iStorage Ltd.
datAshur PRO

FIPS 140-3 Non-Proprietary Security Policy
Version 1.0

List of Tables

List of Figures

1 General

1.1 Overview

The iStorage Ltd. datAshur PRO, datAshur PRO+A and datAshur PRO+C are multi-chip standalone, cryptographic modules that provide hardware-encrypted storage of user data with a USB 3.0 interface. Access to encrypted data is authenticated with user input via the built-in keypad.

1.2 Security Levels

The modules are designed to meet the Security Level 3 requirements for each of the applicable sections documented within ISO/IEC 19790, Section 6 as shown in Table 1.

Table 1: Security Levels

ISO/IEC 24759 Section 6	FIPS 140-3 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-Test	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
	Overall Level:	3

2 Cryptographic Module Specification

2.1 Description

Purpose: The datAshur PRO, datAshur PRO+A and datAshur PRO+C provide hardware-encrypted storage of user data with a USB 3.0 interface. Access to encrypted data is authenticated with user input via the built-in keypad. The modules are designed to interface with a general-purpose computer (GPC) or similar device.

Module Type: The datAshur PRO, datAshur PRO+A and datAshur PRO+C are defined as hardware modules (*refer to ISO/IEC 19790, Section 7.2.2*)

Embodiment: The modules' physical embodiments are defined as multi-chip standalone.

Module Characteristics: User data is protected by 256-bit XTS-AES encryption that secures sensitive information from unauthorized disclosure in the event that the module is lost or stolen. The critical components within the module are encapsulated inside a hard, opaque, production grade epoxy. There is a non-replaceable battery within the module.

The data encryption key (DEK) and other sensitive security parameters (SSPs) are generated within the module, on-demand by an approved NIST SP 800-90A DRBG[1]. The seed for the DRBG is also produced within the module from a hardware-based, NIST SP 800-90B compliant entropy source.

The user interface for the module is an alphanumeric keypad with eleven (11) buttons and three (3) status-indicator LEDs. The LEDs are each a different color (red, green, and blue) and in distinct locations. The keypad accepts the User or Cryptographic Officer (CO) password when creating new credentials and when authenticating to unlock the module. The LEDs provide status information while entering authentication credentials and using the module.

[1] *SP 800-90Ar1 – Recommendation for Random Number Generation Using Determinstic Random Bit Generators*. NIST. (June 2015).

2.1.1 TOEPP and Cryptographic Boundary

The module is a multi-chip standalone cryptographic module whose outer enclosure defines the cryptographic boundary and Tested Operational Environment's Physical Perimeter (TOEPP) (*refer to Figure 1 and Figure 2*).

Figure 1: datAshur PRO and datAshur PRO+A Cryptographic Boundary

Figure 2: datAshur PRO+C Cryptographic Boundary

2.2 Tested and Vendor Affirmed Module Version and Identification

The datAshur PRO, datAshur PRO+A and datAshur PRO+C cryptographic modules are designed to meet the requirements of FIPS 140-3 Security Level 3 (*refer to Table 1*). The modules are available in the following configurations:

- IS-FL-DA3-256-x (USB A)
- IS-FL-DA3C-256-y (USB C)

x = 4, 8, 16, 32, 64, 128, 256, 512 (denotes module's memory capacity in GB)
y = 4, 8, 16, 32, 64, 128, 256 (denotes module's memory capacity in GB)

2.2.1 Tested Operating Environments

The module's operating environment is defined as non-modifiable. The FIPS 140-3 Security Level 3 validated versioning information is shown in Table 2.

