arm

Trusted Firmware-M

Hardware Abstraction Layer

Edison Ai

2020.5.28

Agenda

- Introduction
- Overview Structure
- API Categories
  - Platform Initialization
  - Secure Partition Loader
  - Isolation Interface
  - Interrupt
- Appendix

Introduction

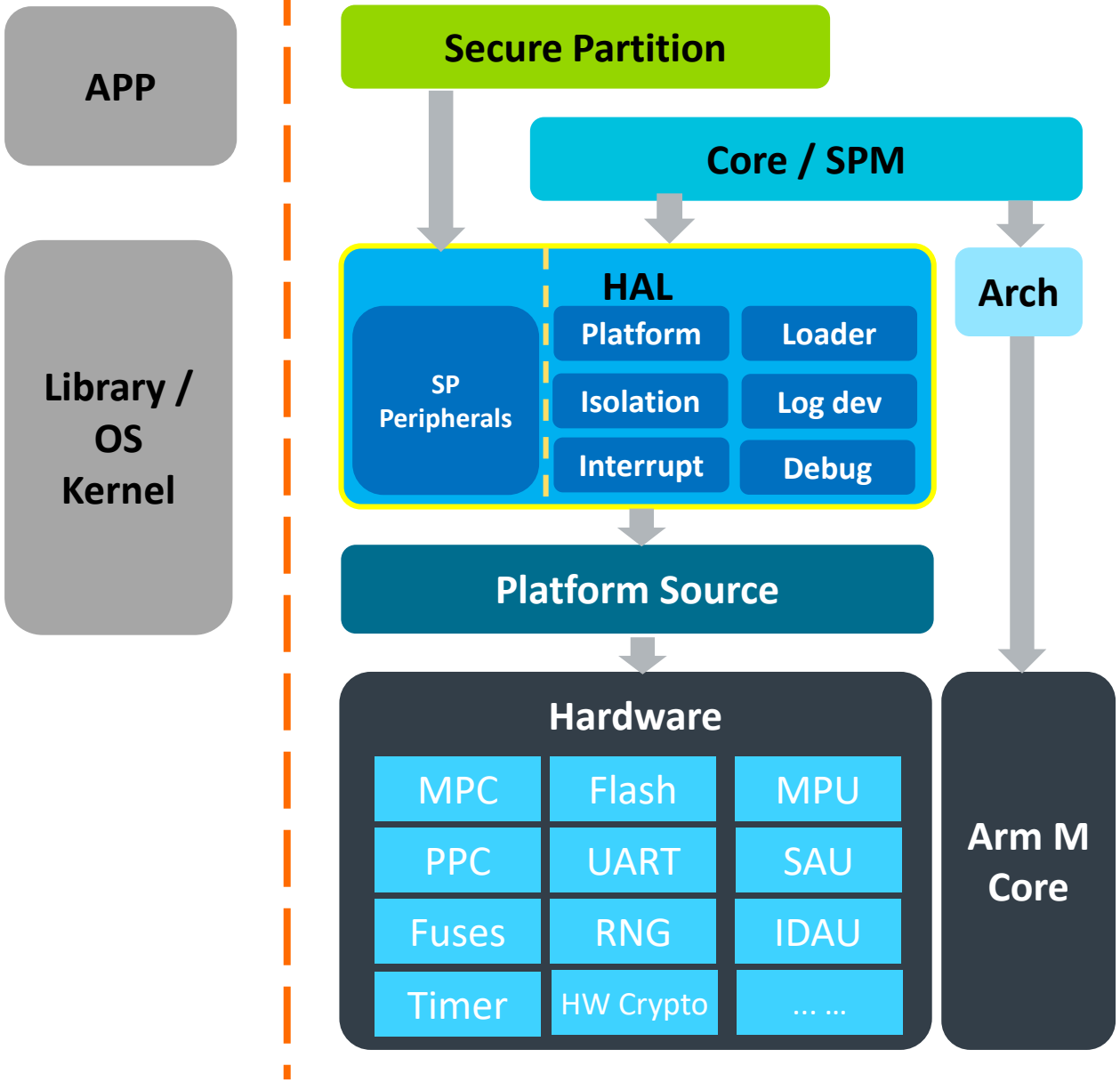
- Higher-level interface, not a device driver API.

