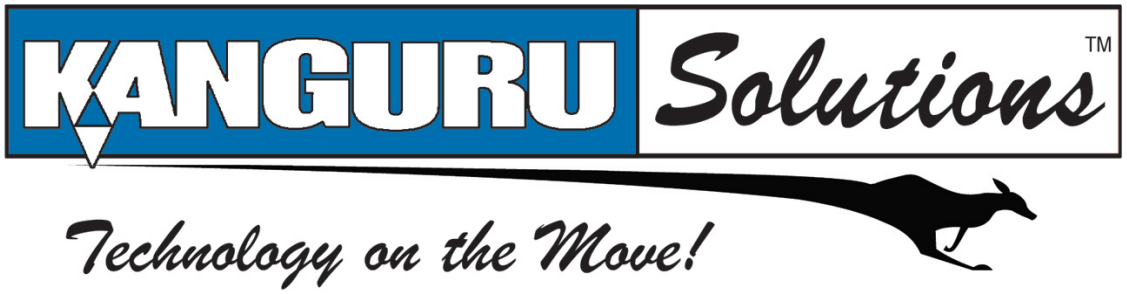

KDH3000-CM

FIPS 140-2 Non-Proprietary Security Policy
Document Revision: 1.0
H.W. Version: 1.0
F.W. Version: V01.04.0000.0000

Revision History

Author(s)	Version	Updates
Nate Cote, Kanguru Solutions	1.0	Initial public release.

Introduction

The "Cryptographic Module" for the Kanguru Defender HDD 3000 is the KDH3000-CM, herein after referred to as "cryptographic module" or "module", (HW Version: 1.0; FW Version: V01.04.0000.0000). It is a FIPS 140-2 Level 2 multi-chip embedded module with an on-chip RISC processor and an integrated hardware cipher engine which supports real time, on the fly AES encryption/decryption of data to secure data at rest. The module is a ruggedized, opaque, tamper-resistant USB disk encryption/file encryption device that connects to an external general purpose computer (GPC) outside of its cryptographic boundary to serve as a secure peripheral storage drive for the GPC. The device connects to the GPC via a Micro USB 3.0/2.0 interface and to the HDD or SSD from a SATA interface. The module is a self-contained device that automatically encrypts and decrypts data copied to and from the drive from the externally connected GPC.

All files distributed with the module that are loaded into the GPC (client application and PC configuration data) are excluded from the validation.

The Kanguru KDH3000-CM has been specifically designed to address sensitive data concerns of Government and security conscious customers in a variety of markets.

Cryptographic Boundary

The physically contiguous cryptographic boundary is defined by the outer perimeter of the epoxy covered PCBA of the device. The cryptographic module does not contain any removable covers, doors or openings. The cryptographic module is available in only one approved configuration:

Table 1 - Kanguru KDH3000-CM

Part Number	*HW Version*	*FW Version*
KDH3000-CM	1.0	V01.04.0000.0000

The cryptographic module can be connected to various capacities of HDD and SSD.

The following photographs (Figures 1 – 6) demonstrate the various views of the module. The cryptographic boundary of the module is defined by the area that the epoxy potting covers, which can be seen in Figure 1 – 3 below.

