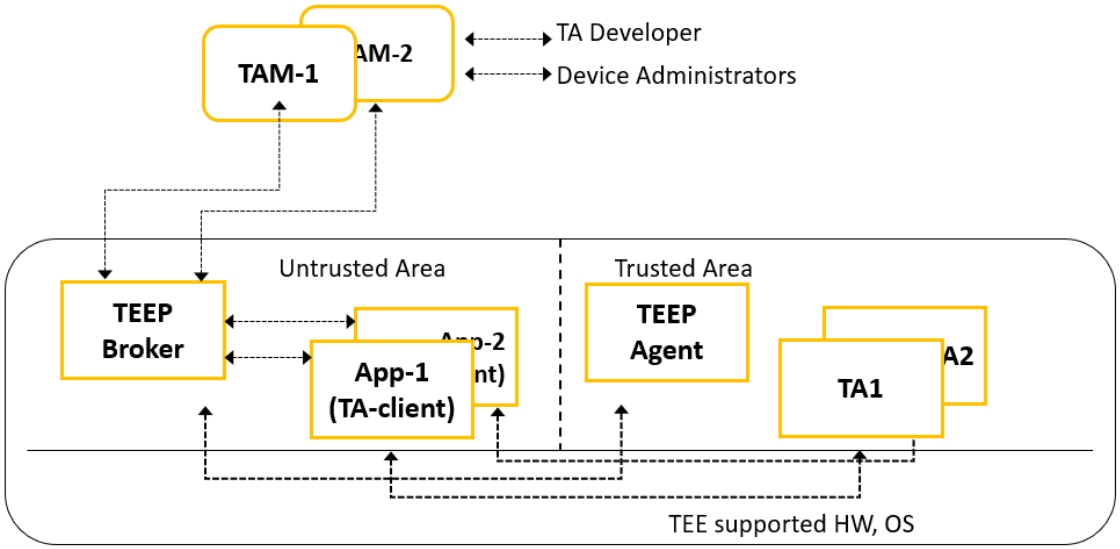
TEEP-DEVICE

The National Institute of Advanced Industrial Science and Technology

2022-02-08

1 Overview of TEEP-Device

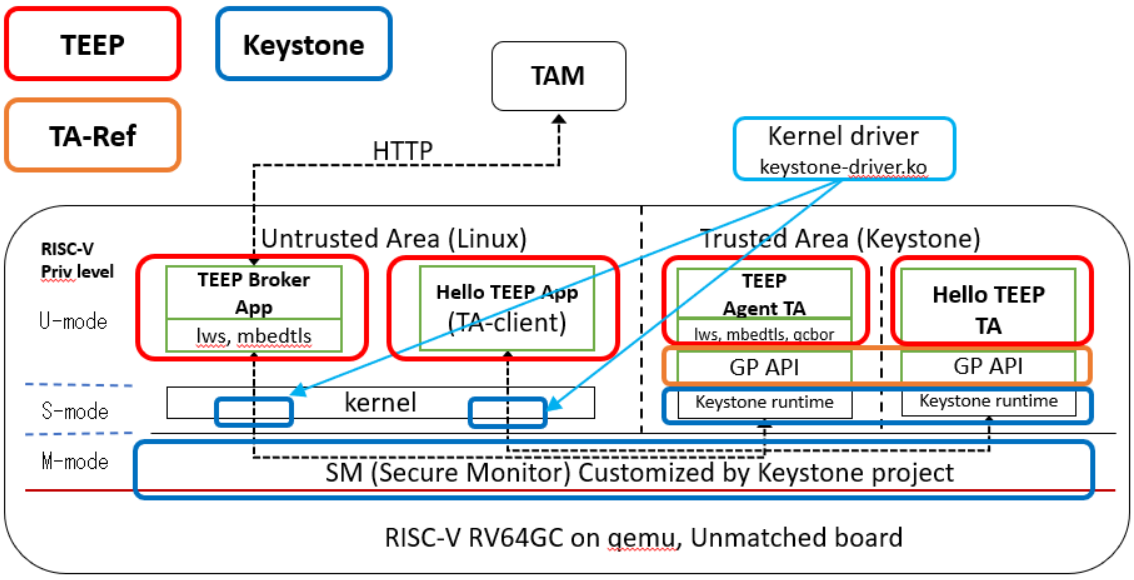


1.1 Features of TEEP-Device

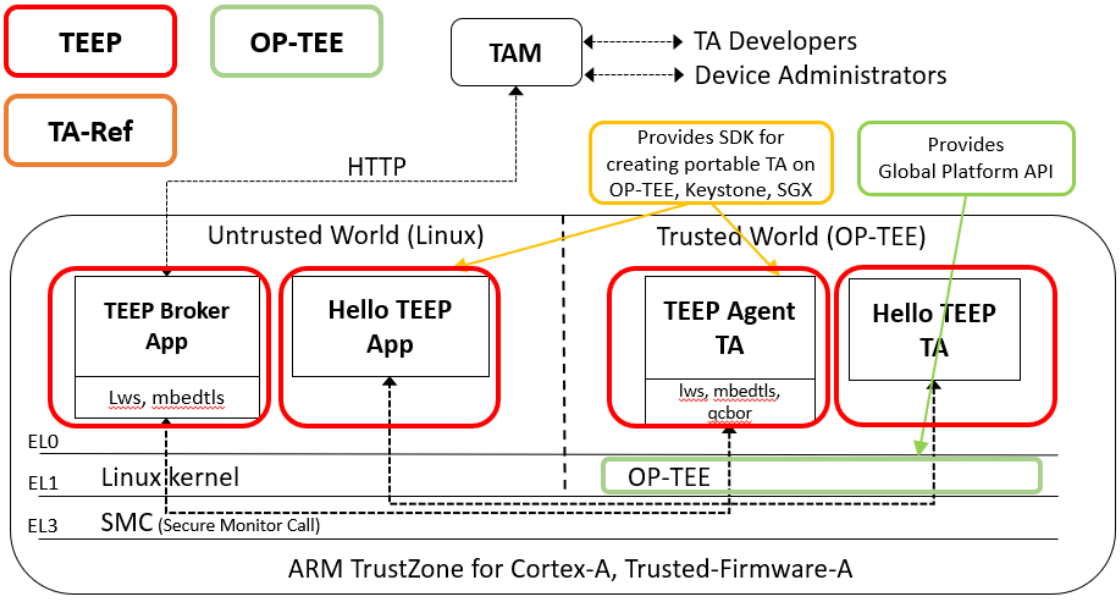
- AIST will prepare

1.2 Components of TEEP-device and TA-Ref

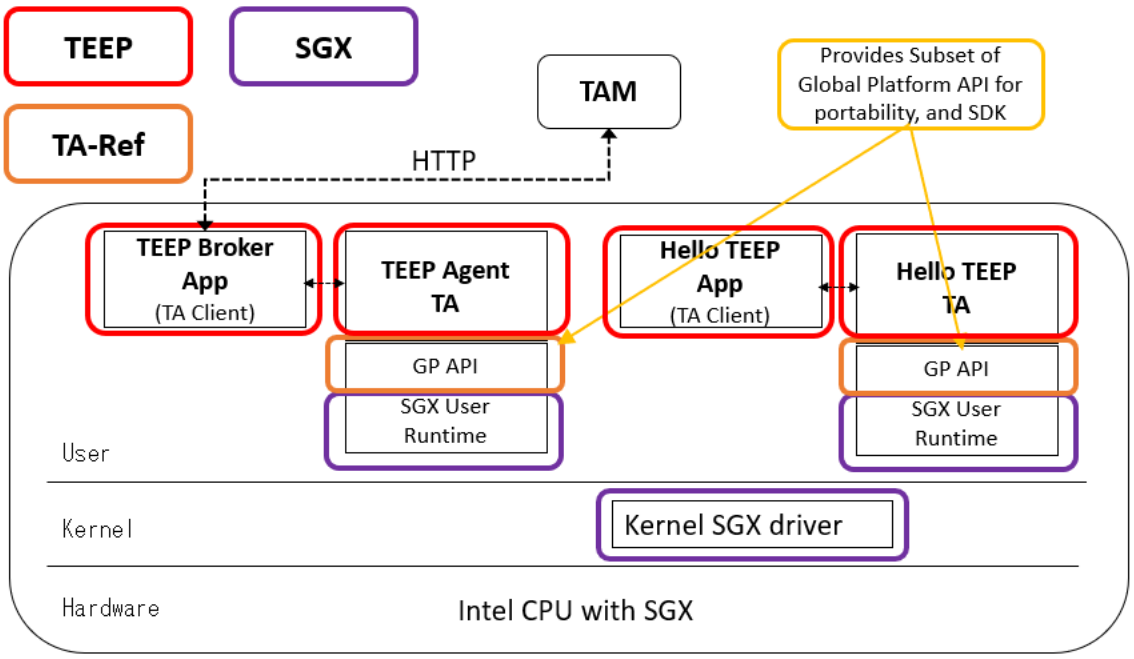
1.2.1 TEEP-device and TA-Ref Components on Keystone



