IBM® NVMe FlashCore™ Module 2
FIPS 140-3 Non-proprietary Security Policy

Security Level 2

Rev. 2.6 – July 24, 2024

IBM® Corporation

Table of Contents

Table of Tables

Table of Figures

1 General

1.1 Scope

This is the security policy associated with the IBM NVMe FlashCore Module 2, a NVMe-connected self-encrypting non-volatile storage hardware module, a Cryptographic Module which is being validated per FIPS 140-3.

This document is designed to meet the FIPS 140-3 standard (see Section 1.2 References 1) and Implementation Guidance (see Section 1.2 References 3) requirements. It is not intended to provide the type of interface details required to develop a compliant application.

1.2 References

1. FIPS PUB 140-3, issued Mar 22, 2019
2. FIPS 140-3 Derived Test Requirements, issued Mar, 2020
3. Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, last updated May 4, 2021
4. TCG Storage Architecture Core Specification, Specification Version 2.01
5. TCG Storage Security Subsystem Class: Opal, Specification Version 2.01
6. TCG Storage Opal SSC Feature Set: PSID Version 1.00
7. TCG Storage Opal SSC Feature Set: Single User Mode, Specification Version 1.00
8. NVM Express Revision 1.2.1

1.3 Acronyms used in this document

AdminSP	Administrative security partition, a TCG term
AES	Advanced Encryption Standard (FIPS 197)
APT	Adaptive Proportion Test
ARM	Advanced RISC Machine
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining, an encryption mode
CKG	Cooperative Key Generation
CLiC	CryptoLite in C
CO	Crypto-Officer
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
DDR4	Double Data Rate 4 memory
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook Mode
ENT	Entropy
FCM2	FlashCore Module 2
FIPS	Federal Information Processing Standard
FKM	Flash Key Management
FPGA	Field Programmable Gate Array
HMAC	Hash-based Message Authentication Code
IC	Integrated Circuit
IG	Implementation Guide
LBA	Logical Block Address
KAT	Known Answer Test
KDF	Key Derivation Function
KEK	Key Encryption Key

LockingSP	Locking Range security partition, a TCG term
MEK	Media Encryption Key
MSID	Manufactured SID, TCG term for a unique per FCM2 public value used as the default
NAND	Not AND (a type of flash memory)
NOR	A type of flash memory
NSSR	NVMe SubSystem Reset
NVMe	Nonvolatile memory express
OFS	Original Factory State
PIN	Personal Identification Number
POST	Power on Self-Test
PSID	Physical SID, TCG term for a unique per FM value public value
RAM	Random Access Memory
RCT	Repetition Count Test
RSA	Rivest Shamir Adleman algorithm
SHA	Secure Hash Algorithm
SID	Security ID, TCG term for Drive Owner CO role's PIN
SLR	SUM Locking Range
SP	Security Policy (per FIPS 140-3)
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
SUM	Single User Mode
SWG	Storage Work Group
TCG	Trusted Computing Group
TEL	Tamper Evident Label
XTS	XEX-based tweaked-codebook mode with ciphertext stealing, an encryption mode

1.4 Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A

Table 1-1 Security Levels

2 Cryptographic module specification

2.1 Overview

The cryptographic module is the IBM NVMe FlashCore Module 2 (FCM2) in its entirety. The cryptographic module will be referred to as the FCM2 throughout this document. This FCM2 uses approved algorithms to provide a number of cryptographic services. Those services include encryption and decryption of user data in hardware, support for cryptographic erase, support for multiple user data Locking Ranges (each of which can be configured for independent access control and protection), and authentication checking of code downloads. The services are provided via FCM2 support of the TCG Opal SSC interface.

The FCM2 is a multiple-chip embedded cryptographic module implementation. The outside surfaces of the FlashCore Module 2 Assembly are the physical cryptographic boundary. The module's logical boundary is comprised of all hardware and firmware components contained within the module's physical boundary. The host interface to the FCM2 is physically a PCIe connector, over which the industry-standard NVMe protocol (see Section 1.2 References 8) is supported. Through the NVMe logical interface the FCM2 supports the TCG SWG Core (see Section 1.2 References 4) and TCG Opal SSC (see Section 1.2 References 5) protocols. All control of the FCM2 via its interfaces is typically through an application on a host system. All human control of an FCM2 is assumed to be through such an application.

The primary cryptographic service supported by the FCM2 is encryption of user data at rest: encrypting user data written to the FCM2 before the resultant ciphertext is written to the FCM2's non-volatile solid-state memory. The FCM2 also supports the complementary decryption function, decrypting that ciphertext from solid-state memory when it is read back. Storing user data in encrypted form enables another cryptographic service the FCM2 supports: cryptographic erase, which nearly instantly renders all previously encrypted user data to be effectively destroyed. The FCM2 supports TCG Opal access controls, which restrict access to use of, and administration of, the encryption and cryptographic erase services.

2.2 Approved Mode of Operation

The FCM2 will operate in a non-compliant state until the Secure Initialization steps detailed in Section 11.1 are performed.

From this non-compliant state, the FCM2 may be securely initialized so that it operates in FIPS 140-3 Mode of operation (hereafter "approved mode"). After the FCM2 has been Securely Initialized and operated per the Security Rules detailed in Section 11.1, the FCM2 will remain in approved mode of operation until either an important error or failure has been detected or a "Revert via OFS" service is performed. An operator controlling the FCM2 can use the "FIPSmode?" service, if it does not return the expected status (see Section 4.5), then the FCM2 is not operating in approved mode.

An operator can cause an FCM2 operating in approved mode to quit approved mode by use of the FCM2's "Revert via OFS" service. This service will zeroize the FCM2's keys and CSPs and transition it through its Original Factory State (OFS) to its non-compliant state. The operator can then cause that FCM2 to return to approved mode by following the Secure Initialization procedure detailed in Section 11.1 again.

To operate the FCM2 is in its, it must be configured properly and it must be operated in accordance with the associated policy restrictions (detailed in Section 11.2). Violating the ongoing policy restrictions would mean that the FCM2 is no longer being operated in its approved mode of operation.

2.2.1 Approved mode

When operated in this mode the FCM2 provides cryptographic services via industry-standard NVMe commands, TCG Opal commands addressed to the TCG AdminSP, and TCG Opal commands addressed to the TCG LockingSP. To operate in approved mode, the Drive Owner must invoke the Activate method on the LockingSP starting from a non-compliant state which itself must start afresh from an OFS state.

Keys and CSPs established in approved mode cannot be used in non-compliant state. This is accomplished by the key zeroization which performed as part of the "Revert via OFS" service.

Similarly, Keys and CSPs established in non-compliant state cannot be used in approved mode. If an FCM2 had been previously operated with a non-FIPS code load, a Locking Range may have been established, though that FCM2 would not have been in approved mode because of the non-FIPS code load. In this case some keys (e.g. the Locking Range's MEK) would have been established with a non-FIPS code load and they cannot be used in approved mode. If the code on that FCM2 is then updated to the FIPS code load, then the FCM2 must be put back into the OFS state by use of one of the Opal methods specified in the "Revert via OFS" service. This service will cause cryptographic erase of all data written to those Locking Ranges as the Locking Range's MEKs are zeroized. Then the drives can be put back into approved mode if all requirements are met.

The FCM2 only supports Single User Mode (SUM), so only a single User has independent access control to read/write/erase a given Locking Range. By default, there is a single "Global Range" that encompasses the whole user data area. "Locking Ranges", when established, are configured to be subsets of the LBA range initially established as a Global Range.

