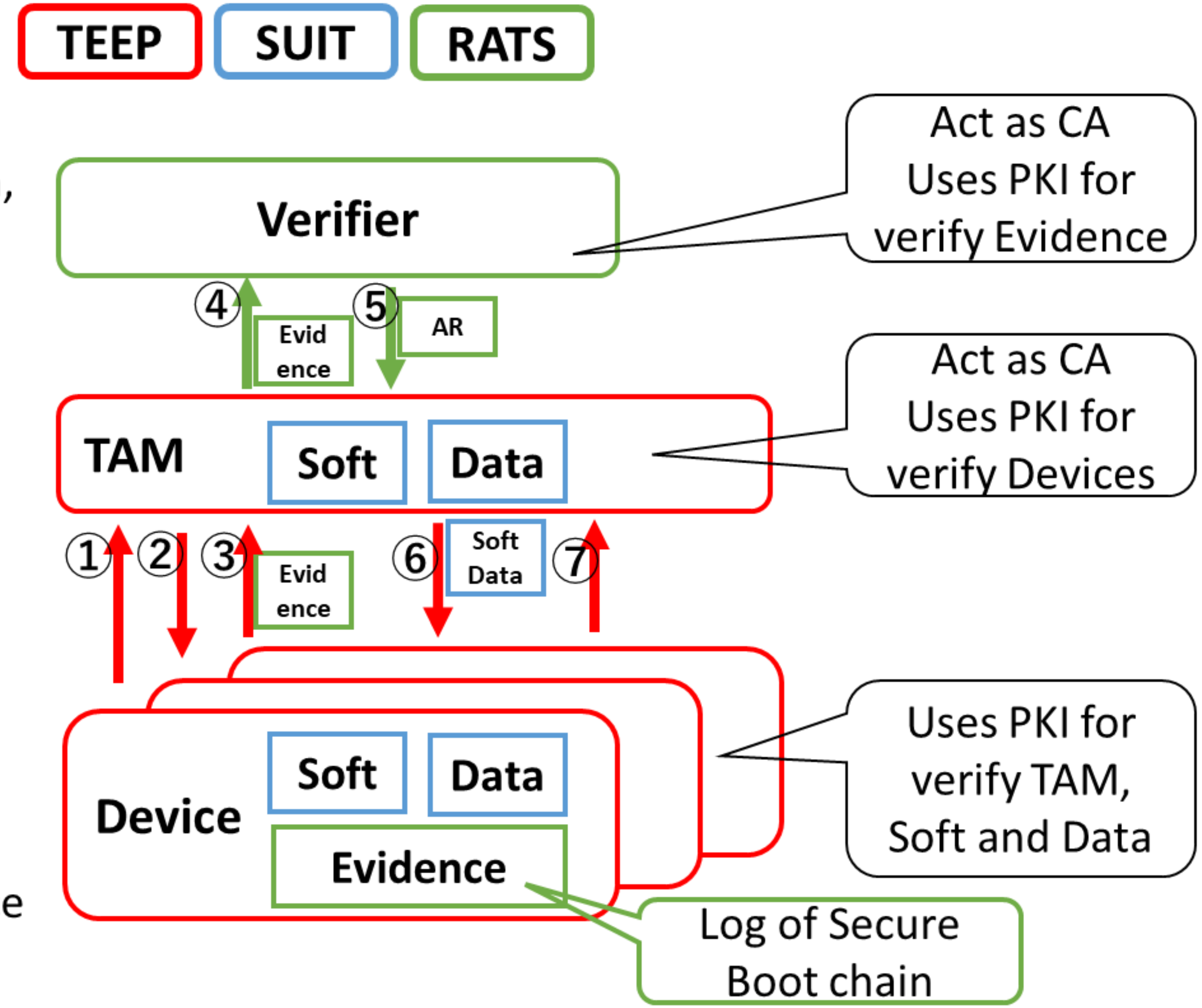
- Responsible area in colors

①② TAM request Device information, Currently installed Soft/Data, supported PKI algorithms, etc.

③④ Sends Evidence of Device to Verifier though TAM.
Evidence contain Log of Secure Boot, Firmware hash, Device key, etc.