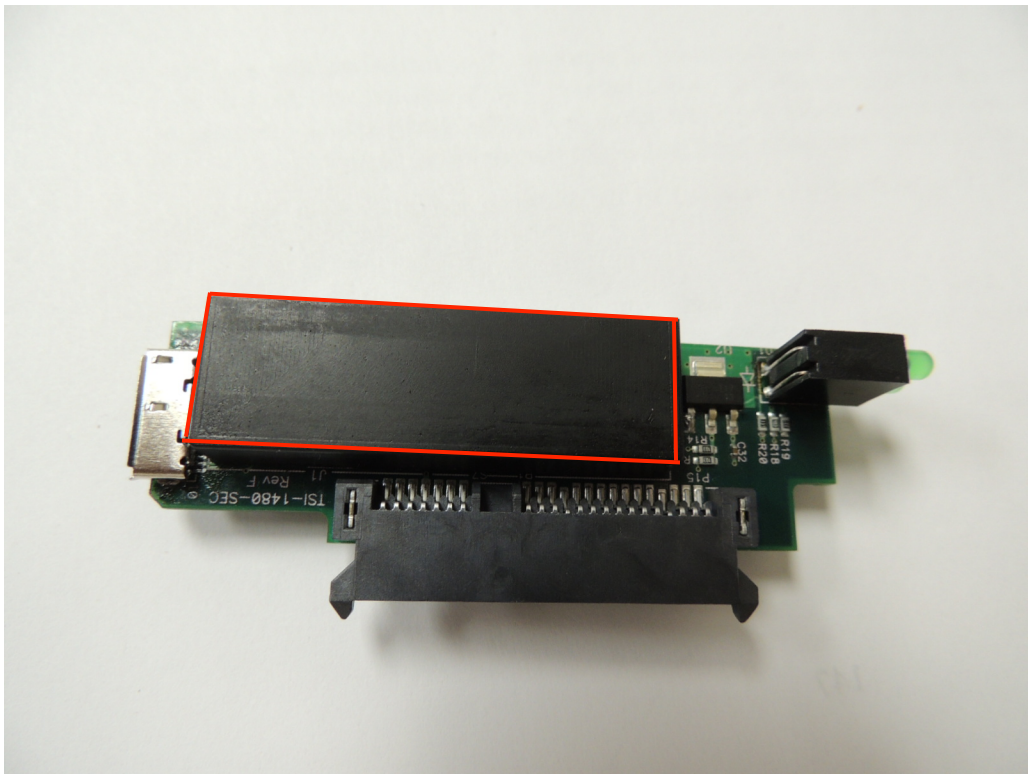

Figure 1 – KDH3000-CM – Top side view. The cryptographic boundary is defined by the area that the epoxy potting covers, which is highlighted in red.

