TF-A debugfs

March 2020

Agenda

- Introduction of ARM TF-A debugfs interface
- TF-A firmware support
- Kernel driver upstream

Debug FS

ARM TF-A debugfs feature

- Problem statement
  - Fragmented protocols to expose firmware debug data
  - e.g. profiling feature uses an ad-hoc SMC interface
- Proposal
  - Provide a generic firmware debug interface
  - Subset of firmware drivers and files exposed in an abstracted hierarchy
- TF-A debugfs run-time service
  - Built within BL31
  - As a debug-only build option (USE_DEBUGFS)
  - A built time configuration file describes what to expose
- Implementation example
  - Provide firmware file abstraction to linux’ debugfs interface
  - Ability to exercise linux userspace tools onto abstracted firmware files

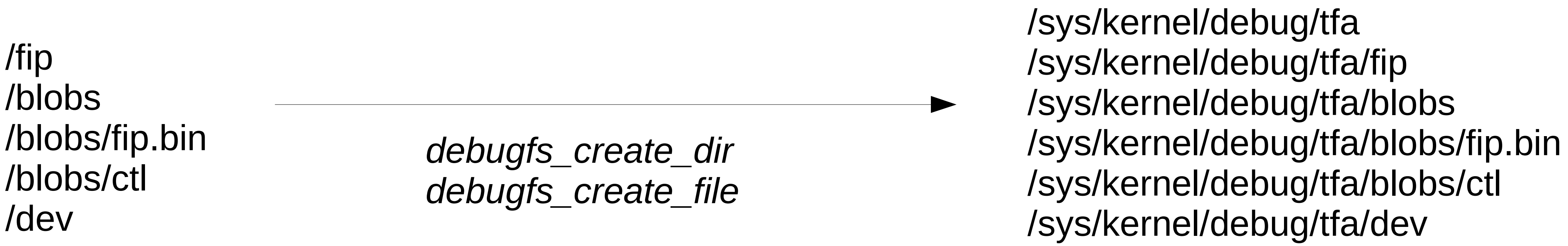
Design

- Leverages a 9p layer in TF-A firmware
  - Inherited from Plan 9 driver model
  - create, open, read, write, close, seek, stat, bind, mount
  - Driver configuration done through read/write rather than IOCTL
- Namespaces
  - ‘#’ and ‘/’ roots for drivers and files
- 9p primitives tunneled through a SiP SMC conduit

- Possible use cases (non-exhaustive)
  - Expose FIP image contents
  - Mount fip image to a folder, exposing contents of FIP files (bl1.bin, bl2.bin etc.)
  - Expose live performance data
  - Expose boot time information

Design (kernel driver)

- Driver initialization phase enumerates firmware hierarchy (walking root '/' directory)
- Files exposed as debugfs entries

