KANGURU SOLUTIONS

Defender 3000 USB Flash Drive

FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

TABLE OF CONTENTS

List of Tables

List of Figures

1 GENERAL

1.1 OVERVIEW

This document forms a Cryptographic Module Security Policy for Kanguru Solutions *Defender 3000™ USB Flash Drive* under the terms of NIST FIPS 140-3.

1.2 SECURITY LEVELS

The module meets the overall requirements of FIPS 140-3 Security Level 3.

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	3

Table 1: Security Levels

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The Kanguru Solutions *Defender 3000™ USB Flash Drive* (*refer to Figure 1*) is a USB 3.0 storage device designed to securely store user's data encrypted with AES 256. The module provides multi-layered physical security protection mechanisms.

Figure 1: Defender 3000™ USB Flash Drive

The *Defender 3000™ USB Flash Drive* has been specifically designed to address sensitive data concerns of Government and security conscious customers in a variety of markets.

Purpose and Use: The *Defender 3000™ USB Flash Drive* is designed to store encrypted user data using AES-XTS 256-bit encryption.

Module Type: Hardware

Module Embodiment: MultiChipStand
The *Defender 3000™ USB Flash Drive* is defined as a multiple chip standalone cryptographic module (*refer to ISO/IEC 19790, Section 7.7.1*).

Module Characteristics:
The critical components within the module are encapsulated inside a hard, opaque, production-grade epoxy, that is further secured within a strong enclosure.

Cryptographic Boundary:
The cryptographic boundary is defined as the perimeter of the module.

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The *Defender 3000™ USB Flash Drive* cryptographic module is designed to meet the requirements of FIPS 140-3 Security Level 3 (*refer to Table 1*). The module is available in the following configuration:

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
KDF3000-16G	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	16GB of user data storage
KDF3000-32G	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	32GB of user data storage
KDF3000-64G	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	64GB of user data storage
KDF3000-128G	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	128GB of user data storage
KDF3000-256G	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	256GB of user data storage
KDF3000-512G	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	512GB of user data storage
KDF3000-1T	KDF3000	2.13.10	Kanguru Defender 3000 Crypto Processor	1TB of user data storage

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 EXCLUDED COMPONENTS

The module does not exclude any components from the requirements of FIPS 140-3.

2.4 MODES OF OPERATION

Modes List and Description:

The module supports a single approved mode of operation that is entered by powering-on the module. There are no non-approved modes, degraded modes or non-approved services available to the module. The module's firmware provides an indicator (i.e., "FIPS ACTIVE") showing the approved configuration which can be queried. This global indicator will be used along with the successful return codes of each service to indicate the module has provided an approved security service. If the module reports "FIPS DEFAULT", the module is awaiting a new password (CO Password) to be set. The module is always running in an approved mode when module reports either "FIPS DEFAULT" or "FIPS ACTIVE". The approved mode cannot be exited.

The module does not support a non-approved or degraded mode of operation. In case of critical error, the module will remain in an error state, until reset. While in its error state, the LED will blink rapidly until it is reset.

Mode Name	Description	Type	Status Indicator
Approved Mode	Only Approved services are supported	Approved	FIPS ACTIVE

Table 3: Modes List and Description

2.5 ALGORITHMS

The *Defender 3000™ USB Flash Drive* cryptographic module supports the approved cryptographic algorithms shown in Table 4.

Approved Algorithms:

The module supports the following approved cryptographic algorithms.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5476	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5476	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A5476	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38F
AES-XTS Testing Revision 2.0	A5476	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38E
ECDSA KeyGen (FIPS186-5)	A5476	Curve - P-256 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5476	Curve - P-256	FIPS 186-5
HMAC DRBG	A5476	Prediction Resistance - Yes Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA2-256	A5476	Key Length - Key Length: 8-2040 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5476	Domain Parameter Generation Methods - P-256 Scheme - ephemeralUnified - KAS Role - responder	SP 800-56A Rev. 3
KDA TwoStep SP800-56Cr2	A5476	MAC Salting Methods - default KDF Mode - counter Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256	SP 800-56C Rev. 2
PBKDF	A5476	Iteration Count - Iteration Count: 1024 Password Length - Password Length: 8-128 Increment 1	SP 800-132

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-4)	A5476	Signature Type - PKCS 1.5 Modulo - 2048	FIPS 186-4
SHA2-256	A5476	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module supports the following vendor affirmed algorithms.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	NIST SP 800-133r2, Section 4 example 1, Section 5.2, and Section 6.1.
CKG XTS	Key Type:Symmetric	N/A	NIST SP 800-133r2 and IG D.H per Section 6.3, approved method #1 and Section 4 example 1. Applicable to AES-XTS compliant to IG C.I because Key_1 and Key_2 are concatenated prior to usage.