2.2.2 SUM Locking Ranges (SLRs)

When invoking the Activate method to enter approved mode, the Drive Owner creates a Locking Range (LR). All LRs created within the FCM2 must be of the Single User Mode (SUM) type. The FCM2 does not support creation of non-SUM LRs, or reclassification of SUM LRs into non-SUM LRs, and any TCG Opal methods attempting either of those will fail with the appropriate error code returned. So, all LRs created in an FCM2 will be, and will remain, "SUM Locking Ranges" (SLRs). SLRs conform to the SUM feature set (see Section 1.2 References 7). Each SLR is controlled and administered solely by the single User role it is associated with per Section 1.2 References 5 and see Section 1.2 References 7, e.g. SLR1 by User2.

TCG Opal implements multiple Cryptographic Officer (CO) roles which operate cooperatively to establish, configure, and administer these SLRs. These roles include, at a minimum, the Drive Owner, the User(s), and the LockingSP Admin(s). While in approved mode, this cooperative operation includes:

1. Creating one or more SLRs (by the Drive Owner)
   - the FCM2 supports a Global Range and the additional creation of up to 3 SLRs
2. Customize the User PIN and LBA range associated with each created SLR (by User(s) only)
3. Lock and Unlock SLRs (by User(s) only)
4. Crypto-Erase of SLRs (by User(s) or Locking SP Admin(s))
5. Crypto-Erase of Global Range (by Locking SP Admin(s))

2.3 Hardware and Firmware Versions

The following FCM2 configurations have been validated:

Model	Hardware	Firmware Version	Distinguishing Features
IBM NVMe FlashCore Module 2 Xlarge	02CL181 TEL part number: 03JN363	2.2.0.99	38.4TB physical capacity
IBM NVMe FlashCore Module 2 Large	02CL183 TEL part number: 03JN363	2.2.0.99	19.2TB physical capacity
IBM NVMe FlashCore Module 2 Medium	02CL185 TEL part number: 03JN363	2.2.0.99	9.6TB physical capacity
IBM NVMe FlashCore Module 2 Small	02CL187 TEL part number: 03JN363	2.2.0.99	4.8TB physical capacity

Table 2-1 Cryptographic Module Tested Configuration

The configurations vary with respect to the memory integrated circuits (ICs) used. The number of parts, part numbers, and storage capacity of those ICs varies between configurations, but these ICs have no cryptographic capability and do not alter the approved services provided.

A complete list of FCM2's components can be found in the master components list. The majority of the components are not described in any further detail here because they are not related to encryption.

The FCM2 drive contains a Xilinx Zynq Ultrascale+ XCZU19EG FPGA (vendor part # = XCZU19EG-L2FFVB1517E4845). That FPGA contains two processor complexes:

- For applications: Quad-core ARM® Cortex™ A53 MPCore™(up to 1.5GHz)
- For real-time: Dual-core ARM Cortex-R5 MPCore™ (up to 600MHz)

Two of the A53 cores, and both of the R5 cores, are powered off and never run.
The first of other two A53 cores runs a forever while loop and the second core runs a bare-metal applications running a modified version of uC/OS-II v.2.61". The first of the A53 cores runs the Flash card (back-end) tasks including the Flash Key Manager (FKM) task. The second of the A53 cores runs the host attach (front-end) NVMe task. The TCG Opal task runs underneath NVMe task. All cryptography is done by either the TCG Opal task or the FKM task, each runs a copy of the IBM Crypto-Lite in C (CLiC) v4.14.24.3852 (c4T3/FlashSysANSIC64)
Two A53 cores have its own memory address space, CPU register files, etc. CSP/SSP is not shared on these two A53 cores, which means only one core has access/control over a certain CSP/SSP.

2.4 Approved and Allowed Algorithms

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A1883	SHA3-384 (H/W) FIPS 202	SHA3	384bits digest	As part of verification of a code load's digital signature (4 byte aligned only *2)
A1884	AES-CBC SP 800-38A	AES CBC mode	128bits key	A primitive used by the AES-CBC-MAC conditioning component for whitening performed as part of entropy processing
A1884	AES-ECB-256 (F/W) FIPS 197	AES ECB mode	256bits key	A primitive used by XTS-AES-256 Encrypt, and by AES key wrap & unwrap
A1884	AES-KEY-UNWRAP (F/W) SP 800-38F	AES-KEY-UNWRAP	256bits key	It's used in the context of TCG authentication
A1884	AES-KEY-WRAP (F/W) SP 800-38F	AES-KEY-WRAP	256bits key	Store the encryption key in ciphertext mode

A1884	AES-XTS-256 Encrypt (F/W)* SP 800-38E	XTS-AES Encrypt	256bits key	To check XTS-AES-256 Encrypt in H/W
A1884	Conditioning Component AES-CBC-MAC SP800-90B	AES-CBC-MAC	Key Length: 128; Payload Length: 384	Whitening performed as part of entropy processing
A1884	Hash DRBG-SHA-512 (F/W) SP 800-90Arev1	DRBG	DRBG with sha 512	Random number generation
A1884	HMAC-SHA-256 (F/W) FIPS 198-1	HMAC-SHA-256	256bits digest	Hash of PINs used to authenticate, as well as a primitive used by the KDF
A1884	KDF SP 800-108rev1	KDF	Key derivation function with HMAC-SHA-256	Key derivation
A1884	KTS SP 800-38F	800-38F. KTS (key wrapping and unwrapping) per IG D.G	SSP establishment methodology providing 256 bits of encryption strength	It's used in the context of TCG authentication
A1884	KTS-IFC (F/W) SP 800-56B Rev. 2	KTS OAEP basic responder with SHA2-256 (*5)	RSA 3072bits private key SSP establishment methodology provides 128 bits of encryption strength	Unencapsulation KEK (key encryption key) by RSA private key with OAEP SHA2-256 method
A1884	RSA Key Generation FIPS 186-4	B.3.3	RSA 3072bits	Generation of RSA key pair at startup
A1884	SHA2-256 (F/W) FIPS 180-4	SHA2	256bits digest	A primitive used by HMAC-SHA-256
A1884	SHA2-512 (F/W) FIPS 180-4	SHA2	512bits digest	A primitive used by DRBG-SHA-512
AES #5897	ECB-AES-256 (H/W) FIPS 197	AES ECB mode	256bits key	A primitive used by XTS-AES-256
AES #5897	XTS-AES-256 Encrypt/Decrypt (H/W)* SP 800-38E	XTS-AES Enc/Dec	256bits key	User Data written by a host application is encrypted; decryption is performed on read
N/A	ENT (P) SP 800-90B	ENT	Physical entropy source based on hardware ring oscillators	Seeding the DRBG
Vendor Affirmed *3	RSA SigVer (H/W) FIPS 186-4	RSA	4096bits modulus size, PKCS scheme v1.5, SHA3-384 hash function	As part of verification of a code load's digital signature
Vendor Affirmed *4	CKG (F/W) SP 800-133rev2	CKG	Cryptographic Key Generation	Cryptographic Key Generation

Table 2-2 Approved Algorithms

Algorithm	Caveat	Use/ Function
AES-KW (No Security Claimed)	IG 2.4.A scenario #1	Obfuscation/ Unobfuscation of an SSP.

Table 2-3 Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

The modules does not support any of the following:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.

Please note that only the algorithms, modes and options listed in the table above are implemented and used by the module, and that the referenced certificates may contain additional, unused algorithms.
* XTS-AES-256 is only used by the FCM2 in the context of storage applications
*2 Only 4-byte aligned inputs are supported, so only 4-byte aligned inputs were verified by CAVP
*3 In accordance with FIPS 140-3 IG C.C, the cryptographic module performs digital signature checking using SHA3- 384 as specified in FIPS PUB 202 (Vendor Affirmed). Per IG C.F, the key sizes for this RSA SigVer implementation are untested.
*4 In accordance with FIPS 140-3 IG D.H, the cryptographic module performs cryptographic key generation for symmetric keys & seeds for asymmetric keys per SP 800-133r2 Sections 4, 5.2, 6.1 and 6.2 (Vendor Affirmed).
*5 KTS-OAEP-basic is used with AES-KW per Section 9.3 of SP800-56Br2.