1.2.2 TEEP-device and TA-Ref Components on OP-TEE



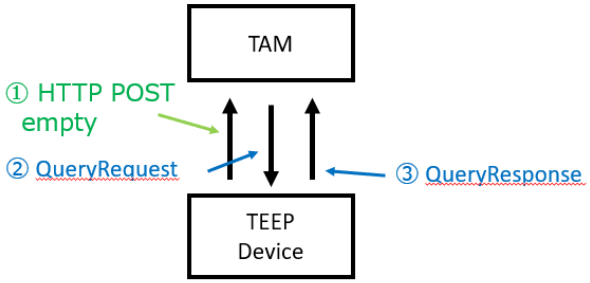
1.2.3 TEEP-device and TA-Ref Components on SGX



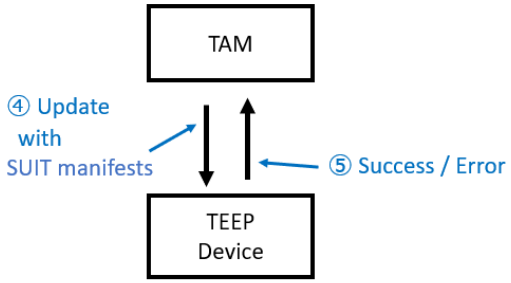
2 TEEP-DEVICE Operations

Four TEEP messages

- QueryRequest Message
- QueryResponse Message
- Update Message <- contains SUIT manifest
- Success Message / Error Message



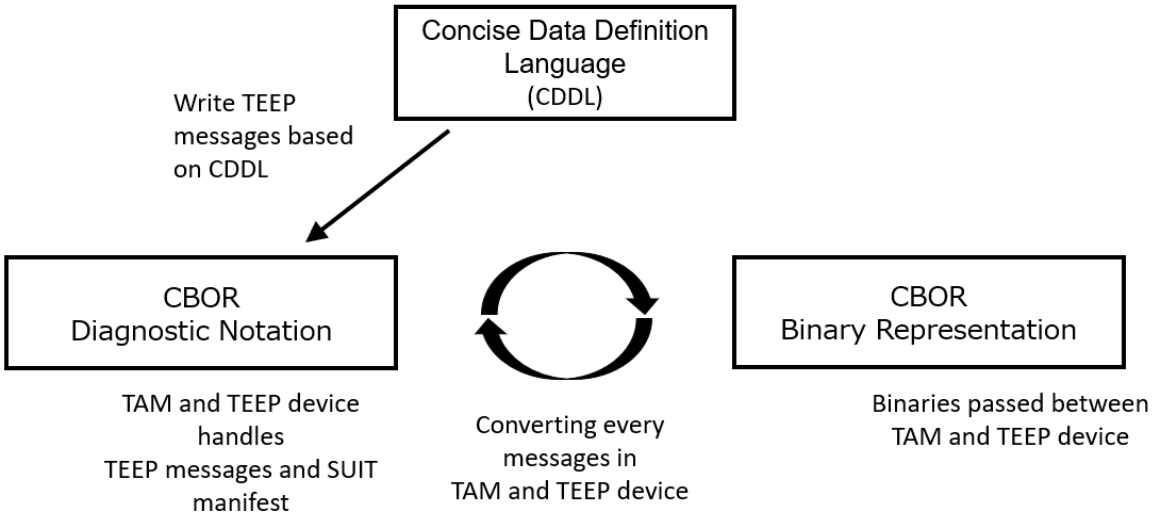
Exchange, Installed Trusted Components
Supported SUIT commands, Cipher suites



TAM sends Trusted Components with / or
associated SUIT manifests

3 CBOR in TEEP-Device

3.1 Three format representations in TEEP and SUIT



3.2 TEEP message format examples

```
D.1.1.  D.1.1.  CBOR Diagnostic Notation
/ query-request = /
[
  1,  / type : TEEP-TYPE-query-request = 1 (uint (0..23)) /
  / options : /
  {
    20 : 0xa0a1a2a3a4a5a6a7a8a9aaabacadaeaf,
           / token = 20 (mapkey) :
             h'a0a1a2a3a4a5a6a7a8a9aaabacadaeaf' (bstr .size
             generated by TAM /
    1 : [ 1 ], / supported-cipher-suites = 1 (mapkey) :
                 TEEP-AES-CCM-16-64-128-HMAC256--256-X25519-E
                 [ 1 ] (array of .within uint .size 4) /
    3 : [ 0 ] / version = 3 (mapkey) :
                 [ 0 ] (array of .within uint .size 4) /
  },
  3   / data-item-requested :
        attestation | trusted-components = 3 (.within uint .s
]
```

```
D.1.2.  D.1.2.  CBOR Binary Representation

  83                    # array(3)
    01                  # unsigned(1) uint (0..23)
    A4                  # map(4)
      14                # unsigned(20) uint (0..23)
      4F                # bytes(16) (8..64)
        A0A1A2A3A4A5A6A7A8A9AAABACADAEAF
      01                # unsigned(1) uint (0..23)
      81                # array(1)
        01              # unsigned(1) within uint .size 4
      03                # unsigned(3) uint (0..23)
      81                # array(1)
        00              # unsigned(0) within uint .size 4
      04                # unsigned(4) uint (0..23)
      43                # bytes(3)
        010203          # "¥x01¥x02¥x03"
    03                  # unsigned(3) .within uint .size 8
```

3.3 SUIT message format examples

```
E.2.  Example 2: SUIT Manifest including the Trusted Component Binary

   ### CBOR Diagnostic Notation of SUIT Manifest

/ SUIT_Envelope_Tagged / 107 ( {
  / suit-authentication-wrapper / 2: << [
    << [
      / suit-digest-algorithm-id: / -16 / cose-alg-sha256 /,
      / suit-digest-bytes: / h'C8363BDF3DCF68F0234A9DD320C2FEA72DE68F46AAE7CE700AFF
    ] >>,
    << / COSE_Sign1_Tagged / 18 ( [
      / protected: / << {
        / algorithm-id / 1: -7 / ES256 /
      } >>,
      / unprotected: / {},
      / payload: / null,
      / signature: / h'E0D2973A7B7185BBDA108458FB68EFAF65CDC
    ] ) >>
  ] >>,
  / suit-integrated-payload / "#tc": h'48656C6C6F2C205365637
  / suit-manifest / 3: << {
    / suit-manifest-version / 1: 1,
    / suit-manifest-sequence-number / 2: 3,
    / suit-common / 3: << {
      / suit-components / 2: [
        [
          h'544545502D446576696365',          / "TEEP-Devic
          h'5365637572654653',                / "SecureFS"
          h'8D82573A926D4754935332DC29997F74', / tc-uuid /
          h'7461'                             / "ta" /
```

```
E.2.1.  CBOR Binary Representation

D8 6B                                    # tag(107) / SUIT_Envelope_Tagged /
   A3                                    # map(3)
      02                                 # unsigned(2) / suit-authentication-wrapper /
      58 73                              # bytes(115)
         82                              # array(2)
            58 24                        # bytes(36)
               82                        # array(2)
                  2F                     # negative(15) / -16 = cose-alg-sha256 /
                  58 20                  # bytes(32)
                     C8363BDF3DCF68F0234A9DD320C2FEA72DE68F46AAE7CE700AFF87085516A335
            58 4A                        # bytes(74)
               D2                        # tag(18) / COSE_Sign1_Tagged /
                  84                     # array(4)
                     43                  # bytes(3)
                        A1               # map(1)
                           01            # unsigned(1) / algorithm-id /
                           26            # negative(6) / -7 = ES256 /
                     A0                  # map(0)
                     F6                  # primitive(22) / null /
                     58 40               # bytes(64)
                        E0D2973A7B7185BBDA108458FB68EFAF65CD031F2283E784129A95D4229F0EB11F8947D3E
```

4 TEEP-Device with docker

4.1 Preparation for Docker

For building teep-device with docker, it is required to install docker on Ubuntu.

For the first time users of docker, please have a look on https://docs.docker.com/engine/

The following installation steps is for Ubuntu 20.04

4.1.1 Installing Docker

```
$ sudo apt update

# Next, install a few prerequisite packages which let apt use packages over HTTPS:
$ sudo apt install apt-transport-https ca-certificates curl software-properties-common

# Then add the GPG key for the official Docker repository to your system:
$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

# Add the Docker repository to APT sources:
$ sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"

# This will also update our package database with the Docker packages from the newly added repo.
# Make sure you are about to install from the Docker repo instead of the default Ubuntu repo:
$ apt-cache policy docker-ce

#Finally, install Docker
$ sudo apt install docker-ce
```

4.1.2 Executing Docker without sudo

By default, the docker command can only be run the root user or by a user in the docker group, which is automatically created during Docker's installation process. If you attempt to run the docker command without prefixing it with sudo or without being in the docker group, you'll get an output like this:

```
docker: Cannot connect to the Docker daemon. Is the docker daemon running on this host?.
```

To avoid typing sudo whenever we run the docker command, add your username to the docker group.

```
$ sudo groupadd docker
$ sudo gpasswd -a $USER docker
# Logout and then log-in again to apply the changes to the group
```

After you logout and login, you can probably run the docker command without `sudo`

```
$ docker run hello-world
```

4.1.3 Create a docker network tamproto

A docker network named tamproto is required when we run teep device with ta-ref for all targets. The local network is required to connect with tamproto service running locally.

```
$ docker network create tamproto_default
```

4.2 Pre-built Docker Image details

The following are the docker images that has pre-built and tested binaries of teep-device with ta-ref. Since this images are already prepared and built already, you can start using it directly without building the teep-device again. Make sure you have account on docker-hub. If not please create one on `dockerhub.com`

Target	docker image
Keystone	trasioteam/teep-dev:keystone
OP-TEE	trasioteam/teep-dev:optee
Intel SGX	trasioteam/teep-dev:sgx
Tamproto	trasioteam/teep-dev:tamproto
Doxygen	trasioteam/teep-dev:doxygen

4.3 Prepartion for building teep-device on docker

4.3.1 Docker images details for building

If we need to build the teep-device, docker images with all necessary packages for building teep-device for all three targets are already available. The details are mentioned below.