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 SECURITY FUNCTION IMPLEMENTATIONS

Name	Type	Description	Properties	Algorithms
DRBG	DRBG	Random bit generation	Standard:NIST SP 800-90A	HMAC DRBG: (A5476) Prediction Resistance: Yes Mode: SHA2-256
Encryption	BC-UnAuth	Symmetric AES encryption	Standards:FIPS 197, NIST SP 800-38A	AES-CBC: (A5476) Direction: Encrypt, Decrypt Key Length: 256 AES-ECB: (A5476) Direction: Encrypt, Decrypt Key Length: 256 AES-XTS Testing Revision 2.0: (A5476) Direction: Encrypt, Decrypt Key Length: 256
ESV	ENT-ESV	NIST SP 800-90B Physical Entropy Source	Standard:NIST SP 800-90B	
HMAC	MAC	HMAC-SHA2-256	Standard:FIPS 198-1	HMAC-SHA2-256: (A5476) Key Length: 8 - 2040 bits, Increment 8-bit
KAS	KAS-Full	Key Agreement Scheme (KAS) per NIST SP 800-56Arev3, KAS-ECC-SSC Per IG D.F Scenario 2 path (2)	Standards:NIST SP 800-56Arev3, NIST SP 800-56Crev2 IG:IG D.F Scenario 2, path (2), split Key	KAS-ECC-SSC Sp800-56Ar3: (A5476) Domain Parameter Generation Methods: P-256 KAS Role: responder

Name	Type	Description	Properties	Algorithms
			Confirmation:No Key Derivation:KDA (separately tested) Caveat:Key establishment methodology provides 128 bits of security strength	KDA TwoStep SP800-56Cr2: (A5476) MAC Salting Methods: default KDF Mode: counter Derived Key Length: 256 Shared Secret Length: 256 ECDSA KeyVer (FIPS186-5): (A5476) Curve: P-256 ECDSA KeyGen (FIPS186-5): (A5476) Curve: P-256 Secret Generation Mode: extra bits
Key Wrap	BC-Auth	AES-KW used for the protection of the data encryption key (DEK) stored within the module	Standard:NIST SP 800-38F	AES-KW: (A5476) Direction: Encrypt, Decrypt Key Length: 256 bits
KTS	KTS-Wrap	Key wrapping used for the entry of the operator's passwords	Standards:FIPS 198-1, NIST SP 800-38A IG D.G:Approved method from IG D.G - key wrapping using a combination of an approved symmetric encryption mode (AES-CBC) and an approved authentication method (HMAC-	HMAC-SHA2-256: (A5476) Key Length: 8 - 2040 bits, Increment 8-bit AES-CBC: (A5476) Direction: Encrypt, Decrypt Key Length: 256 bits

Name	Type	Description	Properties	Algorithms
			SHA2-256) Caveat:Key establishment methodology provides 128 bits of security strength	
PBKDF	PBKDF	Password-Based Key Derivation Function	Standard:NIST SP 800-132	PBKDF: (A5476) Iteration Count: 1024 Password Length: 8 - 128 bits, Increment 1-bit HMAC-SHA2-256: (A5476) Key Length: 8 - 2040 bits, Increment 8-bit SHA2-256: (A5476) Message Length: 0 - 65536 bits, Increment 8-bits
Hash Function	SHA	SHA2-256 hash function	Standard:FIPS 180-4	SHA2-256: (A5476) Message Length: 0 - 65536 bits, Increment 8-bit
SigVer	DigSig-SigVer	RSA Signature Verification (PKCS#1 v1.5)	Standard:FIPS 186-4	RSA SigVer (FIPS186-4): (A5476) Signature Type: PKCS 1.5 Modulo: 2048
Decryption	BC-UnAuth	Symmetric AES decryption	Standards:FIPS 197, NIST SP 800-38A	AES-CBC: (A5476) Direction: Encrypt, Decrypt Key Length: 256 bits

Name	Type	Description	Properties	Algorithms
				AES-ECB: (A5476) Direction: Encrypt, Decrypt Key Length: 256 bits AES-XTS Testing Revision 2.0: (A5476) Direction: Encrypt, Decrypt Key Length: 256 bits
KeyGen_Symmetric	CKG	Symmetric Key Generation	Standard:NIST SP 800-133r1	CKG: () Key Type: Symmetric CKG XTS: () Key Type: Symmetric
KeyGen-Asymmetric	AsymKeyPair-KeyGen	Asymmetric Key Generation	Standards:FIPS 186-5, NIST SP 800-133r1	CKG: () Key Type: Symmetric ECDSA KeyGen (FIPS186-5): (A5476) Key Length: P-256

Table 6: Security Function Implementations

2.7 ALGORITHM SPECIFIC INFORMATION

2.7.1 AES-XTS (IG C.I COMPLIANCE)

In compliance with FIPS IG C.I and NIST SP 800-133rev2 Section 6.3, the module generates AES-XTS Key1 and Key2 independently using the approved DRBG (Cert. #A5476) and verifies that Key1≠Key2 upon generation. AES-XTS is only used for storage purposes per SP 800-38E.

2.7.2 HMAC-SHA2-256 (IG C.L COMPLIANCE)

The following describes compliance with FIPS IG C.L:

A. Not Applicable - The module does not utilize truncated digests.

B. Not Applicable - The module does not utilize truncated digests.

C. Not Applicable - The only use of HMAC in this module is for PBKDF per NIST SP 800-132. Additionally, HMAC outputs are never truncated.

D. The module establishes keys using KAS-ECC-SSC per NIST SP 800-56Arev2 and KDA TwoStep per NIST SP 800-56Cr2. The asymmetric keys used in the key agreement scheme (Device ECDH Public Key and Host ECDH Public Key) have a security strength of 128 bits. The established keys (AES Session Key and MAC Session Key) have a length of 256 bits and a security strength of 128 bits. The preimage resistance strength of the hash function (SHA2-256 Cert. #A5476) used in the HMAC construction to derive the key is 256 bits.

E. The hash function (SHA2-256 Cert. #A5476) used by the module's DRBG.

2.7.3 KAS-ECC (COMPLIANCE TO NIST SP 800-56AREV3 ASSURANCES)

For KAS-ECC, the module satisfies IG D.F Scenario 2, path (2). The key derivation function complies with NIST SP 800-56Cr2 (KDA TwoStep Cert. #A5476). Furthermore, the module obtains the appropriate assurances as required in Section 5.6.2 of NIST SP 800-56Ar3. For KAS-ECC, the module uses C(2e,0s), thus no static key pairs are used as part of the KAS schemes per NIST SP 800-56Ar3. Full public key validations are implemented (NIST SP 800-56Ar3 Section 5.6.2.3.3). No key confirmation is implemented.