⑤ Verifier returns result of checking Evidence as Attestation Result (AR)

⑥⑦ If the AR confirms Device is not hacked, TAM sends Soft/Data to Device



Proprietary implementations in the market

- There are many similar features implemented proprietary in the market. Some example.

  - Automotive: Sending unlock key for Quick Charge after customer paying option
  - Game console: Downloading game App and OTA from Console server
  - Test Equipment: Enabling unlock key for enabling Serial Decode features and Upgrading Sampling rate from the Vendors server
  - Surveillance Camera: Installing dedicated App on camera when service Personalization installs camera at home after customer subscribe the service
  - Healthcare terminal: Updating patients Personalization Data on the terminals at the hospital
  - Video HDD recorder, Set-top box: Updating DRM library or DRM crypto key

Benefits of TEEP/SUIT/RATS vs proprietary implementations

- Proprietary implementation may not use publicly trusted protocol, methodology and cryptographic algorithms
- The Server and Devices may be manufactured by different vendors and still would like to have portability
- Protocol and mechanism defined by authorized organization as IETF provides secure and trustful guidance to all vendors with interoperability
- Improve security level of IoT devices connected on Internet
- Enable IoT business to use Public Certificate Authority

Remarks of assumption on TEEP

- TEE is used as one of the methods of hardware tamper resistance to improve protecting TEEP Protocol transactions, integrity of software stack in TEEP Devices, assuring Secure Boot etc.

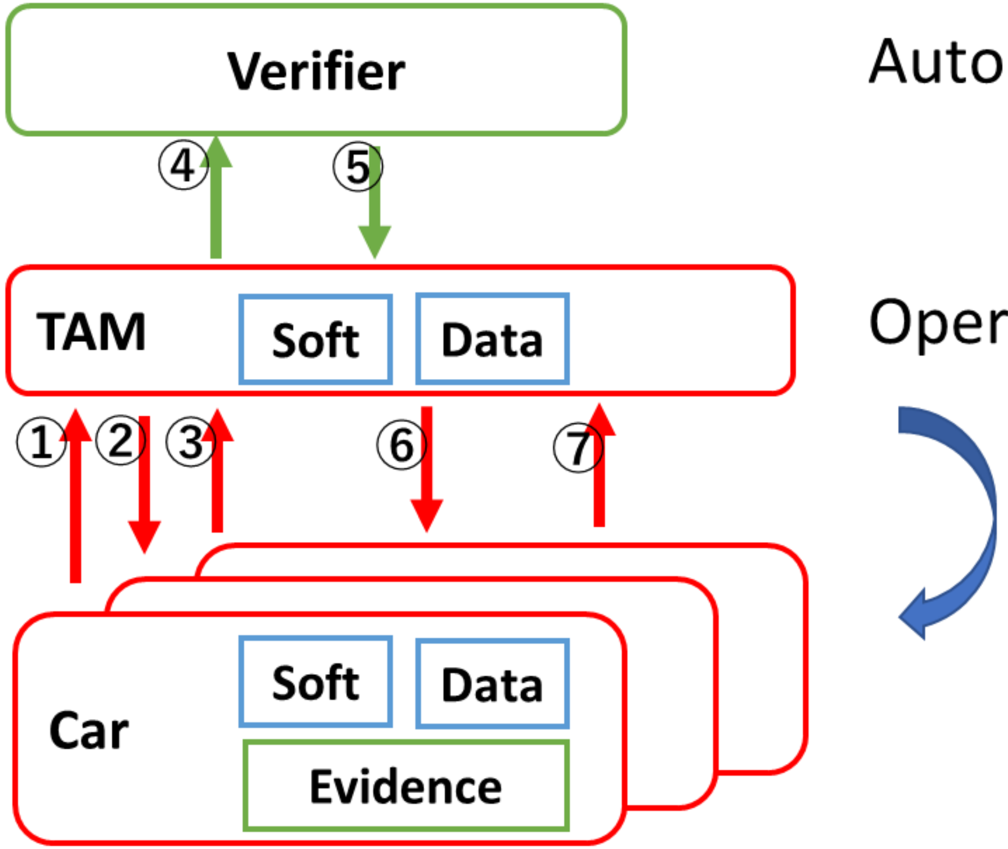
- However, the hardware implementation of TEE hardware support varies among different hardware from none to highly integrated in the CPU.