Table 2: Tested Configurations

Model	Hardware Version	Firmware Version	Processor(s)	Distinguishing Features
datAshur PRO 4GB	IS-FL-DA3-256-4	1.12.4, 1.12.6, 2.00.0	STMicroelectronics 32-bit MCU ARM-based Cortex & Phison Electronics PS2251-13	4GB of user data storage; USB A
datAshur PRO 8GB	IS-FL-DA3-256-8	1.12.4, 1.12.6, 2.00.0		8GB of user data storage; USB A
datAshur PRO 16GB	IS-FL-DA3-256-16	1.12.4, 1.12.6, 2.00.0		16GB of user data storage; USB A
datAshur PRO 32GB	IS-FL-DA3-256-32	1.12.4, 1.12.6, 2.00.0		32GB of user data storage; USB A
datAshur PRO 64GB	IS-FL-DA3-256-64	1.12.4, 1.12.6, 2.00.0		64GB of user data storage; USB A
datAshur PRO 128GB	IS-FL-DA3-256-128	1.12.4, 1.12.6, 2.00.0		128GB of user data storage; USB A
datAshur PRO+A 8GB	IS-FL-DA3A-256-8	1.12.4, 1.12.6, 2.00.0	STMicroelectronics 32-bit MCU ARM-based Cortex & Phison Electronics PS2251-13	8GB of user data storage; USB A
datAshur PRO+A 16GB	IS-FL-DA3A-256-16	1.12.4, 1.12.6, 2.00.0		16GB of user data storage; USB A
datAshur PRO+A 32GB	IS-FL-DA3A-256-32	1.12.4, 1.12.6, 2.00.0		32GB of user data storage; USB A
datAshur PRO+A 64GB	IS-FL-DA3A-256-64	1.12.4, 1.12.6, 2.00.0		64GB of user data storage; USB A
datAshur PRO+A 128GB	IS-FL-DA3A-256-128	1.12.4, 1.12.6, 2.00.0		128GB of user data storage; USB A
datAshur PRO+A 256GB	IS-FL-DA3A-256-256	1.12.4, 1.12.6, 2.00.0		256GB of user data storage; USB A
datAshur PRO+A 512GB	IS-FL-DA3A-256-512	1.12.4, 1.12.6, 2.00.0		512GB of user data storage; USB A
datAshur PRO+C 4GB	IS-FL-DA3C-256-4	1.12.4, 1.12.6, 2.00.0	STMicroelectronics 32-bit MCU ARM-based Cortex & Phison Electronics PS2251-13	4GB of user data storage; USB C
datAshur PRO+C 8GB	IS-FL-DA3C-256-8	1.12.4, 1.12.6, 2.00.0		8GB of user data storage; USB C
datAshur PRO+C 16GB	IS-FL-DA3C-256-16	1.12.4, 1.12.6, 2.00.0		16GB of user data storage; USB C
datAshur PRO+C 32GB	IS-FL-DA3C-256-32	1.12.4, 1.12.6, 2.00.0		32GB of user data storage; USB C
datAshur PRO+C 64GB	IS-FL-DA3C-256-64	1.12.4, 1.12.6, 2.00.0		64GB of user data storage; USB C
datAshur PRO+C 128GB	IS-FL-DA3C-256-128	1.12.4, 1.12.6, 2.00.0		128GB of user data storage; USB C
datAshur PRO+C 256GB	IS-FL-DA3C-256-256	1.12.4, 1.12.6, 2.00.0		256GB of user data storage; USB C

To identify a module covered by this security policy, locate the product hardware identifier from the back side of the module housing in the table above. Then, use the '*Show Version'* service to verify that the

module identifier (Red, Blue, Green LED Blink = datAshur PRO) and firmware version (e.g., Red LED blinks twice = 2.00.0)

2.3 Excluded Components

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

2.4 Modes of Operation

The module supports a single, approved mode of operation with only approved services. There are no non-approved modes, degraded modes, or non-approved services available to the module. Upon successful completion of the pre-operational and conditional self-tests on power-up, the module provides an indicator of the approved mode identified by the three status-indicator (Red, Green, and Blue) LEDs blinking once simultaneously.

2.5 Algorithms

The datAshur PRO, datAshur PRO+A and datAshur PRO+C modules support the approved cryptographic algorithms shown in Table 3.

2.5.1 Approved Algorithms

The module supports the following approved cryptographic algorithms.

Table 3: Approved Algorithms

CAVP Cert.	Algorithm & Standard	Mode / Method	Description / Key Size(s), Key Strength(s)	Use / Function
3749	AES (NIST SP 800-38E[2])	XTS	256-bits	Encryption of user data within storage application only
3757	AES (FIPS 197[3] NIST SP 800-38A, NIST SP 800-38B[4])	ECB CTR	128-bit, 256-bit	Block cipher basis of CTR-DRBG for encryption/decryption of the DEK
3757	CMAC	AES	128-bits	CO/User authentication
1032	DRBG (NIST SP 800-90A, NIST SP-800-133[5])	AES-CTR	256-bits	Random bit generator for the generation of encryption keys and salts
--	ENT (P) (NIST SP-800-90B)	-	384-bits	Entropy source used to seed the DRBG
2459	HMAC (FIPS 198-1[6])	SHA-1	160-bits	Algorithmic basis of PBKDFv2
A777	PBKDFv2 (NIST SP 800-132[7])	HMAC-SHA-1	1 in 10,000,000 (~23 bits)	Derivation of the KEK. Conforms to FIPS 140-3 Implementation Guidance (IG)

[2] *SP 800-38E – Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices*. NIST. (January 2010).
[3] *FIPS 197 – Advanced Encryption Standard (AES)*. NIST. (November 2001).
[4] *SP 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. NIST. (December 2001).
[5] *SP 800-133r2 – Recommendation for Cryptographic Key Generation*. NIST. (June 2020).
[6] *FIPS 198-1 – The Keyed-Hash Message Authentication Code (HMAC)*. NIST. (July 2008).
[7] *SP 800-132 – Recommendation for Password-Based Key Derivation: Part 1: Storage Applications*. NIST. (December 2010).

