arm

PSA Level 2 Certification with TF-M

Ashutosh Singh

Level 2 Requirements

ID	Function Description	TF-Mv1.0-RC1 Support
5.1	F.Initialization	MuscaB1e being a development and test platform doesn't have immutable root of trust, flash is used instead.
5.2	F.Software_Isolation	Level 2 Isolation compliant with Firmware Framework level 2 isolation
5.3	F.Secure_Storage	HUK stub used instead of actual HUK
5.4	F.Firmware_Update	Support in bootloader

https://www.psacertified.org/resources/

arm

Level 2 Security Requirements 2

5.5	F.Secure_State	Using v8-M Trustzone and MPUs, TF-M controls the access to each TF-M Secure Partition by Applications and other Secure partitions and checks the validity of parameters of any operation requested from Applications
5.6	F.Crypto	Currently only supports client supplied keys. Binding to secure storage TBD.
5.7	F.Attestation	
5.8	F.Audit	Not Supported. Only available in Level1 isolation.
5.9	F.Debug	Debug is locked down by the software at firmware initialization instead of ‘debug disable by default in the hardware’.

arm

RC Tag for Level 2 Certification (TF-Mv1.0-RC1)

- What's new since TF-M1.0-Beta
  - PSA Level2 Isolation Support
  - mbedcrypto used in Crypto Secure Service
  - Secure Boot supports Rollback Protection
  - PSA Firmware Framework IPC Support
  - Crypto, SST and Attestation supports both Library and IPC mode
- Collaborative work with labs to finalize the certification
- Musca_B1 as the test vehicle

Focus for next Quarter

- Memory Optimization
  - Profiling of memory usage
  - Review of all components with optimization lens
  - Investigation – define device profiles to cater different device PPA points
- Closing all the security stubs
  - proper HUK handling
  - opaque key support in crypto
  - hardware keys for boot and attestation
- Dual v7-M
- Bootloader - Multiple Image Update Support
- HAL standardization
- Documentation Method. Rollout
- L2 certification collaboration with labs

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