- Abstract the hardware
  - Abstract hardware-oriented operations to support the hardware difference.
  - Make TF-M easy to use the hardware and make it easy to develop the Core and RoT Services that need to access the devices.

- Portability
  - Help user more quick and simple porting to different platform.

- Easy to maintain.

Overview Structure



API Categories

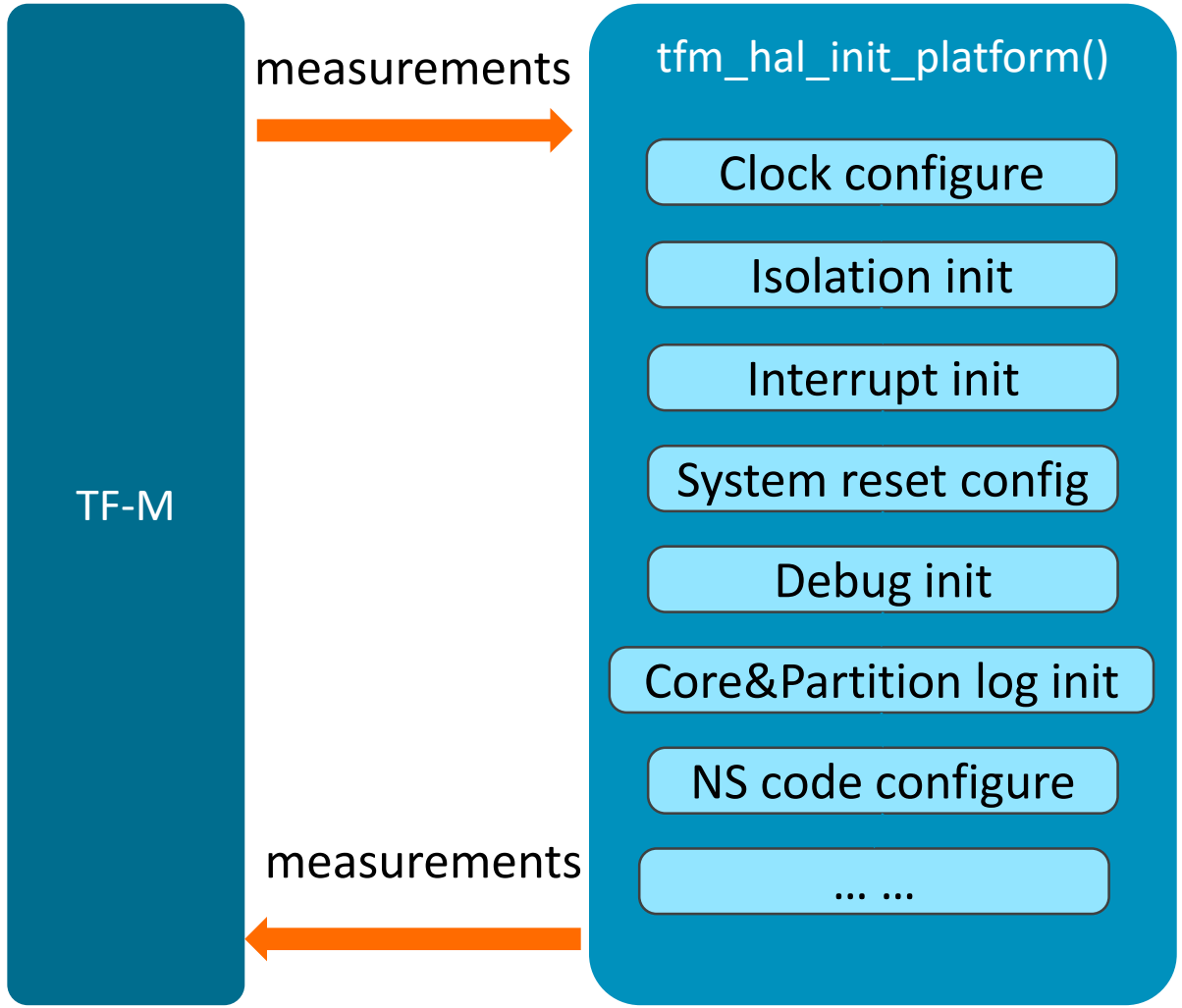
Platform API	tfm_hal_init_platform() tfm_hal_reset_platform() tfm_hal_get_platform_profile() tfm_hal_version()	Provides the platform initialization, platform-specific profile getting, system reset, etc.
Isolation API	tfm_hal_create_isolation_region() tfm_hal_destroy_isolation_region() tfm_hal_switch_isolation_regions() tfm_hal_access_to_region()	Provides the necessary isolation functionalities required by the PSA FF and TBSA-M. And provides functions to SPM to check the validate of memory access.
Loader API	tfm_hal_load_partition() tfm_hal_load_service()	Provides the function to load partition and service and provides the necessary data to SPM.
Log dev API	tfm_hal_output_core_log() tfm_hal_output_service_log()	Provides the log system functions.
Interrupt API	tfm_hal_config_irq() tfm_hal_enable_irq() tfm_hal_disable_irq() tfm_hal_clear_pending_status()	Provides the interrupt functions.
SP Peripherals		Next step and investigating.
Debug		Enhance in the future.
Dual core		Follow the current design.