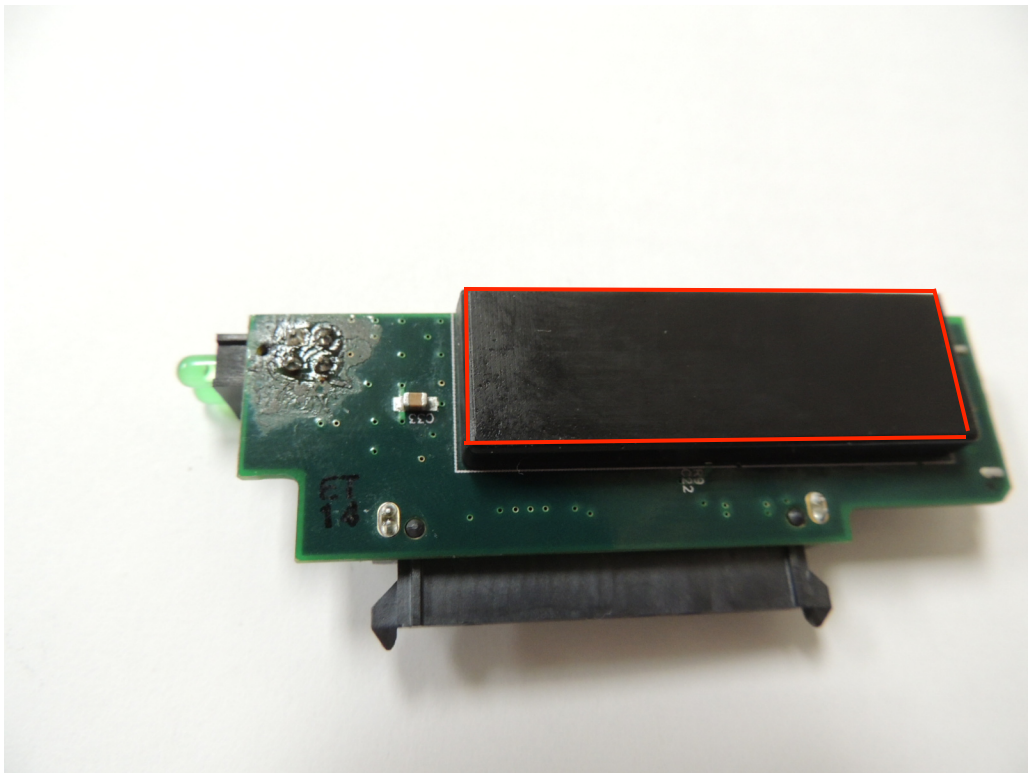

Figure 2 – KDH3000-CM – Bottom side view. The cryptographic boundary is defined by the area that the epoxy potting covers, which is outlined in red.

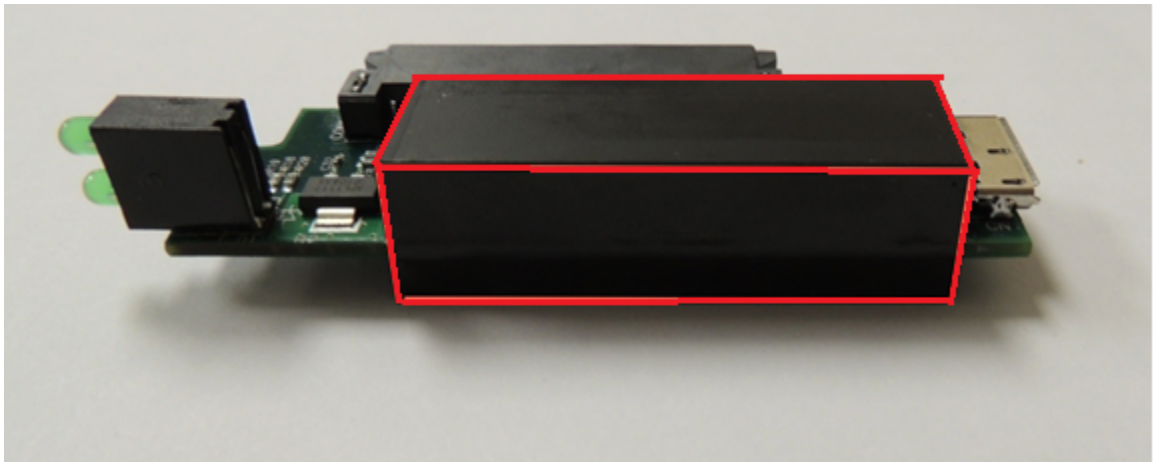

Figure 3 – KDH3000-CM –Right side view. The cryptographic boundary is defined by the area that the epoxy potting covers, which is outlined in red.