2.7.4 RSA PKCS#1 V1.5

The module implements RSA PKCS#1 v1.5 signature verification. The RSA PKCS#1 v1.5 implementation was CAVP tested in accordance with FIPS 186-4 and IG C.K Resolution 6.

2.7.5 PBKDF (IG D.N COMPLIANCE)

The module implements PBKDF in compliance with NIST SP 800-132 and FIPS IG D.N. Specifically, the module implements Option 2a from Section 5.4 of NIST SP 800-132. The Key Encryption Key (KEK) is generated from a password and is used directly to protect the Data Encryption Key (DEK). The DEK is protected using AES-KW (Cert. #A5476). The minimum and maximum length of the PIN used in the key derivation and the probability of having this parameter guessed at random are described in Section 4.1. The module implements an iteration count of 1024, which is greater than the minimum recommendation documented within NIST SP 800-132 - Section 5.2. Keys derived from passwords are only used by the module for storage applications.

2.8 RBG AND ENTROPY

The module includes an internal entropy source for the generation of the DRBG seed. Please refer to the Entropy Source Validation (ESV) certificate #E195. The DRBG is reseeded after each 10,000 uses.

Cert Number	Vendor Name
E195	Kanguru Solutions

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Kanguru Entropy Source	Physical	Kanguru Defender 3000 Crypto Processor	4 bits	1-bit	N/A

Table 8: Entropy Sources

2.9 KEY GENERATION

The module generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90A conforming DRBG (Cert. #A5476) for the encryption and protection of data. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-5 for the facilitation of key agreement in conformance with NIST SP 800-56ar3.

2.10 KEY ESTABLISHMENT

The module supports the establishment of cryptographic keys in conformance with ISO/IEC 19790:2012, Annex D and NIST SP 800-140D. The module uses Elliptical Curve Cryptography (ECC) Co-factor Diffie Hellman (CDH) in conformance with NIST SP 800-56ar3. The module implements KAS-ECC-SSC per NIST SP 800-56A Rev3 (Cert. #A5476) Model C (2e, 0s, ECC CDH) using ECDSA KeyGen (Cert. #A5476), used in conjunction with KDA per NIST SP 800-56Cr2 (Cert. #A5476). Key establishment methodology provides at least 112 bits of encryption strength. This is used to establish secure communication sessions.

The module also supports key establishment using password based key derivation (PBKDF) per NIST SP 800-132.

2.11 INDUSTRY PROTOCOLS

The module relies upon the standard USB and other serial protocols for communication with general purpose computer (GPC) systems.

3 CRYPTOGRAPHIC MODULE INTERFACES

3.1 PORTS AND INTERFACES

The module incorporates physical ports and logical interfaces. The physical ports are defined within Table 9 below.

Physical Port	Logical Interface(s)	Data That Passes
USB Port (Rx,Tx)	Data Input Data Output Control Input Status Output	The USB 3.0 port connects the module to the host computer. It is used to receive user data as well as API calls issued by the host via the USB protocol. The input is received by the module on the Rx line. The USB 3.0 port connects the module to the host computer. It is used to send user data as well as return codes upon completion of API calls issued by the host via the USB protocol. The input is received by the module on the Tx line. The USB 3.0 port connects the module to the host computer. It is used to receive commands as well as API calls issued by the host via the USB protocol. The input is received by the module on the Rx line. Error codes and other status is transmitted from the module to the host computer.
LED	Status Output	Error codes and other status is transmitted by the LED:- Active data transfer with host computer: LED blinks at 3Hz- Error state: LED blinks at rapidly at 16Hz- Pre-operational Self-test status output: LED blinks at 3Hz if all self-tests completed, LED blinks at 16Hz if failed- Continuous Self-test status output: LED blinks at 16Hz if failed- Periodic Self-test status output: LED blinks at 16Hz if failed
USB Port (VCC)	Power	The USB VBUS (+5VDC) powers the module

Table 9: Ports and Interfaces

3.2 TRUSTED CHANNEL SPECIFICATION

The module does not support a Trusted Channel.

4 ROLES, SERVICES, AND AUTHENTICATION

4.1 AUTHENTICATION METHODS

The module supports identity-based authentication for the Cryptographic Officer and User roles in the form of a User ID and Password (Memorized Secret) in conformance with NIST SP 800-140E and SP 800-63B - Section 5.1.1. Passwords must be a minimum of 8 characters (bytes). This is explicitly enforced by the module.

The password must contain three of the following four-character types: lowercase letters, uppercase letters, numeric characters and/or special characters. This greatly increases the passwords entropy. Assuming a mix of lowercase letters, uppercase letters, numeric characters, the password can consist of the following set: uppercase letters, lowercase letters, numbers, and special characters, yielding 95 choices per character. The probability of a successful random attempt is $1/ (10 * 26 * 26 * 95^5) \sim= 1/2^{45}$, which is less than 1/1,000,000. The module only allows for ten (10) unsuccessful authentication attempts. Therefore, the probability of success with multiple attempts in a one-minute period is $10/2^{45}$, which is less than 1/100,000.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
ID/Password	The password is at least 8 bytes in length and includes the numbers, the uppercase letters, the lowercase letters, and the special characters	ID & Password combination used within a challenge/response mechanism	The upper bound for the probability of having the password guessed at random is: 1 / (10 * 26 * 26 * 955) ~= 1/245 < 1/1,000,000	The probability of the consecutive failed authentication attempts in one minute period is approximately 10/ 245 < 1/100,000

Table 10: Authentication Methods

4.2 ROLES

Table 11 lists the roles supported by the module.