				D.N: the module supports option 2a as documented in SP 800-132 § 5.4
3127	SHS (FIPS 180-4[8])	SHA-1	N/A	Primitive within HMAC-SHA-1

2.5.2 Vendor-Affirmed Algorithms

The module supports the following vendor affirmed algorithms.

Table 4: Vendor Affirmed Algorithms

Algorithm	Standard	Modes/ Methods	Description / Key Size(s) / Key Strength(s)	Use/Function
CKG	NIST SP-800-133[9]	Per Section 4	The unmodified output from SP 800-90A DRBG (256 bits)	The unmodified output of the DRBG is used for generating symmetric keys

2.5.3 Non-Approved, Allowed Algorithms

For all approved services the module supports only approved algorithms.

Table 5: Non-Approved, Allowed Algorithms

Algorithm	Caveat	Use/Function
N/A	N/A	N/A

2.5.4 Non-Approved, Allowed Algorithms with No Security Claimed

The module does not support any non-approved algorithms.

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

Algorithm	Caveat	Use / Function
N/A	N/A	N/A

2.5.5 Non-Approved, Not-Allowed Algorithms

The module does not support any non-approved, not allowed algorithms.

Table 7: Non-Approved, Not Allowed Algorithms

Algorithm / Function	Use / Function
N/A	N/A

[8] *FIPS 180-4 – Secure Hash Standard (SHS)*. NIST. (August 2015).
[9] *SP 800-133r2 – Recommendation for Cryptographic Key Generation*. NIST. (June 2020).

2.6 Security Function Implementation

The module does not support key establishment and therefore does not support any key agreement or key transport schemes.

Table 8: Security Function Implementations

Name	Type	Description	SF Properties	Algorithms	Algorithm Properties
N/A	N/A	N/A	N/A	N/A	N/A

2.7 Algorithm Specific Information

The module utilizes only approved algorithms that are tested and validated under the Cryptographic Module Validation Program (CAVP).

2.8 RBG [Random Bit Generator] and Entropy

The module incorporates a NIST SP 800-90A CTR-DRBG (*Cert. #1032*) that is seeded with 384 bits of entropy from a NIST SP 800-90B conforming physical entropy source. The unmodified output of the DRBG is used for generating symmetric keys and salts.

2.9 Key Generation

The module generates cryptographic keys using a NIST SP 800-90A conforming DRBG (*Cert. #1032*) for the encryption and protection of user data.

2.10 Key Establishment

The module does not support key establishment.

2.11 Industry Protocols

The module relies upon the standard USB protocol for communication with general purpose computer (GPC) systems.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The module incorporates both physical ports and logical interfaces.

Table 9: Physical Ports and Logical Interfaces

Physical Port	Logical Interface	Description
USB Port (Rx/Tx)	Data input Data output Control input Status output	The USB Data port connects the module to the host computer. It is used to exchange decrypted user data as well as control and status information for the USB protocol When the drive is locked the USB interface is disabled
Alphanumeric Keypad (0-9)	Data input	The keypad with ten (10) alphanumeric labeled buttons is connected to button inputs. The keypad is used to enter User or CO Password
KEY Button	Control input	The **KEY** button is connected to a button input. It is used to awaken the module from low-power sleep and to control UI flow including selection of the role
3 x LEDs (Red, Green, & Blue)	Status output	Refer to Table 11, Table 12, Table 16, Table 17, Table 18, and Table 19 for details
USB Port (VCC)	Power Input	The USB VBUS (+5VDC) charges the battery and provide power to the module and embedded storage components

3.2 Trusted Channel Specification

The module implements a trusted channel for the input of plaintext SSPs in the form of passwords via the module's keypad. Each key is mapped to a dedicated, physically separated channel. The channel is protected by the physical security mechanisms inherent within the module.

4 Roles, Services, and Authentication

4.1 Authentication Methods

The module supports identity-based authentication in the form of a unique ID / Password combination. The authentication method of both Crypto Officer and User is the password-based authentication technique known as a Memorized Secret in conformance with NIST SP 800-140E and SP 800-63B (*refer to Section 5.1.1*). The Crypto Officer and User roles authenticate via the module's keypad interface. The module does not support a feedback mechanism or output CO or User authentication data outside of the cryptographic boundary.

The module enforces some constraints on the creation of a Password. The following Password forms will be rejected by the module as invalid:

- Identical repeating characters, e.g. 77777777
- Ascending or descending characters e.g. 12345678 or 98765432

The Password from either the User or the CO is input to a PBKDF that produces the Key Encryption Key (KEK) associated to the role. The KEK is used to encrypt or decrypt the DEK with AES CTR (*Cert. #3757*) and authenticate the CO/User using AES CMAC (*Cert. #3757*).