2.5 FCM2 Drive Brick

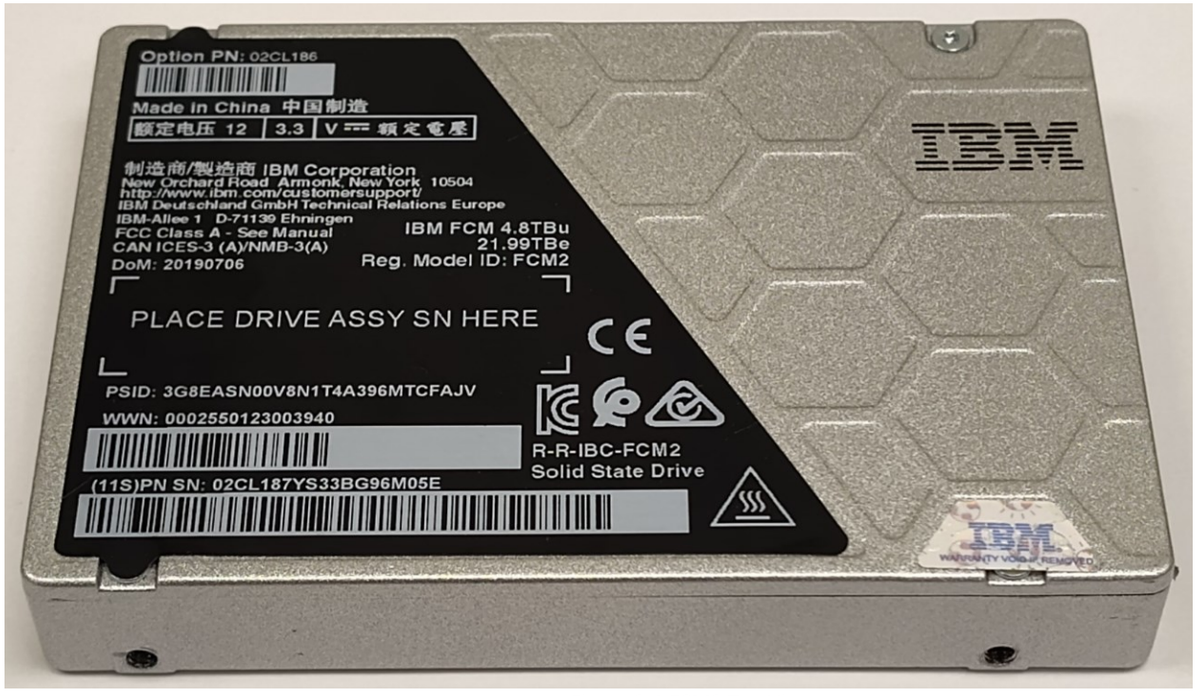

Figure 2-1 FCM2 Top View

The following figure shows placement of TEL1 in red and TEL2 in red.

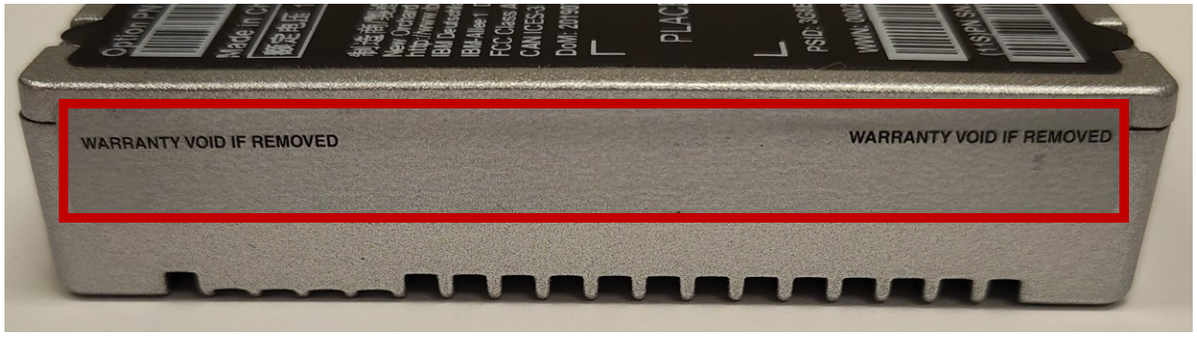

Figure 2-2 FCM2 Front View

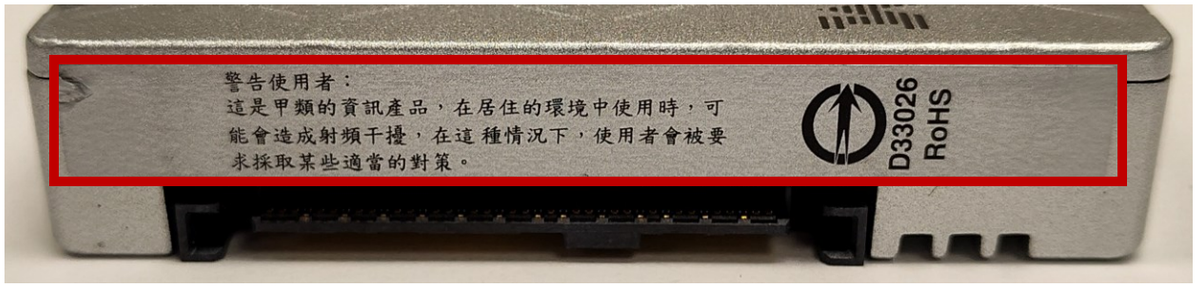

Figure 2-3 FCM2 Back View

2.6 FCM2 Block Diagram

Edge connector is PCIe physically, NVMe logically

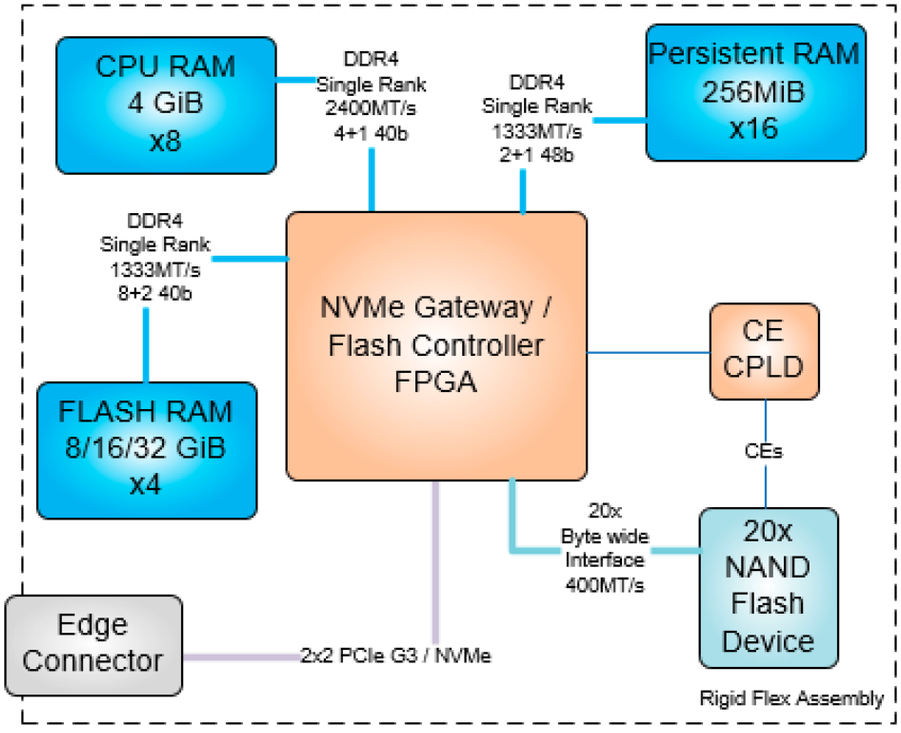

Figure 2-4 FCM2 Block Diagram

3 Cryptographic module interfaces

3.1 Logical to Physical Port Mapping

Physical port	Logical interface	Data that passes over port/interface
PCIe connector	Data In	NVMe protocol commands in
PCIe connector	Data Out	NVMe protocol commands out
PCIe connector	Control Input	Drive control operations
PCIe connector	Status Output	Drive status
PCIe connector	Power Input	N/A

Table 3-1 Ports and Interfaces

Notes: * FCM2 has no control output interface.