Platform Initialization

- tfm_hal_init_platform(uint32_t measurements)

- Measurements:
  - A hint to platform what should to do.
  - Platform expects to set the related bit after each operation.
  - Check the alignment between SPM and platform.

- Cover most of the init functions

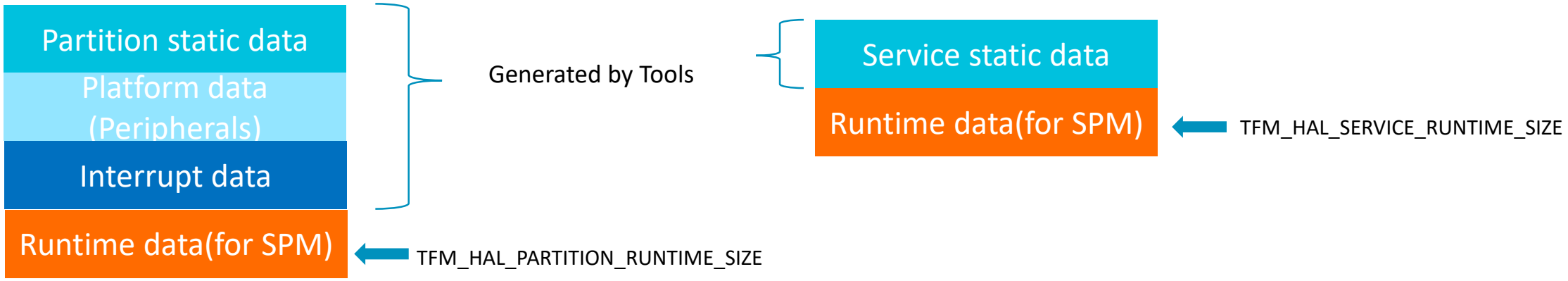


arm

Secure Partition Loader

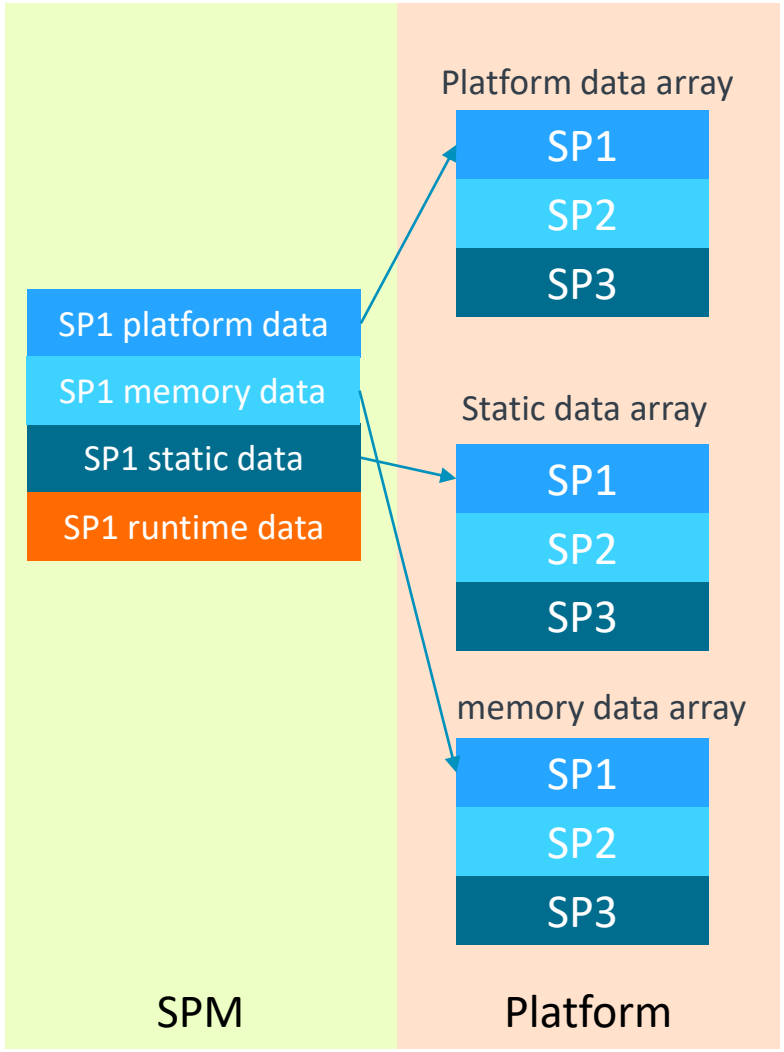