Table 10: Authentication Methods

Name	Description	Mechanism	Strength Each Attempt	Strength Per Minute
ID & Password	CO and User role authentication method The password is at least 8 chars in length	ID & Password combination	The upper bound for the probability of having the password guessed at random is: 1 / (10^8) or 1 in 100,000,000	The probability of the consecutive failed authentication attempts in one minute period is approximately 10^{-7} or 1 chance in 10,000,000

The authentication strength for the module is determined by the Password. The Password is composed of a sequence of decimal digits 0-9, as marked on the keypad buttons, selected by the User or CO. Most of the buttons also bear alphabetic letters (*refer to Figure 1*). The minimum Password length is eight (8) characters[10]. The maximum Password length is 15 characters. The probability of a successful, random guess of a minimum length Password is approximately 10^{-8} or 1 chance in 100,000,000[11].

The module protects against brute-force attempts to guess a role's Password by permitting no more than ten (10) consecutive incorrect guesses before locking out that role. Incorrect Password attempts are counted independently for each role. The probability of an attacker correctly guessing a Password in any time period[12], such as a one-minute interval, is 10^{-7} or 1 chance in 10,000,000.

[10] As per SP 800-63B, in Approved mode the module checks and enforces a minimum password length of eight (8)

[11] Sequential and repeating Passwords are not allowed. For example, the module will reject a Password of 1-2-3-4-5-6-7-8 or 7-6-5-4-3-2-1-0. Attempts to create such a Password will cause the module to indicate an error. There are 270 such combinations.

[12] In this product, a single successful attempt to guess a Password has a probability one in 100,000,000 (10^{-8}). Ten guesses has a probability of one in 10,000,000 ($10*10^{-8}$ or 10^{-7}) of success. The standard requires that the probability of a successful guess be less than one in 100,000 (10^{-5}) in a one-minute period. The authentication mechanism of this module is better than the standard requires, over any time interval—including a one-minute period. A probability of one in 10,000,000 (10^{-7}) is less likely than one in 100,000 (10^{-5}).

4.2 Roles

The module implements level 3, identity-based authentication with two distinct identities, one User identity and one Crypto-Officer identity.

While unauthenticated, the module supports a limited set of services such as checking the module status and zeroizing the module using the Factory Reset service.

Table 11: Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Set CO Password	Keypad command + New CO Password	- Solid Red LED → Solid Green LED (Success)
	Set User Password	Keypad command + New User Password	- Solid Red LED → Solid Green LED (Success)
	Erase Private Partition Data	Keypad commands (Control Input) + CO Password	- Solid Red LED → Solid Red & Green LEDs → Green flickering LED indicating that all data has been deleted
CO / User	Unlock Private Partition (Login)	CO / User ID & Password	- Solid Red LED → Solid Green LED (Success) - Solid Red LED
	Lock Private Partition (Logout)	Keypad command (Control Input) / Remove Power	- Solid Red LED → Fades to off
	Read / Write Private Partition Data	Disk Access	- Blue LED flashes continuously - Read/Write partition data
	Configure Idle Timeout Lock	Keypad command + Timeout Value	- Solid Red LED → Solid Green LED (Success)
	Enable / Disable Read Only	Keypad command (Control Input)	- Solid Red LED → Solid Green LED (Success)
	Show Module Version	Keypad command (Control Input)	- All LEDs illuminate (indicating datAshur PRO) - Red and Green LEDs output firmware version
	View Last Error	Keypad command (Control Input)	
Unauthenticated	Factory Reset (zeroize)	Keypad command (Control Input)	- Solid Red & Green LEDs → Solid Red LED
	Show Status	Keypad command (Control Input)	Returns roles configured on the module: - Red LED blinks continuously for 10 seconds (shows only the CO role exists) - Red & Blue LED blink continuously for 10 seconds (shows both CO & User have been defined)
	Run Self-tests	Power	Refer to Table 16 and Table 17

4.3 Approved Services

The table below summarizes the Approved Services of the module. The SSP Access column identifies the SSPs accessed for each service with codes specifying the kind of access granted during the service operation. SSP access rights are defined as follows:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

Table 12: Approved Services

Name	Description	Approved Security Functions	Keys and / or SSPs	Role	Access Rights to Keys and / or SSPs	Indicator
Configure Idle Timeout Lock	Sets the how long the drive can be idle before needing to reauthenticate	N/A	N/A	CO / User	N/A	Solid Red LED → Solid Green LED (Success)
Erase Private Partition Data	Zeroizes the drive partition	AES (Cert. #3757) DRBG (Cert. #1032) HMAC (Cert. #2459) SHS (Cert. #3127)	DEK DRBG Internal State	CO	DEK (G, E, Z) DRBG Internal State (G, E, Z) User KEK (Z)	Solid Red LED → Solid Green LED (Success)
Enable / Disable Read Only	Sets the data partition to read only	N/A	N/A	CO / User	N/A	Solid Red LED → Solid Green LED (Success)
Factory Reset (Zeroize)	Resets the module to its original factory state This service zeroizes the module	N/A	DEK DRBG Internal State	Unauthenticated	DEK (Z) DRBG Internal State (Z) CO Salt (Z) User Salt (Z)	Solid Red & Green LEDs → Solid Red which fades to off
Lock Private Partition (Logout)	Logout service that locks the drive's storage partition	None	DEK	CO / User	DEK (Z)	Solid Red LED → Fades to off

