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

Security Level 2

Rev. 3.9 – September 18, 2025

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 3, 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 1.3 References 1) and Implementation Guidance (see Section 1.3 References 3) requirements. It is not intended to provide the type of interface details required to develop a compliant application.

This document is non-proprietary. This document may be reproduced in its original entirety.

1.2 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

1.3 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
9. NVM Express Revision 1.3
10. NVM Express Revision 1.4

1.4 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
FCM3	FlashCore Module 3
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 FCM3 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

2 Cryptographic Module Specification

2.1 Overview

The cryptographic module is the IBM NVMe FlashCore Module 3 (FCM3) in its entirety. The cryptographic module will be referred to as the FCM3 throughout this document. This FCM3 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 FCM3 support of the TCG Opal SSC interface.

The FCM3 is a multiple-chip embedded hardware cryptographic module embodiment. The module's cryptographic boundary is comprised of all hardware and firmware components contained within the module's physical enclosure. The host interface to the FCM3 is physically a PCIe connector, over which the industry-standard NVMe protocol (see Section 1.3 References 8) is supported. Through the NVMe logical interface the FCM3 supports the TCG SWG Core (see Section 1.3 References 4) and TCG Opal SSC (see Section 1.3 References 5) protocols. All control of the FCM3 via its interfaces is typically through an application on a host system. All human control of an FCM3 is assumed to be through such an application.

The primary cryptographic service supported by the FCM3 is encryption of user data at rest: encrypting user data written to the FCM3 before the resultant ciphertext is written to the FCM3's non-volatile solid-state memory. The FCM3 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 FCM3 supports: cryptographic erase, which nearly instantly renders all previously encrypted user data to be effectively destroyed. The FCM3 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 FCM3 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 FCM3 may be securely initialized so that it operates in the Approved mode. After the FCM3 has been Securely Initialized and operated per the Security Rules detailed in Section 11.1, the FCM3 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 FCM3 can use the "FIPSmode?" service, if it does not return the expected status (see Section 4.5), then the FCM3 is not operating in Approved mode.

An operator can cause an FCM3 operating in Approved mode to quit Approved mode by use of the FCM3's "Revert via OFS" service. This service will zeroize the FCM3's keys and CSPs and transition it through its Original Factory State (OFS) to its non-compliant state. The operator can then cause that FCM3 to return to Approved mode by following the Secure Initialization procedure detailed in Section 11.1 again.

To operate the FCM3 is in its Approved mode, 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 FCM3 is no longer being operated in its Approved mode of operation.

2.2.1 Approved Mode

When operated in this mode the FCM3 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 an 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 FCM3 had been previously operated with a non-FIPS code load, a Locking Range may have been established, though that FCM3 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 FCM3 is then updated to the FIPS code load, then the FCM3 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 FCM3 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 FCM3 must be of the Single User Mode (SUM) type. The FCM3 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 FCM3 will be, and will remain, "SUM Locking Ranges" (SLRs). SLRs conform to the SUM feature set (see Section 1.3 References 7). Each SLR is controlled and administered solely by the single User role it is associated with per Section 1.3 References 5 and see Section 1.3 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 FCM3 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 FCM3 configurations have been validated:

Model	Hardware	Firmware Version	Distinguishing Features
IBM NVMe FlashCore Module 3 Xlarge	03GH930 TEL part number: 03JN363	3.1.5.99	38.4TB physical capacity
IBM NVMe FlashCore Module 3 Large	03GH932 TEL part number: 03JN363	3.1.5.99	19.2TB physical capacity
IBM NVMe FlashCore Module 3 Medium	03GH934 TEL part number: 03JN363	3.1.5.99	9.6TB physical capacity
IBM NVMe FlashCore Module 3 Small	03GH936 TEL part number: 03JN363	3.1.5.99	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 FIPS services provided.

A complete list of FCM3'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 FCM3 small/medium 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 FCM3 large/xlarge drive contains a Xilinx Versal ACAP FPGA (vendor part # = XCVM1802-2LLEVSVD1760).
That FPGA contains two processor complexes:

- For applications: Dual-core ARM® Cortex™ A72 MPCore
- For real-time: Dual-core ARM Cortex-R5F MPCore

Two of the R5F cores are powered off and never run.

The first of the application 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 application cores runs the Flash card (back-end) tasks including the Flash Key Manager (FKM) task. The second of the application 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) v4.14.27.7548 (c4T3/FlashSysANSIC64) code.
Two application cores have its own memory address space, CPU register files, etc. CSP/SSP is not shared on these two application cores, which means only one core has access/control over a certain CSP/SSP.

See Section 11.1 on how to configure and setup Approved mode on FCM3.