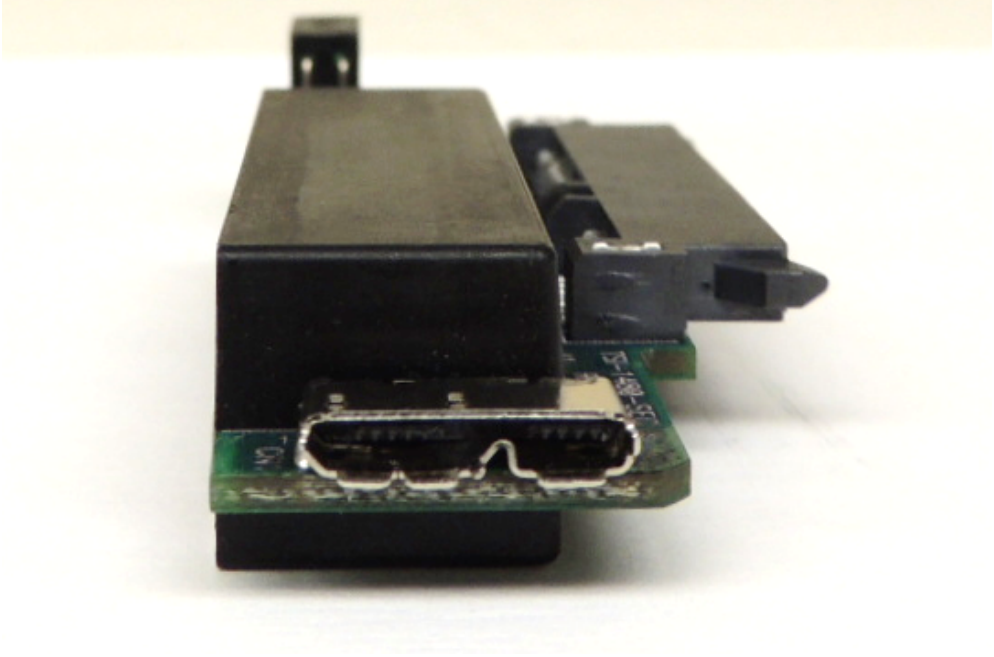

Figure 4 – KDH3000-CM – Front side view demonstrating the Micro USB port.

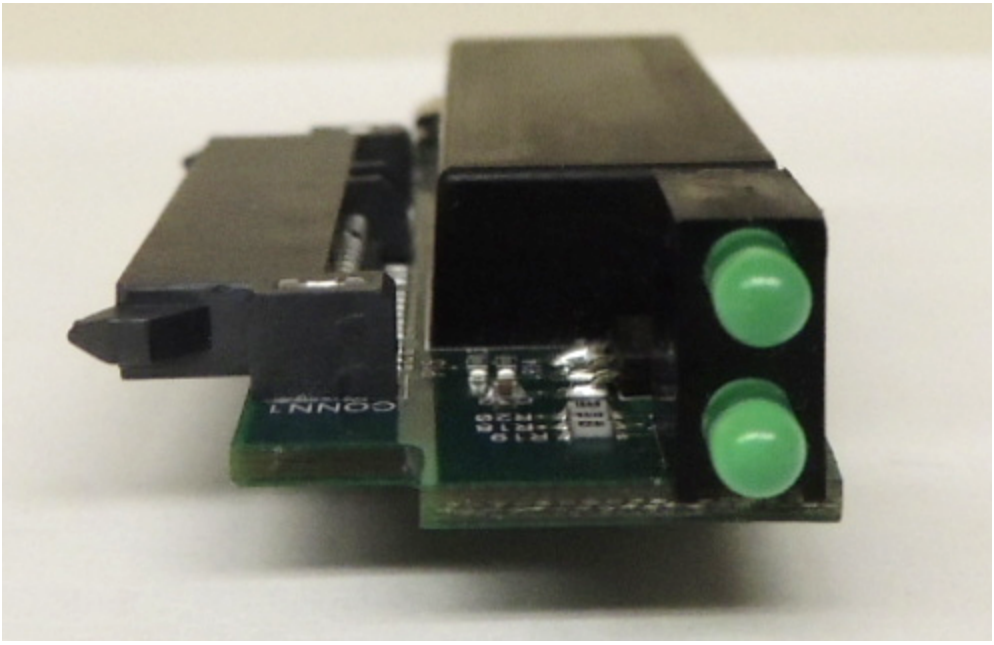

Figure 5 – KDH3000-CM – Back side view demonstrating the LEDs.