Name	Type	Operator Type	Authentication Methods
Crypto Officer (CO)	Identity	Crypto Officer	ID/Password
User	Identity	User	ID/Password
Unauthenticated	Role	Unauthenticated	None

Table 11: Roles

4.3 APPROVED SERVICES

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
(All CO/User Services)	Secure communication session	Return status via the API: 0x0000: success, 0x4002: session invalid	Host ECDH Public Key	Device ECDH Public Key	Encryption HMAC KAS KTS Decryption KeyGen-Asymmetric	Crypto Officer (CO) - Shared Secret (Z): G,E,Z - AES Session Key: G,E - MAC Session Key: G,E - Device ECDH Private Key: G,Z - Device ECDH Public Key: G,R,Z - Host ECDH Public Key: W,Z - DRBG Internal State (V and Key): G,E User - Shared Secret (Z): G,E,Z - AES Session Key: G,E - MAC Session Key: G,E - Device ECDH Private Key: G,Z - Device ECDH Public Key: G,R,Z - Host ECDH Public Key: W,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State (V and Key): G,E
CD Update	Load/Update CD Image to the CD-ROM partition	Return status via the API: 0x0000: success, 0x4002: session invalid, 0x4006: signature verification failed	API call with CD Image, Signature	Status Out (success, session invalid, signature verification failed)	SigVer	Unauthenticated - CD Update Public Key: E
Change CO Password	Create new CO password	Return status via the API: 0x0000: success, 0x8102: configuration invalid	New CO password	Status Out (success, session invalid, wrong password) LED blinks at 16Hz if fatal error	DRBG Key Wrap PBKDF Hash Function	Crypto Officer (CO) - KEK_CO (Key Encryption Key - CO): G,E,Z - Crypto Officer Password: W,Z - CO Password Hash: Z,G - DRBG Internal State (V and Key): G,E
Change User Password	Creates new User Password	Return status via the API: 0x0000: success, 0x8102: configuration invalid	New User password	Status Out (success, session invalid, wrong password) LED blinks at	DRBG Key Wrap PBKDF Hash Function	User - KEK_U (Key Encryption Key - User): G,E,Z - User Password: W,Z - User Password

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				16Hz if fatal error		Hash: Z,G - DRBG Internal State (V and Key): G,E
Close Partition (Logout)	Logout. Locks drive	Return status via the API: 0x0000: success, 0x1602: session invalid, 0x1604: partition has been closed	N/A	Status Out (success, session invalid, partition has been closed) LED blinks at 16Hz if fatal error	None	Crypto Officer (CO) - DEK_CO (Data Encryption Key - CO): Z - AES Session Key: Z - MAC Session Key: Z User - DEK_U (Data Encryption Key - User): Z - AES Session Key: Z - MAC Session Key: Z
Decrypt	Read partition data	Return status via the API: 0x0000: success	Partition Info	Data, Status	Decryption	Crypto Officer (CO) - DEK_CO (Data Encryption Key - CO): E User - DEK_U (Data Encryption Key - User): E
Encrypt	Write partition data	Return status via the API: 0x0000: success	Partition Info	Status	Encryption	Crypto Officer (CO) - DEK_CO (Data Encryption Key - CO): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						User - DEK_U (Data Encryption Key - User): E
Initialize	Create CO password and generate DEK	Return status via the API: 0x0000: success, 0x8102: configuration invalid	CO Password and the drive's partition configuration	Status Out (success, configuration invalid) LED blinks at 16Hz if fatal error	DRBG ESV PBKDF Hash Function KeyGen_Symmetric	Crypto Officer (CO) - DEK_CO (Data Encryption Key - CO): Z,G - KEK_CO (Key Encryption Key - CO): G,E,Z - Crypto Officer Password: W - CO Password Hash: G - Entropy Input: G,E - DRBG Nonce: G,E - DRBG Internal State (V and Key): G,E
Open Partition (Login)	Authenticates either the CO or User to the module	Return status via the API: 0x0000: success, 0x1402: session invalid, 0x1404: partition has been opened, 0x1406:	User ID & Password, and the selected partition	Status Out (success, session invalid, partition has been opened, wrong password) LED blinks at 16Hz if fatal error, the partition is	PBKDF Hash Function	Crypto Officer (CO) - Crypto Officer Password: W,E,Z - KEK_CO (Key Encryption Key - CO): G,E,Z - DEK_CO (Data Encryption Key - CO): E User - User Password:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		wrong password		opened if success		W,E,Z - KEK_U (Key Encryption Key - User): G,E,Z - DEK_U (Data Encryption Key - User): E
Perform Self-Tests	Perform Pre-Operational and Conditional Self-Tests	LED Flashing	N/A	LED blinks at 3Hz if all tests complete LED blinks at 16Hz if failed	None	Unauthenticated - DRBG Internal State (V and Key): G,E
Reset Drive	Erase all files stored on the module and zeroizes all CSPs	Return status via the API: 0x0000: success, 0x8101: session invalid	N/A	Status Out (success, session invalid) Internally zeroize all CSPs except the session keys and generate DEK_CO and configure to the single partition. LED blinks at 16Hz if fatal error	None	Unauthenticated - DEK_CO (Data Encryption Key - CO): Z - DEK_U (Data Encryption Key - User): Z - CO Password Hash: Z - User Password Hash: Z - DRBG Internal State (V and Key): Z
Setup User Password	Create new User password	Return status via the API: 0x0000: success,	Current CO Password and new User Password	Status Out (success, session invalid, wrong	DRBG Key Wrap PBKDF Hash Function	Crypto Officer (CO) - DEK_U (Data Encryption Key - User): G,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		0x8102: configuration invalid		password) LED blinks at 16Hz if fatal error	KeyGen_Symmetric	- KEK_U (Key Encryption Key - User): G,E,Z - User Password: W,E,Z - User Password Hash: G - DRBG Internal State (V and Key): G,E
Show Module Version	Get module ID and version	Return status via the API: 0x0000: success	N/A	Returns module identifier [Defender 3000] and firmware version information [2.13.10], in addition to the approved mode indicator to API call	None	Unauthenticated
Show Error Status	Returns the most recent error details	Return status via the API: 0x0000: success	N/A	Returns the error log to API call	None	Unauthenticated
Show Status	Get the module's status	Return status via the API:	N/A	Reply the service status, the	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		0x0000: success		disk status, or the session establishment status to API call		
Zeroization	Zeroize all keys and CSPs	Return status via the API: 0x0000: success	N/A	Status Out (success) Internally zeroize all CSPs. LED blinks at 16Hz if fatal error	None	Unauthenticated - DEK_CO (Data Encryption Key - CO): Z - DEK_U (Data Encryption Key - User): Z - CO Password Hash: Z - User Password Hash: Z - DRBG Internal State (V and Key): Z - AES Session Key: Z - MAC Session Key: Z