2.4 Approved and Allowed Algorithms

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(Key Strength(s)	Use / Function
A6888	KTS-IFC	KTS	Modulo: 3072; Hash Algorithms: SHA2-256	Decrypt KEK (key encryption key) by RSA private key with OAEP SHA2-256 method
A6888	KTS-IFC (F/W) SP 800-56B Rev. 2	KTS OAEP basic responder with SHA2-256 (*5)	3072-bit modulus providing 128 bits of encryption strength	Unencapsulation KEK (key encryption key) by RSA private key with OAEP SHA2-256 method

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)
A2686	SHA3-384 (H/W) FIPS 202	SHA3	384bits digest	As part of verification of a code load's digital signature (4 byte aligned only)
A2687	AES-ECB (H/W) FIPS 197	AES ECB encrypt/decrypt	256-bits key	A primitive used by XTS-AES-256
A2687	AES-XTS (H/W)* SP 800-38E	XTS-AES Enc/Dec	256-bits key	User Data written by a host application is encrypted; decryption is performed on read
A6888	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
A6888	AES-ECB (F/W) FIPS 197	AES ECB Encrypt/Decrypt	256 bits key	A primitive used by by AES key wrap & unwrap
A6888	AES-KW (F/W) SP 800-38F	AES-KEY-WRAP AES-KEY-UNWRAP	256 bits key	It's used in the context of TCG authentication
A6888	AES-KWP (F/W) SP 800-38F	AES-KEY-WRAP with Padding AES-KEY-UNWRAP with Padding	256 bits key	It's used in the context of TCG authentication
A6888	AES-KWP KTS SP 800-38F	SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G	256-bit keys providing 256 bits of encryption strength	It's used in the context of TCG authentication
A6888	Conditioning Component AES-CBC-MAC SP800-90B	AES-CBC-MAC	Key Length: 128; Payload Length: 384	Whitening performed as part of entropy processing

A6888	Hash DRBG-SHA-512 (F/W) SP 800-90Arev1	DRBG	DRBG with sha SHA2-512	Random number generation
A6888	HMAC-SHA2-256 (F/W) FIPS 198-1	HMAC-SHA2-256	256 bits digest	Hash of PINs used to authenticate, as well as a primitive used by the KDF
A6888	KDF SP 800-108 (rev1)	KDF	Key derivation function with HMAC-SHA2-256	Key derivation
A6888	RSA Key Generation FIPS 186-4	B.3.3	RSA 3072-bits	Generation of RSA key pair at startup
A6888	SHA2-256 (F/W) FIPS 180-4	SHA2-256	256-bits digest	A primitive used by HMAC-SHA2-256
A6888	SHA2-512 (F/W) FIPS 180-4	SHA2-512	512-bits digest	A primitive used by DRBG-SHA-512
AES #5897	AES-ECB (H/W) FIPS 197	AES ECB mode encrypt/decrypt	256-bits key	A primitive used by XTS-AES-256
AES #5897	AES-XTS (H/W)* SP 800-38E	XTS-AES Enc/Dec	256-bits 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	4096 bits 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

The modules does not support any of the following:

- Non-Approved Algorithms Allowed in the Approved Mode of Operation
- Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed
- 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 FCM3 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 FCM3 Drive Brick

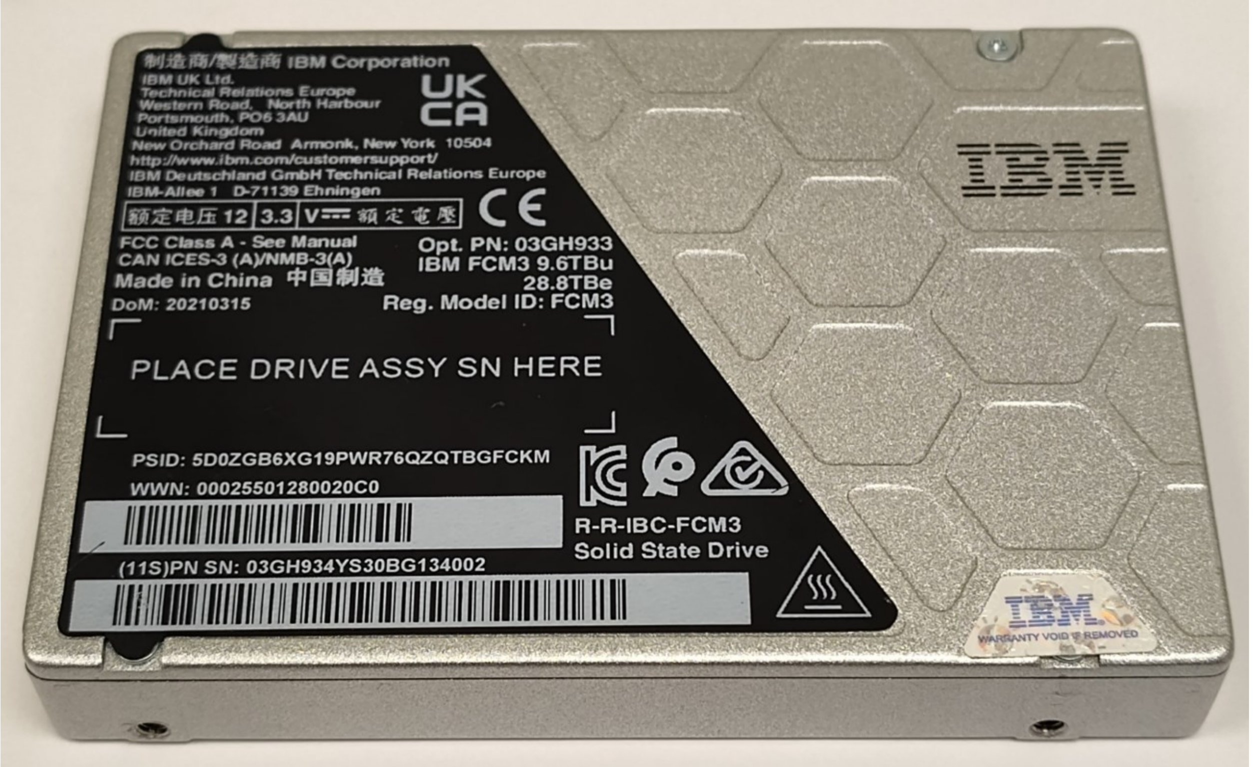
制造商/製造商 IBM Corporation
IBM UK Ltd.
Technical Relations Europe
Western Road, North Harbour
Portsmouth, PO6 3AU
United Kingdom
New Orchard Road Armonk, New York 10504
http://www.ibm.com/customersupport/
IBM Deutschland GmbH Technical Relations Europe
IBM-Allee 1 D-71139 Ehningen
UK CA
额定电压 12 3.3 V⎓ 額定電壓
CE
FCC Class A - See Manual
CAN ICES-3 (A)/NMB-3(A)
Made in China 中国制造
DoM: 20210315
Opt. PN: 03GH933
IBM FCM3 9.6TBu
28.8TBe
Reg. Model ID: FCM3
PLACE DRIVE ASSY SN HERE
PSID: 5D0ZGB6XG19PWR76QZQTBGFCKM
WWN: 00025501280020C0
(11S)PN SN: 03GH934YS30BG134002
R-R-IBC-FCM3
Solid State Drive
IBM
IBM
WARRANTY VOID IF REMOVED