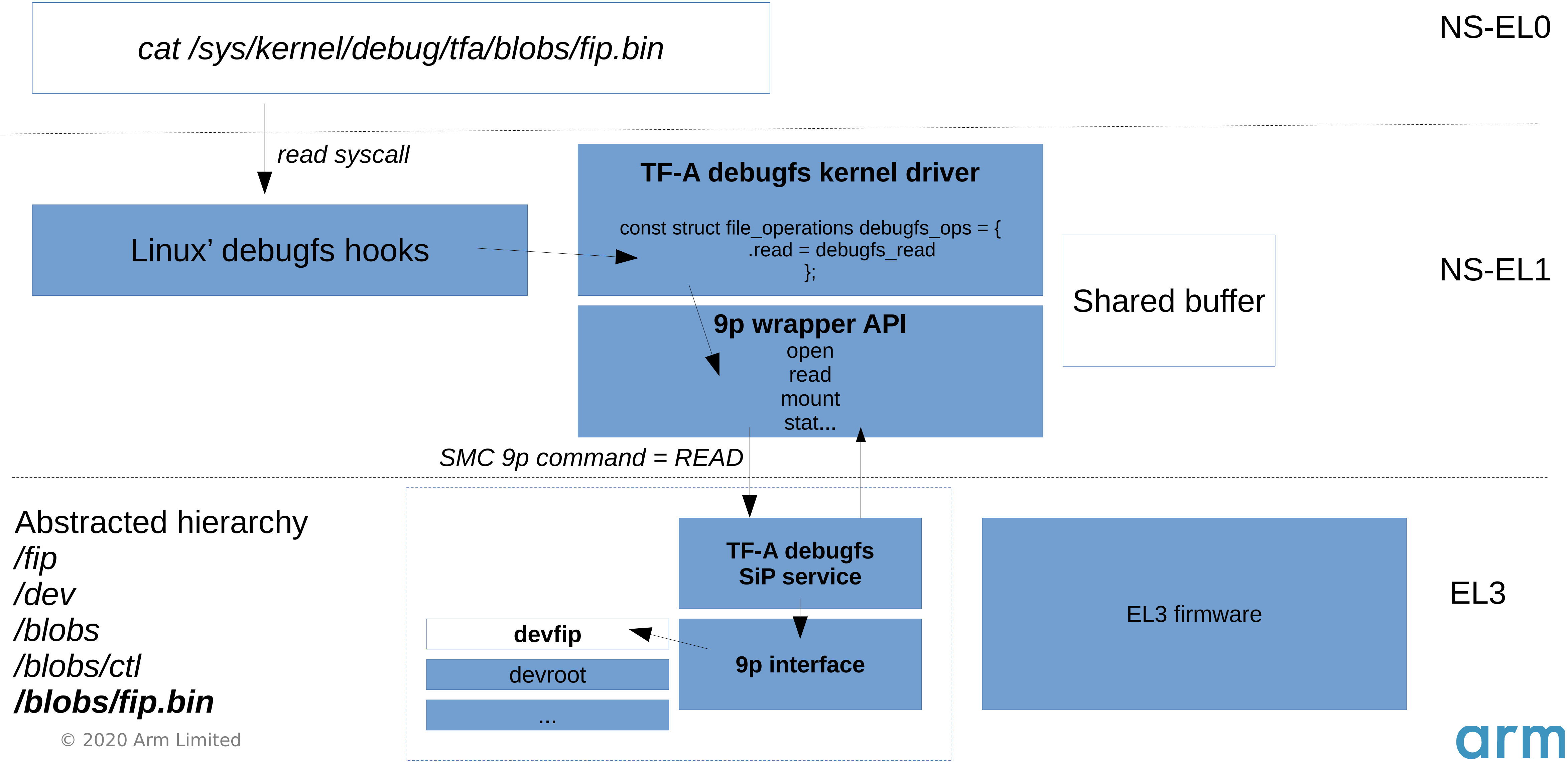


/fip
/blobs
/blobs/fip.bin
/blobs/ctl
/dev

debugfs_create_dir
debugfs_create_file

/sys/kernel/debug/tfa
/sys/kernel/debug/tfa/fip
/sys/kernel/debug/tfa/blobs
/sys/kernel/debug/tfa/blobs/fip.bin
/sys/kernel/debug/tfa/blobs/ctl
/sys/kernel/debug/tfa/dev

Design (kernel driver)



cat /sys/kernel/debug/tfa/blobs/fip.bin

NS-EL0

read syscall

Linux’ debugfs hooks

TF-A debugfs kernel driver

```
const struct file_operations debugfs_ops = {
        .read = debugfs_read
};
```

Shared buffer

NS-EL1

9p wrapper API

open
read
mount
stat...

SMC 9p command = READ

Abstracted hierarchy
/fip
/dev
/blobs
/blobs/ctl
/blobs/fip.bin

TF-A debugfs SiP service

devfip

devroot

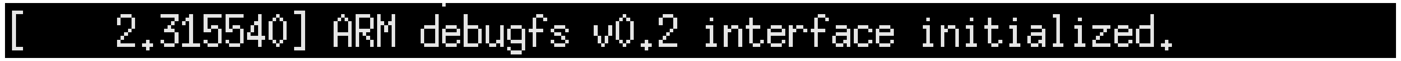
...

