CERDEC Cryptographic Module 1.0.2

Hardware: M2S050TS-1FGG896
Firmware: FreeRTOS 7.0.1; Crypto Engine FW 1.0.2
Custom hardware: Crypto Engine FW 1.0PL

FIPS 140-2 Security Policy

Document Version 0.13

November 12, 2021

Prepared for:

US Army CERDEC
6590 Reconnaissance Street
APG, MD 21005
c5isr.ccdc..army.mil
443-395-7966

Prepared by:

KeyPair Consulting Inc.
846 Higuera St., Suite 2
San Luis Obispo, CA 93401
keypair.us
+1 805.316.5024

Table of Contents

List of Tables

List of Figures

References

Ref	Full Specification Name
	References used in Approved Algorithms Table
[38A]	NIST SP 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001
[180]	FIPS 180-4, *Secure Hash Standard (SHS)*, August 2015
[197]	FIPS 197, *Advanced Encryption Standard (AES)*, November 2001
[198]	FIPS 198-1, *The Keyed Hash Message Authentication Code (HMAC)* , July 2008
	Other References
[140]	FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 2001
[140DTR]	FIPS 140-2 *Derived Test Requirements*, January 2011
[140IG]	*Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*, August 2020
[131A]	SP 800-131A Rev. 2, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019

Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard, see [197]
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CSP	Critical Security Parameter, see [140]
DPA	Differential Power Analysis
DRBG	Deterministic Random Number Generator, see [90A]
DS101	Key fill device serial protocol (EKMS 603)
DTR	Derived Test Requirements, see [140DTR]
ESW	Embedded Software – synonym for “firmware”
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
HMAC	Keyed-Hash Message Authentication Code, see [198]
IC	Integrated Circuit
HMI	Human Machine Interface
IG	Implementation Guidance, see [140IG]
KAT	Known Answer Test

Acronym	Definition
KW	Key Wrap
JTAG	Joint Test Action Group
NDRNG	Non-Deterministic Random Number Generator
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NVM	Non-Volatile Memory (e.g., EEPROM, Flash)
OS	Operating System
MSS	Microcontroller SubSystem
PRF	Pseudo-Random Function
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard, see [180]
SP	Special Publication
SPA	Simple Power Analysis
SPI	Serial Peripheral Interface
UART	Universal Asynchronous Receiver/Transmitter
USB	Universal Serial Bus
XOR	Exclusive OR

1 Overview

This document defines the Security Policy for the US Army CERDEC Cryptographic Module, hereafter denoted the CERDEC CM. The CERDEC CM, validated to FIPS 140-2 overall Level 3, is a single-chip module providing cryptographic primitive services and key management. The CERDEC CM design utilizes a System-on-a-Chip (SoC) with customized hardware.

The CERDEC CM is a non-modifiable environment under the FIPS 140-2 definitions, with a firmware load function to support necessary updates. New firmware versions within the scope of this validation must be validated through the CMVP; any other firmware loaded into the CERDEC CM is out of the scope of this validation and requires a separate FIPS 140-2 validation.

The CERDEC CM conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

The CERDEC CM makes no claims for mitigations of attacks beyond [140] scope.

Table 1: Security Level of Security Requirements

Security Requirement	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

1.1 Versions, Configurations and Modes of Operation

Hardware: M2S050TS-1FGG896
Firmware: FreeRTOS v7.0.1; Crypto Engine FW 1.0.2
Custom hardware: Crypto Engine FW 1.0PL

The CERDEC CM implements a [140] Approved mode of operation, and a non-approved mode. Three output lines (used to drive LED's external to the module) encode the CERDECM CM status as shown next. Additional status detail is available via the Human Machine Interface (HMI). Power-on self test failure is indicated by the "1B0" LED pattern for Firmware Integrity Test failure, "110" LED pattern for Known Answer Test failure, or "BB0" LED pattern for a master-KEK validation failure. In these displays, "B" indicates a blinking LED.