4 Roles, services, and authentication

4.1 Crypto-Erase of User Data

Because all user data written to the FCM2 is encrypted when stored to its internal solid-state media, the data can be cryptographically erased (crypto-erased). The encrypted data, ciphertext, stored is effectively erased when the media encryption key (MEK) used to encrypt it is overwritten (with a fresh MEK) or erased (overwritten with a fixed value such as all zeroes). Because the FCM2 supports the ability to "zeroize" all keys and CSPs, per the FIPS 140-3 key management requirement, the FCM2 supports the capability to "zeroize" any and all MEKs, which in turn crypto-erases all the user data encrypted with those MEKs. The FCM2 supports the capability to zeroize any and all MEKs whether it is in approved mode or not.

It should be noted that user data stored to the FCM2 cannot be reliably destroyed by overwrite from the host because the actual storage space where a given LBA's data is stored moves over time within the FCM2 for multiple reasons including support for wear-leveling. But user data can be reliably destroyed by crypto-erase of the associated MEK. Alternately, all private keys and CSPs can be zeroized at once via Opal methods which cause Revert via OFS (see Section 4.2).

4.2 Revert via OFS

Whether in approved mode or not, the TCG Revert and RevertSP methods may be invoked by an appropriately authenticated Role to put the FCM2 into a non-compliant state. This corresponds to the "Revert via OFS" service and is akin to a "restore to factory defaults" operation. This operation causes zeroization of all CSPs and private (or secret) cryptographic keys. Subsequently, the FCM2 has to be reinitialized before it can return to an approved mode of operation. These Revert and RevertSP methods may be invoked by the Drive Owner, by the AdminSP's Admin, by the LockingSP's Admins, or by an unauthenticated role using the public PSID value (see Section 1.2 References 6).

The TCG Revert and RevertSP methods are also the appropriate method to perform the drive "end of life" procedures.

4.3 Operator Roles

The following explains the Cryptographic Officer and User roles with a *general* description of the purpose and authority of each role. For further details of the services performed by each role while the FCM2 is in approved mode, see Section 4.5.

4.3.1 Cryptographic Officer (CO) Roles

4.3.1.1 Drive Owner

This role corresponds to the SID (Secure ID) Authority on the AdminSP as defined in Opal SSC (see Section 1.2 References 5). This role is used to transition the FCM2 to approved mode. It should be noted that to operate in approved mode, a FIPS validated code version (i.e. FIPS code) must be loaded into the FCM2, and the FCM2 must have booted to that code level. If the FCM2 is not running FIPS code, it cannot be operating in approved mode.

4.3.1.2 Admins (1-4) in LockingSP

When in approved mode, these roles' Authority corresponds to the LockingSP's Admin roles as defined in Opal SSC (see Section 1.2 References 5).

4.3.1.3 Admin1 in AdminSP

When in approved mode, this role's Authority corresponds to the AdminSP's Admin1 role defined in Opal SSC (see Section 1.2 References 5). This role is enabled by default, but can be disabled by the Drive Owner, if desired. When enabled, an authenticated AdminSP Admin1 can invoke the "Revert via OFS" service.

4.3.2 LockingSP User2

When in Approved mode, this role's Authority corresponds to the LockingSP's User role as defined in Opal SSC (see Section 1.2 References 5). This role can unlock (and also lock) the corresponding SLR in the FCM3, so that an operator can read and write data to that SLR. This role can also invoke the Crypto-Erase service of the associated SLR.

4.3.3 Unauthenticated Role

Anyone who has the ability to remove and then restore power to a FCM2 can cause a power cycle which will cause a reset of the FCM2, that is one type of unauthenticated service. Note that since both the MSID and 26-byte PSID are public credentials, "authenticating" with either to gain MSID authority or PSID authority, respectively, amounts to operation in an unauthenticated role. Thus, entering the public PSID value enables unauthenticated invocation of some services (e.g. to invoke the "Revert via OFS" service). No authentication is required to perform the "FIPScode?" and "FIPSmode?" services.

4.4 Authentication

4.4.1 Authentication Type

Role-based authentication of operators is supported. For example, the Drive Owner role has its own unique ID which is associated with a dedicated PIN. The Drive Owner's PIN can be personalized such that it is unique for that role.

For some cases, the authentication is performed in a separate associated service. For example, the Read Unlock service is the authentication required to enable subsequent User Data Read service. If an attempt is made to use the User Data Read service without prior authentication, then the User Data Read will fail.

Authentications which use the TCG interface can provide the operator and PIN in the StartSession method invocation. Or, an operator may use the Authenticate method to authenticate to a role within a Session that has already been started. Authentications persist until the associated session is closed.

4.4.2 Authentication in approved mode

Operators can authenticate by use of either the TCG Authenticate or StartSession methods. The host application can have only a single session open at a time. During a session the application can invoke services for which the authenticated operator(s) have authority. One of security rules enforced by the FCM2 is that the host must not authenticate to more than two operators' roles while in a session.

The host application can authenticate to the "Anybody" authority, which does not have a private credential, for the invocation of some services. Accordingly, the invoked services are effectively unauthenticated services.

4.4.3 Authentication Mechanism, Data and Strength

On every startup, the FCM2 generates a fresh new RSA key pair. The RSA public key is discoverable on TCG protocol and the RSA private key is a secret. Operators first query the FCM2's RSA public key and generate a key encryption key (KEK) outside of the drive. The operator encrypts the new KEK via RSA OAEP SHA2-256 method and sends it to the drive. FCM2 decrypts that message using the RSA private key, and then both parties have agreement upon the KEK. After establishment of the KEK, operators then authenticate with the FCM2 by PINs. Outside of the FCM2, any new PIN to be established is AES key wrapped by the KEK. Once sent inside the FCM2, the message is decrypted via AES Key unwrapping, the KEK is confirmed, and then both parties have agreement upon a new PIN. The provided PIN is salted, hashed and compared to the hash non-volatilely stored when that PIN was established. The salt is stored in a different non-volatile location. Per the TCG SWG Core (see Section 1.2 References 4) specification, PINs have an associated retry attribute ("TryLimit") that controls the number of unsuccessful attempts before the authentication is blocked. The default value of the TryLimit setting is 100 which specifies up to 100 retries and Persistence is TRUE which means that any count of incorrect authentications will not be reset on reboot. The count of incorrect authentications will be reset upon a successful authentication or TCG Revert via OFS (see Section 4.2). Neither the TryLimit nor the Persistence settings can be changed, both have their respective Writeable Flags permanently set to FALSE.