Target	docker image
Keystone	trasioteam/taref-dev:keystone
OP-TEE	trasioteam/taref-dev:optee
Intel SGX	trasioteam/taref-dev:sgx
Doxygen	trasioteam/taref-dev:doxygen

4.4 Building teep-device with Docker

4.4.1 Building teep-device for Keystone with docker

Following commands are to be executed on Ubuntu 20.04.

```
# Clone the tamproto repo and checkout master branch
$ git clone https://192.168.100.100/rinkai/tamproto.git
$ cd tamproto
$ git checkout master
$ docker-compose build
$ docker-compose up &
$ cd ..
# Clone the teep-device repo and checkout suit-dev branch
$ git clone https://192.168.100.100/rinkai/teep-device.git
$ cd teep-device
$ git checkout suit-dev
# Sync and update the submodules
$ git submodule sync --recursive
$ git submodule update --init --recursive
$ cd ..

# Start the docker
$ docker run --network tamproto_default -it --rm -v $(pwd)/teep-device:/home/user/teep-device
      trasioteam/taref-dev:keystone-1.0.0
```

After you start the docker command, you will be logged-in inside the docker container. Following are the commands to be executed inside the docker

```
# [Inside docker image]

$ export TAREF_DIR=/home/user/ta-ref
$ . env/keystone.sh
$ make clean
$ make
$ cd ..

# Build and test
$ cd teep-device/
$ make
$ make test
```

```
make -C platform/keystone test
make[1]: Entering directory '/home/user/teep-device/platform/keystone'
curl http://tamproto_tam_api_1:8888/api/
{"key":"This is sample"}sed "s@http://localhost:8888@http://tamproto_tam_api_1:8888@"
      manifest/hello-ta.json >/home/user/teep-device/platform/keystone/build/hello-ta.json
suit-tool create -i /home/user/teep-device/platform/keystone/build/hello-ta.json -o
      /home/user/teep-device/platform/keystone/build/hello-ta.suit
create done. Serializing
suit-tool sign -m /home/user/teep-device/platform/keystone/build/hello-ta.suit -k
      ../../key/tc-provider-priv.pem -o /home/user/teep-device/platform/keystone/build/signed-hello-ta.suit
curl http://tamproto_tam_api_1:8888/panel/upload \
    -F "file=@/home/user/teep-device/platform/keystone/build/signed-hello-ta.suit;filename=integrated-payload-manifest.cbo
<!-- /*
* Copyright (c) 2020 SECOM CO., LTD. All Rights reserved.
*
* SPDX-License-Identifier: BSD-2-Clause
*/-->
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>TAM UI</title>
</head>
<style>
    table {
        border-collapse: collapse;
    }
    tr {
        border-bottom: dashed #c8c8cb;
    }
    th {
        background: #b4ebfa;
        padding: 0 1em;
    }
    td {
        text-align: center;
```

```
        padding: 0.5em;
    }
</style>
<body>
    <h1>TAM UI</h1>
    <hr>
    <!-- [object Object],[object Object],[object Object],[object Object],[object Object],[object
       Object],[object Object] -->
    <h2>TA Images</h2>
    <table>
        <tr>
            <th>File Name</th>
            <th>Download</th>
            <th>Delete</th>
        </tr>

        <tr>
            <td>dummy</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/dummy">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=dummy">Delete</a></td>
        </tr>

        <tr>
            <td>dummy2.ta</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/dummy2.ta">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=dummy2.ta">Delete</a></td>
        </tr>

        <tr>
            <td>integrated-payload-manifest.cbor</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/integrated-payload-manifest.cbor">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=integrated-payload-manifest.cbor">Delete</a></
        </tr>

        <tr>
            <td>integrated-payload-manifest_hex.txt</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/integrated-payload-manifest_hex.txt">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=integrated-payload-manifest_hex.txt">Delete</a
        </tr>

        <tr>
            <td>suit_manifest_exp1.cbor</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/suit_manifest_exp1.cbor">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=suit_manifest_exp1.cbor">Delete</a></td>
        </tr>

        <tr>
            <td>suit_manifest_expX.cbor</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/suit_manifest_expX.cbor">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=suit_manifest_expX.cbor">Delete</a></td>
        </tr>

        <tr>
            <td>tamproto.md</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/tamproto.md">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=tamproto.md">Delete</a></td>
        </tr>

        <!--
            <tr>
                <td>AAA</td>
                <td>Link</td>
                <td>Delete</td>
            </tr>
            -->
    </table>
    <h2>Upload Image</h2>
    <div>
        <form action="http://tamproto_tam_api_1:8888/panel//upload" method="POST"
       enctype="multipart/form-data">
            <input type="file" name="file">
            <button type="submit">Upload</button>
        </form>
    </div>
</body>
</html>curl http://tamproto_tam_api_1:8888/panel/upload \
    -F "file=@/home/user/teep-device/platform/keystone/build/hello-ta/hello-ta;filename=8d82573a-926d-4754-9353-32dc29997f
<!-- /*
* Copyright (c) 2020 SECOM CO., LTD. All Rights reserved.
*
* SPDX-License-Identifier: BSD-2-Clause
*/-->
<!DOCTYPE html>
<html>
<head>
```

```
    <meta charset="UTF-8">
    <title>TAM UI</title>
</head>
<style>
    table {
        border-collapse: collapse;
    }
    tr {
        border-bottom: dashed #c8c8cb;
    }
    th {
        background: #b4ebfa;
        padding: 0 1em;
    }
    td {
        text-align: center;
        padding: 0.5em;
    }
</style>
<body>
    <h1>TAM UI</h1>
    <hr>
    <!-- [object Object],[object Object],[object Object],[object Object],[object Object],[object
       Object],[object Object],[object Object] -->
    <h2>TA Images</h2>
    <table>
        <tr>
            <th>File Name</th>
            <th>Download</th>
            <th>Delete</th>
        </tr>

        <tr>
            <td>8d82573a-926d-4754-9353-32dc29997f74.ta</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/8d82573a-926d-4754-9353-32dc29997f74.ta">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=8d82573a-926d-4754-9353-32dc29997f74.ta">Delet
        </tr>

        <tr>
            <td>dummy</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/dummy">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=dummy">Delete</a></td>
        </tr>

        <tr>
            <td>dummy2.ta</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/dummy2.ta">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=dummy2.ta">Delete</a></td>
        </tr>

        <tr>
            <td>integrated-payload-manifest.cbor</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/integrated-payload-manifest.cbor">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=integrated-payload-manifest.cbor">Delete</a></
        </tr>

        <tr>
            <td>integrated-payload-manifest_hex.txt</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/integrated-payload-manifest_hex.txt">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=integrated-payload-manifest_hex.txt">Delete</a
        </tr>

        <tr>
            <td>suit_manifest_exp1.cbor</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/suit_manifest_exp1.cbor">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=suit_manifest_exp1.cbor">Delete</a></td>
        </tr>

        <tr>
            <td>suit_manifest_expX.cbor</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/suit_manifest_expX.cbor">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=suit_manifest_expX.cbor">Delete</a></td>
        </tr>

        <tr>
            <td>tamproto.md</td>
            <td><a href="http://tamproto_tam_api_1:8888/TAs/tamproto.md">Get</a></td>
            <td><a href="http://tamproto_tam_api_1:8888/panel/delete?taname=tamproto.md">Delete</a></td>
        </tr>

        <!--
            <tr>
                <td>AAA</td>
                <td>Link</td>
                <td>Delete</td>
```

```
            </tr>
            -->
    </table>
    <h2>Upload Image</h2>
    <div>
        <form action="http://tamproto_tam_api_1:8888/panel//upload" method="POST"
       enctype="multipart/form-data">
            <input type="file" name="file">
            <button type="submit">Upload</button>
        </form>
    </div>
</body>
</html>TAM_URL=http://tamproto_tam_api_1:8888 expect ./script/test.expect
spawn qemu-system-riscv64 -m 4G -bios /home/user/keystone/build/bootrom.build/bootrom.bin -nographic
       -machine virt -kernel /home/user/keystone/build/sm.build/platform/generic/firmware/fw_payload.elf
       -append console=ttyS0 ro root=/dev/vda cma=256M@0x00000000C0000000 -device
       virtio-blk-device,drive=hd0 -drive file=/home/user/keystone/build/buildroot.build/images/rootfs.ext2,format=raw,id=
       -netdev user,id=net0,net=192.168.100.1/24,dhcpstart=192.168.100.128,hostfwd=tcp::10032-:22
       -device virtio-net-device,netdev=net0 -device virtio-rng-pci
overriding secure boot ROM (file: /home/user/keystone/build/bootrom.build/bootrom.bin)
boot ROM size: 53869
fdt dumped at 57968
OpenSBI v0.8
   ____                    _____ ____ _____
  / __ \                  / ____|  _ \_   _|
 | |  | |_ __   ___ _ __ | (___ | |_) || |
 | |  | | '_ \ / _ \ '_ \ \___ \|  _ < | |
 | |__| | |_) |  __/ | | |____) | |_) || |_