Table 2: CERDEC CM Status Indicators

LED3	LED2	LED1	State indication
0	0	0	Powered off or zeroized
0	0	1	Approved mode: AES CBC
0	1	0	Approved mode: AES ECB
0	1	1	Approved mode: AES CTR
1	0	0	Non-approved mode: SPECK
1	0	1	Non-approved mode: SIMON
1	1	0	AES KAT Failure
1	B	0	FW Validation failure
1	1	1	System locked, requires power-cycle to restart.
B	B	0	Invalid master-KEK. Unable to load firmware.
B	B	B	Boot process
B	B	B	Blink in sequence. IN-FACTORY state waiting for loading RED master KEK
0: LED off 1: LED on B: LED Blinking			

No CSPs are shared between approved and non-approved modes. The *System locked* state is entered when configuration is changed, a new key is loaded or after too many (3) failed login attempts.

Only the CO is able to load keys required for Approved (AES-CBC, AES-EBC, or AES-CTR) and non-approved (SIMON or SPECK) encryption modes. Only encryption modes that have a key loaded are enabled and can be selected. To change modes of operation, either the Cryptographic Officer or a user connects to the module with the HMI, and selects the desired encryption mode by selecting the radio button corresponding to the desired encryption mode. AES-CBC, AES-EBC, or AES-CTR are FIPS approved modes. SIMON and SPECK are non-approved modes, and are annotated thus on the HMI. Once the encryption method is successfully changed and confirmed, the module enters a locked state and must be rebooted. Once rebooted, the Module is operating in the selected encryption mode.

1.2 Cryptographic Boundary and Physical Security Policy

The CERDEC CM hardware is an application specific variant of a production grade, low power hybrid SoC/FPGA in the Microsemi SmartFusion2 line, enclosed in a ball grid array IC package. the physical form is shown in Figure 1. The cryptographic boundary is the surfaces, edges and solder ball contacts of the package. The FPGA measures 31mm x 31mm, and has 896 pins.

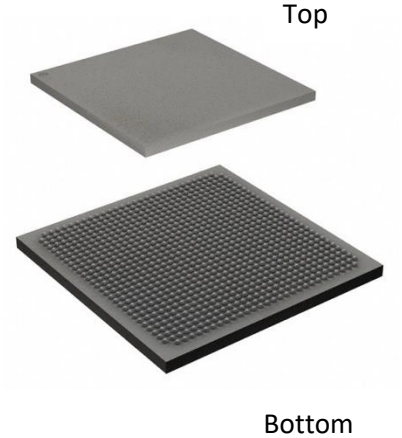

Figure 1: CERDEC CM Physical Form

The packaging material meets [140] single-chip embodiment requirements for opacity, tamper evidence and hardness. The module was only tested at a single temperature, 20ºC (nominal), and no assurance is provided for Level 3 hardness conformance at any other temperature.

The module is installed onto a PCB, leaving only the top surface and edges exposed.

The package shall be inspected as for tamper evidence (scratches or chips in the surface material or surrounding PCB material) on initial installation, on deployment to the new physical environment, and at least once per year.

1.3 Logical Diagram

The nominal SoC-FPGA IC has two major sections: Microcontroller SubSystem (MSS) and Programmable Fabric. The MSS includes dedicated peripherals and memory controllers. The Programmable Fabric incorporates logical elements, memory blocks, and math blocks, and can be configured to form custom subsystems. For the CERDEC CM, two USB2-SOFT USB interfaces and two AES Core G2 (encrypt and decrypt) blocks are incorporated. Figure 2 depicts CERDEC CM major blocks. The fabric is not reprogrammable when the unit is delivered to customers; only the ARM MPU code (Crypto Engine FW) can be updated.