- TEEP is defined as agnostic of TEE hardware implementation.

- The current state of consciousness about contents of Evidence to be sent from Device to Verifier, are log of Secure Boot, hash values of TEEP software stacks to be verified the integrity of Device at the Verifier.

Use cases of TEEP, SUITS, RATS (1/6)

- Automotive



Automotive Manufacture

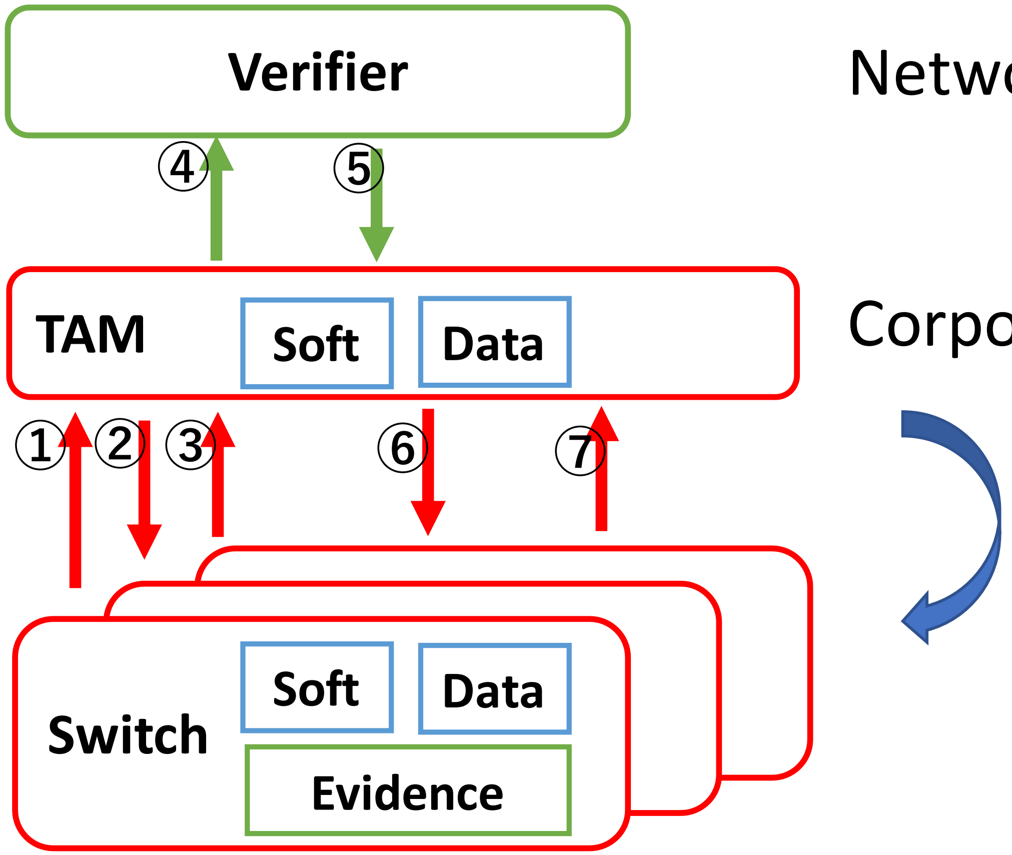
Operators

Usage

- Unlock Quick Charge
- OTA
- Remote monitoring compromised cars
- Remote telemetry acquisition

Use cases of TEEP, SUITS, RATS (2/6)

