TF-M configuration

September 2022

Config structure

Modules

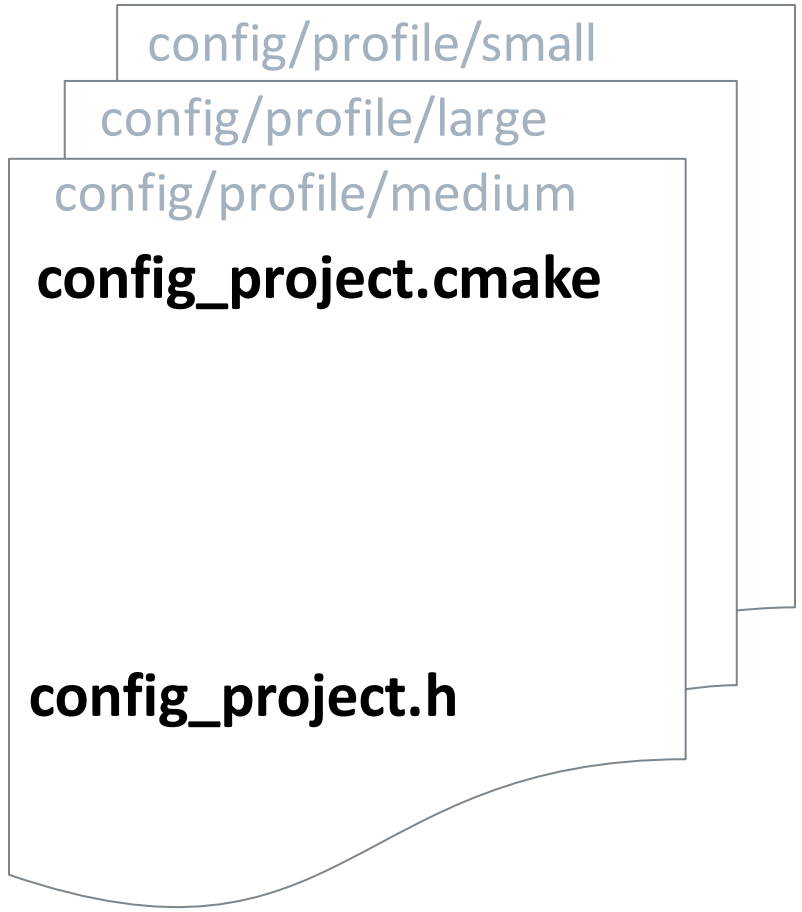
1. Core
2. SPM
3. Platform
4. Partition_Crypto
5. Partition_ITS
6. Partition_PS
7. Partition_Attest
8. Partition_Audit
9. Partition_FWU
10. Partition_Platform
11. BL1
12. BL2
13. MCUBoot
14. Test
15. CC312
16. ADAC

Build configs

- Defines file set for building
- Are CMake variables
- Cross dependent with other CMake variables
- Consistency checks (or KConfig ?)

Component options

- Feature selection in a source
- #define XXX
- Consistency check on option level



* Design illustration, valid for Sep 2022. Not a reference

Config options

Core
- TFM_PLATFORM
- TFM_LIB_MODEL
- PSA_FRAMEWORK_HAS_MM_IOVEC
- TFM_FIH_PROFILE
- TFM_PARTITION_LOG_LEVEL
- TFM_CODE_SHARING
- NUM_MAILBOX_QUEUE_SLOT
- TFM_DUMMY_PROVISIONING
- FORWARD_PROT_MSG
- TFM_PSA_API
- PSA_FRAMEWORK_ISOLATION_LEVEL
- CONFIG_TFM_FLOAT_ABI
- CONFIG_TFM_ENABLE_CP10CP11

SPM
- TFM_ISOLATION_LEVEL
- CONFIG_TFM_CONN_HANDLE_MAX_NUM
- CONFIG_TFM_SPM_BACKEND
- TFM_SPM_LOG_LEVEL
- CONFIG_TFM_HALT_ON_CORE_PANIC
- CONFIG_TFM_LAZY_STACKING
- CONFIG_TFM_ENABLE_FPU
- CONFIG_TFM_DOORBELL_API
- CONFIG_TFM_STACK_WATERMARKS
- CONFIG_TFM_SPM_BACKEND_IPC
- CONFIG_TFM_SPM_BACKEND_SFN
- TFM_PARTITION_NS_AGENT_MAILBOX
- TFM_PARTITION_NS_AGENT_TZ
- TFM_SP_LOG_RAW_ENABLED
- TFM_SPM_LOG_RAW_ENABLED