Table 12: Approved Services

4.4 NON-APPROVED SERVICES

N/A for this module.

4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

The module's firmware is non-modifiable. It does not have the ability to support external software / firmware loading.

5 SOFTWARE/FIRMWARE SECURITY

5.1 INTEGRITY TECHNIQUES

The module incorporates an RSA 2048 PKCS1 v1.5 (Cert. #A5476) digital signature mechanism over its firmware. The digital signature provides integrity as well as authentication.

All commands sent to and from the cryptographic module are protected with HMAC-SHA-256.

The module will transition to its error state upon the failure of either firmware integrity test.

5.2 INITIATE ON DEMAND

The module loads the firmware image from non-volatile memory to on-chip RAM when powering on the module where it then performs the firmware integrity test using the module's RSA-2048 'Firmware Integrity Public Key'. If the test fails, the module enters an error state, the data output interface is inhibited, and the module's LED (status output) blinks at 16Hz.

The firmware integrity test is a part of Pre-Operational Self-Tests. It is automatically executed at power-on or during the Periodic Self-Tests. It can also be invoked by power-cycling the module.

6 OPERATIONAL ENVIRONMENT

6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

Type of Operational Environment: Non-Modifiable

How Requirements are Satisfied:

The module operational environment is defined as non-modifiable. The firmware is a single binary file loaded into the module during manufacturing with write protections assigned to the chip. There are no available mechanisms to modify the firmware once it is installed.

7 PHYSICAL SECURITY

The module is a multiple-chip standalone module and conforms to FIPS 140-3 Security Level 3 physical security requirements. The module is housed within a strong, non-removable, tamper-evident enclosure. The enclosure is opaque within the visible spectrum. In addition, all components are protected with a hard epoxy coating that protects each component from being viewed or probed. Attempts at removing the epoxy will render the module inoperable.

7.1 MECHANISMS AND ACTIONS REQUIRED

The operator of the module should inspect the outer casing of the module each time prior to connecting the module to a computer. If tamper evidence is observed on the outer casing, the module should not be used.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence	Each time the module is used	Upon each use of the module the operator should examine the module for evidence of tamper.

Table 13: Mechanisms and Actions Required

7.2 EFP/EFT INFORMATION

The module supports Environmental Failure Protection (EFP) mechanisms for high/low voltage and temperature extremes (refer to Table 14).

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-100C	EFT	Continues to Operate Normally
HighTemperature	117C	EFT	Undefined Failure
LowVoltage	3.2V	EFT	Shutdown
HighVoltage	9.0V	EFT	Undefined Failure

Table 14: EFP/EFT Information

7.3 HARDNESS TESTING TEMPERATURE RANGES

The module supports and has been tested at the operation, storage and distribution temperatures listed in Table 15. The module's epoxy hardness is assured within these ranges.

Temperature Type	Temperature
LowTemperature	-20C

Temperature Type	Temperature
HighTemperature	85C

Table 15: Hardness Testing Temperatures

8 NON-INVASIVE SECURITY

8.1 MITIGATION TECHNIQUES

The module does not provide protections against non-invasive security methods.

9 SENSITIVE SECURITY PARAMETERS MANAGEMENT

9.1 STORAGE AREAS

The module is designed to encrypt and store arbitrary data with XTS-AES within eMMC memory components. The module physically and logically protects static keys and CSPs. Please refer to Table 16 for additional information.