9p interface

EL3 firmware

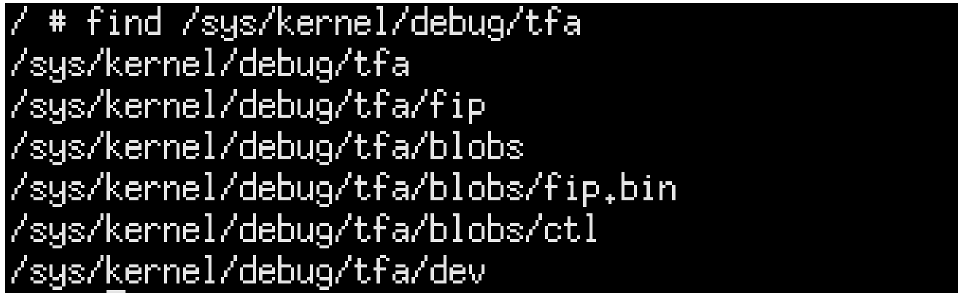
EL3

TF-A debugfs linux kernel driver



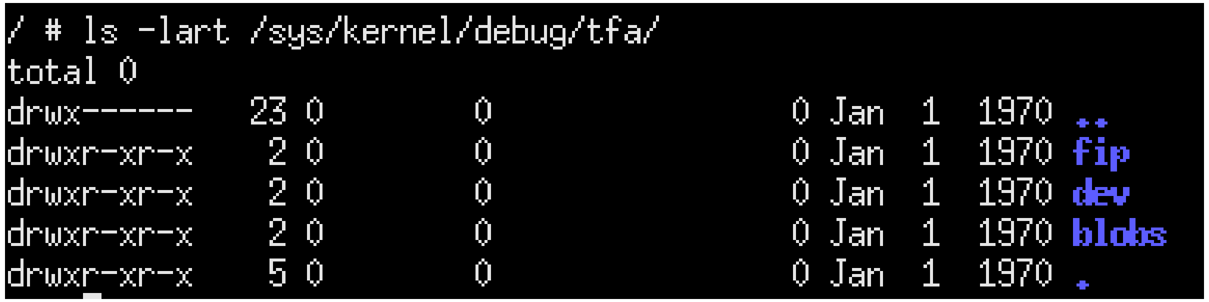
```
[    2.315540] ARM debugfs v0.2 interface initialized.
```

- Driver initialization and abstracted files enumeration



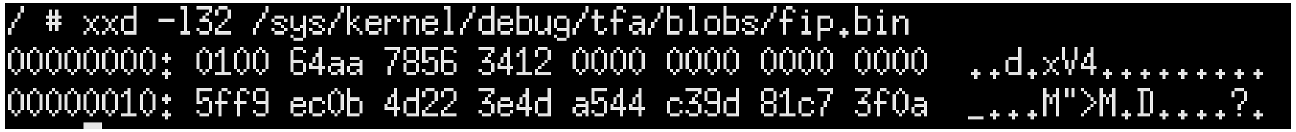
```
/ # find /sys/kernel/debug/tfa
/sys/kernel/debug/tfa
/sys/kernel/debug/tfa/fip
/sys/kernel/debug/tfa/blobs
/sys/kernel/debug/tfa/blobs/fip.bin
/sys/kernel/debug/tfa/blobs/ctl
/sys/kernel/debug/tfa/dev
```