- Why needs it?
  - The platform decide where to put all the partition regions.
  - The platform allocate memory in the link stage for SP.
  - SPM is a logic implantation of PSA FF, only focuses on the partition management.

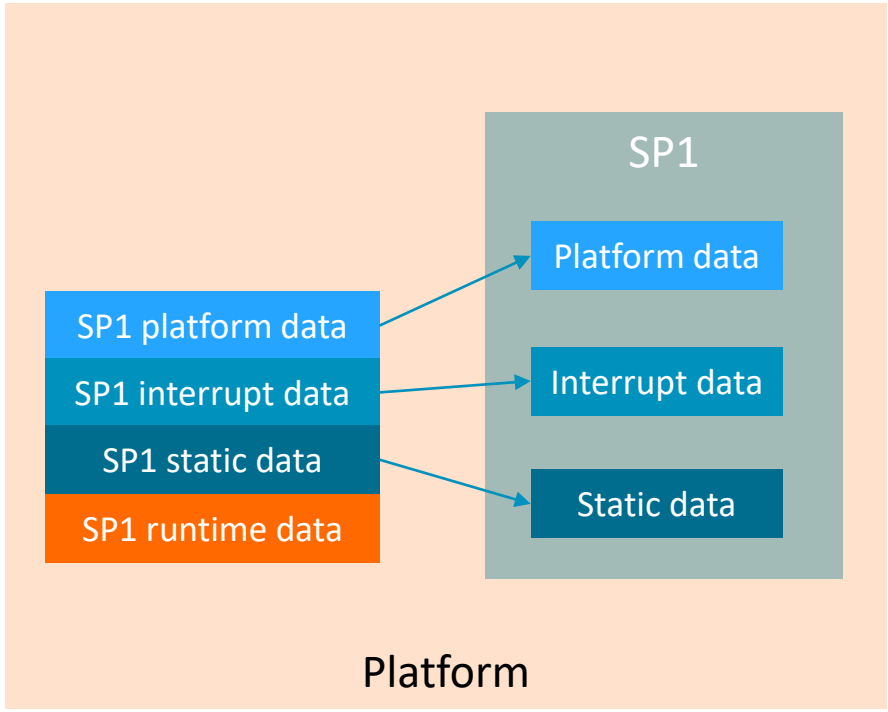
- Platform needs to provide all the necessary memory to SPM.
  - tfm_hal_load_partition()
  - tfm_hal_load_service()



