Trusted Firmware - M

Isolation Level 3 Design Brief

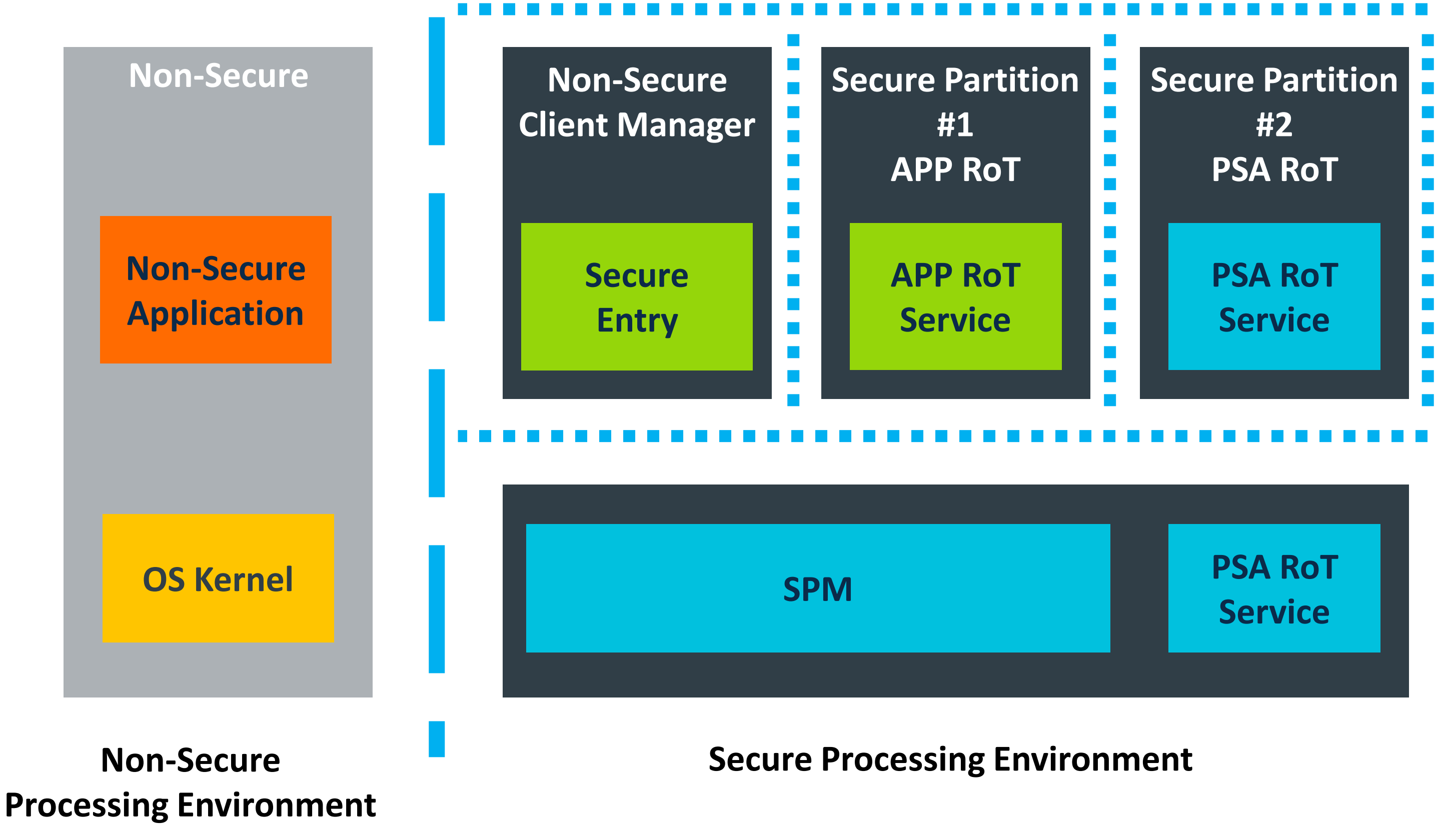
Ken Liu

2020-Jun-23

Content

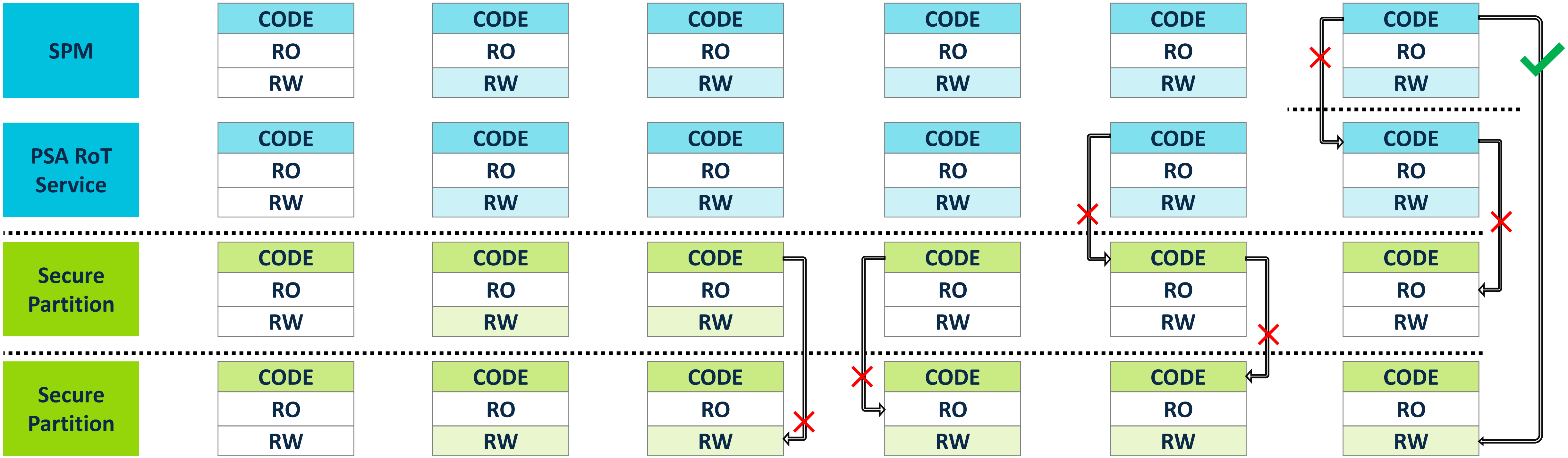
- Isolation Rules and Level 3
- MPU Regions
- Implementation Dependencies

Isolation Level 3


Non-Secure
Non-Secure Application
OS Kernel
Non-Secure Client Manager
Secure Entry
Secure Partition #1 APP RoT
APP RoT Service
Secure Partition #2 PSA RoT
PSA RoT Service
SPM
PSA RoT Service
Non-Secure Processing Environment
Secure Processing Environment

- The secure isolation mechanism based on a fundamental framework (TrustZone, Multiple Core) and necessary supporting hardware (SAU, IDAU, MPC etc).
- The following pages focus on isolation boundaries inside SPE.

Isolation Rules and Level 3



	I1	I2	I3	I4	I5	I6
SPM	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW
PSA RoT Service	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW
Secure Partition	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW
Secure Partition	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW	CODE RO RW