Storage Area Name	Description	Persistence Type
RAM	Random Access Memory	Dynamic
eMMC	Persistent memory storage	Static

Table 16: Storage Areas

9.2 SSP INPUT-OUTPUT METHODS

The module inputs CSPs encrypted with AES CBC and authenticated with HMAC-SHA2-256. The module does not output CSPs. PSPs are output in order to authenticate the module to the connected GPC. Please refer to Table 17 for additional information.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SSP_Input (Encrypted)	External	eMMC	Encrypted	Automated	Electronic	KTS

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SSP_Input (Plaintext)	External	RAM	Plaintext	Automated	Electronic	KAS
SSP_Output (Plaintext)	RAM	External	Plaintext	Automated	Electronic	KAS
Manufacturing	External	eMMC	Plaintext	Automated	Electronic	

Table 17: SSP Input-Output Methods

9.3 SSP ZEROIZATION METHODS

During normal operation, the module explicitly erases copies of CSPs in volatile memory (e.g., RAM) by overwriting with zeros after their use. For CSPs stored in non-volatile memory the module initiates its erase operation to zeroize.

The following methods are used to zeroize the module's CSPs during normal operation.

- 'Zeroization' and 'Reset Drive' service: This service overwrites all CSPs with zeroes and returns the module to its factory default state.
- After ten failed CO authentication attempts the respective CO and User DEKs are erased.
- After ten failed User authentication attempts the respective User DEK is erased.

Zeroization Method	Description	Rationale	Operator Initiation
After Use	SSPs are zeroized after use	SSPs are zeroized after use when no longer needed.	N/A
Reset Drive	SSPs are zeroized by the operator upon resetting device	SSPs are zeroized by overwriting with all zeroes	Initiated by operator
Zeroization service	SSPs are zeroized by the operator via the module's zeroization service. This service is not restricted and can be called at the operator's discretion.	All SSPs are immediately zeroized by overwriting with all zeroes.	Initiated by operator

Table 18: SSP Zeroization Methods

9.4 SSPS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DEK_CO (Data Encryption Key - CO)	Data Encryption / Decryption for Crypto Officer	256 bits - 256 bits	Symmetric - CSP - CSP	KeyGen_Symmetric		Encryption Decryption
DEK_U (Data Encryption Key - User)	Data Encryption / Decryption for User	256 bits - 256 bits	Symmetric - CSP - CSP	KeyGen_Symmetric		Encryption Decryption
KEK_CO (Key Encryption Key - CO)	Key Encryption Key for Crypto Officer. Encrypts DEK_CO	256 bits - 256 bits	Symmetric - CSP - CSP		PBKDF	Key Wrap
KEK_U (Key Encryption Key - User)	Key Encryption Key for User. Encrypts DEK_U	256 bits - 256 bits	Symmetric - CSP - CSP		PBKDF	Key Wrap
Crypto Officer Password	Used to generate the KEK_CO	8 ~ 136 bytes - 8 ~ 136 bytes (refer to Section 4.1)	Password - CSP			PBKDF
User Password	Used to generate the KEK_U	8 ~ 136 bytes - 8 ~ 136 bytes (refer to Section 4.1)	Password - CSP			PBKDF
CO Password Hash	Used for Authentication	128-bits - 128-bits	Hash - CSP			Hash Function

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
User Password Hash	Used for Authentication	128-bits - 128-bits	Hash - CSP			Hash Function
Entropy Input	Used as entropy input to the SP 800-90A DRBG	1024 bits - 256 bits	Entropy - CSP	ESV		DRBG
DRBG Nonce	Used as nonce input to the SP 800-90A DRBG	512 bits - 256 bits	Nonce - CSP	ESV		DRBG
DRBG Internal State (V and Key)	The internal state of the SP 800-90A DRBG (V and Key)	N/A - N/A	Internal State - CSP	DRBG		DRBG
Device ECDH Private Key	Used by the module for key agreement (KAS-SSC per SP 800-56Ar3)	256 bits - 128 bits	Asymmetric Private Key - CSP	KeyGen-Asymmetric		KAS
Shared Secret (Z)	Used to derive the Session Key Material	256 bits - 128 bits	Shared Secret - CSP		KAS	KAS
AES Session Key	Encryption data during secure session	256 bits - 128 bits	Symmetric - CSP - CSP		KAS	KTS
MAC Session Key	MAC Session Key serves to authenticate data during the Secure Session	256 bits - 128 bits	Symmetric - CSP - CSP		KAS	KTS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CD Update Public Key	Validates the CD ROM partition	2048 bits - 112 bits	Asymmetric - PSP - PSP			SigVer
Device ECDH Public Key	Used by the module for key agreement (KAS-SSC per SP 800-56Ar3)	256 bits - 128 bits	Asymmetric - PSP - PSP	KeyGen-Asymmetric		KAS
Host ECDH Public Key	Used by the module for key agreement	256 bits - 128 bits	Asymmetric - PSP - PSP			KAS

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DEK_CO (Data Encryption Key - CO)		eMMC:Encrypted		After Use Reset Drive Zeroization service	KEK_CO (Key Encryption Key - CO):Encrypted By
DEK_U (Data Encryption Key - User)		eMMC:Encrypted		After Use Reset Drive Zeroization service	KEK_U (Key Encryption Key - User):Encrypted By
KEK_CO (Key Encryption Key - CO)		RAM:Plaintext		After Use	DEK_CO (Data Encryption Key - CO):Encrypts
KEK_U (Key Encryption Key - User)		RAM:Plaintext		After Use	DEK_U (Data Encryption Key - User):Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Crypto Officer Password	SSP_Input (Encrypted)	RAM:Plaintext		After Use	KEK_CO (Key Encryption Key - CO):Derives
User Password	SSP_Input (Encrypted)	RAM:Plaintext		After Use	KEK_U (Key Encryption Key - User):Derives
CO Password Hash		RAM:Plaintext		Reset Drive Zeroization service	Crypto Officer Password:Generated From
User Password Hash		RAM:Plaintext		Reset Drive Zeroization service	User Password:Generated From
Entropy Input		RAM:Plaintext		After Use	
DRBG Nonce		RAM:Plaintext		After Use	
DRBG Internal State (V and Key)		RAM:Plaintext		Reset Drive Zeroization service	
Device ECDH Private Key		RAM:Plaintext		After Use Zeroization service	Device ECDH Public Key:Paired With
Shared Secret (Z)		RAM:Plaintext		After Use	Device ECDH Private Key:Derived From Host ECDH Public Key:Derived From
AES Session Key		RAM:Plaintext		After Use Zeroization service	Shared Secret (Z):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
MAC Session Key		RAM:Plaintext		After Use Zeroization service	Shared Secret (Z):Derived From
CD Update Public Key	Manufacturing	eMMC:Plaintext		N/A	
Device ECDH Public Key	SSP_Output (Plaintext)	RAM:Plaintext		After Use Zeroization service	Device ECDH Private Key:Paired With
Host ECDH Public Key	SSP_Input (Plaintext)	RAM:Plaintext		After Use	