  \____/| .__/ \___|_| |_|_____/|____/_____|
        | |
        |_|
Platform Name             : riscv-virtio,qemu
Platform Features         : timer,mfdeleg
Platform HART Count       : 1
Firmware Base             : 0x80000000
Firmware Size             : 204 KB
Runtime SBI Version       : 0.2
Domain0 Name              : root
Domain0 Boot HART         : 0
Domain0 HARTs             : 0*
Domain0 Region00          : 0x0000000080000000-0x000000008003ffff ()
Domain0 Region01          : 0x0000000000000000-0xffffffffffffffff (R,W,X)
Domain0 Next Address      : 0x0000000080200000
Domain0 Next Arg1         : 0x0000000082200000
Domain0 Next Mode         : S-mode
Domain0 SysReset          : yes
[SM] Initializing ... hart [0]
[SM] Keystone security monitor has been initialized!
Boot HART ID              : 0
Boot HART Domain          : root
Boot HART ISA             : rv64imafdcsu
Boot HART Features        : scounteren,mcounteren,time
Boot HART PMP Count       : 16
Boot HART PMP Granularity : 4
Boot HART PMP Address Bits: 54
Boot HART MHPM Count      : 0
Boot HART MHPM Count      : 0
Boot HART MIDELEG         : 0x0000000000000222
Boot HART MEDELEG         : 0x000000000000b109
[    0.000000] OF: fdt: Ignoring memory range 0x80000000 - 0x80200000
[    0.000000] Linux version 5.7.0-dirty (build-user@0285aa096bcc) (gcc version 10.2.0 (GCC), GNU ld
       (GNU Binutils) 2.35) #1 SMP Mon Jan 31 07:22:50 UTC 2022
[    0.000000] initrd not found or empty - disabling initrd
[    0.000000] Zone ranges:
[    0.000000]   DMA32    [mem 0x0000000080200000-0x00000000ffffffff]
[    0.000000]   Normal   [mem 0x0000000100000000-0x000000017fffffff]
[    0.000000] Movable zone start for each node
[    0.000000] Early memory node ranges
[    0.000000]   node   0: [mem 0x0000000080200000-0x000000017fffffff]
[    0.000000] Initmem setup node 0 [mem 0x0000000080200000-0x000000017fffffff]
[    0.000000] cma: Reserved 256 MiB at 0x00000000c0000000
[    0.000000] software IO TLB: mapped [mem 0xfbfff000-0xfffff000] (64MB)
[    0.000000] SBI specification v0.2 detected
[    0.000000] SBI implementation ID=0x1 Version=0x8
[    0.000000] SBI v0.2 TIME extension detected
[    0.000000] SBI v0.2 IPI extension detected
[    0.000000] SBI v0.2 RFENCE extension detected
[    0.000000] SBI v0.2 HSM extension detected
[    0.000000] riscv: ISA extensions acdfimsu
[    0.000000] riscv: ELF capabilities acdfim
[    0.000000] percpu: Embedded 17 pages/cpu s31784 r8192 d29656 u69632
[    0.000000] Built 1 zonelists, mobility grouping on.  Total pages: 1033735
[    0.000000] Kernel command line: console=ttyS0 ro root=/dev/vda cma=256M@0x00000000C0000000
[    0.000000] Dentry cache hash table entries: 524288 (order: 10, 4194304 bytes, linear)
[    0.000000] Inode-cache hash table entries: 262144 (order: 9, 2097152 bytes, linear)
```

```
[    0.000000] Sorting __ex_table...
[    0.000000] mem auto-init: stack:off, heap alloc:off, heap free:off
[    0.000000] Memory: 3783452K/4192256K available (6486K kernel code, 4184K rwdata, 4096K rodata,
      235K init, 318K bss, 146660K reserved, 262144K cma-reserved)
[    0.000000] Virtual kernel memory layout:
[    0.000000]       fixmap : 0xffffffcefee00000 - 0xffffffceff000000   (2048 kB)
[    0.000000]       pci io : 0xffffffceff000000 - 0xffffffcf00000000   (  16 MB)
[    0.000000]      vmemmap : 0xffffffcf00000000 - 0xffffffcfffffffff   (4095 MB)
[    0.000000]      vmalloc : 0xffffffd000000000 - 0xffffffdfffffffff   (65535 MB)
[    0.000000]       lowmem : 0xffffffe000000000 - 0xffffffe0ffe00000   (4094 MB)
[    0.000000] SLUB: HWalign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[    0.000000] rcu: Hierarchical RCU implementation.
[    0.000000] rcu:     RCU restricting CPUs from NR_CPUS=8 to nr_cpu_ids=1.
[    0.000000] rcu:     RCU debug extended QS entry/exit.
[    0.000000] rcu: RCU calculated value of scheduler-enlistment delay is 25 jiffies.
[    0.000000] rcu: Adjusting geometry for rcu_fanout_leaf=16, nr_cpu_ids=1
[    0.000000] NR_IRQS: 0, nr_irqs: 0, preallocated irqs: 0
[    0.000000] plic: mapped 53 interrupts with 1 handlers for 2 contexts.
[    0.000000] riscv_timer_init_dt: Registering clocksource cpuid [0] hartid [0]
[    0.000000] clocksource: riscv_clocksource: mask: 0xffffffffffffffff max_cycles: 0x24e6a1710,
      max_idle_ns: 440795202120 ns
[    0.000139] sched_clock: 64 bits at 10MHz, resolution 100ns, wraps every 4398046511100ns
[    0.003268] Console: colour dummy device 80x25
[    0.004510] Calibrating delay loop (skipped), value calculated using timer frequency.. 20.00
      BogoMIPS (lpj=40000)
[    0.004648] pid_max: default: 32768 minimum: 301
[    0.008142] Mount-cache hash table entries: 8192 (order: 4, 65536 bytes, linear)
[    0.008251] Mountpoint-cache hash table entries: 8192 (order: 4, 65536 bytes, linear)
[    0.032748] rcu: Hierarchical SRCU implementation.
[    0.034792] smp: Bringing up secondary CPUs ...
[    0.034885] smp: Brought up 1 node, 1 CPU
[    0.043732] devtmpfs: initialized
[    0.048633] random: get_random_u32 called from bucket_table_alloc.isra.0+0x4e/0x154 with
      crng_init=0
[    0.050882] clocksource: jiffies: mask: 0xffffffff max_cycles: 0xffffffff, max_idle_ns:
      7645041785100000 ns
[    0.051029] futex hash table entries: 256 (order: 2, 16384 bytes, linear)
[    0.058032] NET: Registered protocol family 16
[    0.106766] vgaarb: loaded
[    0.108138] SCSI subsystem initialized
[    0.109627] usbcore: registered new interface driver usbfs
[    0.109985] usbcore: registered new interface driver hub
[    0.110126] usbcore: registered new device driver usb
[    0.119911] clocksource: Switched to clocksource riscv_clocksource
[    0.133399] NET: Registered protocol family 2
[    0.137106] tcp_listen_portaddr_hash hash table entries: 2048 (order: 4, 81920 bytes, linear)
[    0.137406] TCP established hash table entries: 32768 (order: 6, 262144 bytes, linear)
[    0.138176] TCP bind hash table entries: 32768 (order: 8, 1048576 bytes, linear)
[    0.140751] TCP: Hash tables configured (established 32768 bind 32768)
[    0.141743] UDP hash table entries: 2048 (order: 5, 196608 bytes, linear)
[    0.142333] UDP-Lite hash table entries: 2048 (order: 5, 196608 bytes, linear)
[    0.143909] NET: Registered protocol family 1
[    0.146746] RPC: Registered named UNIX socket transport module.
[    0.146794] RPC: Registered udp transport module.
[    0.146810] RPC: Registered tcp transport module.
[    0.146826] RPC: Registered tcp NFSv4.1 backchannel transport module.
[    0.146913] PCI: CLS 0 bytes, default 64
[    0.152595] workingset: timestamp_bits=62 max_order=20 bucket_order=0
[    0.171645] NFS: Registering the id_resolver key type
[    0.172381] Key type id_resolver registered
[    0.172422] Key type id_legacy registered
[    0.172521] nfs4filelayout_init: NFSv4 File Layout Driver Registering...
[    0.173077] 9p: Installing v9fs 9p2000 file system support
[    0.174388] NET: Registered protocol family 38
[    0.174639] Block layer SCSI generic (bsg) driver version 0.4 loaded (major 253)
[    0.174745] io scheduler mq-deadline registered
[    0.174819] io scheduler kyber registered
[    0.182005] pci-host-generic 30000000.pci: host bridge /soc/pci@30000000 ranges:
[    0.182673] pci-host-generic 30000000.pci:       IO 0x0003000000..0x000300ffff -> 0x0000000000
[    0.183162] pci-host-generic 30000000.pci:      MEM 0x0040000000..0x007fffffff -> 0x0040000000
[    0.185545] pci-host-generic 30000000.pci: ECAM at [mem 0x30000000-0x3fffffff] for [bus 00-ff]
[    0.186497] pci-host-generic 30000000.pci: PCI host bridge to bus 0000:00
[    0.186684] pci_bus 0000:00: root bus resource [bus 00-ff]
[    0.186807] pci_bus 0000:00: root bus resource [io  0x0000-0xffff]
[    0.186827] pci_bus 0000:00: root bus resource [mem 0x40000000-0x7fffffff]
[    0.187630] pci 0000:00:00.0: [1b36:0008] type 00 class 0x060000
[    0.190793] pci 0000:00:01.0: [1af4:1005] type 00 class 0x00ff00
[    0.191116] pci 0000:00:01.0: reg 0x10: [io  0x0000-0x001f]
[    0.191293] pci 0000:00:01.0: reg 0x20: [mem 0x00000000-0x00003fff 64bit pref]
[    0.193360] pci 0000:00:01.0: BAR 4: assigned [mem 0x40000000-0x40003fff 64bit pref]
[    0.193639] pci 0000:00:01.0: BAR 0: assigned [io  0x0000-0x001f]
[    0.199034] virtio-pci 0000:00:01.0: enabling device (0000 -> 0003)
[    0.261614] Serial: 8250/16550 driver, 4 ports, IRQ sharing disabled
[    0.267751] printk: console [ttyS0] disabled
[    0.268616] 10000000.uart: ttyS0 at MMIO 0x10000000 (irq = 2, base_baud = 230400) is a 16550A
```

```
[    0.295219] printk: console [ttyS0] enabled
[    0.301931] [drm] radeon kernel modesetting enabled.
[    0.310973] random: fast init done
[    0.312161] random: crng init done
[    0.322438] loop: module loaded
[    0.336498] virtio_blk virtio0: [vda] 122880 512-byte logical blocks (62.9 MB/60.0 MiB)
[    0.336799] vda: detected capacity change from 0 to 62914560
[    0.359644] libphy: Fixed MDIO Bus: probed
[    0.365061] e1000e: Intel(R) PRO/1000 Network Driver - 3.2.6-k
[    0.365247] e1000e: Copyright(c) 1999 - 2015 Intel Corporation.
[    0.365739] ehci_hcd: USB 2.0 'Enhanced' Host Controller (EHCI) Driver
[    0.365959] ehci-pci: EHCI PCI platform driver
[    0.366248] ehci-platform: EHCI generic platform driver
[    0.366614] ohci_hcd: USB 1.1 'Open' Host Controller (OHCI) Driver
