coCrypt CM1+

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.3

Date: 2016-02-09

Information Grade: NON-PROPRIETARY

Document Revision History

Revision	Date	Notes
0.1	2015-04-07	Created document
0.2	2015-07-06	Updated tables and figures
1.0	2015-08-27	Revised during FIPS operational test
1.1	2015-10-05	Prepared for public release.
1.2	2015-10-21	Updated FW Version
1.3	2016-02-09	Corrected figure 4 and added condition for physical hardness testing

Table of Contents

Table of Figures

List of Tables

1 Module Overview

The coCrypt CM1+ is a USB compatible hardware encryption device that resides in the data path between a USB host controller and a USB or micro SD Card (via SDIO) storage device. It applies Advanced Encryption Standard (AES) encryption at the sector level to protect data at rest from intentional or inadvertent disclosure. The coCrypt CM1+ loads its cryptographic keys over an external RS-232 interface, logically and physically separated from the data path.

coCrypt CM1+ supports multiple key lengths (128, 192, and 256 bits) and up to 32 different keys per user. Each key can be allocated any non-overlapping sector range on the storage medium. The coCrypt CM1+ is a multi-chip embedded module and is encapsulated in a hard, opaque, tamper-evident coating. The validated version of the product is:

Hardware Version: PCBA P/N HGD-59401600 with PCB P/N HGD-59300063, Rev G

Firmware Version: coCrypt CM1+ HW v1.8.8.4, CM1+ FW v1.8.7.5, Host Controller FW v1.0.5.8

Figure 1 shows a conceptual diagram of the module. Figure 2 and Figure 3 show the actual module, where the cryptographic boundary encompasses the entire device.

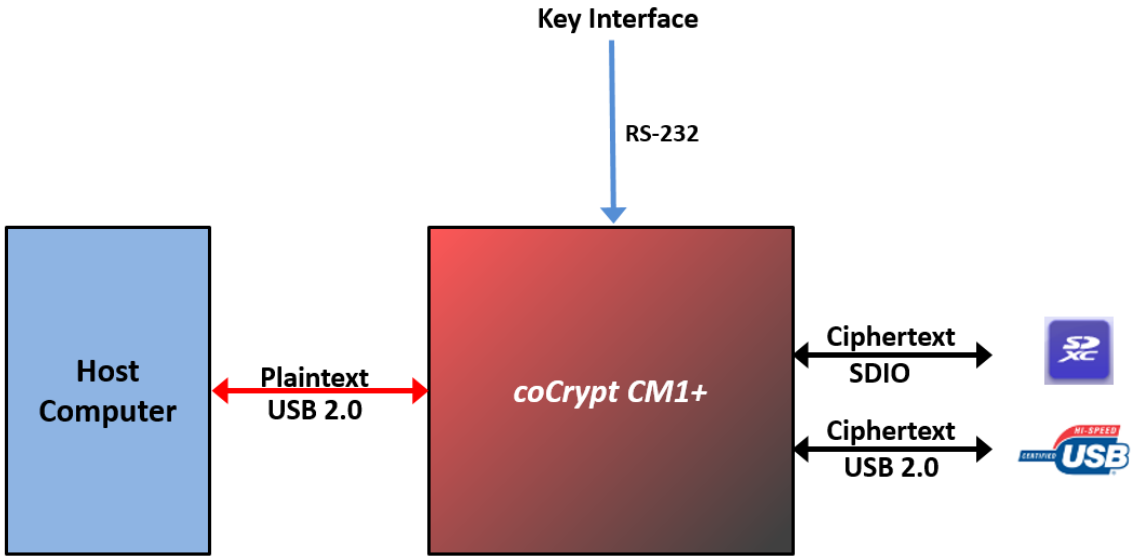

Figure 1: The coCrypt CM1+ conceptual diagram.

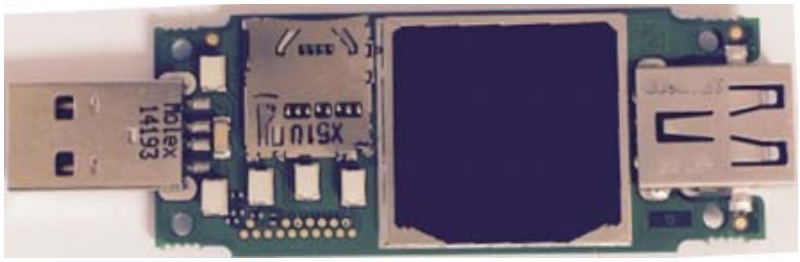

Figure 2: The coCrypt CM1+ module (top view) – The boundary encompasses the entire device.