arm

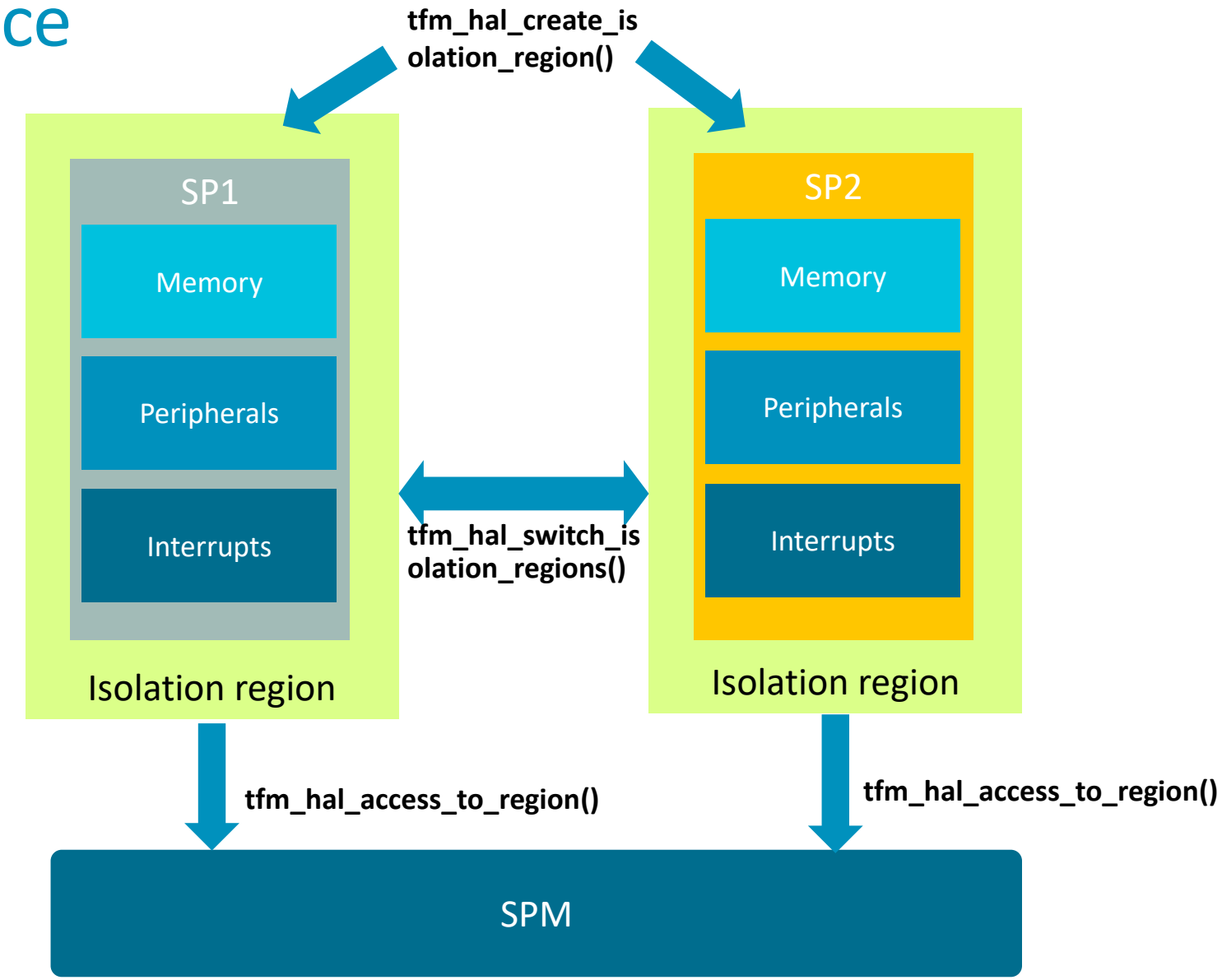
What change to TF-M by loader API?