- Network Equipment Vendors



Network Equipment Manage Server

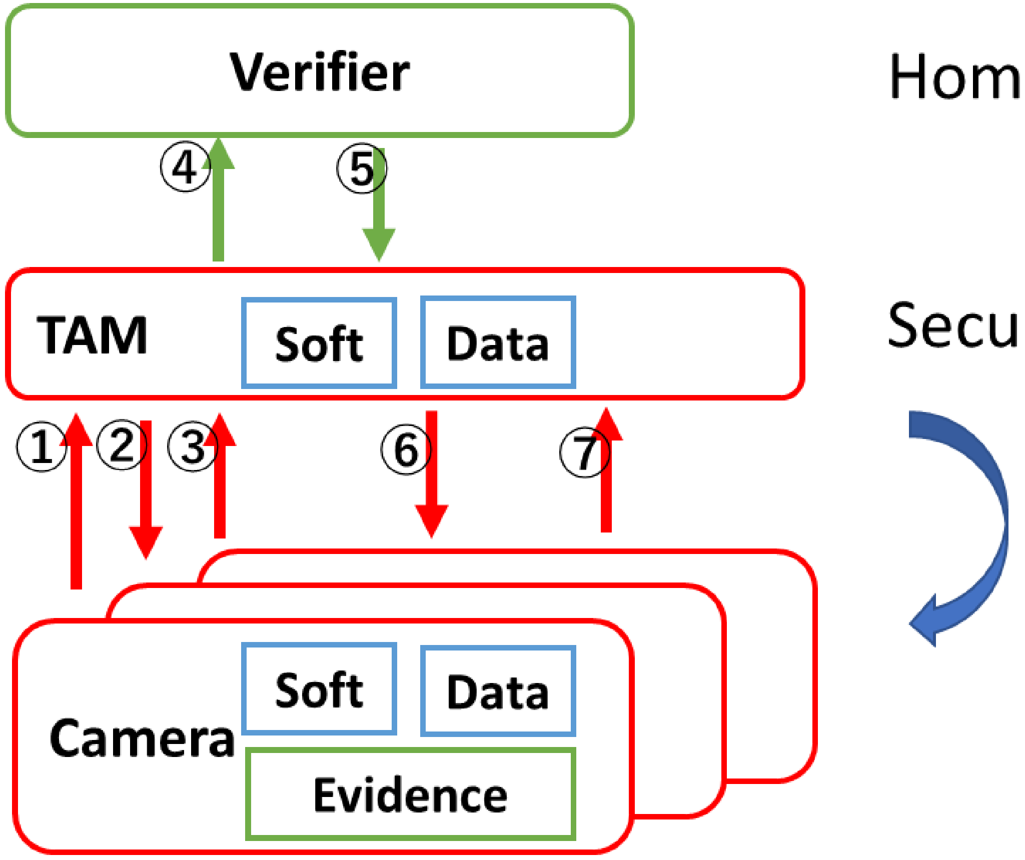
Corporate IT department server

Usage

- Update CA certificate
- OTA
- Disable compromised device

Use cases of TEEP, SUITS, RATS (3/6)