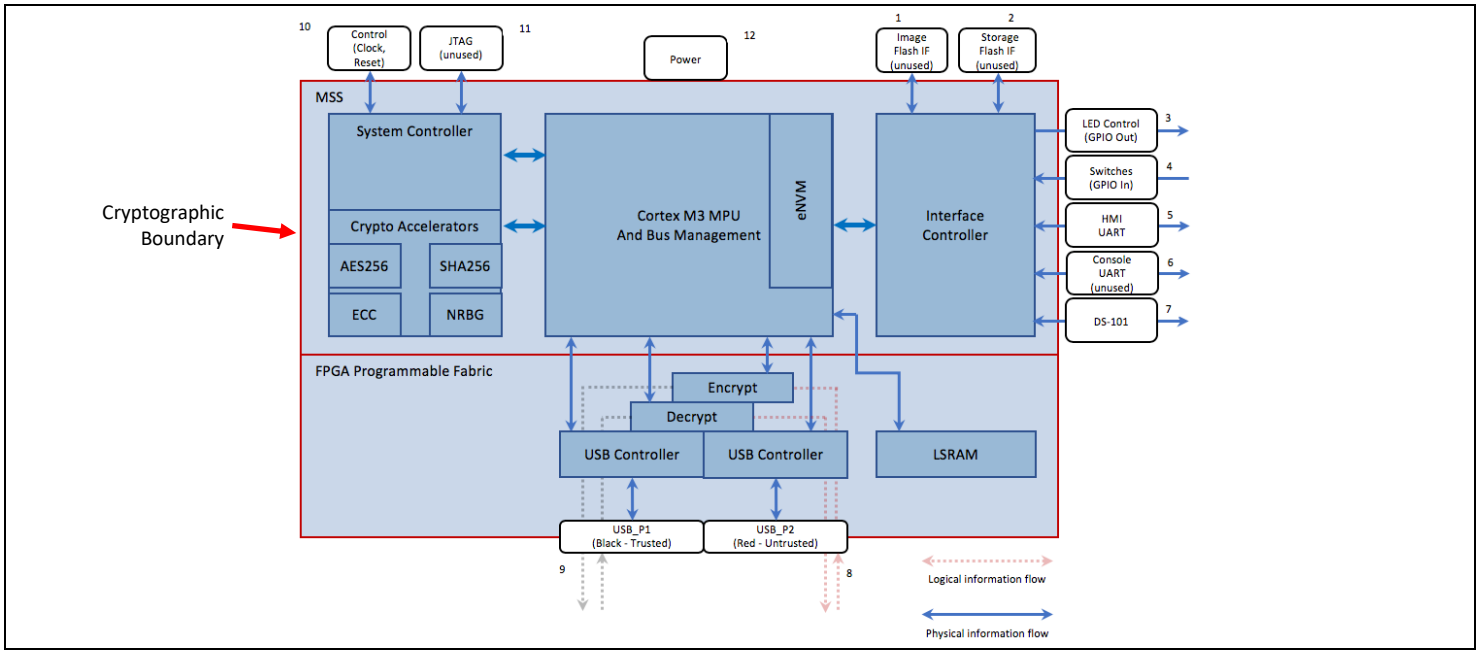

Figure 2: CERDEC CM Block Diagram

Table 3: Ports and Interfaces

ID	Port	Description	Logical Interface Type
1, 2	SPI	Flash memory interfaces - unused	Disabled in the module.
3	GPIO	LEDs: LED1, LED2, LED3	Status output LEDs (status, mode indicators; see above)
4	GPIO	Switches: S1, S2	Control input (to initiate Zeroization)
5	HMI UART	HMI port	Control input, Data input, Data out, Status out
6	Console UART	Console port - unused	Disabled in the module.
7	DS 101	FPGA UART Port 0; DS-101 Key loader interface	Control input, Data input, Status out
8	USB_P2	Red (untrusted) USB	Control input, Data input, Data out, Status out
9	USB_P1	Black (trusted) USB	Control input, Data input, Data out, Status out
10	Reset	Reset input	Control input (signal from external switch to initiate reset)
	CLK	Clock oscillator input	Control input
11	JTAG	Debug - unused	Permanently disabled (M2S050TS configuration option)
12	Power	2.5V, 3.3V, ground	Power

2 Cryptographic Functionality

The CERDEC CM implements the Approved and Allowed cryptographic functions listed below. *Note: any item in curly braces { } is CAVP tested but not used by the module.*

Table 4: Approved Algorithms

Cert	Algorithm	Mode	Strength	Functions, Caveats
374*	AES [197], [38A]	CBC, ECB, CTR, {CFB, OFB} [38A]	Key sizes: {128}, {192}, 256	Encryption and decryption, KEK validation.
1860	HMAC [198]	HMAC-SHA-256	Key sizes: {128}, 256	Message verification.
2472	SHS [180]	SHA-256		Message digest generation.