[    0.366916] ohci-pci: OHCI PCI platform driver
[    0.367265] ohci-platform: OHCI generic platform driver
[    0.369838] usbcore: registered new interface driver uas
[    0.370177] usbcore: registered new interface driver usb-storage
[    0.371710] mousedev: PS/2 mouse device common for all mice
[    0.373699] usbcore: registered new interface driver usbhid
[    0.373889] usbhid: USB HID core driver
[    0.375880] NET: Registered protocol family 10
[    0.382090] Segment Routing with IPv6
[    0.382604] sit: IPv6, IPv4 and MPLS over IPv4 tunneling driver
[    0.384985] NET: Registered protocol family 17
[    0.386370] 9pnet: Installing 9P2000 support
[    0.386758] Key type dns_resolver registered
[    0.402943] EXT4-fs (vda): mounting ext2 file system using the ext4 subsystem
[    0.411203] EXT4-fs (vda): mounted filesystem without journal. Opts: (null)
[    0.411696] VFS: Mounted root (ext2 filesystem) readonly on device 254:0.
[    0.414508] devtmpfs: mounted
[    0.451434] Freeing unused kernel memory: 232K
[    0.452285] Run /sbin/init as init process
[    0.616587] EXT4-fs (vda): re-mounted. Opts: (null)
Starting syslogd: OK
Starting klogd: OK
Running sysctl: OK
Saving random seed: OK
Starting network: udhcpc: started, v1.32.0
udhcpc: sending discover
udhcpc: sending select for 192.168.100.128
udhcpc: lease of 192.168.100.128 obtained, lease time 86400
deleting routers
adding dns 192.168.100.3
OK
Starting dropbear sshd: OK
Welcome to Buildroot
buildroot login: root
Password: sifive
PS1='##"## '
# PS1='##"## '
#### insmod keystone-driver.ko || echo 'err"or'
[    4.980033] keystone_driver: loading out-of-tree module taints kernel.
[    4.987299] keystone_enclave: keystone enclave v1.0.0
#### cd /root/teep-device
#### ls -l
total 1359
-rwxr-xr-x    1 root     root         98088 Feb  8  2022 eyrie-rt
-rwxr-xr-x    1 root     root        437480 Feb  8  2022 hello-app
-rwxr-xr-x    1 root     root        142432 Feb  8  2022 hello-ta
-rwxr-xr-x    1 root     root        247416 Feb  8  2022 teep-agent-ta
-rwxr-xr-x    1 root     root        470568 Feb  8  2022 teep-broker-app
#### ./hello-app hello-ta eyrie-rt
[debug] UTM : 0xffffffff80000000-0xffffffff80100000 (1024 KB) (boot.c:127)
[debug] DRAM: 0x179800000-0x179c00000 (4096 KB) (boot.c:128)
[debug] FREE: 0x1799bb000-0x179c00000 (2324 KB), va 0xffffffff001bb000 (boot.c:133)
[debug] eyrie boot finished. drop to the user land ... (boot.c:172)
hello TA
#### ./hello-app 8d82573a-926d-4754-9353-32dc29997f74.ta eyrie-rt
[Keystone SDK] /home/user/keystone/sdk/src/host/ElfFile.cpp:26 : file does not exist -
       8d82573a-926d-4754-9353-32dc29997f74.ta
[Keystone SDK] /home/user/keystone/sdk/src/host/Enclave.cpp:209 : Invalid enclave ELF
./hello-app: Unable to start enclave
#### ./teep-broker-app --tamurl http://tamproto_tam_api_1:8888/api/tam_cbor
teep-broker.c compiled at Feb  8 2022 05:59:40
uri = http://tamproto_tam_api_1:8888/api/tam_cbor, cose=0, talist=
[debug] UTM : 0xffffffff80000000-0xffffffff80100000 (1024 KB) (boot.c:127)
[debug] DRAM: 0x179800000-0x179c00000 (4096 KB) (boot.c:128)
[debug] FREE: 0x1799c6000-0x179c00000 (2280 KB), va 0xffffffff001c6000 (boot.c:133)
[debug] eyrie boot finished. drop to the user land ... (boot.c:172)
[1970/01/01 00:00:07:7731] NOTICE: POST: http://tamproto_tam_api_1:8888/api/tam_cbor
[1970/01/01 00:00:07:7746] NOTICE: (hexdump: zero length)
[1970/01/01 00:00:07:7782] NOTICE: created client ssl context for default
[1970/01/01 00:00:07:7797] NOTICE: http://tamproto_tam_api_1:8888/api/tam_cbor
[1970/01/01 00:00:08:0379] NOTICE:
```

```
[1970/01/01 00:00:08:0387] NOTICE: 0000: 83 01 A5 01 81 01 03 81 00 04 43 01 02 05 14 48
       ..........C....H
[1970/01/01 00:00:08:0396] NOTICE: 0010: 77 77 77 77 77 77 77 77 15 81 00 02
       wwwwwwww....
[1970/01/01 00:00:08:0406] NOTICE:
[1970/01/01 00:00:08:0529] NOTICE: POST: http://tamproto_tam_api_1:8888/api/tam_cbor
[1970/01/01 00:00:08:0544] NOTICE:
[1970/01/01 00:00:08:0550] NOTICE: 0000: 82 02 A4 14 48 77 77 77 77 77 77 77 77 08 80 0E
       ....Hwwwwwwww...
[1970/01/01 00:00:08:0556] NOTICE: 0010: 80 0F 80                                        ...

[1970/01/01 00:00:08:0565] NOTICE:
[1970/01/01 00:00:08:0591] NOTICE: created client ssl context for default
[1970/01/01 00:00:08:0697] NOTICE: http://tamproto_tam_api_1:8888/api/tam_cbor
[1970/01/01 00:00:08:1965] NOTICE:
[1970/01/01 00:00:08:1974] NOTICE: 0000: 82 03 A2 0A 81 59 01 66 D8 6B A2 02 58 73 82 58
       .....Y.f.k..Xs.X
[1970/01/01 00:00:08:1987] NOTICE: 0010: 24 82 2F 58 20 63 70 90 82 1C BB B2 67 95 42 78    $./X
       cp.....g.Bx
[1970/01/01 00:00:08:1998] NOTICE: 0020: 7B 49 F4 5E 14 AF 0C BF AD 9E F4 A4 F0 B3 42 B9
       {I.^..........B.
[1970/01/01 00:00:08:2010] NOTICE: 0030: 23 35 56 05 AF 58 4A D2 84 43 A1 01 26 A0 F6 58
       #5V..XJ..C..&..X
[1970/01/01 00:00:08:2020] NOTICE: 0040: 40 55 43 31 6F D5 98 E6 CA 53 EE 38 3D AD 90 8C
       @UC1o....S.8=...
[1970/01/01 00:00:08:2031] NOTICE: 0050: C6 10 DB 9F D6 F7 4F BA BF C4 CD 28 79 CA 3C C7
       ......O....(y.<.
[1970/01/01 00:00:08:2045] NOTICE: 0060: 6F 72 D7 3D A7 DD 76 45 E6 D7 E9 55 17 D1 82 F5
       or.=..vE...U....
[1970/01/01 00:00:08:2055] NOTICE: 0070: 64 9F 10 0D BD 49 97 0A 7B 62 C9 72 27 A6 CE CA
       d....I..{b.r'...
[1970/01/01 00:00:08:2064] NOTICE: 0080: 68 03 58 EA A5 01 01 02 01 03 58 86 A2 02 81 84
       h.X.......X.....
[1970/01/01 00:00:08:2073] NOTICE: 0090: 4B 54 45 45 50 2D 44 65 76 69 63 65 48 53 65 63
       KTEEP-DeviceHSec
[1970/01/01 00:00:08:2082] NOTICE: 00A0: 75 72 65 46 53 50 8D 82 57 3A 92 6D 47 54 93 53
       ureFSP..W:.mGT.S
[1970/01/01 00:00:08:2091] NOTICE: 00B0: 32 DC 29 99 7F 74 42 74 61 04 58 56 86 14 A4 01
       2.)..tBta.XV....
[1970/01/01 00:00:08:2100] NOTICE: 00C0: 50 FA 6B 4A 53 D5 AD 5F DF BE 9D E6 63 E4 D4 1F
       P.kJS.._....c...
[1970/01/01 00:00:08:2109] NOTICE: 00D0: FE 02 50 14 92 AF 14 25 69 5E 48 BF 42 9B 2D 51
       ..P....%i^H.B.-Q
[1970/01/01 00:00:08:2117] NOTICE: 00E0: F2 AB 45 03 58 24 82 2F 58 20 00 11 22 33 44 55
       ..E.X$./X .."3DU
[1970/01/01 00:00:08:2128] NOTICE: 00F0: 66 77 88 99 AA BB CC DD EE FF 01 23 45 67 89 AB
       fw.........#Eg..
[1970/01/01 00:00:08:2136] NOTICE: 0100: CD EF FE DC BA 98 76 54 32 10 0E 19 87 D0 01 0F
       ......vT2.......
[1970/01/01 00:00:08:2143] NOTICE: 0110: 02 0F 09 58 54 86 13 A1 15 78 4A 68 74 74 70 3A
       ...XT....xJhttp:
[1970/01/01 00:00:08:2151] NOTICE: 0120: 2F 2F 74 61 6D 70 72 6F 74 6F 5F 74 61 6D 5F 61
       //tamproto_tam_a
[1970/01/01 00:00:08:2158] NOTICE: 0130: 70 69 5F 31 3A 38 38 38 38 2F 54 41 73 2F 38 64
       pi_1:8888/TAs/8d
[1970/01/01 00:00:08:2170] NOTICE: 0140: 38 32 35 37 33 61 2D 39 32 36 64 2D 34 37 35 34
       82573a-926d-4754
[1970/01/01 00:00:08:2177] NOTICE: 0150: 2D 39 33 35 33 2D 33 32 64 63 32 39 39 39 37 66
       -9353-32dc29997f
[1970/01/01 00:00:08:2184] NOTICE: 0160: 37 34 2E 74 61 15 02 03 0F 0A 43 82 03 0F 14 48
       74.ta.....C....H
[1970/01/01 00:00:08:2191] NOTICE: 0170: AB A1 A2 A3 A4 A5 A6 A7                         ........

[1970/01/01 00:00:08:2197] NOTICE:
command: 20
execute suit-set-parameters
command: 1
execute suit-condition-vendor-identifier
command: 2
execute suit-condition-class-identifier
command: 19
execute suit-set-parameters
command: 21
execute suit-directive-fetch
fetch_and_store component
[1970/01/01 00:00:08:2432] NOTICE: GET: http://tamproto_tam_api_1:8888/TAs/8d82573a-926d-4754-9353-32dc29997f74.ta
[1970/01/01 00:00:08:2444] NOTICE: created client ssl context for default
[1970/01/01 00:00:08:2450] NOTICE: http://tamproto_tam_api_1:8888/TAs/8d82573a-926d-4754-9353-32dc29997f74.ta
component download 142432
store component
  device   = TEEP-Device
  storage  = SecureFS
  filename = 8d82573a-926d-4754-9353-32dc29997f74.ta
finish fetch
command: 3
```

```
execute suit-condition-image-match
end of command seq
[1970/01/01 00:00:08:9585] NOTICE: POST: http://tamproto_tam_api_1:8888/api/tam_cbor
[1970/01/01 00:00:08:9589] NOTICE:
[1970/01/01 00:00:08:9592] NOTICE: 0000: 82 05 A1 14 48 77 77 77 77 77 77 77 77
       ....Hwwwwwwww
[1970/01/01 00:00:08:9597] NOTICE:
[1970/01/01 00:00:08:9606] NOTICE: created client ssl context for default
[1970/01/01 00:00:08:9610] NOTICE: http://tamproto_tam_api_1:8888/api/tam_cbor
[1970/01/01 00:00:08:9854] NOTICE: (hexdump: zero length)
#### ls -l
total 1500
-rw-------    1 root     root        142432 Jan  1 00:00 8d82573a-926d-4754-9353-32dc29997f74.ta
-rwxr-xr-x    1 root     root         98088 Feb  8  2022 eyrie-rt
-rwxr-xr-x    1 root     root        437480 Feb  8  2022 hello-app
-rwxr-xr-x    1 root     root        142432 Feb  8  2022 hello-ta
-rwxr-xr-x    1 root     root        247416 Feb  8  2022 teep-agent-ta
-rwxr-xr-x    1 root     root        470568 Feb  8  2022 teep-broker-app
#### ./hello-app 8d82573a-926d-4754-9353-32dc29997f74.ta eyrie-rt
[debug] UTM : 0xffffffff80000000-0xffffffff80100000 (1024 KB) (boot.c:127)
[debug] DRAM: 0x179800000-0x179c00000 (4096 KB) (boot.c:128)
[debug] FREE: 0x1799bb000-0x179c00000 (2324 KB), va 0xffffffff001bb000 (boot.c:133)
[debug] eyrie boot finished. drop to the user land ... (boot.c:172)
hello TA
97f74.ta.secstor.plain-4754-9353-32dc29997f74.ta 8d82573a-926d-4754-9353-32dc2999
cmp: 8d82573a-926d-4754-9353-32dc29997f74.ta.secstor.plain: No such file or directory
####  done
```