I1
Only Code is executable

I2
Only Private Data is Writable

I3
Private Data is protected from prevented domain

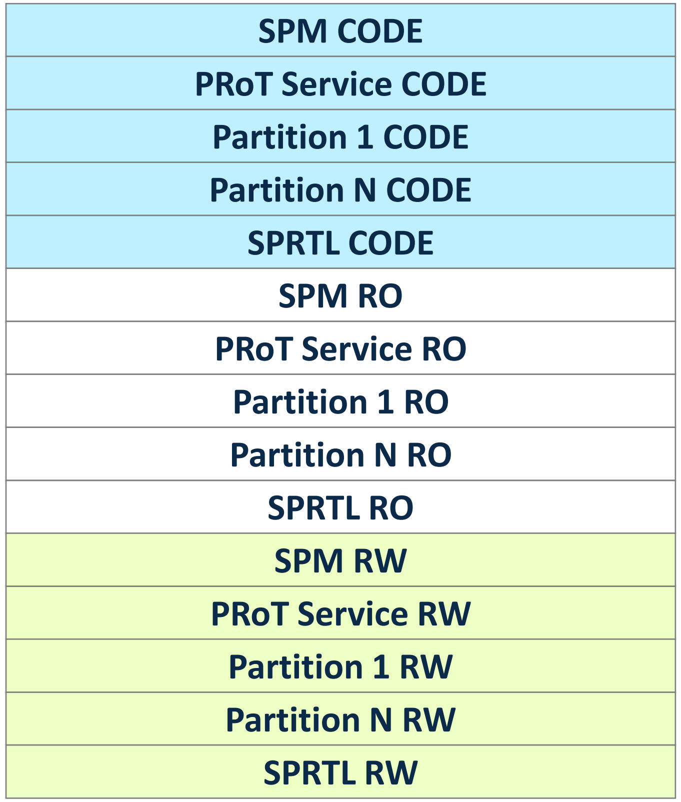
I4
Code/RO Data is protected from prevented domain

I5
Code can’t be executed from other domain

I6
Everything is protected, SPM is an exception for data

MPU Regions – Image Layout Matters

- To save the runtime initialization effort, group the CODE/RO/RW for all components.
- Also could save the MPU regions.
- Possible MPU Region Attributes:
    - Privileged Read-Only
    - All Privileged Level Read-Only
    - Privileged Read-Write
    - All Privileged Level Read-Write
    - Execution Never
    - Privileged Execution Never (8.1 Feature)



SPM CODE
PRoT Service CODE
Partition 1 CODE
Partition N CODE
SPRTL CODE
SPM RO
PRoT Service RO
Partition 1 RO
Partition N RO
SPRTL RO
SPM RW
PRoT Service RW
Partition 1 RW
Partition N RW
SPRTL RW

MPU Regions – Combinations

Memory Assets	I1 I2 I3	I4	I5	I6
SPM CODE	ALL RO	P RO	P RO	P RO
PROT Service CODE				ALL RO PXN
Active Partition CODE		ALL RO	ALL RO PXN	
SPRTL CODE		ALL RO	ALL RO PXN	ALL RO PXN
SPM RO	ALL RO XN	P RO XN	P RO XN	P RO XN
PROT Service RO				ALL RO XN
Active Partition RO		ALL RO XN	ALL RO XN	
SPRTL RO		ALL RO XN	ALL RO XN	ALL RO XN
SPM RW	P RW XN	P RW XN	P RW XN	P RW XN
PROT Service RW				ALL RW XN
Active Partition RW	ALL RW XN	ALL RW XN	ALL RW XN	
SPRTL RW (1)	ALL RW XN + 1	ALL RW XN + 1	ALL RW XN + 1	ALL RW XN + 1
Partition Peripheral	ALL RW XN + N	ALL RW XN + N	ALL RW XN + N	ALL RW XN + N
Minimal Numbers	**5**	**8**	**8**	**8**

1. SPRTL RW contains per-SP data pointer maintained by SPM.
SPRTL or SP can’t update it even it looks as ‘RW’.

Implementation Dependencies

- Rely on HAL Isolation Interfaces
- Secure Peripherals sharing between partitions are not permitted, dynamic setting of peripheral protection components may be necessary.

arm

Thank You

Danke

Merci

谢谢

ありがとう

Gracias

Kiitos

감사합니다

धन्यवाद

شكرًا

ধন্যবাদ

תודה