Updates on TF-M HAL API

Kevin Peng

2020-09-17

Agenda

Write in your subtitle here

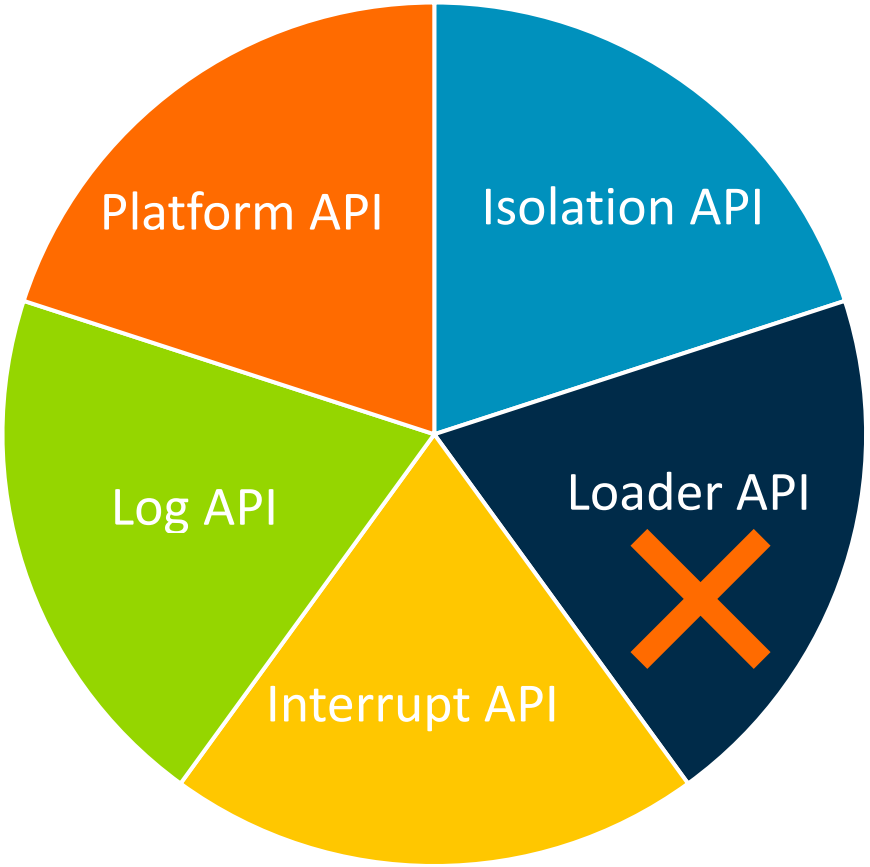
- HAL for Secure Partitions
- HAL for Secure Partition Manager
- Progress

SPM HAL

- Was a full stack, heavy HAL
- Is a very light-weight, thin HAL

APIs

- Log API – not changed
- Interrupt API - WIP
- Loader API – Removed
  - Feature design, currently no use case
- Platform API - Tailored a bit
  - Removed one API
  - Simplified one API
  - became the old HAL API
- Isolation API – totally new design
  - Simplified
  - Closer to HW



arm

API Changes

	Previous version	Current version
Platform APIs	tfm_hal_init_platform()	tfm_hal_init_platform()
	tfm_hal_reset_platform()	tfm_hal_reset_platform()
	~~tfm_hal_get_meminfo()~~	
Isolation APIs	~~tfm_hal_create_isolation_region()~~	tfm_hal_set_spe_boundary()
	~~tfm_hal_destroy_isolation_region()~~	tfm_hal_isolation_init()
	~~tfm_hal_switch_isolation_regions()~~	tfm_hal_enable_memory_access()
	~~tfm_hal_config_isolation_region()~~	tfm_hal_disable_memory_access()
	~~tfm_hal_access_to_region()~~	tfm_hal_memory_has_access()

Progress

- Design Docs
  - Platform API – API finalized
  - Log API - API finalized
  - Isolation API
- Platform API
  - “Implemented”
- Log API
  - SPM log – patch for review
  - SP log – coming soon
- Isolation API
  - isolation feature branch
  - Re-implemented Isolation L1 and L2
  - Prototyping on Isolation L3

arm

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