The PINs have a variable length of 128 to 256 bits. Per the policy security rules, the FCM2 only allows programming of PINs that are of length 128 bits or longer (see Section 11.1's Rule 7). This PIN length results in a probability of at most $1/2^{128}$ (i.e. less than 10^{-38}) for the PIN to be guessed in a single random attempt.

Each authentication attempt requires 39ms on average for the FCM2 to complete. This means that at most (60*1000)/39 (= 1538) attempts can, on average, be made in one minute. So the probability of multiple random attempts succeeding in guessing a PIN in a one minute period is at most $1538/2^{128} = 4.52 \times 10^{-36}$.

For PIN-based authentications (e.g., TCG SID, TCG Admins 1-4, etc.), they're considered as 'memorized secret' authentication mechanism.

4.4.4 Personalizing Authentication Data

The SID is initially set to the value of the manufactured value (MSID). This is a device-unique public value which is 128 to 256 bits long. The Security Rules (see Section 11) for the FCM2 requires that the PIN values must be "personalized" to private values using the "Set PIN" service. The Drive Owner PIN can be set to a different value by use of the TCG Set Method.

4.5 Approved Mode Services

The following tables details the FIPS 140-3 services the FCM2 provides when in approved mode. It shows which services (Approved Security Functions) can be invoked or used by which authenticated operators (Access Control). in terms of the and operator access control. Note the following:

- Use of the services described below is compliant only when the FCM2 is in approved mode.
- Not shown are the security functions which underlie the higher-level algorithms shown below (e.g. DRBG-SHA-512 as part of ENT (P))
- Operator authentication is not shown in this table, but an operator must have appropriately authenticated to the role shown in the Operator Access Control column to use/invoke the service shown in the Service Name column of the same row
- Some security functions listed are used solely to protect / encrypt keys and CSPs.
- Input and output details of TCG Opal (or NVMe) methods used to invoke the services below are defined by the TCG Opal (or NVMe) standards.
- Unauthenticated services (e.g. FIPScode?) do not provide access to private keys or CSPs
- The User Data Read/Write service implements the lock-based authentication model.
    - Power-cycling the module re-locks the previously unlocked service.
    - The lock-based authentication model remains secure as the currently authenticated operator remains in physical control of the module interfaces until power off.

Role	Service	Input	Output
Drive Owner	Set PIN	PIN	Operation status
	Activate SLR	PIN	Operation status
	Enable / Disable AdminSP Admin	PIN	Operation status
	Revert via OFS	PIN	Operation status
AdminSP Admin1	Set PIN	PIN	Operation status
	Revert via OFS	PIN	Operation status
LockingSP Admin1-4	Set PIN	PIN	Operation status
	Enable / Disable LockingSP Admin(s)	PIN	Operation status
	Crypto-Erase of SLR	PIN	Operation status
	Revert via OFS	PIN	Operation status
LockingSP User2	Set PIN	PIN	Operation status
	Set Geometry	PIN	Operation status
	Lock / Unlock SLR for Rd/Wr	PIN	Operation status
	Crypto-Erase of SLR	PIN	Operation status
Unauthenticated	User Data Read *	NVMe read command	Operation status with data
	User Data Write *	NVMe write command with data	Operation status
	Cold boot	Power-cycle FCM2 drive	Card boots up
	Reset module	NVMe reset command	Card resets and boots up
	FIPSmode?	NVMe identify controller command	Operation status with identify controller response
	FIPScode?	NVMe identify controller command	Operation status with identify controller response
	Get Version	NVMe identify controller command	Operation status with identify controller response
	KEK setup	TCG vendor specific command	Operation status
	Board report	NVMe vendor specific command	Operation status with board report data
	DRBG generate bytes	TCG random service command	Operation status with random bytes

	Firmware download	Firmware image	Operation status

Table 4-1 Roles, Service Commands, Input and Output

Notes: * the drive first needs to be unlocked by an authenticated role.

Role	Authentication Method	Authentication Strength
Drive Owner	PIN protected by AES key wrap	128 to 256 bits PIN and 256 bits key in AES key unwrap
AdminSP Admin1	PIN protected by AES key wrap	128 to 256 bits PIN and 256 bits key in AES key unwrap
LockingSP Admin1-4	PIN protected by AES key wrap	128 to 256 bits PIN and 256 bits key in AES key unwrap
LockingSP User2	PIN protected by AES key wrap	128 to 256 bits PIN and 256 bits key in AES key unwrap

Table 4-2 Roles and Authentication

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs*		Indicator
Set PIN	Change operator authentication data	AES-KW; SHA-256; AES-KW (No Security Claimed);	SID PIN; LockingSP Admin1-4 PINs; AdminSP Admin1 PIN; LockingSP User2 PIN; KEK; LBA Range Root Key	Drive Owner, AdminSP Admin1, LockingSP Admin1-4/LockingSP User2	SID PIN	W	TCG set method returns GOOD
					LockingSP Admin1-4 PINs	W	
					AdminSP Admin1 PIN	W	
					LockingSP User2 PIN	W	
					KEK	E	
					LBA Range Root Key	E	
Activate SLR	Allocate a SUM Locking Range (SLR)	AES-KW; SHA-256	SID PIN; KEK	Drive Owner	SID PIN	W, E	TCG activate method returns GOOD
					KEK	E	
Firmware load	Load firmware image. If the downloaded firmware image signature checks, then the FCM2 will boot to the new code at next reboot.	RSA SigVer; SHA3-384	FW Verification Key	None *	E		New code boots on boot following firmware load

	Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.						
Enable / Disable AdminSP Admin	Enable / Disable the AdminSP Admin1	AES-KW; SHA-256	SID PIN; KEK	Drive Owner	SID PIN	W, E	TCG set method returns GOOD
					KEK	E	
Enable / Disable LockingSP Admin(s)	Enable / Disable a LockingSP Admin	AES-KW; SHA-256	LockingSP Admin1-4 PINs; KEK	Locking SP Admin1 - 4	LockingSP Admin1-4 PINs	W, E	TCG set method returns GOOD
					KEK	E	
Set Geometry	Set the starting LBA and size of the SLR.	AES-KW; SHA-256	LockingSP User2 PINs; KEK	Locking SP User2	LockingSP User2 PIN	W, E	TCG set method returns GOOD
					KEK	E	
Lock / Unlock SLR for Rd/Wr	Block or allow read (decrypt) / write (encrypt) of user data in a range.	AES-KW; SHA-256; AES-KW (No Security Claimed); KDF;	LockingSP User2 PIN; KEK; LBA Range Root Key	Locking SP User2	LockingSP User2 PIN	W, E	TCG set method returns GOOD
					KEK;	E;	
					LBA Range Root Key	E	
User Data	Encryption/decryption of user data	XTS-AES-256	LBA Range MEKs	None	E		NVMe read/write command returns GOOD