Table 20: SSP Table 2

10 SELF-TESTS

10.1 PRE-OPERATIONAL SELF-TESTS

The module performs pre-operational self-tests and conditional self-tests (refer to Section 10.2). Both self-tests ensure that the module is not corrupted, and the cryptographic algorithms work as expected. During self-tests, data output (via the data output interface) is inhibited. The module services are not available until the self-tests have completed successfully.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
RSA SigVer (FIPS186-4) (A5476)	RSA 2048 PKCS1 v1.5 Digital Signature Verification	RSA 2048 Digital Signature Verification	SW/FW Integrity	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Performed During module power-on, on-demand, and on a periodic basis

Table 21: Pre-Operational Self-Tests

For the above error case, the device can be powered cycle to reinitiate the power-up self-tests.

Please note: An RSA signature verification known-answer test (KAT) is performed prior to the firmware integrity test being performed.

10.2 CONDITIONAL SELF-TESTS

The following conditional self-tests are performed upon power-up, on-demand and periodically.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt (A5476)	256-bit - Encryption KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Encrypt KAT	Power-on, On-demand & Periodically (11 mins)
AES-CBC Decrypt (A5476)	256-bit - Decryption KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Decrypt KAT	Power-on, On-demand & Periodically (11 mins)
AES-ECB Encrypt (A5476)	256-bit - Encryption KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Encrypt KAT	Power-on, On-demand & Periodically (11 mins)
AES-ECB Decrypt (A5476)	256-bit - Decryption KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Decrypt KAT	Power-on, On-demand & Periodically (11 mins)
AES-KW Wrap (A5476)	256-bit - Key Wrap KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Key Wrap KAT	Power-on, On-demand & Periodically (11 mins)

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-KW Unwrap (A5476)	256-bit - Key Unwrap KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Key Unwrap KAT	Power-on, On-demand & Periodically (11 mins)
AES-XTS Testing Revision 2.0 Encrypt (A5476)	256-bit - Encryption KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Encrypt KAT	Power-on, On-demand & Periodically (11 mins)
AES-XTS Testing Revision 2.0 Decrypt (A5476)	256-bit - Decryption KAT	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Decrypt KAT	Power-on, On-demand & Periodically (11 mins)
AES-XTS Key Gen (Ref: IG C.I)	XTS Key Validity	--	Critical Function	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Key1 is not equal to Key2	Generation of DEK_CO or DEK_U
HMAC DRBG (A5476)	Instantiate, Generate and Reseed	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Instantiate, Generate and Reseed KAT	Power-on, On-demand & Periodically (11 mins)
KAS-ECC-SSC Sp800-56Ar3 (A5476)	Private Key:256-bit Public Key: 256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on, On-demand & Periodically (11 mins)

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDA TwoStep SP800-56Cr2 (A5476)	Shared Secret: 256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on, On-demand & Periodically (11 mins)
Entropy Source	APT/RCT	APT/RCT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Repetition Count Test and Adaptive Proportion Test	Continuous
HMAC-SHA2-256 (A5476)	256-bit	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on, On-demand & Periodically (11 mins)
ECDSA KeyGen (FIPS186-5) (A5476)	ECC CDH P-256 keypair pairwise consistency test.	PCT	PCT	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	ECC CDH keypair generation during key agreement when 'Open Partition' service is called.	Performed immediately after key generation during key agreement
ECDSA KeyVer (FIPS186-5) (A5476)	ECC CDH P-256 Public Key Validation	PKV	Critical Function	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Full Public Key Validation of host public key	Performed immediately after key generation during key agreement
PBKDF (A5476)	Salt 256-bit, Password: 8-bytes	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on, On-demand & Periodically (11 mins)

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A5476)	N/A	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Compares output with expected result	Power-on, On-demand & Periodically (11 mins)
RSA SigVer (FIPS186-4) (A5476)	RSA 2048 & SHA2-256	KAT	CAST	Success: LED blinks at 3Hz Error: LED blinks at 16Hz	Signature Verification KAT	Power-on, On-demand & Periodically (11 mins)

Table 22: Conditional Self-Tests

10.3 PERIODIC SELF-TEST INFORMATION

The module performs all self-tests automatically (with no operator intervention) every 11 minutes after being powered-on.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A5476)	RSA 2048 Digital Signature Verification	SW/FW Integrity	11 minutes	Automatic