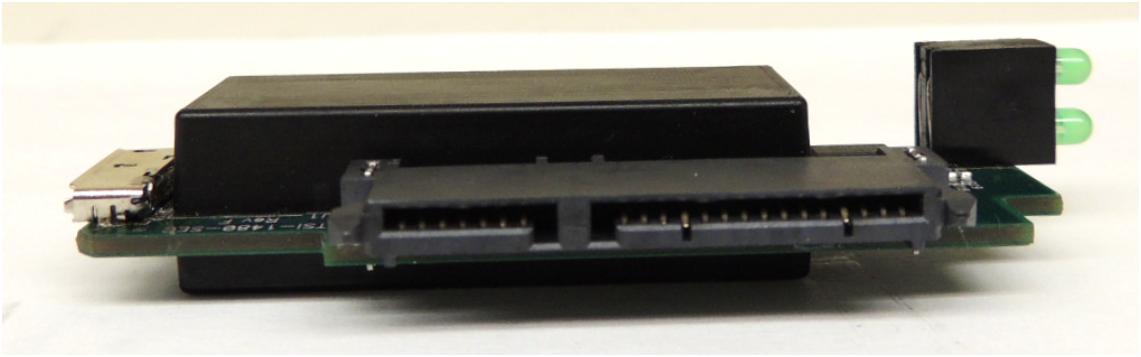

Figure 6 – KDH3000-CM – Left side view demonstrating the SATA port.

Security Level Specification

Security Requirements Area	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Exhibit 1 – *Security Level Table*

Approved algorithms

The cryptographic module supports the following Approved algorithms for secure data storage:

- AES with 256-bit key in XTS mode Encrypt/Decrypt (Cert. #1623)
- SHA-256 (Cert. #2144)
- NIST800-90 DRBG Hash_DRBG mode with SHA256 core (Cert. #376)

Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length. This module provides 256 bits of equivalent encryption strength.

Non-Approved algorithms

- NDRNG (HWRNG to generate seeds for the DRBG)

Physical Ports and Logical Interfaces

A single physical Micro USB3.0/2.0 port is exposed on the top front side of the module (see Figure 4) that supports all logical interfaces (data input, data output, control input, status output, power) from the GPC. A SATA port (see Figure 6) is exposed at the side for data interface with the storage disk. Two light emitting diodes (LEDs) are located at the bottom of epoxied unit for power and status output. The cryptographic module does not contain a maintenance interface. Exhibit 2 summarizes the physical ports and logical interfaces:

Physical Port	Logical Interface
Micro USB3.0 / 2.0	Data Output Data Input Control Input Status Output Power
SATA HDD/SSD	Data Output Data Input Power
LED	Status Output

Exhibit 2 – *Specification of Cryptographic Module Physical Ports and Logical Interfaces*

Security rules

The following specifies security rules under which the cryptographic module shall operate in accordance with FIPS 140-2:

- The cryptographic module does not support a non-FIPS mode of operation and only operates in an Approved mode of operation. The module is configured at production time with the approved firmware and approved configuration settings.
- The cryptographic module provides logical separation between all of the data input, control input, data output and status output interfaces. The module receives external power inputs through the defined power interface.
- The cryptographic module supports identity based authentication for all services that utilize CSPs and Approved security functions.
- The data output interface is inhibited during self-tests, zeroization, and when error states exist.
- When the cryptographic module is in an error state, it ceases to provide cryptographic services, inhibits all data outputs, and provides status of the error.
- The cryptographic module does not support multiple concurrent operators.

- When the cryptographic module is powered off and subsequently powered on, the results of previous authentications are not retained, and the cryptographic module requires the operator to be re-authenticated using identity based authentication.
- The cryptographic module protects CSPs from unauthorized disclosure, unauthorized modification and unauthorized substitution.
- The cryptographic module protects public keys from unauthorized modification, and unauthorized substitution.
- The cryptographic module satisfies the FCC EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).
- The cryptographic module implements the following self-tests:

  Power-up self-tests

  - Firmware integrity test (SHA256 HASH verification)
  - SHA-256 KAT
  - AES-256 XTS Encrypt KAT
  - AES-256 XTS Decrypt KAT
  - SP800-90 DRBG KAT
  - Critical functions Test: Continuous test on non-Approved NDRNG (HWRNG)

  Conditional self-test

  - Continuous test on SP800-90 DRBG
  - Continuous test on non-Approved NDRNG (HWRNG)
  - Critical functions: CSP integrity test (via SHA25 HASH verification)
- Manual key entry is not supported and the cryptographic module does not implement manual key entry tests.
- The cryptographic module does not support bypass capability and does not implement bypass tests.
- The module has two LEDs: one LED shows power status, and the other LED provides status that the module is in the Approved mode of operation or if there is activity.
- The status indicator output by the module when a power-up self-test or conditional self-test fails or if the module enters into an error state is flashing on the status output LED in a continuous fashion.
- All maintenance related services (i.e. maintenance role, physical maintenance interface, logical maintenance interface) are not applicable.
- Plaintext CSP output is not supported.