Read / Write	to/from a SLR. Access control to this service is provided through Lock/Unlock SLR for Rd/Wr	Decryption/ Encryption (Symmetric Key)					
Crypto-Erase of SLR	Erase user data in a SUM Locking range by changing its associated MEK	DRBG Symmetric Key; AES-KW; SHA-256	LockingSP Admin1-4 PINs; LockingSP User2 PIN; KEK; LBA Range Root Key; LBA Range MEKs; DRBG EI; DRBG Seed; DRBG C; DRBG V;	LockingSP Admin1 - 4	LockingSP Admin1-4 PINs;	W, E	TCG Erase Method returns GOOD
					LockingSP User2 PIN;	E	
					KEK;	Z	
					LBA Range Root Key;	Z	
				LockingSP User2	User2PINs	W, E;	TCG GenKey/Erase Method returns GOOD
					KEK	E;	
					LBA Range Root Key	G, E, Z;	
					LBA Range MEKs	G, Z;	
					DRBG EI	G, E;	
					DRBG Seed	G, E;	
					DRBG C	G, E;	
					DRBG V	G, E;	
Revert via OFS	Exit approved mode. Note: FCM2 will enter non-compliant state.	DRBG Symmetric Key; AES-KW; SHA-256	SID PIN; LockingSP Admin1-4 PINs; AdminSP Admin1 PIN; LockingSP User2 PIN; KEK; LBA Range Root Key; LBA Range MEKs; RSA private key; RSA public key; DRBG EI; DRBG Seed; DRBG C; DRBG V;	Drive Owner	SID PIN	W, E, Z	TCG LockingSPObj.Revert(), TCG AdminSPObj.Revert() returns GOOD
					LockingSP Admin1-4 PINs	Z	
					AdminSP Admin1 PIN	Z	
					LockingSP User2 PIN	Z	
					KEK	E, Z	
					LBA RangeRoot Key	G, E, Z	
					LBA Range MEKs	G, Z	
					RSA private key	Z	
					RSA public key	Z	
					DRBG EI	G, E, Z	
					DRBG Seed	G, E, Z	
					DRBG C	G, E, Z	
					DRBG V	G, E, Z	
				AdminSP Admin1	SID PIN	Z	TCG AdminSPObj.Revert()
					LockingSP Admin1-4 PINs	Z	
					AdminSP Admin1 PIN	W, E, Z	

					LockingSP User2 PIN	Z	
					KEK	E, Z	
					LBA RangeRoot Key	G, E, Z	
					LBA Range MEKs	G, Z	
					RSA private key	Z	
					RSA public key	Z	
					DRBG EI	G, E, Z	
					DRBG Seed	G, E, Z	
					DRBG C	G, E, Z	
					DRBG V	G, E, Z	
				Locking SP Admin1 - 4	LockingSP Admin1-4 PINs	W, E, Z	TCG LockingSP.RevertSP()
					LockingSP User2 PIN	Z	
					KEK	E, Z	
					LBA RangeRoot Key	Z	
					LBA Range MEKs	Z	
Power On	Firmware integrity check on boot (Pre-operational self-test)	RSA SigVer; Generate RSA key-pair	FW Verification Key; RSA private key; RSA public key; KEK; DRBG EI; DRBG Seed; DRBG C; DRBG V;	None	FW Verification Key	E	Cold-Boot or Power-On-Reset and drive boots up
					RSA private key	G, Z	
					RSA public key	G, Z	
					KEK	Z	
					DRBG EI	Z	
					DRBG Seed	Z	
					DRBG C	Z	
					DRBG V	Z	
FIPSmode?	Reports whether, from a drive perspective, the drive is in approved mode	None	None	None	N/A		NVMe Identify: Controller Identify, bytes 3600-3607 (set to “FIPSmode”)
FIPScode?	Reports whether the code level in operation was FIPS validated	None	None	None	N/A		NVMe Identify: Controller Identify, bytes 3616-3623 (set to “FIPScode”)
Get Version	Reports code version	None	None	None	N/A		NVMe Identify: Controller Identify, bytes 64-71
		DRBG	DRBG EI;	None	DRBG EI	G, E	

DRBG Generate Bytes	Returns a SP800-90Arev1 DRBG Random Number of # of bytes requested up to 50		DRBG Seed; DRBG C; DRBG V;		DRBG Seed	G, E	TCG Random() method returns GOOD
					DRBG C	G, E	
					DRBG V	G, E	
KEK setup	Establish KEK during startup	KTS-OAEP-basic responder with SHA2-256	KEK; RSA private key; RSA public key	None	KEK	W	TCG kek setup() method returns GOOD
					RSA private key	E	
					RSA public key	R	
Board report	Dump FCM status	N/A	N/A	None	N/A		Board report trigger and dump commands return GOOD

Table 4-3 Approved Services

* This is unauthenticated as per clause (c) of IG 4.1.A.

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 = Zeroise: The module zeroises the SSP.

5 Software/Firmware security

FCM2 firmware image has a RSA 4096 with sha3-384 digital signature appended, it’s checked during firmware download and startup. If non-IBM image is downloaded, the firmware download procedure will return failure and reject it. The original image in NOR flash won’t be updated at all. On every startup, a similar check occurs and put the card in fault state when it fails.

6 Operational Environment

N/A
The FCM2 operates in a “limited operational environment”. Specifically, the operational environment cannot be modified while the FCM2 is in operation, and no code can be added or deleted. Firmware can be replaced or upgraded with a signed firmware download operation. If the code download’s digital signature checks as authentic, then the FCM2 will boot to it following the next cold boot and so will begin operating with the new firmware image.

See Section 11.1 on how to configure and setup approved mode on FCM2.

7 Physical Security

7.1 Mechanisms

The FCM2 is a multi-chip embedded module that has the following physical security:

1. Built of production-grade components which have standard passivation
2. Two opaque tamper-evident labels (TELs) on the FCM2. There is one TEL on each end of the FCM2. See "Figure 7-1 TEL1 BSMI Label" for placement of TEL1 and Figure 7 2 TEL2 BSMI Label for placement of TEL2. The TELs are applied during IBM's manufacturing process. They protect against physical access to the electronics by board removal and prevent electronic design visibility.
3. Tamper-evident security labels applied by IBM manufacturing prevent FlashCore Module 2 Assembly cover removal for access to or visibility of the solid-state memory
4. Exterior of the FCM2 is opaque
5. The tamper-evident labels (TELs) cannot be penetrated, or removed and reapplied, without that tamper being readily evident
6. The TELs cannot be easily replicated with a low attack time

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Inspect physical tamper evidence TEL1-2	At least once per month	Visual inspection on the tamper evidence TELs

Table 7-1 Physical Security Inspection Guidelines

The operator is required to inspect the FCM2 periodically for any of the following types of tamper evidence:

- Flaking, folding, or ripping of TELs or metal case
  - Figure 7-3 Tampered TEL1 illustrates tamper evidence on TEL1
  - Figure 7-4 Tampered TEL2 illustrates tamper evidence on TEL2
- Security label over screws is missing or penetrated
- Text attributes (e.g. size, font, orientation, etc.) on security label does not match the original TEL
- TEL label cutouts do not match original

If evidence of tampering is apparent, the operator must assume the FCM2 has been compromised and so should decommission that FCM2. At a minimum the operator must discontinue using that FCM2 in any way that relies on that FCM2's cryptographic capabilities. Once tampering of a TEL has been detected, the FCM2 cannot thereafter ever be considered to be in approved mode.

7.1.1 Figure 1 – TEL1 and TEL2

Figure shows TEL1 the BSMI label and TEL2 Warrantee Label.