- Firmware files listing

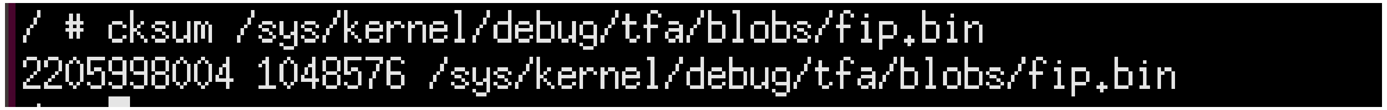


```
/ # ls -lart /sys/kernel/debug/tfa/
total 0
drwx------   23 0        0                0 Jan  1  1970 ..
drwxr-xr-x    2 0        0                0 Jan  1  1970 fip
drwxr-xr-x    2 0        0                0 Jan  1  1970 dev
drwxr-xr-x    2 0        0                0 Jan  1  1970 blobs
drwxr-xr-x    5 0        0                0 Jan  1  1970 .
```

- Linux userspace tools usage

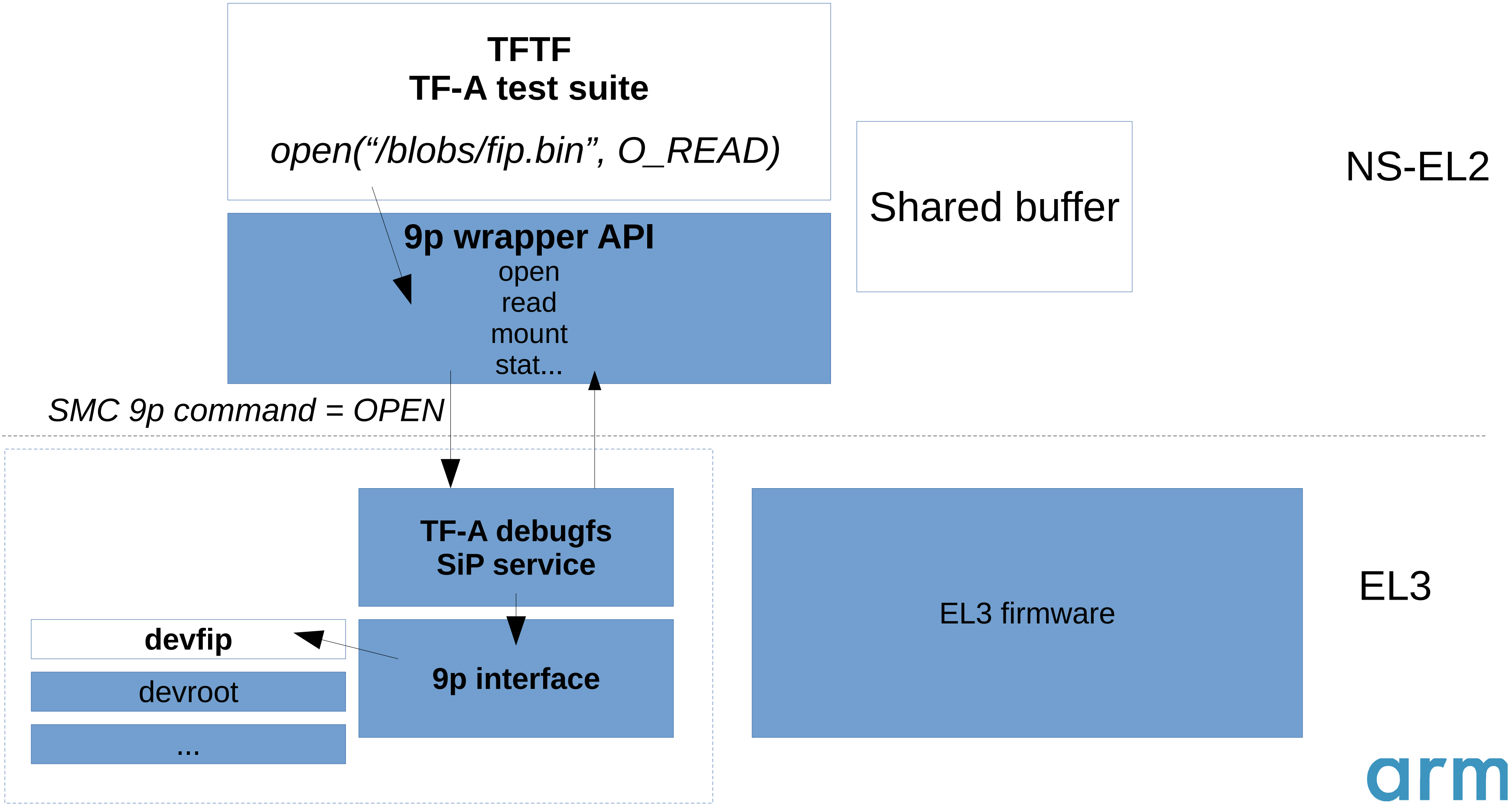


```
/ # xxd -l32 /sys/kernel/debug/tfa/blobs/fip.bin
00000000: 0100 64aa 7856 3412 0000 0000 0000 0000  ..d.xV4.........
00000010: 5ff9 ec0b 4d22 3e4d a544 c39d 81c7 3f0a  _...M">M.D....?.
```



```
/ # cksum /sys/kernel/debug/tfa/blobs/fip.bin
2205998004 1048576 /sys/kernel/debug/tfa/blobs/fip.bin
```

