Commonly Asked Questions

TF-M: What does vendor need to implement?
Non-Secure Processing Environment

Secure Processing Environment

Non-secure partition
- Application firmware
- OS libraries
- OS kernel

IPC and Service API

Crypto service
- Crypto Service
- Secure Storage
- Attestation service
- Provisioning service
- Audit Log
- Vendor applets

Secure Non-Privileged Domain
- Secure Storage
- Initial attestation service
- TBSA HAL API
- Vendor applets

Secure Privileged Domain
- TFM Crypto
- TBSA Platform APIs
- Initial attestation service
- Secure Partition Manager
- Boot loader

TPM
- HW Keys
- Crypto Accelerator
- NV Counter
- ……

TBSA Platform APIs

Initial attestation service

Audible Log

TPM

Initial attestation service

Initial attestation service

Vendor applets

Vendor applets

Vendor applets
Commonly Asked Questions

Is the trust boundary same as privilege boundary?
Commonly Asked Questions

NS and S Interrupt handling?
Trusted Firmware M - The Big Picture

Non-Secure Processing Environment

Non-secure partition
- Application firmware
- Service API
- OS libraries
- OS kernel

Non-Secure Partition
- Crypto Service
- Secure Storage
- Attestation service
- Provisioning service
- Audit Log
- Vendor applets

Secure Processing Environment

Secure Non-Privileged Domain
- TFM Crypto
- TBSA Platform APIs
- Initial attestation service
- ...

Secure Privileged Domain
- Initial attestation service
- Secure Service API
- Bootloader
- TBSA HAL API
- Hardware
- HW Keys
- Crypto Accelerator
- NV Counter
- SAU/MPC/PPC

Vendor applets

Trusted Firmware M - The Big Picture
Commonly Asked Questions

What happens in multi bus master scenarios?
Trusted Firmware M - The Big Picture

Non-Secure Processing Environment

- Non-secure partition
  - Application firmware
  - Service API
  - OS libraries
  - OS kernel

Non-Secure Processing Environment

- Crypto Service
- Secure Storage
- Attestation service
- Provisioning service
- Audit Log
- Vendor applets

Secure Processing Environment

- TFM Crypto
- TBSA Platform APIs
- Initial attestation service
- ...

Secure Non-Privileged Domain

- Secure Partition Manager
- Bootloader

Hardware

- HW Keys
- Crypto Accelerator
- NV Counter
- SAU/MPC/PPC

TBSA HAL API
Commonly Asked Questions

Scheduling on secure side?
How to get involved

Trusted Firmware Website

• [https://www.trustedfirmware.org/index.html](https://www.trustedfirmware.org/index.html)

TF-M codebases

• [https://git.trustedfirmware.org/](https://git.trustedfirmware.org/)

TF-M Dev Team @ Connect HKG18

• Abhishek Pandit
• Ashutosh Singh

Get in touch

• Come round LITE hacking room
• Schedule a meeting via [hkg18.pathable.com](hkg18.pathable.com)

More info on [developer.arm.com](developer.arm.com)
Thank You!
Danke!
Merci!
谢谢!
ありがとう!
Gracias!
Kiitos!
감사합니다
धन्यवाद
Firmware upgrade

- Update client downloads the FW
- Bootloader validates the new image
- Swap the images
- Perform BIST in runtime and mark SPE and NSPE as ‘safe’
- If not, revert back
ARMv8-M TrustZone overview
ARMv8-M Secure and Non-secure states

### Non-secure

- **Application Code**
  - Thread Mode: MSP_NS
  - PSP_NS

- **Exception Code**
  - Handler Mode: MSP_NS

### Secure

- **Application Code**
  - Thread Mode: MSP_S
  - PSP_S

- **Exception Code**
  - Handler Mode: MSP_S
ARMv8-M additional states

Existing Handler and Thread Modes mirrored with Secure and Non-secure States

Secure and Non-Secure code run on a single CPU

Secure state for trusted code

- New Secure stack pointers for robust operation
  - MSP and PSP → MSP_NS, PSP_NS, MSP_S and PSP_S

Dedicated resources

- Separate memory protection units for S and NS
- Private SysTick timer for each state
- Secure side can configure target domain of interrupts