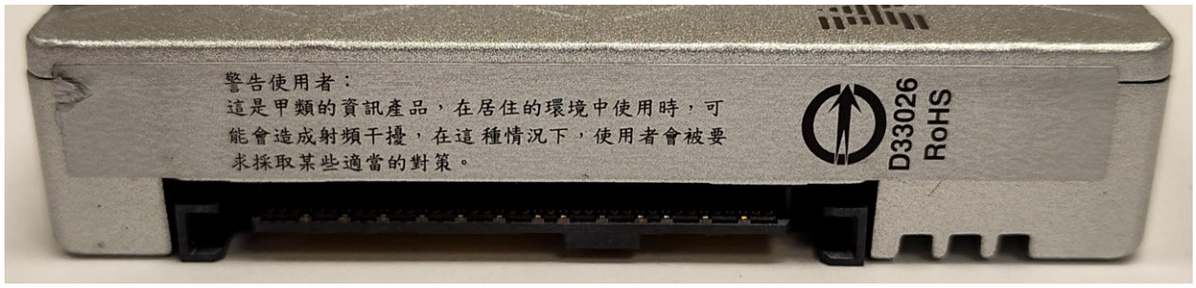

Figure 7-1 TEL1 BSMI Label

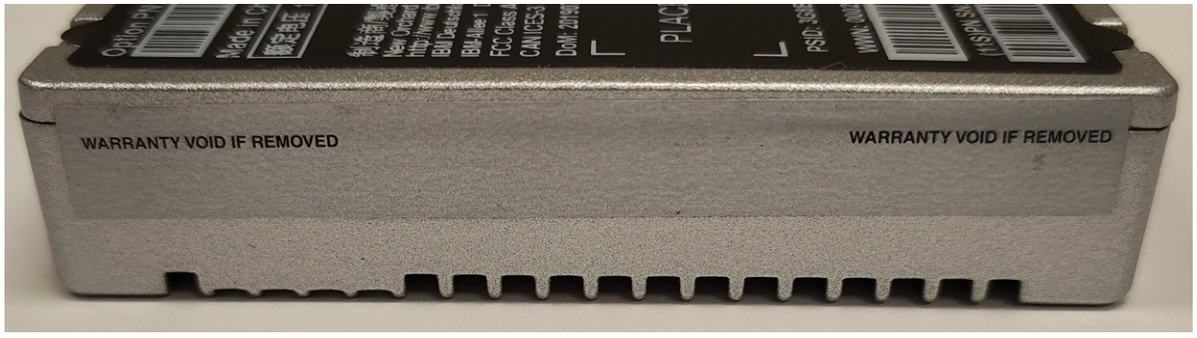

Figure 7-2 TEL2 BSMI Label

7.2 TELs on ends of FCM2

To provide tamper-evidence of FlashCore Module 2 Assembly cover removal:

7.2.1 Figure 2 – tampered TEL1

Showing tamper-evidence on TEL1

Figure 7-3 Tampered TEL1

Where flaking and general distress are seen at each end of the label

7.2.2 Figure 3 – tampered TEL2

Showing tamper evidence of TEL2

Figure 7-4 Tampered TEL2

Where flaking and general distress are seen at each end of the label

8 Non-invasive security

The FCM2 does not claim to non-invasive security relevant to FIPS 140-3 validation.

9 Sensitive security parameters management

9.1 Cryptographic Keys and CSPs

The following table defines the keys / CSPs and the operators / services which use them.

Note that:

- The use of PIN CSPs to authenticate is implied by the operator access control
- All non-volatile storage of keys and CSPs is internal to the FCM2 and to which there is no logical or physical access from outside of the FCM2
- The FCM2 uses a SP 800-90Arev1 DRBG and adopts the Hash_DRBG mechanism
- Non-SSPs are not shown in this table
- The module implements a manual distribution using an electronic entry mechanism for SSP input and output per IG 9.5.A.
- There is no audit feature supported which is security-relevant.
- The AES key wrap implemented by the FCM2 is used for key transport (unwrapping PIN CSPs passed into the module).
- A no security claimed AES-KW implemented by the FCM2 is used for obfuscating stored SSPs as described in the table below.

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
SID PIN	128 to 256 bits size / 128 to 256 bits strength	SHA-256 #A1884	Set by operator	Import Encrypted via AES-KW	This PIN is setup or changed by the drive owner	Non-volatile, hashed via SHA-256	Revert via OFS	Use to authenticate as Drive Owner
						RAM, Plaintext	After authentication service	
LockingSP Admin1-4 PINs	128 to 256 bits size / 128 to 256 bits strength	SHA-256 #A1884	Set by operator	Import Encrypted via AES-KW	These PINs are setup or changed by the corresponding admins	Non-volatile, hashed via SHA-256	Revert via OFS	Use to authenticate as a LockingSP Admin
						RAM, Plaintext	After authentication service	
AdminSP Admin1 PIN	128 to 256 bits size / 128 to 256 bits strength	SHA-256 #A1884	Set by operator	Import Encrypted via AES-KW	These PINs are setup or changed by the	Non-volatile, hashed via SHA-256	Revert via OFS	Use to authenticate as AdminSP Admin1

					corresponding admin	RAM, Plaintext	After authentication service	
LockingSP User2 PIN	128 to 256 bits size / 128 to 256 bits strength	SHA-256 #A1884	Set by operator	Import Encrypted via AES-KW	These PINs are setup or changed by the corresponding users	Non-volatile, hashed via SHA-256	Revert via OFS	Use to authenticate as a LockingSP User
						RAM, Plaintext	After authentication service	
LBA Range Root Key	256 bits size / 256 bits strength	KDF SP800-108 #A1884	Generated from DRBG	N/A	N/A	Non-volatile, obfuscated	Revert via OFS; Crypto-Erase of SLR	Use to derive LBA Range MEKs
LBA Range MEKs	256 bits size each / 256 bits strength each	AES-XTS #AES 5897	These 2 keys are derived from the LBA range root key using the approved SP800-108rev1 KDF	N/A	These 2 keys are derived from the LBA range root key using the approved SP800-108rev1 KDF	CPU RAM, plaintext	Revert via OFS; Crypto-Erase of SLR; Auto-zeroized after use	Use in Encrypt / Decrypt User Data
DRBG EI	1024 bits/ 256 bit strength	Hash DRBG #A1884	Generated using the module's ENT (P)	N/A	N/A	CPU RAM, plaintext	Revert via OFS; Power On; Auto-zeroized after use	Use in services which use the DRBG
DRBG Seed	888bits*/ 256 bit strength	Hash DRBG #A1884	Generated using the module's ENT (P)	N/A	This seed is generated using the module's ENT (P)	CPU RAM, plaintext	Power On; Auto-zeroized after use	Use in services which use the DRBG
DRBG C	DRBG intermediate values C (888 bits each) / 256 bit strength	Hash DRBG #A1884	Generated using the module's ENT (P)	N/A	This is generated using the module's ENT (P)	CPU RAM, plaintext	Revert via OFS; Power On	Use in services which use the DRBG
DRBG V	DRBG intermediate values V (888 bits	Hash DRBG #A1884	Generated using the	N/A	This is generated using the	CPU RAM, plaintext	Revert via OFS; Power On	Use in services which use the DRBG

	each) / 256 bit strength		module's ENT (P)		module's ENT (P)			
FW Verification Key	4096bits size / 152 bits strength	RSA digital signature (Vendor affirmed)	Pre-loaded; Generated externally and hardcoded into the module	N/A	N/A	Non-volatile, plaintext	N/A	Use in firmware load test signature verification
RSA private key	3072 bits size / 128 bits strength	RSA KeyGen (FIPS186-4) #A1884	Generated by FCM2 on power up	N/A	N/A	CPU RAM; stored in CLiC library	Revert via OFS; Power On	Use in KEK establishment
RSA public key	3072 bits size / 128 bits strength	RSA KeyGen (FIPS186-4) #A1884	Generated by FCM2 on power up	Exported in plaintext	N/A	CPU RAM; stored in CLiC library	Revert via OFS; Power On	Use in KEK establishment
KEK	256 bits size / 256 bits strength	AES-KW A1884	N/A	Import Encrypted via RSA	This key is generated by operators and is used to unwrap the TCG keys/CSPs on authentication.	CPU RAM, plaintext	Revert via OFS; Power On	Use in unwrap of any encrypted PIN during authentication

Table 9-1 SSPs

* per https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Arev1r1.pdf; Table 2, seedlen

RBG entropy source:

Entropy sources	Minimum number of bits of entropy	Details
Hardware ring oscillator	1024 bits	The entropy source provides 128-bits of entropy for each 128-bit output from the vetted conditioning component (AES-CBC-MAC Cert. #A1884). The module's DRBG is seeded with 1024 bits of output, thus providing 1024 bits of entropy.