Figure 2-1 FCM3 Top View

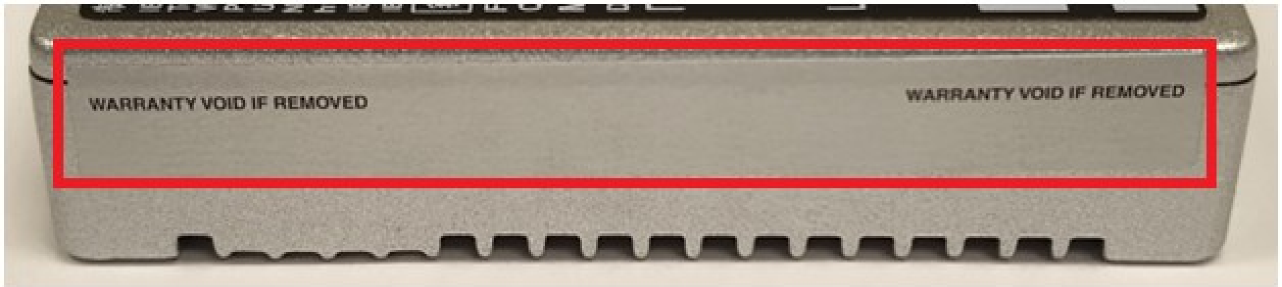

Figure 2-2 FCM3 Front View

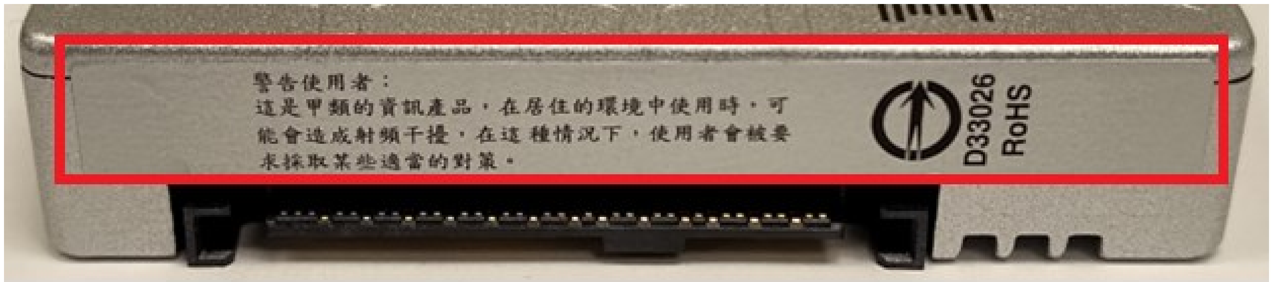
警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可
能會造成射頻干擾，在這 種情況下，使用者會被要
求採取某些適當的對策。
D33026
RoHS

