IBM® NVMe FlashCore™ Module
FIPS 140-2 Non-proprietary Security Policy
Security Level 1

Rev. 1.1 – March 4, 2019
IBM Corporation

Table of Contents

1 Introduction

1.1 Scope

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

This document is designed to meet the FIPS 140-2 standard (Appendix C) and Implementation Guidance (section 14.1) 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

Requirement Area	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	2*
Finite State Model	1
Physical Security	2**
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interface / Electromagnetic Compatibility (EMI / EMC)	1
Self – Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

* by use of TCG Opal commands

** Level 2 because of the FCM's Tamper Evident Labels (TELs)

1.3 References

1. FIPS PUB 140-2, issued May 25, 2001
2. Derived Test Requirements for FIPS PUB 140-2, issued Jan. 4, 2011
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, last updated May 25, 2018
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

1.4 Acronyms used in this document

AdminSP	Administrative security partition, a TCG term
AES	Advanced Encryption Standard (FIPS 197)
CBC	Cipher Block Chaining, an encryption mode
CO	Crypto-Officer
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
FCM	FlashCore Module
LBA	Logical Block Address
KAT	Known Answer Test
LockingSP	Locking Range security partition, a TCG term
MEK	Media Encryption Key
MSID	Manufactured SID, TCG term for a unique per FCM public value used as the default PIN
POST	Power on Self-Test
PSID	Physical SID, TCG term for a unique per FM value public value
SID	Security ID, TCG term for Drive Owner CO role's PIN
SLR	SUM Locking Range
SP	Security Policy (per FIPS 140-2)
SUM	Single User Mode
XTS	XEX-based tweaked-codebook mode with ciphertext stealing, an encryption mode

2 Cryptographic Module Description

2.1 Overview

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

The FCM is a multiple-chip embedded cryptographic module implementation. The outside surfaces of the FlashCore Module 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 FCM is physically a PCIe connector, over which the industry-standard NVMe protocol [8] is supported. Through the NVMe logical interface the FCM supports the TCG SWG Core [4] and TCG Opal SSC [5] protocols. All control of the FCM via its interfaces is typically through an application on a host system. All human control of an FCM is assumed to be through such an application.

The primary cryptographic service supported by the FCM is encryption of user data at rest: encrypting user data written to the FCM before the resultant ciphertext is written to the FCM's non-volatile solid-state memory. The FCM 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 FCM supports: cryptographic erase, which nearly instantly renders all previously encrypted user data to be effectively destroyed. The FCM supports TCG Opal access controls, which restrict access to use of, and administration of, the encryption and cryptographic erase services.

2.2 Logical to Physical Port Mapping

FIPS 140-2 Interface	Module Ports
Data In	NVMe connector
Data Out	NVMe connector
Control Input	NVMe connector
Status Output	NVMe connector
Power Input	NVMe connector

2.3 Hardware and Firmware Versions

The following FCM configurations have been validated:

Native Capacity	Hardware Part #	Firmware Version
19.2 TB	01EK231	1.3.0.91
9.6 TB	01EK232	1.3.0.91
4.8 TB	01EK233	1.3.0.91

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.

2.4 FIPS Approved and Allowed Algorithms

Algorithm (implementation in)	Certificate #	Associated Standard	Usage
AES-KEY-WRAP (F/W)*	AES #5898	SP 800-38F	Only used as part of self-test at POST
AES-KEY-UNWRAP (F/W)*	AES #5898	SP 800-38F	Only used as part of self-test at POST
XTS-AES-256 Encrypt (F/W)**	AES #5898	SP 800-38E	To check XTS-AES-256 Encrypt in H/W
AES-256 (F/W)	AES #5898	FIPS 197	A primitive used by XTS-AES-256 Encrypt, and by AES key wrap & unwrap
CBC-AES-128 (F/W)	AES #5898	SP 800-38A	Whitening performed as part of entropy processing
CKG (F/W)	Vendor Affirmed *5	SP 800-133	Cryptographic Key Generation
NDRNG (H/W)	Allowed	SP 800-90B	Seeding the DRBG
DRBG-SHA-512 (F/W)	DRBG #2454	SP 800-90A	Random number generation
SHA2-512 (F/W)	SHA #4648	FIPS 180-4	A primitive used by DRBG-SHA-512
KDF	KBKDF #244	SP 800-108	Key derivation
HMAC-SHA-256 (F/W)	HMAC #3872	FIPS 198-1	A primitive used by the KDF
SHA2-256 (F/W)	SHA #4648	FIPS 180-4	Hash of PINs used to authenticate, as well as a primitive used by HMAC-SHA-256
XTS-AES-256 Encrypt/Decrypt (H/W)**	AES #5897	SP 800-38E	User Data written by a host application is encrypted; decryption is performed on read
AES-256 (H/W)	AES #5897	FIPS 197	A primitive used by XTS-AES-256
SHA3-384 (H/W)	SHA-3 #62	FIPS 202	As part of verification of a code load's digital signature (4 byte aligned only *3)
RSA-4096 (H/W)	Vendor Affirmed *4	FIPS 186-4	As part of verification of a code load's digital signature