- The cryptographic module does not contain dedicated physical ports for CSP input/output.
- The power interfaces cannot be used to drive power to external targets.
- The continuous comparison self-tests related to twin implementations are not applicable.
- Upon authenticating into a particular role, it is not possible to switch into another role without re-authenticating.
- The cryptographic module does not provide feedback in regards to authentication data.
- The finite state model does not support the following states: maintenance, CSP output.
- The cryptographic module is not a radio and does not support any wireless interfaces or OTAR.
- The requirements of FIPS 140-2 Section 4.11 are not applicable; the cryptographic module is not designed to mitigate specific attacks beyond the scope of FIPS 140-2.

Identification and Authentication Policy

Exhibit 3 defines the roles, type of authentication, and associated authenticated data types supported by the cryptographic module:

Role	Type of Authentication	Authentication Data
Master/Cryptographic Officer: responsible for initialization, physical security inspection, and administrative functions.	Identity-based	Password (8 to 136 bytes)
User: the end user of the product that utilizes the module under the direction of the Master/Cryptographic Officer.	Identity-based	Password (8 to 136 bytes)

Exhibit 3 - *Roles and Required Identification and Authentication (FIPS 140-2 Table C1)*

In order to properly initialize the module to operate in FIPS Approved mode after receiving the module from the factory, the Master/Cryptographic Officer must:

1) Authenticate using the factory default password.
2) Run the doIdentify command to verify that the drive is unlocked.
3) Change the Master/Cryptographic Officer Password.

Exhibit 4 defines the strength of the implemented identity-based authentication mechanism (password verification) by discussing the probabilities associated with random attempts, and multiple consecutive attempts towards subverting the implemented authentication mechanisms:

Authentication Mechanism	**Strength of Mechanism: Random attempted breach**	**Strength of Mechanism: Multiple consecutive attempts in a one-minute period**
Password verification	Less than 1/256^8	Less than 25/256^8 The module zeroizes after 25 failed attempts.

Exhibit 4 - *Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)*

Access Control Policy

The list of roles, services, cryptographic keys & CSPs, and types of access to the cryptographic keys & CSPs that are available to each of the authorized roles via the corresponding services.

Role			Service	Cryptographic Keys & CSPs	Type(s) of Access to CSPs
No Role	Master/ Cryptographic Officer	User			
X			**SelfTests**: performs the full suite of required power-up self-tests.	N/A	N/A
X			**EnumerateDevices**: This function polls the computer to find attached devices and returns device names and mount locations.	N/A	N/A
X			**OpenSession:** This function uses the device mount location to open a session for sending sensitive data to the module	N/A	N/A
X			**CloseSession:** This function tells the controller to close the session	N/A	N/A
X	X	X	**doIdentify:** This function gets status information from module (Show Status)	N/A	N/A
	X		**doAuthInit:** This function generates keys to restrict access to the encrypted (private) area of the module.	Master/Cryptographic Officer Password DEK (Data Encryption/ Data Decryption Key) KEK (Key Encryption/Key Decryption Key)	Enter, Store Generate, Store Generate, Store