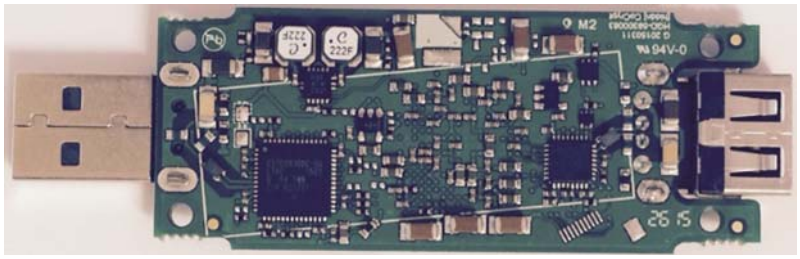

Figure 3: The coCrypt CM1+ module (bottom view) – The boundary encompasses the entire device.

2 Security Level

The cryptographic module meets the overall requirements applicable to FIPS 140-2 security level 3.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
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 Test	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

3.1 Approved Mode of Operation

The validated coCrypt CM1+ cryptographic module always operates in FIPS-mode, and supports FIPS approved and allowed algorithms as follows:

- Advanced Encryption Standard (AES) [#1] with 128-, 192-, and 256-bit keys for encryption and decryption in CBC mode (Cert. #3362)
- AES (Cert. #3362, key wrapping; key establishment methodology provides 192 bits of encryption strength)

The operator can verify that the module is the correct FIPS validated version in the following way: firstly, the overall product name is labeled with an identifier starting with CC01. Secondly, by entering the admin menu, the FW versions can be identified to match the version information on the certificate. Refer to the “[hiddn] coCrypt User Manual”, Chapter 5 for exact step-by-step procedure for verifying the version information.

3.2 Non-FIPS Mode of Operation

The validated coCrypt CM1+ cryptographic module does not support non-FIPS modes of operation.

4 Ports and Interfaces

Figure 4 shows the interfaces to the module. It also shows the CM1+ crypto core that encrypts data, and the Storage Media Controller module, which provides bridging to the USB and the SDIO protocol.

The coCrypt CM1+ receives data encryption keys over the Key Interface (E4) in encrypted form. Status messages intended for the operator are transmitted over this interface. Extended status information is provided on the Status Interface (E5).

When key loading is completed the coCrypt CM1+ checks if a USB storage device is present at the Device USB Interface (E3). If found, this is presented to the host computer connected to the Host USB Interface (E1). If no USB device is found, the next step is to attempt to detect a microSD card connected to the Device SDIO Interface (E2). If a micro SD card is found, this storage device is presented to the host computer over the Host USB Interface (E1). Depending on the type of storage device present, a status message is provided over the Key Interface (E4).

The Utility Interface (E6) provides inputs for resetting and zeroizing the module.

The Power Interface (E7) provides 5.0V supply and 3.7V LiPo battery power.