- Home Security Appliances



Home Security Service provider

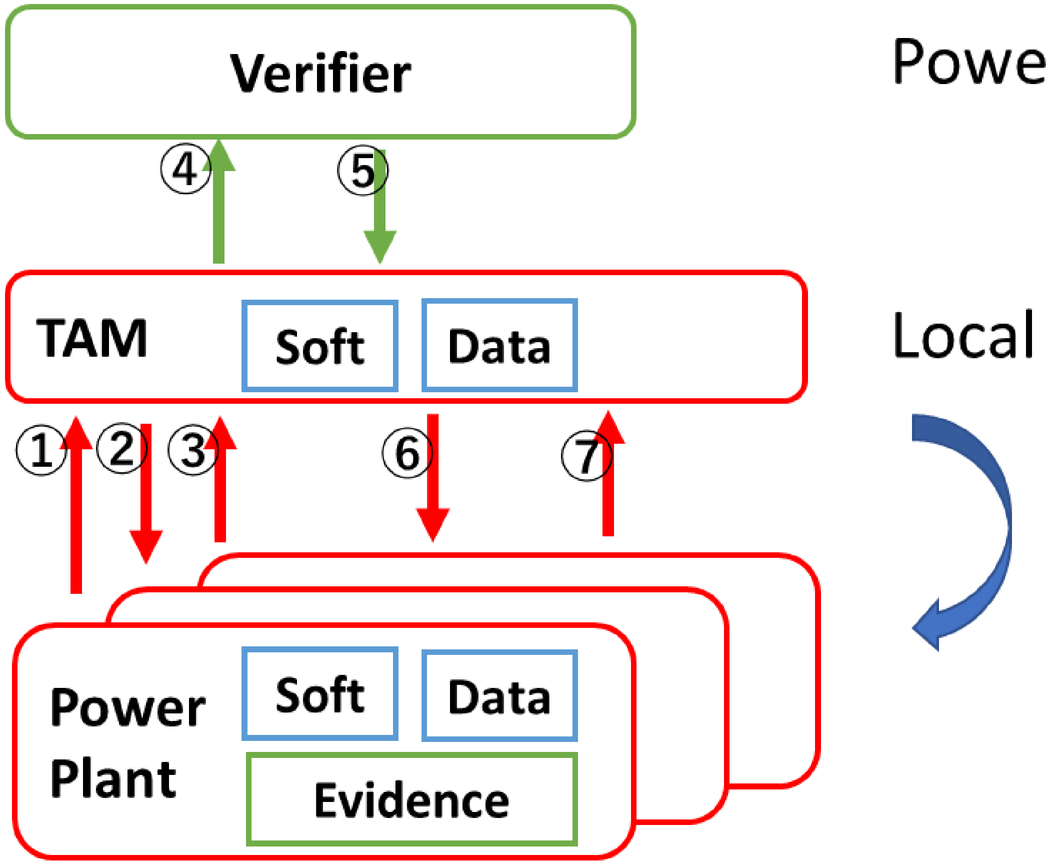
Security Camera Vendor

Usage

- Install security service app when customer subscribes
- OTA
- Disable compromised device

Use cases of TEEP, SUITS, RATS (4/6)

- Electric Power Plants



Power Plant Vendors

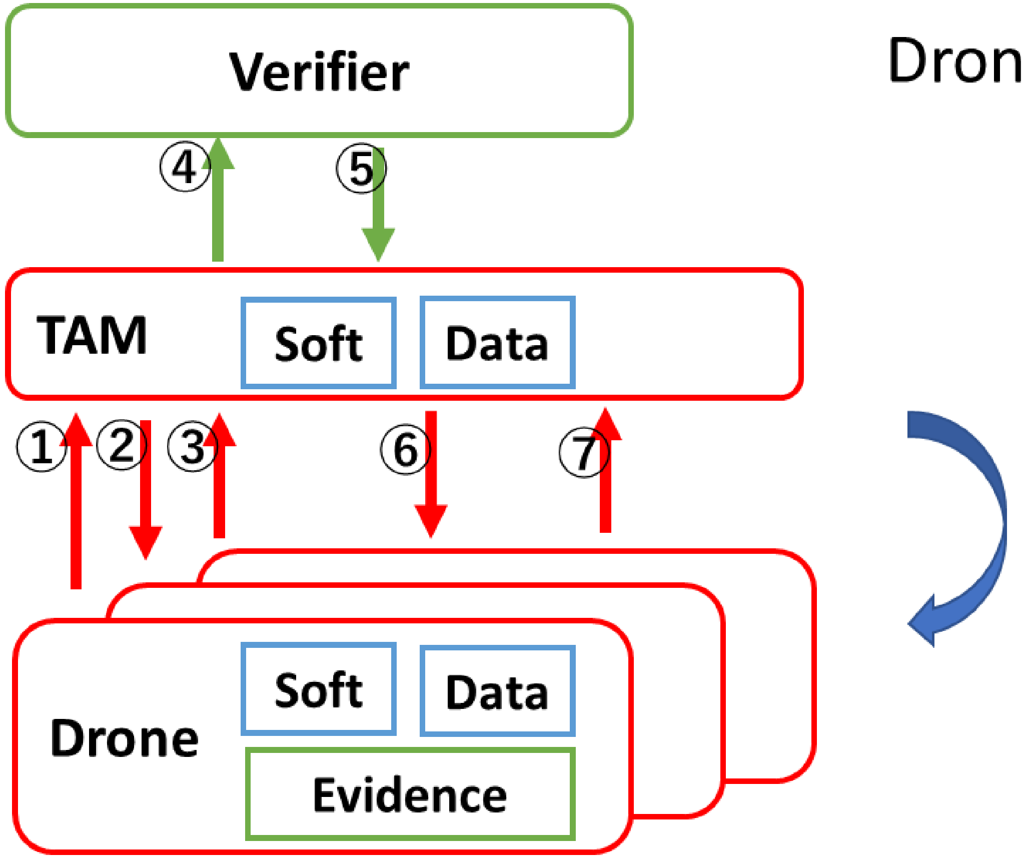
Local Government Power Mgmt Server

Usage

- Install security service app for country emergency
- Shut down power plants when a plant is in danger