Table 9-2 Non-Deterministic Random Number Generation Specification

9.2 Temporary CSPs

No matter if the FCM2 is in approved mode or non-compliant state, all the temporary keys and CSPs are zeroized when they are no longer needed.

9.3 Control Output Interface

No additional logical interface in FCM2 module.

10 Self-tests

10.1 Self-Tests

The NVMe identify controller command indicates failure of self-tests. Instead of reporting “NoErrors” as required by the approved mode, the identify controller command will show “FailAAAA” where AAAA are ASCII characters providing additional detail on the type of self-test failure. Self-tests may be invoked on-demand via power-cycle.

All errors result in the module entering a "fenced" error state. The two fenced error states are referred to as "Self-Test Failed" and "Operational Test Failed". These error states cannot be normally recovered from without returning the module to the manufacturer for servicing, although IBM also suggests attempting an NVMe "NVM Subsystem Reset" (NSSR) first to attempt to have the module re-run the self-tests.

Function Tested	Self-Test	KAT Implementation	If this KAT test fails
Firmware Integrity Test	Pre-Operational Self-Test	RSA-4096 with SHA3-384	Enters FIPS Self-Test Fail State
Firmware Load Test	Conditional Firmware Load Test	RSA-4096 with SHA3-384	Firmware Load operation fails
SHA2-256	CAST	Hash KAT performed	Enters FIPS Self-Test Fail State
AES-256-KEY-WRAP	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
AES-256-KEY-UNWRAP	CAST	Decrypt KAT performed	Enters FIPS Self-Test Fail State
DRBG (SHA-512)	CAST	DRBG Instantiate/Generate KAT performed	Enters FIPS Self-Test Fail State
SP 800-108rev1 KDF with HMAC-SHA2-256	CAST	KDF and HMAC KAT performed	Enters FIPS Self-Test Fail State
AES-ECB-256	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
XTS-AES-256	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
CBC-AES-128	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
SHA3-384 (H/W)	CAST	Digest KAT performed	Enters FIPS Self-Test Fail State
RSA-4096 (H/W)	CAST	Verify KAT performed	Enters FIPS Self-Test Fail State
XTS-AES-256 (H/W)	CAST	Encrypt performed	Enters FIPS Self-Test Fail State
ECB-AES-256 (H/W)	CAST	Decrypt performed	Enters FIPS Self-Test Fail State
ECB-AES-256 (H/W)	CAST	Encrypt performed	Enters FIPS Self-Test Fail State
KTS-OAEP 3072 with SHA2-256	CAST	RSA decrypt KAT performed	Enters FIPS Self-Test Fail State
Entropy source APT & RCT	CAST (at Power-On and during Entropy Generation)	APT and RCT performed on entropy source samples	Enters FIPS Self-Test Fail State

XTS Key1 != XTS Key 2	Conditional critical function test (Before Key Usage)*	Not a KAT	Enters FIPS Self-Test Fail State
RSA pair-wise consistency test (PCT)	Conditional Pairwise Consistency test (Before Key Usage)*2	Encrypt with public key and decrypt with private key, then compare the answer	Enters FIPS Self-Test Fail State

Table 10-1 Self-tests

* This check is made each time a Root Key is expanded, by two key derivations, into XTS's Key1 and Key2.
*2 The RSA PCT is performed upon module startup right after generation of the keypair and therefore prior to any export. The purpose of the keypair is only for key transport.

The Entropy source is continuously tested by a Repetition Count Test (RCT) and Adaptive Proportion Test (APT).

SP 800-90Arev1 DRBG Instantiate and Generate Health Tests are addressed by destructing the existing instance and instantiating a new one each time a random number is to be generated. A KAT test is run against the new SP 800-90Arev1 instantiation to assure it is sound before it is used. The DRBG is then used to generate a random number by processing ENT (P) samples.

A Continuous Random Number Generator Test (CRNGT) is performed on the output of the DRBG. The first random number generated after power up is not used, and SHA2-256 hash of each subsequently generated new random number is compared to the SHA2-256 of the immediately previous generated random number. The continuous test fails if the two numbers match indicating the output of the DRBG has not changed (i.e. is stuck).

11 Life-cycle assurance

11.1 Establishing approved mode and exit conditions

The FCM2 does not typically change mode across power cycles and resets. However, certain operations can result in the FCM2 exiting approved mode. In some of these situations (e.g. failure of the Power On Self Test), the FCM2 cannot be restored to approved mode and in that case could not provide any further Approved service.

The administrator guidance and product documentation may be acquired by contacting the following email addresses:
gkimbue@us.ibm.com
nehal@us.ibm.com

The following are the security rules for establishment and operation of the FCM2 in the approved mode. Further detail is available in the appropriate sections of this document.

1. Cryptographic Officers: At receipt of the product examine the shipping packaging and the product packaging to ensure it has not been accessed during shipping by the trusted courier.
2. Cryptographic Officers and Users: At installation, and periodically thereafter, examine the Tamper Evident Labels (TELs) installed at time of manufacture for tamper evidence.
3. Cryptographic Officers and Users: At installation, and periodically thereafter, query the FCM2's firmware's code level to be sure it matches the FIPS validated firmware level (see section 2.3). Additionally, use the "FIPScode?" service to assure the firmware identifies itself as "FIPScode" (i.e. that the proper compile time options were used when it was built).
4. Cryptographic Officers: A key encryption key needs to be established for any future TCG authentication. First the FCM public key needs to be queried, generate a 256bits KEK, encrypt it by the RSA public key and pass it down to FCM.
5. Cryptographic Officers: At installation, determine if the FCM2 has been used previously (e.g. has a SLR already been established?). If so, then invoke the "Revert via OFS" service to zeroize all previously established secret keys and CSPs and remove any SLRs.
6. Cryptographic Officers: Transition the FCM2 to approved mode by invoking the Activate method for each SLR to be created
7. Cryptographic Officers and Users: At installation, set all operator PINs applicable for the approved mode to private values of 128 to 256 bits length by use of approved mode: Drive Owner, Admins, and Users. The default authentication data is forcefully replaced upon first-time authentication, otherwise it won't be in approved mode of operation.
8. Cryptographic Officers (specifically LockingSP Admins) to operate in approved mode: Set ReadLockEnabled and WriteLockEnabled to "True" on each activated SLR. Periodically thereafter the ReadLockEnabled and WriteLockEnabled settings should be checked to be sure they have not been modified.
9. Cryptographic Officers: Use the "FIPSmode?" service to assure the firmware sees itself as being in approved mode.
10. Cryptographic Officers: At installation, disable the "Makers" authority by use of the TCG Set method.
11. After secure establishment is complete, do a power-on reset to clear authentications established during establishment.
12. Users: do a GenKey of each SLR's Media Encryption Key (MEK)
13. Cryptographic Officers: verify that the FCM2 indicates it is running "FIPSmodeNoErrors".

If all of these steps are followed correctly, the FCM2 will be in approved mode of operation. It should be noted that all of the conditions detailed above must continue to be met to remain in approved mode. Failure to follow these steps would result in the module operating in a non-compliant state.

11.2 Ongoing Policy Restrictions

Each time a new CO role is to be assumed, the current Session must be closed, and a new Session started (or do a power-on reset), so that the previous authentication to the previous CO authority is cleared.

12 Mitigation of Other Attacks Policy

The FCM2 does not claim to mitigate against any other attacks relevant to FIPS 140-3 validation.

-- End --