Figure 2-3 FCM3 Back View

2.6 FCM3 Block Diagram

Edge connector is PCIe physically, NVMe logically

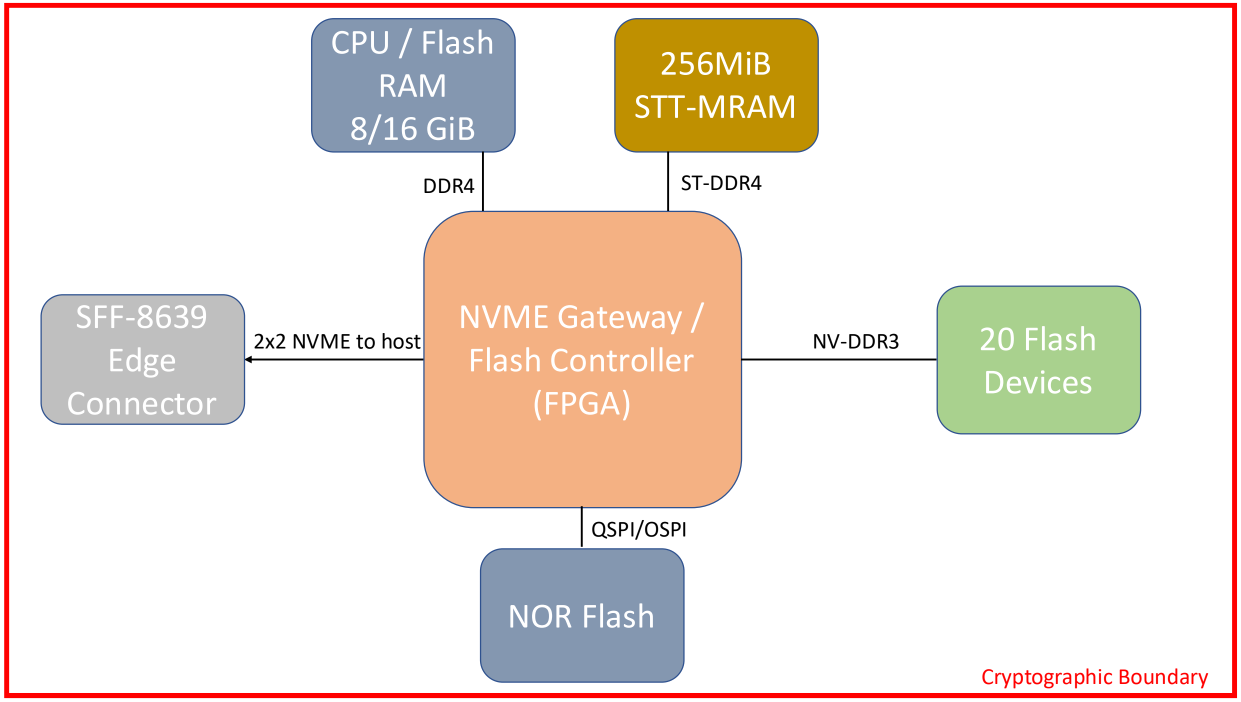

Figure 2-4 FCM3 Block Diagram

3 Cryptographic Module Interfaces

3.1 Logical to Physical Port Mapping

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

Table 3-1 Ports and Interfaces

Notes: * FCM3 has no control output interface.

4 Roles, Services, and Authentication

4.1 Crypto-Erase of User Data

Because all user data written to the FCM3 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 FCM3 supports the ability to "zeroize" all keys and CSPs, per the FIPS 140-3 key management requirement, the FCM3 supports the capability to "zeroize" any and all MEKs, which in turn crypto-erases all the user data encrypted with those MEKs. The FCM3 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 FCM3 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 FCM3 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.

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 FCM3 into an 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 FCM3 has to be reinitialized before it can return to 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 1.3 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 FCM3 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 1.3 References 5). This role is used to transition the FCM3 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 FCM3, and the FCM3 must have booted to that code level. If the FCM3 is not running FIPS code, it cannot be operating in Approved mode.

4.3.1.2 LockingSP Admin1-4

When in Approved mode, these roles' Authority corresponds to the LockingSP's Admin roles as defined in Opal SSC (see Section 1.3 References 5).

4.3.1.3 AdminSP Admin1

When in Approved mode, this role's Authority corresponds to the AdminSP's Admin1 role defined in Opal SSC (see Section 1.3 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 User Roles

4.3.2.1 LockingSP User2

When in Approved mode, this role's Authority corresponds to the LockingSP's User role as defined in Opal SSC (see Section 1.3 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

Anyone who has the ability to remove and then restore power to a FCM3 can cause a power cycle which will cause a reset of the FCM3, 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.

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

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 FCM3 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 and upon Revert via OFS, the FCM3 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 initiate a key establishment process by querying the RSA public key, generating one or two key encryption keys (KEKs) - two can take advantage of the dual port architecture, and encrypting it/them via RSA OAEP SHA2-256 method. FCM3 decrypts the message, checks the key encryption key and then both parties have agreement upon the KEK(s). Operators then authenticate with the FCM3 by providing a PIN. The PIN is AES key wrapped/unwrapped by the established KEK. 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 1.3 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. Neither the TryLimit nor the Persistence settings can be changed, both have their respective Writeable Flags permanently set to FALSE.

The PINs have a fixed length of 256 bits. Per the policy security rules, the FCM3 only allows programming of PINs that are of length 256 bits (see Section 11.1's Rule 7). This PIN length results in a probability of at most $1/2^{256}$ (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 FCM3 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 $1538/2^{256}$.

For PIN-based authentications (e.g., TCG SID, TCG Admins 1-4, etc.), they're considered as 'memorized secret' authentication mechanism as per SP 800-63B.