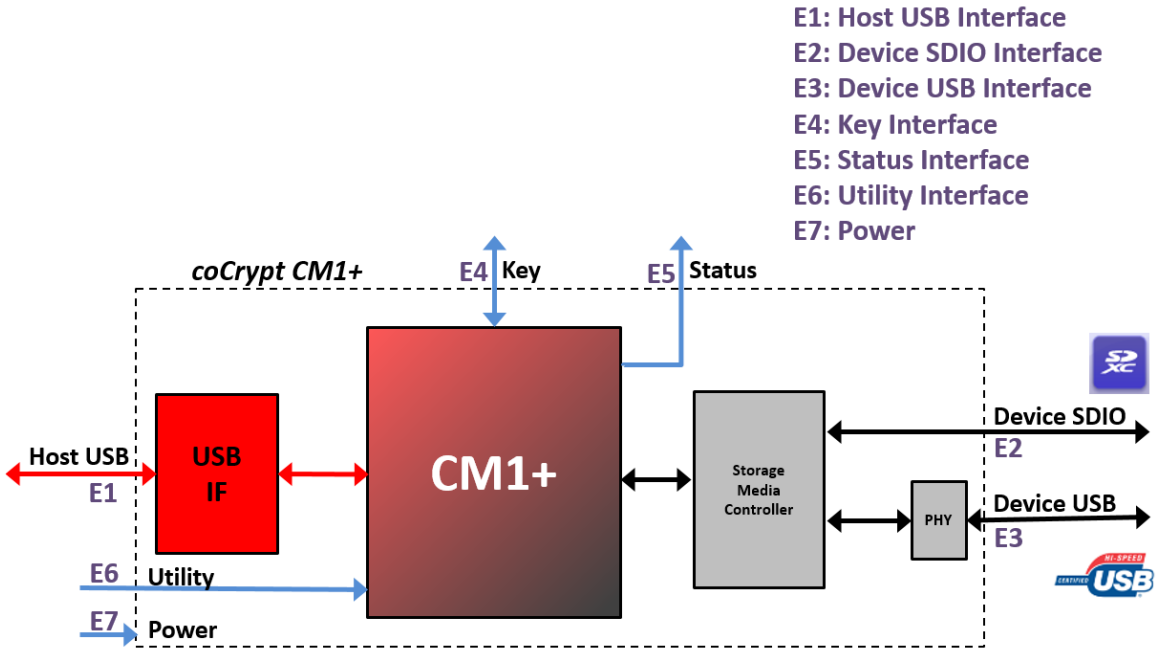

Figure 4: The coCrypt CM1+ ports and interfaces

Table 2: Logical & Physical Interfaces

Physical Port Interface	Description	Logical Interfaces Types
E1: Host USB Interface	Interface to host computer for reading/writing plaintext data.	Data Input Data Output Control Input Status Output
E2: Device SDIO Interface	Interface to SDIO storage device. Connected to microSD reader on board.	Data Input Data Output Control Input Status Output
E3: Device USB Interface	Interface to USB storage device. Connected to USB receptacle on board.	Data Input Data Output Control Input Status Output
E4: Key Interface	RS-232 interface for loading keys (encrypted) and sending status messages to the operator.	Data Input Control Input Status Output
E5: Status Interface	Extended status information.	Status Output
E6: Utility Interface	Zerioze input for immediate clearing of key material. Also contains Reset input.	Control Input
E7: Power Interface	Power input from USB and connection to rechargeable LiPo battery. Power output to SDIO storage (microSD card) and USB device.	Power

5 Identification and Authentication Policy

5.1 Assumption of roles

The coCrypt CM1+ cryptographic module supports two distinct operator roles, User and Crypto Officer. The cryptographic module enforces the separation of roles using identity-based operator authentication. The operator of the cryptographic module is uniquely identified by possession of the correct Key Token (smart card) which is uniquely assigned to each individual operator. Possession of the particular Key Token also establishes the role that is assigned to the operator.

Table 3: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	AES 192-bit Keys
Crypto Officer	Identity-based operator authentication	AES 192-bit Keys

Table 4: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Crypto Officer Key	The probability that a random attempt will succeed or a false acceptance will occur is 2^{-192}, which is less than 1/1,000,000. Authenticating to the module is limited by a timeout period longer than one (1) second, resulting in a probability of successfully authenticating to the module within one minute is $< 60*2^{-192}$, which is less than 1/100,000. Maximum number of authentication attempts within one minute is 60.
User Key	The probability that a random attempt will succeed or a false acceptance will occur is 2^{-192}, which is less than 1/1,000,000. Authenticating to the module is limited by a timeout period longer than one (1) second, resulting in a probability of successfully authenticating to the module within one minute is $< 60*2^{-192}$, which is less than 1/100,000. Maximum number of authentication attempts within one minute is 60.

6 Access Control Policy

6.1 Roles and Services

Table 5: Services Authorized for Roles

Role	Authorized Services	Description
Crypto Officer	Crypto Officer Authentication	This service authenticates the Crypto Officer to the coCrypt CM1+ cryptographic module.
	Set Crypto Officer Key	This service loads the Crypto Officer Key into the coCrypt CM1+ cryptographic module.
	Set User Key	This service loads the User Key into the coCrypt CM1+ cryptographic module.
	Set Device Keys	This service loads Device Keys into the coCrypt CM1+ cryptographic module.
	Set Media Resident Keys	This service loads the Media Resident Keys into the coCrypt CM1+ cryptographic module.
User	User Authentication	This service authenticates the User to the coCrypt CM1+ cryptographic module.
	Set Media User Keys	This service loads the Media User Keys into the coCrypt CM1+ cryptographic module.
	Encrypt Data	This service encrypts plaintext user data passed into the cryptographic module.
	Decrypt Data	This service decrypts encrypted user data passed into the cryptographic module.
Unauthenticated	Show Status	This service provides the status of the cryptographic module.
	Self-Test	This service executes the cryptographic algorithm test for the AES security function using a known answer test, and firmware integrity tests using a 16-bit EDC.
	Zeroization	This service erases all plaintext Critical Security Parameters (CSPs) that are stored in the coCrypt CM1+ cryptographic module (volatile and non-volatile) memory.
	Reset	This service erases all plaintext Critical Security Parameters (CSPs) that are stored in the coCrypt CM1+ cryptographic module volatile memory.

6.2 Definition of Critical Security Parameters

Table 6 presents the defined Critical Security Parameters (CSPs) and their descriptions.