Use cases of TEEP, SUITS, RATS (5/6)

- Drone



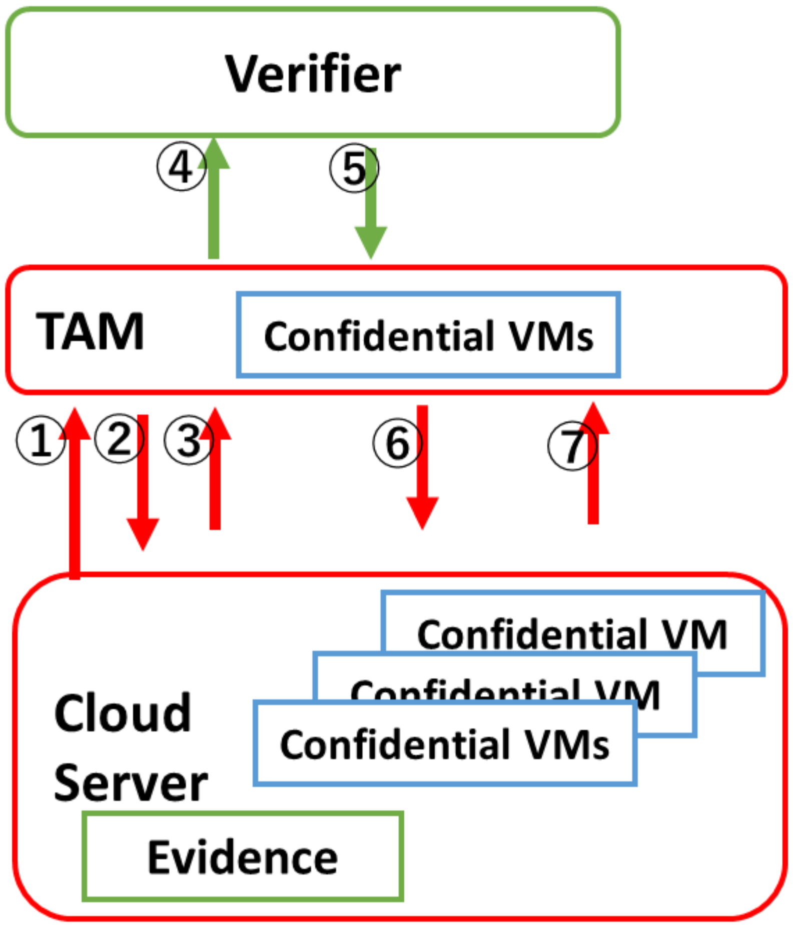
Drone Vendors

Usage

- Install Drone ID app for drone registration
- Disable drone when it falls into enemy hands

Use cases of TEEP, SUITS, RATS (6/6)

- Confidential Computing



Cloud Vendor, Distro Vendors

Cloud Vendor’s, VM orchestration server

Usage

- Install/Update/Delete Confidential VMs which can not read from Host CPU
- Confidentiality of User’s data inside VM is technically assured

Current status, what is remaining for RFC

- TEEP draft status
  - Almost WG last call, the draft is in stable status

- TEEP Protocol draft depends on SUIT and RATS drafts which are not RFC yet

I-D.ietf-rats-eat:

I-D.ietf-rats-reference-interaction-models:

I-D.ietf-suit-manifest:

I-D.ietf-suit-mti:

I-D.ietf-suit-trust-domains:

I-D.ietf-suit-report:

Require all I-D above to be RFC for TEEP Protocol to become RFC

Estimation is one and a half years to complete

Supply Chain Security and RATS, COSE

- Objective of Supply Chain Integrity, Transparency and Trust (SCITT) initiative
  - Assure trustworthy operation of Software Supply Chain systems

- SCITT is based on RATS and COSE

- RATS and COSE plays key role on SCITT