Name	Description	Approved Security Functions	Keys and / or SSPs	Role	Access Rights to Keys and / or SSPs	Indicator
Read / Write Private Partition Data	Encrypts and writes inbound data or reads and decrypts outbound data	AES (Cert. #3749)	DEK	CO / User	DEK (E)	Blue LED flashes continuously
Run Self-tests	Runs the modules Pre-operational and Conditional self-tests	None	None	Unauthenticated	None	Refer to Table 16 and Table 17 for indicator values
Set CO Password	Sets the CO Password	AES (Cert. #3757) DRBG (Cert. #1032) HMAC (Cert. #2459) PBKDF (Cert. #A777) SHS (Cert. #3127)	CO KEK DEK DRBG Internal State	CO	CO KEK (G, E) CO IV Key (G, E) CO Salt (G, E) DEK (Z) DRBG State (G, E, Z)	- Solid Red LED → Solid Green LED (Success) - Solid Green LED (Error)
Set User Password	Sets the User Password	AES (Cert. #3757) DRBG (Cert. #1032) HMAC (Cert. #2459) PBKDF (Cert. #A777) SHS (Cert. #3127)	User KEK DEK (E) DRBG State	CO	User KEK (G, E) User IV Key (G, E) User Salt (G, E) DEK (Z) DRBG State (G, E, Z)	- Solid Red LED → Solid Green LED (Success) - Solid Green LED (Error)
Show Module Version	Requests the modules identifier and version information	None	None	CO / User	None	LEDs all flash on momentarily followed by red LED blinking out major version number and then green LED blinking out minor version number
Show Status	Returns roles configured on the module	None	None	Unauthenticated	None	- Red LED blinks continuously for 10 seconds (shows only the CO role exists) - Red & Blue LED blink continuously for 10 seconds (shows both CO & User have been defined)

Name	Description	Approved Security Functions	Keys and / or SSPs	Role	Access Rights to Keys and / or SSPs	Indicator
Unlock Private Partition (Login)	CO / User login service that unlocks the drive's storage partition.	AES (Cert. #3757) DRBG (Cert. #1032) HMAC (Cert. #2459) PBKDF (Cert. #A777) SHS (Cert. #3127)	CO KEK DEK	CO / User	CO/User KEK (G, E, Z) CO/User IV Key (G, E, Z) CO/User Salt (E)	- Solid Red LED → Solid Green LED (Success) - Solid Red LED → Fades to off (Error)
View Last Error	Requests last known error	None	None	CO / User	None	Refer to Table 19 for indicator values

4.4 Non-Approved Services

The module does not support any non-approved services.

4.5 External Software/Firmware Loading

The module does not support external software / firmware loading.

5 Software/Firmware Security

5.1 Integrity Techniques

This module firmware is non-modifiable and as such, does not support firmware upgrades. When powered-on, components within the module perform a firmware integrity check. Failure of any firmware integrity check puts the module into an error state which is signaled by the LED status indicators not illuminating.

5.2 Initiate on Demand

A firmware integrity check may be performed by powering the module off and then on.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The module is built upon a custom operational environment that is non-modifiable.

7 Physical Security

The multi-chip standalone cryptographic module includes the following physical security mechanisms, conforming to FIPS 140-3 Level 3 requirements:

1. Production grade components
2. Hard, opaque, tamper-evident enclosure with embedded, hard epoxy covering all security relevant components.
3. Memory protection enabled to prevent read-out of firmware, RAM, or NVRAM

7.1 Mechanisms and Actions Required

The cryptographic boundary for the module is the aluminum case as shown in Figure 1. On each use, the user should check the module for physical damage, cracks, scratches, or other evidence of tampering such as the integrity of the end cap. While holding the body of the module, a firm tug on the lanyard should not show movement of the end cap or the body.

7.2 EFP/EFT

This module does not implement explicit environmental failure protection mechanisms (EFP). The module conforms to the FIPS 140-3 environmental failure testing (EFT) requirements.

Table 13: EFP/EFT

	Temperature / Voltage Measurement	EFP / EFT	Shutdown, Zeroization, Undefined Failure, Known Error Sate or Continues to Operate Normally[13]
Low Temperature	-100°C	EFT	Continues to Operate Normally
High Temperature	145°C	EFT	Undefined Failure
Low Voltage	2.5V	EFT	Shutdown
High Voltage	10.1V	EFT	Undefined Failure

7.3 Hardness Testing Temperature Ranges

The module supports and has been tested at the operation, storage and distribution temperatures listed in Table 14. The module's epoxy and outer enclosure hardness are assured within these ranges.