Table 6: Critical Security Parameter Definitions

CSP	Description/Usage
Media Resident Key (MRK)	Up to 32 AES 128-, 192-, or 256-bit resident component (key share) of AES media keys (Media Device Key) – Usage optional
Media User Key (MUK)	Up to 32 AES 128-, 192-, or 256-bit User component (key share) of AES media keys (Media Device Key)
Media Device Key (MDK)	Up to 32 AES 128-, 192-, or 256-bit key for encrypting and decrypting data to and from the protected storage media. If MRK is in use: MDK(n) = MUK(n) XOR MRK(n), for n=0..31 If MRK is not in use: MDK(n) = MUK(n), for n=0..31
Crypto Officer Key	AES 192-bit key for encrypting link layer communications between operator token and the cryptographic module; used to authenticate operator in Crypto Officer role.
User Key	AES 192-bit key for encrypting link layer communications between operator token and the cryptographic module; used to authenticate operator in User role.
Device Key 1	AES 192-bit key for encrypting Media User Key attributes.
Device Key 2	AES 192-bit key for encrypting the Media User Key.

6.3 Definition of Public Keys

There are no public keys contained in the coCrypt CM1+ cryptographic module.

6.4 Definition of CSPs Modes of Access

Table 7 defines the relationship between access to CSPs and the different module services. The following modes of access are used within the table:

- R = Read: The Module reads the CSP.
- W = Write: The Module writes the CSP.
- I = Input: The Module receives the CSP. (i.e., it enters the module).
- Z = Zeroize: The module zeroizes the CSP in both volatile and non-volatile memory.
- V = Zeroize Volatile: The module zeroizes the CSP in volatile memory.

Table 7: CSP Access Rights within Roles & Services

	CSPs						
Authorized Services	**Media Resident Key**	**Media User Key**	**Media Device Key**	**Crypto Officer Key**	**User Key**	**Device Key 1**	**Device Key 2**
Crypto Officer Authentication				R			
Set Crypto Officer Key				I R W			
Set User Key				R	I W		
Set Device Keys				R		I W	I W
Set Media Resident Keys	I W			R			
User Authentication					R		
Set Media User Keys	R	I R V	W		R	R	R
Encrypt Data			R				
Decrypt Data			R				
Show Status							
Self-Test							
Zeroization	Z	V	V	Z W	Z	Z	Z
Reset	V	V	V	V	V	V	V

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the coCrypt CM1+ cryptographic module does not contain a modifiable operational environment.

8 Security Rules

The coCrypt CM1+ cryptographic module's design corresponds to the coCrypt CM1+ cryptographic module's security rules.

8.1 Security Rules Derived from FIPS 140-2

1. The cryptographic module provides two distinct operator roles. These are the User role, and the Crypto Officer role.
2. The cryptographic module provides identity-based authentication.
3. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
4. The cryptographic module encrypts and decrypts communications with the Key Token using the AES algorithm and 192-bit key length.
5. The cryptographic module encrypts and decrypts data using the AES algorithm.
6. The cryptographic module performs the following Power up Self-Tests:
   - Firmware Integrity Test (16-bit CRC EDC)
   - AES Known Answer Test for encrypt and decrypt using 256-bit key
7. If the integrity test fails, the module provides the status "No CM detected".
8. If a power up self-test fails, the module goes into the state "ALARM STATE" and the module will become inactive.
9. The cryptographic module performs the following Critical Functions:
   - Bypass Detection. The ciphertext is continuously compared to the plaintext and if 3 AES blocks are detected equal the module will immediately enter "ALARM STATE" and block data transfers.
   - MRK Integrity Tests. The MUK is loaded together with a known answer. A hardware function validates the expected response and if there is a mismatch, the module immediately enters an "ALARM STATE".
10. Data output is closed during error states, zeroization and self-tests.
11. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
12. The module does not support concurrent operators.

8.2 Security Rules Imposed by the Vendor

The Crypto Officer must follow the procedures outlined in the "[hiddn] coCrypt User Manual" (Chapter 4) to initialize the cryptographic module from its default manufacturing state and after zeroization.

The operator must identify that the module is the correct FIPS validated version as previously described in Section 3.1.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The coCrypt CM1+ cryptographic boundary is protected using a tamper resistant, hard, production grade, opaque epoxy encapsulation of all non-excluded circuitry and components within the module. The module is designed so that removal of this epoxy and penetration attempts cause serious damage, and any attempt to open the enclosure shows clear tamper evidence. Hardness testing was only performed at ambient temperature (23°C); no assurance is provided for Level 3 hardness conformance at any other temperature.

9.2 Operator Required Actions

The operator is required to inspect the coCrypt CM1+ cryptographic module upon every usage of the device, for evidence of attempts to tamper with the module. In the event of tamper evidence, please contact the organization or company that provided the module immediately.

10 Mitigation of Other Attacks Policy

The FIPS 140-2 Area 11 Mitigation of Other Attacks requirements are not applicable because the coCrypt CM1+ cryptographic module does not address attacks outside of the scope of FIPS 140-2.