				NDRNG Seeds DRBG Internal State (C and V)	Generate Generate
	X		**doAuthAdmin:** This function unlocks the device using Master/Cryptographic Officer Password, so disk can be mounted	Master/Cryptographic Officer Password DEK (Data Encryption/ Data Decryption Key) KEK (Key Encryption/Key Decryption Key)	Enter, Verify Execute Execute
		X	**doAuthUser:** This function unlocks the device using User Password, so disk can be mounted	User Password DEK (Data Encryption/ Data Decryption Key) KEK (Key Encryption/Key Decryption Key)	Enter, Verify Execute Execute
	X		**addUserPassword:** This function sets the User Password to the module to restrict access to the encrypted (private) area of the module.	User Password DEK (Data Encryption/ Data Decryption Key) KEK (Key Encryption/Key Decryption Key)	Enter, Verify Execute Execute
X			**removeUserPassword:** This function unauthenticates the user password	N/A	Enter, Execute
	X	X	**doUnAuth:** This function closes (disables access to) the encrypted (private) area of module so that this area cannot be accessed.	N/A	N/A
	X	X	**isUnlocked:** This function gets the status of the encrypted partition	N/A	N/A
		X	**changePasswordUser:** This function changes the User Password from old password to new password.	Master/Cryptographic Officer Password	Enter, Verify, Update
	X		**changePasswordAdmin:** This function changes the Master/Cryptographic Officer Password from old password to new password.	User Password	Enter, Verify, Update
X			**setReadAddress:** This function sets the beginning of the read address for the hidden area. The controller converts the offset to the memory address and sets a pointer to it. Sequential reads increment the pointer address automatically	N/A	N/A

X			**setWriteAddress:** This function sets the beginning of the write address for the hidden area. The controller converts the offset to the memory address and sets a pointer to it. Sequential writes increment the pointer address automatically	N/A	N/A
X			**readChunk**: Requests from the controller to return a 256byte chunk of data from the hidden area. The chunk is read from the address that was set with setReadAddress	N/A	N/A
X			**writeChunk:** Tells the controller to write a 256byte chunk of data to the hidden area. The chunk is written to the address that was set with setWriteAddress.	N/A	N/A
X			**eraseSector:** Tells the controller to erase a 4k sector of the hidden area. Blocks are overwritten with zeroes.	N/A	N/A
X			**writeVcdEnable:** This function tells the controller to either allow or disallow writing to the CD-Rom partition. There is a memory address in SRAM that is configured and checked by the update functions before writing is permitted. The controller changes this bit depending on the parameters of this function.	N/A	N/A
X			**writeVcdBlock:** This function sends a block of 512bytes to the controller for writing to the CD-Rom partition.	N/A	N/A
X			**GetLastSystemError:** This function returns the last error that occurred while running the application.	N/A	N/A
X			**Zeroize:** Actively destroys all CSPs.	All CSPs	Destroy

Exhibit 5 – *Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4)*

Physical Security Policy

The following physical security mechanisms are implemented by the cryptographic module:

- Production grade components
- Opaque tamper resistant epoxy without any gaps or openings
- Strong adhesive materials that prevent dismantling the module without causing severe damage.
- Chips and pin connectors are coated with epoxy.

NOTICE: The FIPS 140-2 Area 5 physical security testing was performed at ambient temperature; Kanguru Solutions does not claim any FIPS 140-2 Area 5 physical security protection beyond the ambient temperature.

Exhibit 6 summarizes the actions required by the Master/Cryptographic Officer Role to ensure that physical security is maintained.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Production grade components	N/A	N/A
Opaque non-removable potting material	As often as feasible	Inspect the entire perimeter for scratches, scrapes, gouges, cuts and any other signs of tampering. Remove the unit from service when any such markings are found.

Exhibit 6 - *Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)*

Mitigation of Other Attacks Policy

This module is not designed to mitigate against any attacks that are outside the scope of FIPS 140-2.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	**N/A**	**N/A**

Exhibit 7 - *Mitigation of Other Attacks (FIPS 140-2 Table C6)*

Acronyms

- HDD – Hard Disk Drive
- SSD – Solid-State Drive
- PCBA – Printed Circuit Board Assembly

References

- FIPS PUB 140-2
- FIPS PUB 140-2 DTR
- FIPS PUB 140-2 Implementation Guidance
- FIPS 197 - AES
- FIPS 180-4 - SHS
- RSA PKCS#1 V2.1
- SP800-90