4.4.2 Building teep-device for Optee with docker

Following commands are to be executed on Ubuntu 20.04.
The following commands will run a server in the current terminal session.

```
# Clone the tamproto repo and checkout master branch
$ git clone https://192.168.100.100/rinkai/tamproto.git
$ cd tamproto
$ git checkout master
$ docker-compose build
$ docker-compose up &
$ cd ..
```

The following commands run on new terminal will clone teep-device and to run docker.

```
# Clone the teep-device repo and checkout suit-dev branch
$ git clone https://192.168.100.100/rinkai/teep-device.git
$ cd teep-device
$ git checkout suit-dev

# Sync and update the submodules
$ git submodule sync --recursive
$ git submodule update --init --recursive
$ cd ..

# Start the docker
$ docker run --network tamproto_default -it --rm -v $(pwd)/teep-device:/home/user/teep-device
       trasioteam/taref-dev:optee
```

After you start the docker command, you will be logged-in inside the docker container. Following are the commands to be executed inside the docker

```
# [Inside docker image]

$ export TAREF_DIR=/home/user/ta-ref
$ PATH=/home/user/optee/toolchains/aarch64/bin:$PATH
$ . env/optee_qemu.sh
$ make clean
$ make
$ cd ..

# Build and test
$ cd teep-device/
$ make
$ make test
```

```
======= OUTPUT TO BE PUT HERE =======
```

4.4.3 Building teep-device for Keystone with docker

5 Clone and Building teep-device without docker

Clone the teep-device source code and build it for Keystone, OPTEE and SGX. To build please refer to ta-ref.pdf->preparation section

- https://192.168.100.↩ 100/rinkai/ta-ref/-/blob/teep-device-tb-slim/docs/ta-ref.pdf

5.1 Install Doxygen-1.9.2

This PDF was generated using Doxygen version 1.9.2. To install `doxygen-1.9.2` following procedure is necessary.