arm

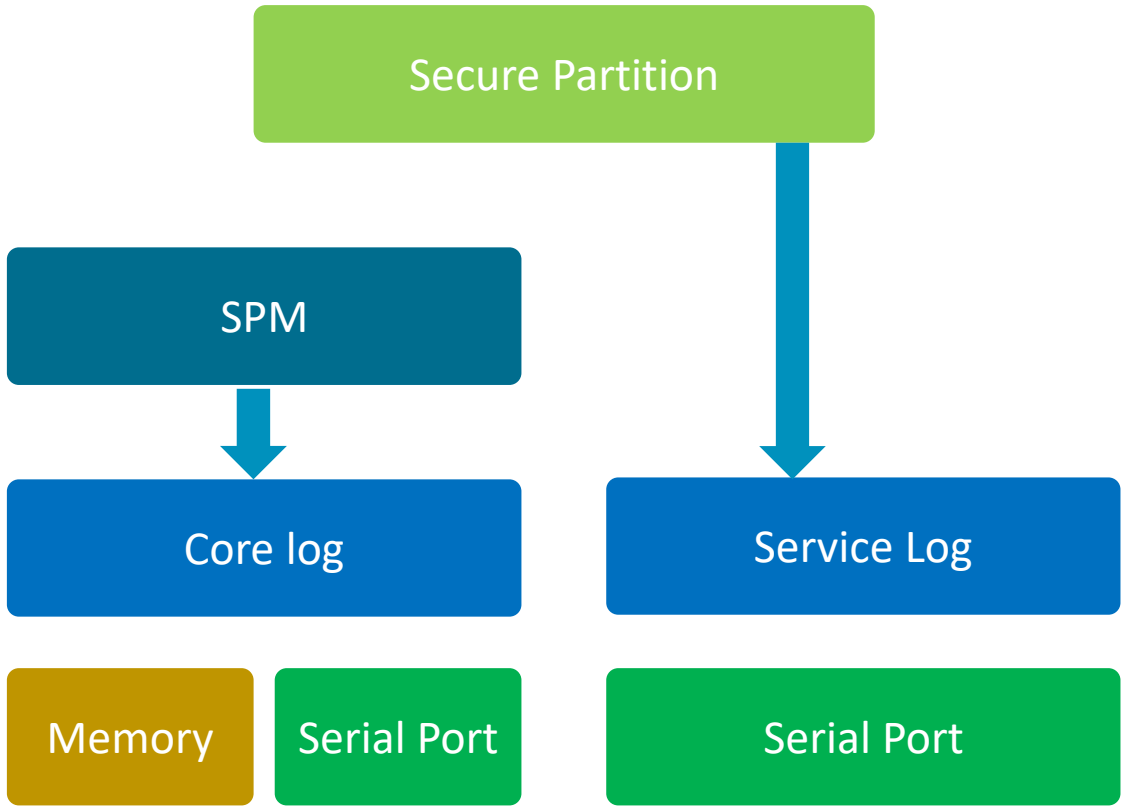
Isolation Interface



arm

Log Interface

- Support flexible logging devices



arm

Interrupt Interface

- tfm_hal_status_t tfm_hal_config_irq(struct tfm_hal_interrupt_t *intr)

```
struct tfm_hal_interrupt_t {
    size_t count;
    struct tfm_hal_irq_data_t irqs[];
};
struct tfm_hal_irq_data_t {
    int32_t line;
    psa_signal_t signal;
    uint32_t priority;
    bool secure_state;
    struct tfm_hal_partition_t *sp;
    tfm_hal_interrupt_isr_t isr;
};
```

Appendix

- Patch link: https://review.trustedfirmware.org/c/trusted-firmware-m/+/4076

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