test_crypto Documentation

June 2022

1 Introduction

The test_crypto library implements the common cryptographic functions found in the Secure Hardware Extension (SHE). This document covers the construction and usage of these functions.

2 Implemented Primitives

The following primitives are available as a module:

- Encryption/Decryption: AES-ECB (Electronic Code Book) and AES-CBC (Cipher Block Chaining).
- Hash Function: Miyaguchi-Preneel Compression.
- MAC: Cipher-based MAC with AES as the pseudorandom function.

2.1 AES

The standardized cipher used for encryption/decryption and also as a subroutine where a pseudorandom function is needed.
Enables the following functions:

- CMD_ENC_ECB: ECB-mode encryption. This function is used by the following function(s):
  - CMD_INIT_RNG: Initializes the seed and derives a key for the PRNG.
  - CMD_RND: Returns a vector of 128 random bits.
  - Memory Update Verification: Generates a verification message which can be transferred to the backend to prove the successful update.
- CMD_ENC_CBC: CBC-mode encryption. This function is used by the following function(s):
  - Memory Update: The process for memory updates (the process that calls CMD_LOAD_KEY).
  - CMD_EXPORT_RAM_KEY: Exports the RAM_KEY into a format protected by SECRET_KEY.
- CMD_DEC_ECB: ECB-mode decryption.
- CMD_DEC_CBC: CBC-mode decryption. This function is used by the following function(s):
  - CMD_LOAD_KEY: Updates an internal key of SHE.
- Miyaguchi-Preneel Compression (referred to as M-P Compression).
- Cipher-based Message Authentication Code (referred to as CMAC).

2.2 Miyaguchi-Preneel Compression

The M-P Compression function uses AES-ECB as a pseudorandom function in order to generate a hash value.
Enables the following functions:

- Key derivation (referred to as KDF).
- CMD_EXTEND_SEED: Extend the seed and the current PRNG_STATE by calling the function and supplying 128 bit of entropy.

2.3 KDF

The key derivation function uses a key (or any other secret value) and generates another key.
Enables the following functions:

- CMD_INIT_RNG.
- Memory Update.
- CMD_LOAD_KEY.
- CMD_EXPORT_RAM_KEY.
- Memory Update Verification.
- CMD_DEBUG: Used to activate any internal debugging facilities of SHE.

2.4 CMAC

The CMAC uses AES-ECB as as pseudorandom function in order to generate an authentication code. Enables the following functions:

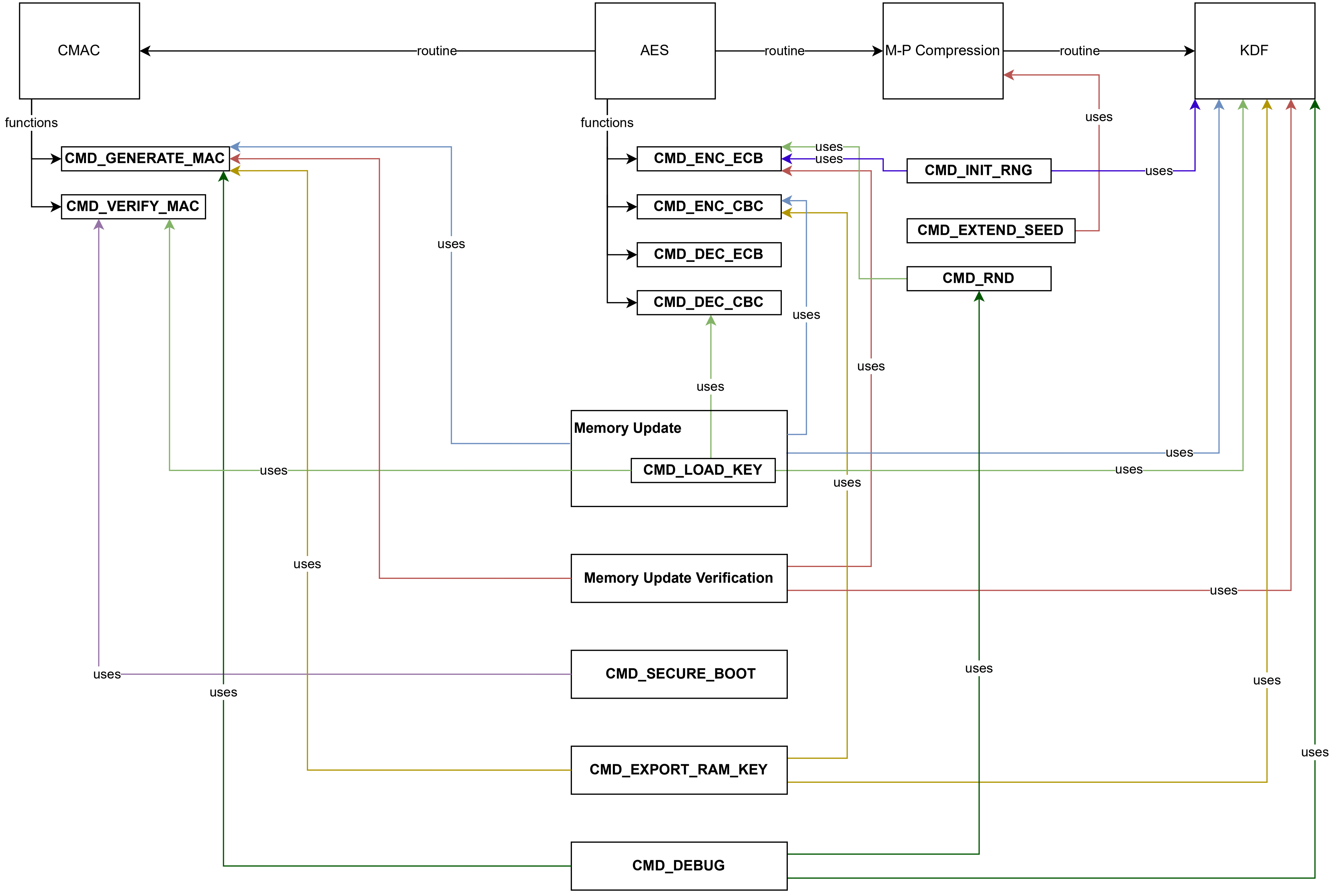
- CMD_GENERATE_MAC: Generates a MAC of a given message with the help of a key. This function is used by the following function(s):
  - Memory Update.
  - Memory Update Verification.
  - CMD_EXPORT_RAM_KEY.
  - CMD_DEBUG.
- CMD_VERIFY_MAC: Verifies the MAC of a given message with the help of a key identified by KEY_ID against a provided MAC. This function is used by the following function(s):
  - CMD_LOAD_KEY.
  - CMD_SECURE_BOOT: SHE verifies the MAC of the bootloader.

Note

All the above primitives have been implemented, as have all of the above functions that have test vectors in the SHE spec.

2.5 Flowchart

The following flowchart details the relations between the functions discussed above.


CMAC
routine
AES
routine
M-P Compression
routine
KDF
functions
CMD_GENERATE_MAC
CMD_VERIFY_MAC
functions
CMD_ENC_ECB
CMD_ENC_CBC
CMD_DEC_ECB
CMD_DEC_CBC
CMD_INIT_RNG
CMD_EXTEND_SEED
CMD_RND
Memory Update
CMD_LOAD_KEY
Memory Update Verification
CMD_SECURE_BOOT
CMD_EXPORT_RAM_KEY
CMD_DEBUG
uses