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 256 bits long. The Security Rules (see Section 11) for the FCM3 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 FCM3 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 operator access control, note the following:

- Use of the services described below is compliant only when the FCM3 is in Approved mode.
- Not shown are the security functions which underline 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.
- Some services such as User data read / write have indirect access control provided through enable, disable, lock, and unlock services used by an authenticated operator.
- 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
	Enable Secure Key Passing **	TCG vendor specific command	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	Reseat FCM3 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(s) 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.
** service is optional and has no impact. Secure key passing is enabled by default and cannot be disabled due to programmatic checks

Role	**Authentication Method**	**Authentication Strength**
Drive Owner (CO)	PIN (Memorized Secret) protected by AES key wrap (Single Factor Cryptographic Software)	1 in 2^256 per attempt, with a maximum of 1,538 attempts per minute. (Memorized Secret). 1 in 2^150 per attempt, with a maximum of 7.85 attempts per minute. (Single Factor Cryptographic Software).
AdminSP Admin1 (CO)	PIN (Memorized Secret) protected by AES key wrap (Single Factor Cryptographic Software)	1 in 2^256 per attempt, with a maximum of 1,538 attempts per minute. (Memorized Secret) 1 in 2^150 per attempt, with a maximum of 7.85 attempts per minute. (Single Factor Cryptographic Software)
LockingSP Admin1-4 (CO)	PIN (Memorized Secret) protected by AES key wrap (Single Factor Cryptographic Software)	1 in 2^256 per attempt, with a maximum of 1,538 attempts per minute. (Memorized Secret) 1 in 2^150 per attempt, with a maximum of 7.85 attempts per minute. (Single Factor Cryptographic Software)
LockingSP User2 (User)	PIN (Memorized Secret) protected by AES key wrap (Single Factor Cryptographic Software)	1 in 2^256 per attempt, with a maximum of 1,538 attempts per minute. (Memorized Secret) 1 in 2^150 per attempt, with a maximum of 7.85 attempts per minute. (Single Factor Cryptographic Software)

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-KWP;
		SHA2-256;
		AES-KWP KTS
			SID PIN;
			LockingSP Admin1-4 PINs;
				Drive Owner, AdminSP Admin1,	SID PIN	W	TCG set method returns GOOD

					LockingSP Admin1-4 PINs	W	

			AdminSP Admin1 PIN; LockingSP User2; PIN; KEKs; LBA Range Root Key	LockingSP Admin1-4/User1-8	AdminSP Admin1 PIN LockingSP User2 PIN KEK LBA Range Root Key	W W, E E E	
Activate SLR	Allocate a SUM Locking Range (SLR)	AES-KWP; SHA2-256; AES-KWP KTS	SID PIN; KEKs	Drive Owner	SID PIN KEK	W, E E	TCG activate method returns GOOD
Firmware load	Load firmware image. If the downloaded firmware image signature checks, then the FCM3 will boot to the new code at next reboot. 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.	RSA SigVer; SHA3-384	FW Verification Key	None *	E		New code boots on boot following firmware load
Enable / Disable AdminSP Admin	Enable / Disable the AdminSP Admin1	AES-KWP; SHA2-256; AES-KWP KTS	SID PIN KEKs	Drive Owner	SID PIN KEK	W, E E	TCG set method returns GOOD
Enable / Disable LockingSP Admin(s)	Enable / Disable a LockingSP Admin	AES-KWP; SHA2-256; AES-KWP KTS	LockingSP Admin1-4 PINs; KEKs	LockingSP Admin1- 4	LockingSP Admin1-4 PINs KEK	W, E E	TCG set method returns GOOD
Set Geometry	Set the starting LBA and size of the SLR.	AES-KWP; SHA2-256; AES-KWP KTS	LockingSP User2 PIN; KEKs	LockingSP User2	LockingSP User2 PIN KEK	W, E E	TCG set method returns GOOD
Lock / Unlock SLR for Rd/Wr	Block or allow read (decrypt) / write (encrypt) of user data in a range.	AES-KWP; SHA2-256; AES-KWP KTS	LockingSP User2 PIN; KEKs; LBA Range Root Key	LockingSP User2	LockingSP User2 PIN KEK;	W, E E;	TCG set method returns GOOD

					LBA Range Root Key	E	
User Data Read / Write	Encryption/decryption of user data to/from a SLR. Access control to this service is provided through Lock/Unlock SLR for Rd/Wr	AES-XTS	LBA Range MEKs	None	E		NVMe read/write command returns GOOD
Crypto-Erase of SLR	Erase user data in a SUM Locking range by changing its associated MEK	CKG; AES-KWP; SHA2-256; AES-KWP KTS	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	Locking SP User2 PIN	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: FCM3 will enter unestablished state.	CKG; AES-KWP; SHA2-256; AES-KWP KTS	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;	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	

			DRBG V;		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	
				LockingSP 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). This maps to the 'Performs Self-Tests' mandatory service.	RSA SigVer;
		RSA KeyGen
			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	
Reset Module	Runs all POSTs and zeroizes keys & CSPs in RAM. This maps to the 'Perform zeroization' mandatory service.	None	None	None	All SSPs	Z	Factory Reset
FIPSmode?	Reports whether, from a drive perspective, the drive is in Approved mode. This corresponds to	None	None	None	N/A		NVMe Identify: Controller Identify, bytes 3600-3607 (set to "FIPSmode")

	the Show Status mandatory service.						
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	Report code version. This maps to the Show Module’s Versioning Information mandatory service.	None	None	None	N/A		NVMe Identify: Controller Identify, bytes 64-71

DRBG Generate Bytes	Returns a SP800-90Ar1 DRBG Random Number of # of bytes requested up to 50	DRBG	DRBG EI;
			DRBG Seed;
			DRBG C;
			DRBG V;
				None	DRBG EI	G, E	TCG Random() method returns GOOD