Table 5: Allowed Algorithms

Cert	Algorithm	Mode	Strength	Functions, Caveats
374*	AES [197], [38A]	CBC, {ECB, CTR, CFB, OFB} [38A]	Key sizes: {128}, {192}, 256	Unwrap encryption key used for transport

** AES-CTR, provided with Certificate #374 addresses CMVP counter requirements as:*

- Counter initial value is loaded during the key fill process. A 128 bit incrementing counter is used to update the counter block.
- An internal IV register and CTR mode counter is used as a loadable counter for CTR mode to assure use of current counter following power cycle.
- The algorithm vendors tested the algorithm sub-system in simulators to verify their correctness before licensing them to be incorporated into complete cryptographic modules. It is not practical to provide the direct access to the algorithms necessary in order to retest them within the CERDEC actual cryptographic module.

Table 6: Non-Approved Cryptographic Functions

Algorithm	Description
SIMON	Encryption and decryption.
SPECK	Encryption and decryption.

2.1 Critical Security Parameters

All CSPs (secret keys and authentication data) implemented by the module are specified in Table 7. The CERDEC CM does not implement asymmetric cryptography (as such, no public or private keys). The module does not output CSPs.

Table 7: Critical Security Parameters

CSP	Description/Usage	EST	STO	OUT	DES
FW-VK	HMAC-SHA256 256-bit secret key used for embedded software verification.	E1, E3	S1	N/A	D1
Master-KEK	AES-256 master key encryption key, used to encrypt all other CSPs.	E1, E2, E3	S2	N/A	D2
Password	14-18 character operator authentication password (instances: two minimum, maximum limited by available memory).	E3, E4	S4	N/A	D4
RB-Cipher	AES-256 secret key used for encryption and decryption over the Red/Black USB interfaces.	E1	S1	N/A	D1
SK-Comp	Split knowledge key component.	E5	S3	N/A	D3

EST: Key establishment methods (inclusive of key generation, key agreement, key derivation and key diversification methods, consistent with the current [140IG] D.2).

- E1: Encrypted (AES-CBC) using Master-KEK, and transported into the module via DS-101 key loader on a physically isolated port.
- E2: Reconstituted using Shamir's secret sharing (split knowledge). Shares (SK-Comp) provided by two separate authenticated COs.
- E3: Default values loaded into the module during factory provisioning phase.
- E4: Updated by *Change Password* service, associated by User identifier.
- E5: Provided to the module during the *Recover* service in plaintext, as split-knowledge key components.

STO: Storage methods

- S1: Stored in on-chip eNVM, encrypted by Master-KEK; memory location (pointer) key-to-entity association
- S2: Stored in on-chip eNVM in plaintext; memory location (pointer) key-to-entity association
- S3: Stored temporarily in RAM during key re-constitution.
- S4: Stored in on-chip eNVM as SHA-256 Hash

(DES) CSP Destruction

- D1: Destruction of Master-KEK renders S1 storage keys unusable
- D2: Overwritten by zeros as a consequence of SW1+SW2 asserted simultaneously (the *Zeroize* service).
- D3: Overwritten with zeros immediately following the *Configure* service process to reconstitute the Master-KEK.
- D4: Destruction of Master KEK removes all user functionality except Master-KEK recovery by two authenticated COs..

3 Roles, Authentication and Services

The CERDEC CM:

- Does not support a maintenance role.
- Clears previous authentications on power cycle.
- Does not permit concurrent operations by operators in different roles.

Table 8 lists all operator roles supported by the CERDEC CM. Identity Based Authentication of each operator and their access to roles and services is as described below.

Table 8: Roles Supported by the CERDEC CM

Role ID	Role Description
CO	Cryptographic Officer - operational role for device and key management, and CO role administration.
User	User – operational role for key management and user role administration.

3.1 Password verification authentication method

CERDEC CM passwords are entered using the HMI, and require a minimum of 14 one-byte characters and accept a maximum of 18 characters. The password character space is restricted to 94 characters (the printable ASCII characters except the space character – see https://en.wikipedia.org/wiki/ASCII#Printable_characters).