Table 14: Hardness Testing Temperature Ranges

	Hardness Tested Temperature Measurement
Low Temperature	-20°C
High Temperature	60°C

8 Non-Invasive Security

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

9 Sensitive Security Parameter (SSP) Management

The module incorporates Critical Security Parameters (CSPs) in the form of secret keys and passwords. The module does not utilize Public Security Parameters (PSPs) e.g. public keys.

9.1 Storage Areas

The module is a data storage device designed to encrypt and store arbitrary data using AES-XTS within its eMMC memory components. The module physically and logically protects CSPs when they are present within the module. Please refer to Table 15 for additional information.

[13] For EFP, states can be *Shutdown* or *Zeroise*; for EFT, states can be Shutdown, Zeroization, Undefined Failure, Known Error Sate or Continues to Operate Normally.

9.2 SSP Input/Output Methods

Passwords are input into the module by the operator via the module's dedicated keypad. These are the only SSPs entered into the module. The operator's KEK is derived from the associated password using PBKDFv2[14]. (Note, the KEK is used as part of the module's data storage application only). The DEK is stored encrypted with AES CTR.

The module does not output or establish SSPs using key agreement or key transport methods.

9.3 SSP Zeroization Methods

Zeroization is the erasure of CSPs from volatile and non-volatile storage. The module initiates an erase cycle to zeroize SSPs stored in NVRAM. Copies of SSPs in RAM are zeroized by setting the memory locations to zeros. This process occurs when the module is factory reset or when the module detects a brute-force attack.

There are two kinds of brute-force attacks. Ten consecutive failed attempts to unlock the module as the User is the first type of brute-force attack and will zeroize the User CSPs. After this type of attack, the CO will be able to unlock the module, recover user data, and permit the setup of a new User Password. However, if there is no CO Password, the user data partition will be permanently unrecoverable, leaving the module in the factory reset and blank state with an empty user data partition.

The second kind of brute-force attack is against the CO Password. Ten consecutive failed attempts to unlock the module as CO will zeroize all SSPs for both the CO and User roles, including the DEK. The module will be left in the factory reset and blank state with an empty user data partition.

9.3.1 Zeroization via Factory Reset

A Factory Reset will zeroize all SSPs, settings, and user data from the module. After this operation, the operator must reinitialize the module per Section 11.1 before data may be written to the user data partition.

Starting with the module disconnected from the USB port,

1. Press and hold the **7** button. Press and release the **KEY** button. Release the **7** button. The red and green LEDs will alternate. If the LEDs do not illuminate, connect the module to a USB power source and charge the battery for at least one minute. Disconnect the module from USB and restart this procedure.
2. Enter the sequence **999**. The red and green LEDs will continue to alternate.
3. Press and hold the **7** button. Press and release the **KEY** button. Release the **7** button. If the procedure is correctly performed, the red and green LEDs will illuminate together while the module zeroizes.
4. On completion, the LEDs turn off.

[14] Per FIPS SP800-132 and FIPS140IG § D.6, the materials derived from PBKDFv2 are used only for "protection of electronically stored data or for the protection of data protection keys."

9.4 Sensitive Security Parameters (SSPs)

Table 15: Sensitive Security Parameters

Key / CSP Name	Strength	Security Function & Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroization	Use & Related Keys
DRBG Internal State (V and Key)	256 bits	CTR-DRBG (Cert. #1032)	Internally: from DRBG	Input: N/A Output: N/A	N/A	Plaintext in RAM (Static)	Zeroized on module lock, connect, after generation of CSPs, power-off, and zeroization service	Internal state of the DRBG
Entropy Input	256-bits	ENT (P)	Internally: from Entropy Source	Input: N/A Output: N/A	N/A	Plaintext in RAM (Dynamic)	Zeroized immediately after use	DRBG seed material
User Password	8-15 chars	N/A	N/A	Input: Manual / Direct Entry Output: N/A	N/A	Plaintext temporarily in RAM (Dynamic)	Zeroized immediately after use	Used to authenticate the User and derive the User's KEK and IV Key
CO Password	8-15 chars	N/A	N/A	Input: Manual / Direct Entry Output: N/A	N/A	Plaintext temporarily in RAM (Dynamic)	Zeroized immediately after use	Used to authenticate the CO and derive the CO's KEK and IV Key
DEK	256 bits	AES-XTS (AES Cert. #3749)	CTR-DRBG	Input: N/A Output: N/A	N/A	Encrypted by KEK (Dynamic)	Zeroized on module lock, timeout, power-off, and zeroization service	Data encryption and decryption using AES-XTS
User KEK	128 bits	AES CTR (Cert. #3757)	N/A	Input: N/A Output: N/A	Derived from User Password and Salt using PBKDFv2	Plaintext temporarily in RAM (Dynamic)	Zeroized immediately after use	Encryption/Decryption of the DEK
CO KEK	128 bits	AES CTR (Cert. #3757)	N/A	Input: N/A Output: N/A	Derived from CO Password and Salt using PBKDFv2	Plaintext temporarily in RAM (Dynamic)	Zeroized immediately after use	Encryption/Decryption of the DEK
User Salt	128 bits	PBKDF (Cert. #A777)	CTR-DRBG	Input: N/A Output: N/A	N/A	Plaintext in RAM (Static)	Zeroized on zeroization service (Factory Reset)	Used with User password to create User KEK and User Key
CO Salt	128 bits	PBKDF (Cert. #A777)	CTR-DRBG	Input: N/A Output: N/A	N/A	Plaintext in RAM (Static)	Zeroized on zeroization service (Factory Reset)	Used with User password to create CO KEK and CO Key