5.1.1 Install Required Packages

Install following packages on Ubuntu 18.04

```
sudo apt install doxygen-latex graphviz texlive-full texlive-latex-base latex-cjk-all
```

Above packages required to generate PDF using doxygen.

5.1.2 Build and Install

```
git clone https://github.com/doxygen/doxygen.git
cd doxygen
mkdir build
cd build
cmake -G "Unix Makefiles" ..
make
sudo make install
```

5.2 Tamproto Setup

To test teep-device, have to run TAM server on the PC.

Prerequisites

```
sudo apt install rustc npm
sudo pip3 install --upgrade git+https://github.com/ARMmbed/suit-manifest-generator.git@v0.0.2
```

Build and Install

```
git clone https://github.com/ko-isobe/tamproto.git
cd tamproto
git checkout cef99c07b669a49c2748b0c0ff0412ec1628b686 -b 2020-12-18
npm install
```

Make sure your PC is configures with IP address for network connectivity with TEEP device for further testing.

5.3 Keystone

Build `teep-device` with Keystone. Make sure Keystone and its supporting sources have been build already.

5.3.1 Clone and Build

Prepare the environment setup

```
export TEE=keystone
export KEYSTONE_DIR=<path to keystone dir>
export PATH=$PATH:$KEYSTONE_DIR/riscv/bin
export KEYEDGE_DIR=<path tokeyedge dir>
export KEEDGER8R_DIR=<path to keedger8r dir>
```

Clone and Build

```
git clone https://192.168.100.100/rinkai/teep-device.git
cd teep-device
git submodule sync --recursive
git submodule update --init --recursive
make
```

5.3.2 Check teep-device by running hello-app and teep-broker-app

To check teep-device on Unleased, we need to run TAM server and networking with Unleased dev board

5.3.3 Run Tamproto (TAM Server)

First start the TAM server on PC. Make sure IP address configured on PC and Unleased development board.

```
cd tamproto
npm app.js
JWKBaseKeyObject {
  keystore: JWKStore {},
  length: 4096,
  kty: 'RSA',
  kid: 'sWpWma0lDp_RfHKdtkGSVTYQaMIVQaKhESVmzjaW9jc',
  use: '',
  alg: '' }
192.168.0.5
Express HTTP  server listening on port 8888
Express HTTPS server listening on port 8443
```

Once TAM server is up, you see above messages

5.3.4 Copy the hello-app and teep-broker-app binaries to Unleased

5.3.4.1 Manual Copy

- Conneect to Unleased over serial console then assign IP address `ifconfig eth0 192.168.0.6`
- Copy the binaries from build PC over SSH (user:root, password: sifive)

Here `192.168.0.6` is IP Address of Unleased board

```
scp platform/keystone/build/hello-ta/hello-ta root@192.168.0.6:/root/teep-device
scp platform/keystone/build/hello-app/hello-app root@192.168.0.6:/root/teep-device
scp platform/keystone/build/teep-agent-ta/teep-agent-ta root@192.168.0.6:/root/teep-device
scp platform/keystone/build/teep-broker-app/teep-broker-app root@192.168.0.6:/root/teep-device
scp $KEYSTONE_DIR/sdk/rts/eyrie/eyrie-rt root@192.168.0.6:/root/teep-device
scp platform/keystone/build/libteep/ree/mbedtls/library/lib* root@192.168.0.6:/usr/lib/
scp platform/keystone/build/libteep/ree/libwebsockets/lib/lib* root@192.168.0.6:/usr/lib/
```

5.3.4.2 Write to SD card

Please follow below below steps to write the teep-device binaries to SD-card

- Insert SD card to your PC for Unleashed
- Edit `platform/keystone/script/sktinst.sh`
  - Check SD-card device name detected on yor PC and fix `prefix=?`
  - `export prefix=/dev/mmcblk0`
- execute `script/sktinst.sh` as follows
  - `cd platform/keystone; script/sktinst.sh`
- Move the sd to unleashed board and boot it

5.3.5 Check hello-app and teep-broker-app on Unleased

There are two methods to connect to Unleased.

- Serial Port using minicom (/dev/ttyUSB0)
- Over SSH: `ssh root@192.168.0.6`; password is `sifive`

Setup envrionment in Unleased (create /root/env.sh file and add following lines)

```
export PATH=$PATH:/root/teep-device
export TAM_HOST=tamproto_tam_api_1
export TAM_PORT=8888
insmod keystone-driver.ko
```

5.3.5.1 Run hello-app

```
$ source env.sh
[ 2380.618514] keystone_driver: loading out-of-tree module taints kernel.
[ 2380.625305] keystone_enclave: keystone enclave v0.2
$ cd teep-device/
$ ./hello-app hello-ta eyrie-rt
hello TA
$
```

5.3.5.2 Run teep-broker-app

Use the TAM server IP address (i.e 192.168.0.5)

```
./teep-broker-app --tamurl http://192.168.0.5:8888/api/tam_cbor
```