					DRBG Seed	G, E	
					DRBG C	G, E	
					DRBG V	G, E	
Enable Secure Key Passing (SKP)	Enable secure key passing	SHA2-256	SID PIN	Drive Owner	E		TCG skp enable() method returns GOOD

KEK(s) setup	Establish KEK(s) during startup	KTS-IFC	KEKs;
			RSA public key;
			RSA private 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

The module's approved integrity technique is RSA SigVer FIPS 186-4 with 4096-bit modulus and SHA3-384 (vendor affirmed), conducted on the module’s executable code which is in the form of a pre-compiled firmware binary image. FCM3 firmware image has an 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 puts the card in an error state when it fails.

The firmware integrity test can be performed on-demand by the operator by power-cycling the module or by invoking the NSSR command via the ‘Reset Module’ service.

6 Operational Environment

The FCM3 operates in a “limited operational environment”. Specifically, the operational environment cannot be modified while the FCM3 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 FCM3 will boot to it following the next cold boot and so will begin operating with the new firmware image.

Per the FIPS 140-3 CMVP Management Manual section 'Partial validations and non-applicable areas', the following statement applies: "Section 6.6, Operational Environment may be designated as Not Applicable if the operational environment for the cryptographic module is a limited or non-modifiable operational environment and Section 6.7, Physical Security greater than Security Level 1.”

The module has a limited operational environment and is being validated at physical security level 2. As such, this section of FIPS 140-3 requirements is not applicable.

7 Physical Security

7.1 Mechanisms

The FCM3 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 7-3 Tampered TEL1 for placement of TEL1 and Figure 7-4 Tampered TEL2 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 3 Assembly cover removal for access to or visibility of the solid-state memory.
4. Exterior of the FCM3 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 FCM3 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.
- FCM3 assembly lid does not sit evenly or looks deformed.

If evidence of tampering is apparent, the operator must assume the FCM3 has been compromised and so should decommission that FCM3. At a minimum the operator must discontinue using that FCM3 in any way that relies on that FCM3's cryptographic capabilities. Once tampering of a TEL has been detected, the FCM3 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 Warranty Label

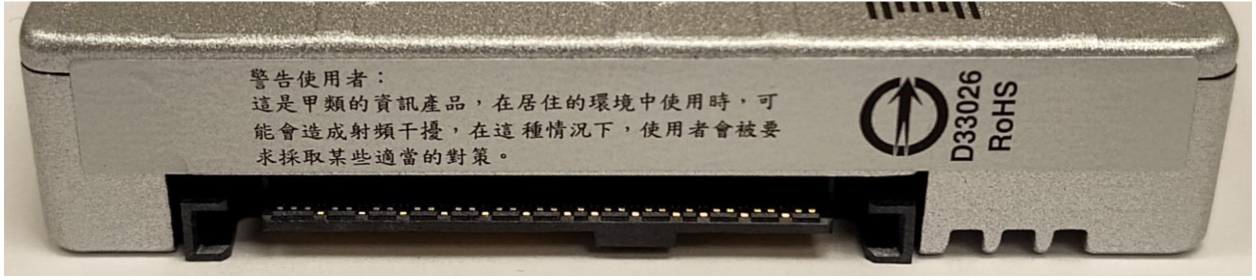
警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可
能會造成射頻干擾，在這 種情況下，使用者會被要
求採取某些適當的對策。
D33026
RoHS

Figure 7-1 TEL1 BSMI Label

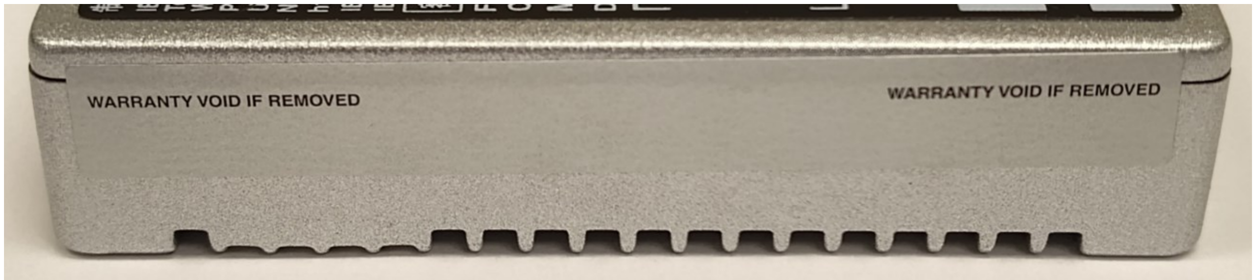

Figure 7-2 TEL2 BSMI Label

7.2 Tamper Evidence

To provide tamper-evidence of FlashCore Module 3 Assembly cover removal:

7.2.1 Figure 2 – Tampered TEL1

Showing tamper-evidence on TEL1

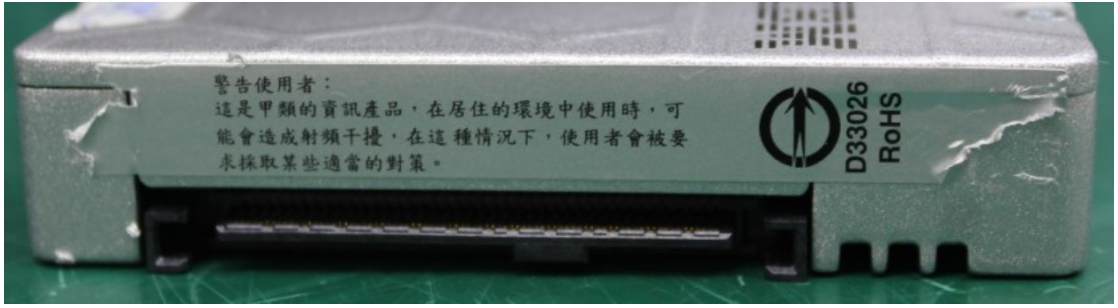
警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可
能會造成射頻干擾，在這種情況下，使用者會被要
求採取某些適當的對策。
D33026
RoHS

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

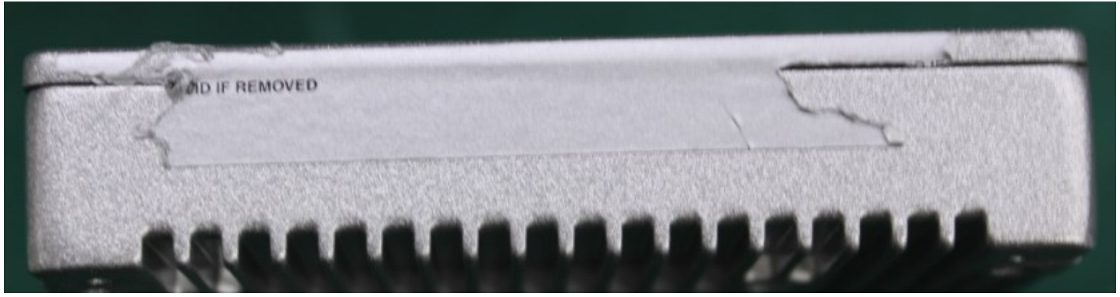

Figure 7-4 Tampered TEL2

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

8 Non-invasive Security

The FCM3 does not claim 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 FCM3 and to which there is no logical or physical access from outside of the FCM3.
- The FCM3 uses a SP 800-90Ar1 DRBG and adopts the Hash_DRBG mechanism.
- Non-critical security parameters are not shown in this table.
- There is no audit feature supported which is security-relevant.
- The module implements a manual distribution using an electronic entry mechanism for SSP input and output per IG 9.5.A.

Key/SSP Name/Type	**Strength**	**Security Function and Cert. Number**	**Generation**	**Import/Export**	**Establishment**	**Storage**	**Zeroisation**	**Use & related keys**
SID PIN	256 bits size / 256 bits strength	SHA2-256 #A6888, AES-KW #A6888, AES-KWP KTS #A6888	Set by operator	Import Encrypted via AES-KWP KTS	N/A	Non-volatile, hashed via SHA2-256	Revert via OFS	Use to authenticate as Drive Owner
						RAM, Plaintext RAM, encrypted via AES-KWP if SKP enabled	After authentication service	
LockingSP Admin1-4 PINs	256 bits size / 256 bits strength	SHA2-256 #A6888, AES-KW #A6888, AES-KWP KTS #A6888	Set by operator	Import Encrypted via AES-KWP KTS	N/A	Non-volatile, hashed via SHA2-256	Revert via OFS	Use to authenticate as a LockingSP Admin
						RAM, Plaintext RAM, encrypted via AES-KWP if SKP enabled	After authentication service	
AdminSP Admin1 PIN	256 bits size / 256 bits strength	SHA2-256 #A6888, AES-KW	Set by operator	Import Encrypted via AES-KWP KTS	N/A	Non-volatile, hashed via SHA2-256	Revert via OFS	Use to authenticate as AdminSP Admin1

		#A6888, AES-KWP KTS #A6888				RAM, Plaintext RAM, encrypted via AES-KWP if SKP enabled	After authentication service	
LockingSP User2 PIN	256 bits size / 256 bits strength	SHA2-256 #A6888, AES-KW #A6888, AES-KWP KTS #A6888	Set by operator	Import Encrypted via AES-KWP KTS	N/A	Non-volatile, hashed via SHA2-256	Revert via OFS	Use to authenticate as a LockingSP User. Used to encrypt the LBA Range Root Key in storage
						RAM, Plaintext RAM, encrypted via AES-KWP if SKP enabled	After authentication service	
LBA Range Root Key	256 bits size / 256 bits strength	KDF SP800-108 #A6888	Generated from DRBG	N/A	N/A	Non-volatile, encrypted via AES-KW	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,
		AES-XTS #A2687
			These 2 keys are derived from the LBA range root key using the approved SP800-108rev1 KDF	N/A	N/A	CPU RAM, plaintext	Revert via OFS;
							Crypto-Erase of SLR;
							Auto-zeroized after use
								Use in Encrypt / Decrypt User Data

DRBG EI	1024 bits (03GH934 and 03GH936)	Hash DRBG #A6888	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

	592 bits (03GH932 and 03GH930)							
DRBG Seed	1024 bits (03GH934 and 03GH936)*	Hash DRBG #A6888	Generated using the module's ENT (P)	N/A	N/A	CPU RAM, plaintext	Power On; Auto -zeroized after use	Use in services which use the DRBG
	592 bits (03GH932 and 03GH930)							