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt (A5476)	KAT	CAST	11 minutes	Automatic
AES-CBC Decrypt (A5476)	KAT	CAST	11 minutes	Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB Encrypt (A5476)	KAT	CAST	11 minutes	Automatic
AES-ECB Decrypt (A5476)	KAT	CAST	11 minutes	Automatic
AES-KW Wrap (A5476)	KAT	CAST	11 minutes	Automatic
AES-KW Unwrap (A5476)	KAT	CAST	11 minutes	Automatic
AES-XTS Testing Revision 2.0 Encrypt (A5476)	KAT	CAST	11 minutes	Automatic
AES-XTS Testing Revision 2.0 Decrypt (A5476)	KAT	CAST	11 minutes	Automatic
AES-XTS Key Gen (Ref: IG C.I)	--	Critical Function	N/A	N/A
HMAC DRBG (A5476)	KAT	CAST	11 minutes	Automatic
KAS-ECC-SSC Sp800-56Ar3 (A5476)	KAT	CAST	11 minutes	Automatic
KDA TwoStep SP800-56Cr2 (A5476)	KAT	CAST	11 minutes	Automatic
Entropy Source	APT/RCT	CAST	Continuous	Automatic
HMAC-SHA2-256 (A5476)	KAT	CAST	11 minutes	Automatic

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-5) (A5476)	PCT	PCT	N/A	N/A
ECDSA KeyVer (FIPS186-5) (A5476)	PKV	Critical Function	N/A	N/A
PBKDF (A5476)	KAT	CAST	11 minutes	Automatic
SHA2-256 (A5476)	KAT	CAST	11 minutes	Automatic
RSA SigVer (FIPS186-4) (A5476)	KAT	CAST	11 minutes	Automatic

Table 24: Conditional Periodic Information

10.4 ERROR STATES

The module supports the following error states. All data via the data output interface is inhibited whilst within an error state. No cryptographic functions are available whilst the module is in an error state.

Name	Description	Conditions	Recovery Method	Indicator
Soft Error	Soft Error State	Transitions to this state for all non-critical errors	Automatic	LED Blink Pattern, Error Code
Hard Error	Hard Error State	Transitions to this state for all self-test errors	Power-Cycle	LED Blink Pattern, Error Code

Table 25: Error States

10.5 OPERATOR INITIATION OF SELF-TESTS

The operator can initiate the self-tests at any time by power-cycling the module or via the 'Perform Self-Tests' command.

11 LIFE-CYCLE ASSURANCE

There are no specific maintenance requirements.

11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

The User must configure and enforce the following initialization procedures:

1. Connect the *Defender 3000™ USB Flash Drive* to a GPC. The module will enumerate onto the GPC and register its CD ROM partition. Locate and run the application located on the CD-ROM partition.
2. Follow the instructions presented by the application to 'Initialize' the module. Setup the new CO password and continue to login to the device.
3. Click on the Kanguru icon in the system tray to bring up a pull-up menu and select the "About" option. The application will display the firmware and application versions and identifiers. Verify that the firmware version matches what is listed in Table 2.

11.2 ADMINISTRATOR GUIDANCE

Upon receipt of the module an operator must follow the initialization procedure outlined in Section 11.1. This establishes the operator as the Cryptographic Officer (CO) with a valid ID and password.

The module is designed to securely store authorized user's data files using physical and logical security methods. A user may transfer files to the device via a compatible PC or similar device. Over the life of the device an operator may:

- Initialize the device as a single operator (CO only).
- Initialize the device for multiple operators (CO and User).
- Transfer files to the device for secure storage.
- Reset the device effectively erasing all data and security parameters.

Services available to the CO role are listed in Table 12.

11.3 NON-ADMINISTRATOR GUIDANCE

The cryptographic officer must establish access for additional operators. Additional operators will be assigned to the User role. An operator under the User role shall authenticate and transfer files to the device via a compatible PC or similar device. Services available to the User role are listed in Table 12.

11.4 DESIGN AND RULES

In the approved mode of operation, the module shall adhere to the following rules:

- The module prohibits operator passwords less than 8 characters.
- The module generates at a minimum 256 bits of entropy for use in key generation (refer to ESV validation #E195).
- The cryptographic module satisfies the requirements of FIPS 140-3 IG C.I for AES-XTS key generation (i.e., key_1 ≠ key_2).

- The cryptographic module does not output CSPs in any form.
- The cryptographic module enters its defined error state upon failure of self-tests, ceasing cryptographic services.
- The approved DRBG is used for generating cryptographic keys.
- The cryptographic module enforces identity-based authentication for security relevant services.
- The operator can invoke the module to perform the Pre-Operational and Conditional self-tests on-demand by power-cycling the module.
- The module performs firmware integrity test as part of the Pre-Operational self-tests at power-on, prior to each operator authentication, on demand and automatically after a set period of time.
- The module does not support concurrent operators.
- The module does not support the manual entry of SSPs.
- The module inhibits data output via the data output interface during self-tests, SSP generation, error states and zeroization.
- Modification of PSPs by unauthorized operators is prohibited.
- The module does not support bypass mechanisms.
- The module does not support maintenance role.
- The module does not support the loading of firmware.
- The operator cannot change roles without first exiting from the currently assumed role.
- Cryptographic keys derived from passwords conformant with NIST standard Special Publication (SP) 800-132 - 'Recommendation for Password-Based Key Derivation' (PBKDF) may only be used in storage applications.

11.5 END OF LIFE

Upon the need to decommission the module, the CO should perform a ‘Reset Drive’ operation to securely overwrite all security parameters which makes all stored data unrecoverable. The module can then be repurposed or physically scrapped.

12 MITIGATION OF OTHER ATTACKS

This module is not designed to mitigate other attacks beyond the scope of FIPS 140-3 requirements.