User IV Key	128 bits	AES CMAC (Cert. #3757)	N/A	Input: N/A Output: N/A	Derived from User Password and Salt using PBKDFv2	Plaintext in RAM (Static)	Zeroized immediately after use	Used to authenticate the User
CO IV Key	128 bits	AES CMAC (Cert. #3757)	N/A	Input: N/A Output: N/A	Derived from CO Password and Salt using PBKDFv2	Plaintext in RAM (Static)	Zeroized immediately after use	Used to authenticate the CO

10 Self-Tests

When the module powers on, it performs a sequence of self-tests. If any of these tests fails, the drive will enter an error state. The module will not perform any cryptographic services and will output no user data in the error state. The module also performs continuous self-tests. The only way to clear a module error state is to cycle the power.

10.1 Pre-Operational Self Tests

When the module fails a pre-operational self-test, it enters the error state described in Table 16 and Table 18 below. Clearing this error state requires that the module be power cycled.

Table 16: Per-Operational Self-Tests

Algorithm	Test Properties	Test Method	Type	Indicator	Details
CRC-32	CRC-32	Cyclic Redundancy Check	CRC-32	Success: All three LEDs blink once simultaneously Error: LED will not illuminate; the module shuts down	A CRC is an error detection code (EDC) that is calculated over the firmware binary and verified as part of the firmware integrity tests
CRC-16	CRC-16	Cyclic Redundancy Check	CRC-16		

10.2 Conditional Self-Tests

When the module fails a conditional self-test, it enters an error state described in Table 17 and Table 18. Clearing this error state requires that the module be power cycled.

Table 17: Conditional Self-Tests

Algorithm	Test Properties	Test Method	Indicator	Details	Condition
AES ECB Cert. #3757	128-bit Key	KAT	Success: All three LEDs blink once simultaneously Error: LEDs illuminate two times in circling pattern, red then green then blue – Red LED illuminates.	Encrypt KAT	Power-on
AES ECB Cert. #3757	128-bit Key	KAT	Success: All three LEDs blink once simultaneously Error: LEDs illuminate two times in circling pattern, red then green then blue – Red LED illuminates.	Decrypt KAT	Power-on
AES CMAC Cert. #3757	128-bit Key	KAT	Success: All three LEDs blink once simultaneously Error: LEDs illuminate two times in circling pattern, red then green then blue – Red LED illuminates.	Generation KAT	Power-on
AES XTS Cert. #3749	256-bit Key	KAT	Success: All three LEDs blink once simultaneously Error: Illuminates red LED	Encrypt KAT	Power-on

Algorithm	Test Properties	Test Method	Indicator	Details	Condition
AES-XTS Cert. #3749	256-bit Key	KAT	Success: All three LEDs blink once simultaneously Error: Illuminates red LED	Decrypt KAT	Power-on
CTR-DRBG Cert. #1032	384-bit	KAT	Success: All three LEDs blink once simultaneously Error: LEDs illuminate two times in circling pattern, red then green then blue – Red LED illuminates.	Instantiate and Generate KAT	Power-on
PBKDFv2 Cert. #A777	Password (8 chars)	KAT	Success: All three LEDs blink once simultaneously Error: LEDs illuminate two times in circling pattern, red then green then blue – Red LED illuminates.	PBKDF KAT using known password	Power-on
Entropy Source	N/A	APT/RCT	Success: All three LEDs blink once simultaneously Error: LEDs illuminate two times in circling pattern, red then green then blue – Red LED illuminates.	Adaptive Proportion Test and Repetition Count Test performed on the entropy source	Continuous
AES-XTS Key Generation	XTS Key Validity: Key #1 ≠ Key #2	N/A	Error: Illuminates red LED	Per IG C.I after AES-XTS key generation test to ensure keys are unique: Key #1 ≠ Key #2	Creation of DEK
Password Integrity	N/A	Manual Key Entry	Success: When setting passwords, the module will illuminate its red LED for a few seconds Any other indication means the password do not match	Requires passwords to be entered twice	Setting CO or User Password

10.3 Periodic Self-Tests

The module authentication component performs periodic self-tests each time it powers on and prior to authentication by the operator. Once authenticated, the authentication component enters a low-power state. It may be awakened to rerun the self-tests by disconnecting the module from USB and then powering the module on by pressing the **KEY** button.