Keyboard presses used to enter the password are displayed as asterisks ('*'). The password is transported from the HMI to the CM using HMI Interface, wrapped in SHA256. The HMI responds to invalid username / password combinations with two messages: "Username is not found" and "Incorrect password. Try again."

The probability that a random attempt will succeed in generating an identical SHA-256 hash is:

- 1/(2^256) = 8.64E-78 (better than the 1 in 1,000,000 required by 140-2).

The probability that a random attempt will succeed selected the identical password method is:

- 1/(94^14) = 2.38E-28 (better than the 1 in 1,000,000 required by 140-2).

The CERDEC CM enforces a maximum of 3 failed authentication attempts. The probability that a random attempt will succeed over a one-minute interval is:

- 3/(94^14) = 7.13E-28 (better than the 1 in 100,000 required by 140-2).

3.2 Services

All services implemented by the CERDEC CM are listed in the tables below along with CSP access per service.

Table 9: Unauthenticated Services

Service	Description	Service access to CSPs
Cipher	Provide encryption and decryption of traffic through the Red / Black USB interfaces.	Executes using the selected RB-Cipher key. Execute Algorithm.
Connect	Establish a CM secure communications connection.	
Disconnect	Close a CM connection.	
Restart	Restart the CM (inclusive of power-on self-tests) by pressing the physical reset button.	
Self Test	Upon module startup, verify CSP is valid, conduct KAT, and validate software integrity.	Use the Master-KEK to decrypt CSP and validate CSP by checking the 12-byte CSP tag. Read CSP Validate software integrity against the signature stored in CSP. Read CSP
Shutdown	Shut down the CM by removing power to the CM.	
Status	HMI issues configuration changes to CryptoEngine. Upon status change, an ACK message includes current status details.	Use HMI ACK messages to update status. Read/Write CSP.
Zeroize (Factory reset)	Destroy Master-KEK as an aspect of a module “factory” reset, returning the module to the uninitialized configuration.	Zeroize: Overwrites Master-KEK, which renders FW-VK and RB-Cipher unusable. Write CSP.

The Master-KEK key is used to decrypt any CSP prior to use.

The *Cipher* service is the flow of traffic in and out of the red and black USB ports using the RB-Cipher key. Unlike other services, this communications path does not use the HMI communications path other than to be enabled for use. The *Cipher* service is either enabled or disabled, and does not implement bypass. The selection of the RB-Cipher key instance for use with the *Cipher* service (as opposed to SIMON or SPECK keys) decrypts and loads the RB-Cipher key into the dedicated hardware (Cert#374) AES engine.

The *Connect* service establishes a connection between the Crypto Engine and the HMI application for all HMI message traffic.

The *Disconnect* service closes the HMI channel, requiring a new *Connect* request to restart HMI communications.

The *Status* service provides operational information, such as current encryption mode, in response to initial HMI connect or HMI status change commands. Current status information is provided in the HMI Ack response to authenticated users and is used to update the HMI. LEDs illuminate to indicate current device status as discussed in Table 2.

The *Zeroize* service is invoked by simultaneous assertion (logic 0) of the SW1 and SW2 inputs.

Table 10: Authenticated Services

Service	Description	CO	User	CSP Access
Change password	Update a CO or user password.	X	X	Password is SHA256 encrypted; verifies old Password, updates Password with new value received as input. Write CSP.
Configure	CO: List, load or remove keys. User: List keys; select traffic encryption algorithm key.	X	X	Uses Master-KEK to encrypt loaded keys; Update FW-VK with new value; RB-Cipher: input new keys or delete existing keys. Read/Write CSP.
FW Update	Update embedded firmware.	X		Verify FW image or patch using FW-VK.
Login	Authenticate a CO or user operator.	X	X	The *Login* service authenticates the operator to a role using the Password. The assigned role is fixed when the account is created. The user cannot change roles. Read CSP.
Recover	Reconstitute the Master-KEK using Shamir's secret sharing.	X		Recovers Master-KEK, using SK-Comp shares input over the HMI interface. Write CSP.
Add/Remove User	CO: Add new user with type and password, or Remove existing user.	X		Password is SHA256 encrypted. User type (Admin, User). Username, Password, and Type are received as input. Write CSP.
Shutdown	HMI issues shutdown command	X	X	Authenticated user issues Shutdown command
Restart	HMI issues restart command	X	X	Authenticated user issues Restart command

The *Configure* service allows the operator to list RB-Cipher options (as descriptions - the key value is not output), load or remove a RB-Cipher key, load or remove a secure communications key.