DRBG C	DRBG intermediate values C (888 bits each)	Hash DRBG #A6888	Generated using the module's ENT (P)	N/A	N/A	CPU RAM, plaintext	Revert via OFS; Power On	Use in services which use the DRBG
DRBG V	DRBG intermediate values V (888 bits each)	Hash DRBG #A6888	Generated using the module's ENT (P)	N/A	N/A	CPU RAM, plaintext	Revert via OFS; Power On	Use in services which use the DRBG
FW Verification Key**	4096 bits size / 152 bits strength	RSA SigVer (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	KTS-IFC	RSA KeyGen (FIPS186-4) #A6888	N/A	N/A	CPU RAM, plaintext	Revert via OFS; Power On	Use in KEKs establishment
RSA public key	3072 bits size / 128 bits strength	KTS-IFC	RSA KeyGen (FIPS186-4) #A6888	Exported in plaintext	N/A	CPU RAM, plaintext	Revert via OFS; Power On	Use in KEKs establishment
KEKs	256 bits size / 256 bits strength	AES-KWP #A6888, AES-KWP KTS #A6888	N/A	Import Encrypted via KTS-IFC	N/A	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.800-90Ar1.pdf; Table 2, seedlen

****** Please note that the 'FW Verification Key' is not considered an SSP per ISO/IEC section 7.5 and is only included in the table for completeness.

RBG entropy source:

Entropy sources	Minimum number of bits of entropy	Details
Hardware ring oscillator	1024 bits (03GH934 and 03GH936)	The entropy source provides 128-bits of entropy per 128-bits of output from the AES-CBC-MAC vetted conditioner (CAVP Cert. #A6888) for the 03GH934 and 03GH936 modules. The entropy source provides 74-bits of entropy per 128-bits of output from the AES-CBC-MAC vetted conditioner for the 03GH932 and 03GH930 modules. Due to oversampling and conditioning the module's DRBG is seeded with 1024 bits of entropy data, which is enough to support its maximum security strength.
	592 bits (03GH932 and 03GH930)	

Table 9-2 Non-Deterministic Random Number Generation Specification

9.2 Temporary CSPs

No matter the FCM3 is in Approved mode or non-Approved mode, all the temporary keys and CSPs are zeroized when they are no longer needed.

10 Self-tests

10.1 Self-Tests

A firmware integrity check (Pre-operational firmware integrity test) is performed as part of the power on process using the same SHA3-384/RSA-4096 digital signature. The CPU cores are not allowed to run until and unless the firmware integrity check is run successfully. All the self-tests mentioned in this section can be performed on-demand by the operator by power-cycling the module or by invoking the NSSR command via the 'Reset Module' service.

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-KW-WRAP	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
AES-256-KW-UNWRAP	CAST	Decrypt KAT performed	Enters FIPS Self-Test Fail State
AES-256-KWP-WRAP	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
AES-256-KWP-UNWRAP	CAST	Decrypt KAT performed	Enters FIPS Self-Test Fail State
Hash DRBG (SHA-512)	CAST	DRBG KAT performed	Enters FIPS Self-Test Fail State
HMAC-SHA2-256	CAST	HMAC KAT performed	Enters FIPS Self-Test Fail State
ECB-AES-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
AES-ECB-256 (H/W)	CAST	Encrypt performed	Enters FIPS Self-Test Fail State

AES-ECB-256 (H/W)	CAST	Decrypt performed	Enters FIPS Self-Test Fail State
XTS-AES-256 (H/W)	CAST	Encrypt KAT performed	Enters FIPS Self-Test Fail State
SP 800-108rev1 KDF with HMAC-SHA2-256	CAST	KDF KAT performed	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
KTS-OAEP 3072 with SHA2-256	CAST	RSA decrypt KAT performed	Enters FIPS Self-Test Fail State
RSA pair-wise consistency (3072 bit modulus)	Conditional pair-wise 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
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

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

SP 800-90Ar1 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 800-90Ar1 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).

A firmware download test which checks the authenticity of the firmware download, is performed on any attempted firmware update to the FCM3. If the SHA3-384/RSA-4096 digital signature of the firmware update does not check, the firmware download is aborted.

11 Life-cycle assurance

11.1 Establishing Approved mode and exit conditions

The FCM3 does not typically change mode across power cycles and resets. However, certain operations can result in the FCM3 exiting Approved mode. In some of these situations (e.g. failure of the Power On Self Test), the FCM3 cannot be restored to Approved mode and in that case could not provide any further FIPS 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 FCM3 in a FIPS 140-3 Approved manner. 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 FCM3'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: Up to two key encryption keys (KEK(s)) need 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 FCM3 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 FCM3 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 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 these 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 initialization is complete, do a power-on reset to clear authentications established during initialization.
12. Users: Do a GenKey of each SLR's Media Encryption Key (MEK)
13. Cryptographic Officers: Verify that the FCM3 indicates it is running "FIPSmodeNoErrors".

If all of these steps are followed correctly, the FCM3 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 instructions 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

The FCM3 does not claim to mitigate against any other attacks relevant to FIPS 140-3 validation.

- End --