Platform
- TFM_CODE_SHARING_PLATFORM_LISTS
- TFM_PXN_ENABLE
- TFM_EXCEPTION_INFO_DUMP
- CONFIG_TFM_FP
- TFM_PLAT_SPECIFIC_MULTI_CORE_COMM
- DEBUG_AUTHENTICATION
- SECURE_UART1
- OTP_NV_COUNTERS_RAM_EMULATION
- TFM_NS_NV_COUNTER_AMOUNT
- PLATFORM_DEFAULT_BL1
- PLATFORM_DEFAULT_ATTEST_HAL
- PLATFORM_DEFAULT_NV_COUNTERS
- PLATFORM_DEFAULT_CRYPTO_KEYS
- PLATFORM_DEFAULT_ROTPK
- PLATFORM_DEFAULT_IAK
- PLATFORM_DEFAULT_UART_STDOUT
- PLATFORM_DEFAULT_NV_SEED
- PLATFORM_DEFAULT_OTP
- PLATFORM_DEFAULT_OTP_WRITEABLE
- PLATFORM_DEFAULT_PROVISIONING
- PLATFORM_IS_FVP
- ARM_V80M_ARCH
- PLATFORM_HAS_ISOLATION_L3_SUPPORT
- PLATFORM_SP_STACK_SIZE
- CONFIG_TFM_ENABLE_FP
- CONFIG_TFM_ENABLE_MVE
- CONFIG_TFM_ENABLE_MVE_FP

Partition_Crypto
- CRYPTO_HW_ACCELERATOR
- TFM_PARTITION_CRYPTO
- CRYPTO_TFM_BUILTIN_KEYS_DRIVER
- CRYPTO_ENGINE_BUF_SIZE
- CRYPTO_CONC_OPER_NUM
- CRYPTO_RNG_MODULE_DISABLED
- CRYPTO_KEY_MODULE_DISABLED
- CRYPTO_AEAD_MODULE_DISABLED
- CRYPTO_MAC_MODULE_DISABLED
- CRYPTO_HASH_MODULE_DISABLED
- CRYPTO_CIPHER_MODULE_DISABLED
- CRYPTO_ASYM_SIGN_MODULE_DISABLED
- CRYPTO_ASYM_ENCRYPT_MODULE_DISABLED
- CRYPTO_KEY_DERIVATION_MODULE_DISABLED
- CRYPTO_IOVEC_BUFFER_SIZE
- CRYPTO_NV_SEED
- CRYPTO_SINGLE_PART_FUNCS_DISABLED
- CRYPTO_STACK_SIZE

Partition_ITS
- TFM_PARTITION_INTERNAL_TRUSTED_STORAGE
- ITS_CREATE_FLASH_LAYOUT
- ITS_RAM_FS
- ITS_VALIDATE_METADATA_FROM_FLASH
- ITS_MAX_ASSET_SIZE
- ITS_NUM_ASSETS
- ITS_BUF_SIZE
- ITS_STACK_SIZE

Partition_PS
- TFM_PARTITION_PROTECTED_STORAGE
- PS_CREATE_FLASH_LAYOUT
- PS_ENCRYPTION
- PS_RAM_FS
- PS_ROLLBACK_PROTECTION
- PS_VALIDATE_METADATA_FROM_FLASH
- PS_MAX_ASSET_SIZE
- PS_NUM_ASSETS
- PS_CRYPTO_AEAD_ALG
- PS_STACK_SIZE

Partition_Attest
- TFM_PARTITION_INITIAL_ATTESTATION
- SYMMETRIC_INITIAL_ATTESTATION
- ATTEST_INCLUDE_OPTIONAL_CLAIMS
- ATTEST_INCLUDE_COSE_KEY_ID
- ATTEST_TOKEN_PROFILE
- ATTEST_STACK_SIZE
- ATTEST_INCLUDE_TEST_CODE

Partition_Audit
- TFM_PARTITION_AUDIT_LOG

Partition_FWU
- TFM_PARTITION_FIRMWARE_UPDATE
- TFM_FWU_BOOTLOADER_LIB
- PSA_FWU_MAX_BLOCK_SIZE
- TFM_FWU_BUF_SIZE
- FWU_STACK_SIZE

Partition_Platform
- TFM_PARTITION_PLATFORM
- PLATFORM_SERVICE_INPUT_BUFFER_SIZE
- PLATFORM_SERVICE_OUTPUT_BUFFER_SIZE

User level → Kconfig

Advanced → config_xxx.h

* Design illustration, valid for Sep 2022. Not a reference