The module data encryption component performs periodic self-tests while the module is connected and mounted to a host computer. These tests are executed automatically every 15 minutes.

10.4 Error States

Table 18: Error States

State Name	Description	Conditions	Recovery Mode	Indicator
Hard Error	Hard Error State	Transitions to this state for all errors	Power-Cycle	Illuminates Red LED

To verify that the module is in good working order, power it on by connecting it to a USB power source. The three status indicator LEDs will blink simultaneously, indicating that firmware integrity tests and KATs have passed successfully.

When using the *View Last Error* service, the module will report the error as a sequence of LED blinks. The following table summarizes the LED patterns that the module emits for each logged error.

Table 19: Logged Error Codes

Logged Error	Code	LED Pattern
None	0	Green
Entropy Health Failure	1	Red
DRBG Failure	2	Red Green
Credential Storage Failure	3	Red Red
Encryption Component Health Failure	4	Red Green Green

10.5 Operator Initiation of Self-Tests

The operator may initiate all self-tests (pre-operational and conditional cryptographic algorithm self-tests) at any time by powering on the module (either by inserting the module into a USB port or by pressing the **KEY** button once).

11 Life-Cycle Assurance

Power-up self-tests are run based on user action. For a module that is unlocked and in-use for an extended period of time, the user is encouraged to disconnect and reconnect the module to re-run self-tests.

11.1 Installation, Initialization, and Startup Procedures

After a module is assembled in the factory, production release firmware is programmed into the electronics, the circuit board is coated with epoxy, and the module is sealed with an epoxy adhesive. The factory configures the module with a DEK, loads product documentation into the secure, encrypted data partition, and then prepares the module for first use by the user.

There is no default Password set at the factory. On first use, the user must create either a User or a CO Password. Subsequently, data on the encrypted partition may be read, modified, or deleted.

A new module comes from the factory preloaded with product documentation and with a DEK defined. No Password is set when the module leaves the factory. Before the first use and before the secure encrypted data partition can be accessed, a User or CO Password must be set. After this is done, the module is ready for operation.

11.2 Administrator Guidance

Before the first use a CO Password (8 – 15 characters) must be set (this password should not be disclosed). After this is done, the module is ready for operation. Press the **KEY** button once, then press

the **KEY** button twice. Enter the CO password and press the **KEY** button twice. Enter the CO password again and press the **KEY** button twice.

The module's administrator's guide is shipped with the module.

An operator may choose to Factory Reset the module before first use if the provenance of the module is unknown or suspect. Performing a Factory Reset will guarantee that the encrypted data partition is blank and unformatted on first use and that a new DEK is generated when the first Password is set.

If the module is zeroized, it will become blank in the same way that a Factory Reset causes the module to be made blank. There will be no DEK defined, it will have neither a User Password nor a CO Password defined, and on first use the encrypted data partition must be formatted.

11.3 Non-Administrator Guidance

The CO may choose to configure the module for dual roles i.e. CO and User. In such instances, a User password must be established and set by the CO.

11.4 Design and Rules of Operation

To meet the requirements for FIPS 140-3 Security Level 3, the module enforces the following security rules:

- The cryptographic module provides two distinct operator roles: User and Cryptographic Officer (CO).
- The cryptographic module provides identity-based authentication.
- Upon removing power from the module, the authentication session is cleared.
- When the module has not been placed in a valid role or is in an error state, the operator shall not have access to any cryptographic service.
- Passwords must not be disclosed.
- The operator can command the module to perform self-tests at any time by cycling the power.
- All data output is inhibited during pre-operational and conditional self-tests, zeroization, key generation, and authentication.
- The module is an encrypted storage drive that utilizes PBKDFv2 (NIST SP 800-132) and AES-XTS (FIPS 197 and NIST SP 800-38e). These algorithms can only be used for the protection of data at rest.

12 Mitigation of Other Attacks

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

13 Appendix A: Abbreviations and Definitions

Term	Definition
AES	Advanced Encryption Standard
CO	Cryptographic Officer
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR-DRBG	Counter-Mode Deterministic Random Byte Generator
DEK	Data Encryption Key
DRBG	Deterministic Random Byte Generator
ECB	Electronic Code Book
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
GPC	General Purpose Computer
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
KEK	Key Encryption Key
LED	Light Emitting Diode
NIST	National Institute of Standards and Technology
NVRAM	Non-volatile Random Access Memory
PBKDFv2	Password Based Key Derivation Algorithm Version 2
PSP	Public Security Parameter
RAM	Random Access Memory
Salt	Random value used to improve security of cryptographic algorithms
SHA-1	Secure Hash Algorithm 1
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
TOEPP	Tested Operating Environment Physical Perimeter
USB	Universal Serial Bus
XTS-AES	AES cipher mode used to encrypt user data in mass storage
Zeroization	The process of erasing cryptographic security keys and parameters