Design (TFTF)



Abstracted hierarchy
/fip
/dev
/blobs
/blobs/ctl
/blobs/fip.bin

Debug FS

Integrated in TFTF test suite

```
--
Running test suite 'DebugFS'
Description: Test ARM SiP DebugFS service

> Executing 'Expose filesystem'
  TEST COMPLETE                                                 Passed

******************************* Summary *******************************

[...]

> Test suite 'Performance tests'
                                                                Passed
> Test suite 'SMC calling convention'
                                                                Passed
> Test suite 'PMU Leakage'
                                                                Passed
> Test suite 'DebugFS'
                                                                Passed
=================================
Tests Skipped : 53
Tests Passed  : 56
Tests Failed  : 0
Tests Crashed : 0
Total tests   : 109
=================================
NOTICE:  Exiting tests.
```

```
[…]

        /* open non-existing directory */
        fd = open("/dummy", O_READ);
        if (fd >= 0) {
                tftf_testcase_printf("open succeeded fd=%d\n", fd);
                return TEST_RESULT_FAIL;
        }

        /**************** Root directory listing *************/
        /* open root directory */
        fd = open("/", O_READ);
        if (fd < 0) {
                tftf_testcase_printf("open failed fd=%d\n", fd);
                return TEST_RESULT_FAIL;
        }

        /* read directory entries */
        iteration = 0;
        ret = read(fd, &dir, sizeof(dir));
        while (ret > 0) {
                if (compare_dir(root_dir_expected, iteration++,
                                &dir) == false) {
                        dir_print(&dir);
                        return TEST_RESULT_FAIL;
                }

                ret = read(fd, &dir, sizeof(dir));
        }

        /* close root directory handle */
        ret = close(fd);
        if (ret < 0) {
                tftf_testcase_printf("close failed ret=%d\n", ret);
                return TEST_RESULT_FAIL;
        }

        /**************** FIP operations *************/
        /* mount fip */
        ret = mount("#F", "/fip", "/blobs/fip.bin");
        if (ret < 0) {
                tftf_testcase_printf("mount failed ret=%d\n", ret);
                return TEST_RESULT_FAIL;
        }

[...]
```

Artifacts

- Design proposed for discussion to TF-A ML
  - https://lists.trustedfirmware.org/pipermail/tf-a/2019-November/000123.html

- Documentation
  - https://git.trustedfirmware.org/TF-A/trusted-firmware-a.git/tree/docs/components/debugfs-design.rst
  - https://git.trustedfirmware.org/TF-A/trusted-firmware-a.git/tree/docs/components/arm-sip-service.rst

- Sample linux kernel driver
  - https://lkml.org/lkml/2020/3/11/563

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
תודה