The *Recover* service uses Shamir's secret sharing algorithm to accept unique key components from two authenticated COs, to reconstitute the Master-KEK. The Master-KEK cannot be recovered with only a single component. SK-Comp values are zeroized after completion of the *Recover* service.

4 Self-test

4.1 Power-On Self-tests

On power-on or reset, the CERDEC CM performs self-tests as described in Table 11 below, automatically without operator intervention. All power-on self-tests must be completed successfully prior to any other use of cryptography by the CERDEC CM. If KEK validation fails, the system enters an Error state (ERRKek). If firmware integrity check fails, the system enters an Error state (Err2). If any other power-on self-test fails, the system enters the FSM *ERR* state, with the *Power-on self-test failure* indicator as shown in Table 2. The CERDEC CM inhibits all cryptographic processing and will not provide services unless all self-tests have successfully completed. The host device can reset the CERDEC CM to retry the power-on self-test, which on successful execution clears the error state.

Successful completion of self-test and the [140] approved mode of operation is indicated by any of the approved state indicators shown in Table 2 (001, 010, 011). Once an HMI connection is successfully established, the CERDEC CM replies with a HMI-ACK message that also contains: current CM firmware version and Encryption Method (AES-CBC, AES-EBC, AES-CTR, SPECK, or SIMON).

Table 11: Power-On Self-Tests

Test Target	Description
AES (Cert#374)	Critical Function Test, AES-256-CBC Decrypt CSP, verify CSP is valid format.
AES (Cert#374)	Separate AES-256 CBC Encrypt and Decrypt KATs.
FW Integrity (using HMAC (Cert#1860)	HMAC-SHA256 integrity test over all embedded firmware in the cryptographic boundary. Inclusive of the HMAC-SHA256 KAT and SHA-256 KAT per IG 9.3.

4.2 Conditional Self-Tests

The module implements the conditional self-tests in Table 12 during firmware updates. A failure of the FW Load test results in a *FW Update* service error response on the HMI as described in [CS} section 2.6.2 and [CESS} section 3.2. the image that failed authentication is discarded, automatically clearing the error state. The CM must be restarted to return to normal operations.

Table 12: Conditional Self-Tests

Test Target	Description
FW Load	When new firmware is loaded into the CERDEC CM using the Update service, the CERDEC CM verifies the integrity of the entire firmware image using HMAC-SHA-256 (Cert#1860).

5 Security Rules and Guidance

The CERDEC CM implements and enforces the following security rules:

- No additional interface or service is implemented by the CERDEC CM which would provide access to CSPs.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- Data output is inhibited during self-tests, zeroization, and error states.
- During boot and self-tests, only the HMI port is open to accept an HMI connection request. All other ports are closed.
- USB Red and Black ports are activated after successful completion of software integrity test, self-test, AES KAT, and the operating configuration is loaded.
- Default passwords (12345678901234) for initial Admin users (Admin1, Admin2) should be changed on receipt.
- To assure security, when using AES-CTR encryption mode, do not load KEY+IV repeatedly into a single CM, or into multiple CM.
- Passwords must be 14 – 18 Printable characters. This is enforced by the HMI.
- As described in section 3 of the FIPS 140-2 CO and User Guidelines, a separate encryption key is required for AES, SPECK and SIMON encryption methods. Once the CO loads an appropriate key for an encryption method, and the CM is reboot/reset, the corresponding encryption method is activated.
- As described in Appendix A, Section 1.2 of the FIPS 140-2 CO and User Guidelines. CM firmware can be updated by an authenticated CO. The CM firmware image and associated Firmware Update Authentication Key are encrypted, and will be provided from the CM authority.