Upon execution, you see following log

```
teep-bro[ 2932.269897] ------------[ cut here ]------------
[ 2932.274191] WARNING: CPU: 4 PID: 164 at /home/arun/projects/ks-0.3/keystone/riscv-linux/mm/page_alloc.c:3926
       __alloc_pages_nodemask+0x150/a
[ 2932.287053] Modules linked in: keystone_driver(O)
[ 2932.291716] CPU: 4 PID: 164 Comm: teep-broker-app Tainted: G        W  O     4.15.0-00060-g65e929792fb9-dirty
       #4
[ 2932.301867] Call Trace:
[ 2932.304314] [<0000000036e46dc0>] walk_stackframe+0x0/0xa2
[ 2932.309686] [<00000000893dfe1c>] show_stack+0x26/0x34
[ 2932.314725] [<00000000c57ed7ce>] dump_stack+0x5e/0x7c
[ 2932.319759] [<00000000a68ce031>] __warn+0xca/0xe0
[ 2932.324445] [<00000000bec1f8a6>] warn_slowpath_null+0x2c/0x3e
[ 2932.330176] [<00000000e8c56bf2>] __alloc_pages_nodemask+0x14c/0x8da
[ 2932.336426] [<00000000ec1f9596>] __get_free_pages+0xc/0x52
[ 2932.341920] [<000000003e8cccc8>] epm_init+0x158/0x1a0 [keystone_driver]
[ 2932.348502] [<0000000032e4188b>] create_enclave+0x56/0xb0 [keystone_driver]
[ 2932.355447] [<000000008a656a96>] keystone_create_enclave+0x16/0x40 [keystone_driver]
[ 2932.363174] [<000000003bbf2147>] keystone_ioctl+0x132/0x164 [keystone_driver]
[ 2932.370288] [<00000000755f7993>] do_vfs_ioctl+0x76/0x4f4
[ 2932.375582] [<00000000b88b9c1d>] SyS_ioctl+0x36/0x60
[ 2932.380533] [<00000000aae667a5>] check_syscall_nr+0x1e/0x22
[ 2932.386132] ---[ end trace 66814e3a8c80ec12 ]---
ker.c compiled at Feb 16 2021 11:17:21
uri = http://192.168.0.5:8888/api/tam_cbor, cose=0, talist=
[1970/01/01 00:48:56:0796] NOTICE: POST: http://192.168.0.5:8888/api/tam_cbor
[1970/01/01 00:48:56:0798] NOTICE: (hexdump: zero length)
[1970/01/01 00:48:56:0801] NOTICE: created client ssl context for default
[1970/01/01 00:48:56:0802] NOTICE: http://192.168.0.3:8888/api/tam_cbor
[1970/01/01 00:48:56:0861] NOTICE:
[1970/01/01 00:48:56:0862] NOTICE: 0000: 83 01 A4 01 81 01 03 81 00 14 1A 77 77 77 77 04
       ...........wwww.
[1970/01/01 00:48:56:0862] NOTICE: 0010: 43 01 02 03 02                                    C....

[1970/01/01 00:48:56:0862] NOTICE:
[1970/01/01 00:48:56:0871] NOTICE: POST: http://192.168.0.5:8888/api/tam_cbor
[1970/01/01 00:48:56:0871] NOTICE:
[1970/01/01 00:48:56:0871] NOTICE: 0000: 82 02 A4 14 1A 77 77 77 77 08 80 0E 80 0F 80
       .....wwww......
[1970/01/01 00:48:56:0872] NOTICE:
[1970/01/01 00:48:56:0873] NOTICE: created client ssl context for default
[1970/01/01 00:48:56:0874] NOTICE: http://192.168.0.5:8888/api/tam_cbor
[1970/01/01 00:48:56:0962] NOTICE:
[1970/01/01 00:48:56:0962] NOTICE: 0000: 82 03 A2 0A 81 59 01 37 A2 02 58 72 81 58 6F D2
       .....Y.7..Xr.Xo.
[1970/01/01 00:48:56:0963] NOTICE: 0010: 84 43 A1 01 26 A0 58 24 82 02 58 20 75 80 7C 54
       .C..&.X$..X u.|T
[1970/01/01 00:48:56:0963] NOTICE: 0020: 62 40 D2 14 E5 7B D5 C4 6A 7C E5 2D ED B0 3D 0E
       b@...{..j|.-..=.
[1970/01/01 00:48:56:0964] NOTICE: 0030: CC 80 75 F3 F7 E0 65 B3 60 CE AD 85 58 40 54 81
       ..u...e.`...X@T.
[1970/01/01 00:48:56:0964] NOTICE: 0040: 49 CD CA D8 17 72 CC EA 61 4A 19 99 05 AB 97 33
       I....r..aJ.....3
[1970/01/01 00:48:56:0965] NOTICE: 0050: EA 48 D7 1F 13 AE 33 0D 47 FF F5 B8 6C 5C 9B 7A
       .H....3.G...l\.z
[1970/01/01 00:48:56:0965] NOTICE: 0060: BB 12 BC 2D FE 9C 20 6A C8 7F E2 28 58 74 E0 74    ...-..
       j...(Xt.t
[1970/01/01 00:48:56:0965] NOTICE: 0070: A3 BD C4 DA B9 20 C4 37 35 8F 67 46 90 76 03 58    .....
       .75.gF.v.X
[1970/01/01 00:48:56:0966] NOTICE: 0080: BE A5 01 01 02 01 03 58 60 A2 02 44 81 81 41 00
       .......X`..D..A.
[1970/01/01 00:48:56:0966] NOTICE: 0090: 04 58 56 86 14 A4 01 50 FA 6B 4A 53 D5 AD 5F DF
       .XV....P.kJS.._.
[1970/01/01 00:48:56:0967] NOTICE: 00A0: BE 9D E6 63 E4 D4 1F FE 02 50 14 92 AF 14 25 69
       ...c.....P....%i
[1970/01/01 00:48:56:0967] NOTICE: 00B0: 5E 48 BF 42 9B 2D 51 F2 AB 45 03 58 24 82 02 58
       ^H.B.-Q..E.X$..X
[1970/01/01 00:48:56:0968] NOTICE: 00C0: 20 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE
       .."3DUfw........
[1970/01/01 00:48:56:0968] NOTICE: 00D0: FF 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32
       ..#Eg........vT2
[1970/01/01 00:48:56:0969] NOTICE: 00E0: 10 0E 19 87 D0 01 F6 02 F6 09 58 4E 86 13 A1 15
       ..........XN....
[1970/01/01 00:48:56:0969] NOTICE: 00F0: 78 44 68 74 74 70 3A 2F 2F 31 39 32 2E 31 36 38
       xDhttp://192.168
[1970/01/01 00:48:56:0970] NOTICE: 0100: 2E 31 31 2E 33 3A 38 38 38 38 2F 54 41 73 2F 38
       .0.5:8888/TAs/8
[1970/01/01 00:48:56:0970] NOTICE: 0110: 64 38 32 35 37 33 61 2D 39 32 36 64 2D 34 37 35
       d82573a-926d-475
[1970/01/01 00:48:56:0971] NOTICE: 0120: 34 2D 39 33 35 33 2D 33 32 64 63 32 39 39 39 37
       4-9353-32dc29997
[1970/01/01 00:48:56:0971] NOTICE: 0130: 66 37 34 2E 74 61 15 F6 03 F6 0A 43 82 03 F6 14
       f74.ta.....C....
[1970/01/01 00:48:56:0972] NOTICE: 0140: 1A 77 77 77 78                                    .wwwx

[1970/01/01 00:48:56:0972] NOTICE:
```

```
[1970/01/01 00:48:56:0983] NOTICE: GET: http://192.168.0.5:8888/TAs/8d82573a-926d-4754-9353-32dc29997f74.ta
[1970/01/01 00:48:56:0984] NOTICE: created client ssl context for default
[1970/01/01 00:48:56:0985] NOTICE: http://192.168.0.5:8888/TAs/8d82573a-926d-4754-9353-32dc29997f74.ta
teep_message_unwrap_ta_image: msg len 234110
Decrypt
Decrypt OK: length 174887
Verify
Signature OK 0 130552
ta_store_install: ta_image_len = 130552 ta_name=8d82573a-926d-4754-9353-32dc29997f74
[1970/01/01 00:49:01:9453] NOTICE: POST: http://192.168.0.5:8888/api/tam_cbor
[1970/01/01 00:49:01:9454] NOTICE:
[1970/01/01 00:49:01:9454] NOTICE: 0000: 82 05 A1 14 1A 77 77 77 77
      .....wwww
[1970/01/01 00:49:01:9454] NOTICE:
[1970/01/01 00:49:01:9456] NOTICE: created client ssl context for default
[1970/01/01 00:49:01:9457] NOTICE: http://192.168.0.5:8888/api/tam_cbor
[1970/01/01 00:49:01:9505] NOTICE: (hexdump: zero length)
```

5.4 OPTEE

Build `teep-device` with OPTEE. So make sure OPTEE and its supporting sources have been build already.

5.4.1 Clone and Build

Prepare the environment setup

```
export TEE=optee
export OPTEE_DIR=<optee_3.9.0_rpi3 dir>
export PATH=$PATH:$OPTEE_DIR/toolchains/aarch64/bin:$OPTEE_DIR/toolchains/aarch32/bin
```

Clone and Build

```
git clone https://192.168.100.100/rinkai/teep-device.git
cd teep-device
git submodule sync --recursive
git submodule update --init --recursive
make
```

5.4.2 Check teep-device by running hello-app and teep-broker-app on RPI3

To check teep-device on RPI3, we need to run TAM server on PC and networking with RPI3 board

5.4.3 Run Tamproto (TAM Server)

First start the TAM server on PC. Make sure IP address configured on PC and RPI3 board.

```
cd tamproto
npm app.js
JWKBaseKeyObject {
  keystore: JWKStore {},
  length: 4096,
  kty: 'RSA',
  kid: 'sWpWma0lDp_RfHKdtkGSVTYQaMIVQaKhESVmzjaW9jc',
  use: '',
  alg: '' }
192.168.0.5
Express HTTP server listening on port 8888
Express HTTPS server listening on port 8443
```

Once TAM server is up, you see above messages

5.4.4 Copy the hello-app and teep-broker-app binaries to RPI3

5.4.4.1 Copy binaries over SSH to RPI3

- Connect to RPI3 over serial console(/dev/ttryUSB0) then assign IP address `ifconfig eth0 192.168.0.7`
- Copy the binaries from build PC over SSH (user:root) to RPI3

```
TODO - Further update required
```

5.4.4.2 Write to SD card

Please follow below below steps to write the teep-device binaries to SD-card

- Insert SD card to your PC for Unleashed
- Copy the binaries to SD card
- Move the sd to RPI3 board and boot it

```
TODO - Further update required
```

5.4.5 Check hello-app and teep-broker-app on RPI3

There are two methods to connect to RPI3.

- Serial Port using minicom (/dev/ttyUSB0)
- Over SSH: `ssh root@192.168.0.7`

```
TODO - Further update required
```

5.4.5.1 Run hello-app

```
TODO - Further update required
```

5.4.5.2 Run teep-broker-app

Use the TAM server IP address (i.e 192.168.0.3)

```
./teep-broker-app --tamurl http://192.168.0.3:8888/api/tam_cbor
```

Execution logs

```
TODO - Further update required
```

5.5 SGX

Build `teep-device` with SGX. Make sure SGX and its supporting sources have been build already.

5.5.1 Clone and Build on SGX

Prepare the environment setup

```
export TEE=pc
source /opt/intel/sgxsdk/environment
```

Clone and Build

```
git clone https://192.168.100.100/rinkai/teep-device.git
cd teep-device
git submodule sync --recursive
git submodule update --init --recursive
make
```

5.5.2 Check teep-device by running hello-app & teep-broker-app on SGX

To check teep-device on SGX, we need to run TAM server on PC and networking with SGX machine

5.5.3 Run Tamproto (TAM Server)

First start the TAM server on PC. Make sure IP address configured on PC and SGX machine.

```
<p />
cd tamproto
npm app.js
JWKBaseKeyObject {
  keystore: JWKStore {},
  length: 4096,
  kty: 'RSA',
  kid: 'sWpWma0lDp_RfHKdtkGSVTYQaMIVQaKhESVmzjaW9jc',
  use: '',
  alg: '' }
192.168.0.5
Express HTTP  server listening on port 8888
Express HTTPS server listening on port 8443
<p />
```

Once TAM server is up, you see above messages

5.5.4 Copy hello-app & teep-broker-app binaries to SGX

Copy the binaries to SGX/NUC machine over SSH

```
TODO - Further update required
```

If source is build natively on the SGX/NUC machine, then just copy the binaries to test PATH.

```
TODO - Further update required
```

5.5.5 Check hello-app and teep-broker-app on SGX

```
TODO - Further update required
```

5.5.5.1 Run hello-app

```
TODO - Further update required
```

5.5.5.2 Run teep-broker-app

If your TAM server IP address is 192.168.0.3, then you

```
./teep-broker-app --tamurl http://192.168.0.3:8888/api/tam_cbor
```

Execution logs

```
TODO - Further update required
```