* No claim of any service or cryptographic protection associated with use of AES Key Wrap and Unwrap is made

** XTS-AES-256 is only used by the FCM in the context of storage applications

*3 Only 4-byte aligned inputs are supported, so only 4-byte aligned inputs were verified by CAVP

*4 In accordance with FIPS 140-2 IG A.11, the cryptographic module performs digital signature checking using SHA3-384 as specified in FIPS PUB 202 (Vendor Affirmed)

*5 In accordance with FIPS 140-2 IG D.12, the cryptographic module performs cryptographic key generation per SP 800-133 (Vendor Affirmed)

2.5 Self-Tests

Function Tested	Self-Test	KAT Implementation	If this KAT test fails
SHA2-256	Power-On	Hash KAT performed	Enters FIPS Self-Test Fail State
AES-KEY-WRAP	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
AES-KEY-UNWRAP	Power-On	Decrypt KAT performed	Enters FIPS Self-Test Fail State
DRBG (SHA-512)	Power-On	DRBG KAT performed	Enters FIPS Self-Test Fail State
HMAC-SHA-256	Power-On	HMAC KAT performed	Enters FIPS Self-Test Fail State
AES-256	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
XTS-AES-256	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
CBC-AES-128	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
SHA3-384 (H/W)	Power-On	Digest KAT performed	Enters FIPS Self-Test Fail State
RSA-4096 (H/W)	Power-On	Verify KAT performed	Enters FIPS Self-Test Fail State
AES-256 (H/W)	Power-On	Encrypt/Decrypt performed	Enters FIPS Self-Test Fail State
XTS-AES-256 (H/W)	Power-On	Encrypt KAT performed	Enters FIPS Self-Test Fail State
SP 800-108 KDF	Power-On	KDF KAT performed	Enters FIPS Self-Test Fail State
XTS Key1 != XTS Key 2	Conditional*	Not a KAT	Enters FIPS Self-Test Fail State

* This check is made each time a Root Key is expanded, by two key derivations, into XTS's Key1 and Key2.
The Non-Approved but Allowed Non-Deterministic Random Number Generator (NDRNG) is continuously tested by a Repetition Count Test (RCT).

A new SP 800-90A 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 800-90A instantiation to assure it is sound before it is used. The DRBG is then used to generate a random number by processing NDRNG 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 FCM. If the SHA3-384/RSA-4096 digital signature of the firmware update does not check, the firmware download is aborted.

A firmware integrity check 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.

2.6 FIPS 140-2 Approved Mode of Operation

The FCM will operate in a non-FIPS mode until the Secure Initialization steps detailed in Section 7.1 are performed. Before FIPS mode is established, the FCM is in, what will be called here, an "unestablished state".

From this non-FIPS mode, the FCM may be securely initialized so that it operates in FIPS 140-2 Mode of operation (hereafter "FIPS Mode"). After the FCM has been Securely Initialized and operated per the Security Rules detailed in Section 7.1, the FCM will remain in FIPS 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 FCM can use the "FIPSmode?" service, if it does not return the expected status (see Section 4.1), then the FCM is not operating in FIPS mode.

An operator can cause an FCM operating in FIPS Mode to quit FIPS Mode by use of the FCM's "Revert via OFS" service. This service will zeroize the FCM's keys and CSPs and transition it through its Original Factory State

(OFS) to its unestablished state. The operator can then cause that FCM to return to FIPS Mode by following the Secure Initialization procedure detailed in Section 7.1 again.

To operate the FCM is in its FIPS Mode, it must be configured properly and it must be operated in accordance with the associated policy restrictions (detailed in Section 7.2). Violating the ongoing policy restrictions would mean that the FCM is no longer being operated in its FIPS Mode of operation.

2.6.1 FIPS mode

When operated in this mode the FCM 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 FIPS mode, the Drive Owner must invoke the Activate method on the LockingSP starting from an unestablished state which itself must start afresh from an OFS state.

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

Similarly, Keys and CSPs established in non-FIPS mode cannot be used in FIPS mode. If an FCM had been previously operated with a non-FIPS code load, a Locking Range may have been established, though that FCM would not have been in FIPS 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 FIPS mode. If the code on that FCM is then updated to the FIPS code load, then the FCM 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 FIPS mode if all requirements are met.

The FCM 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.

2.6.2 SUM Locking Ranges (SLRs)

When invoking the Activate method to enter FIPS mode, the Drive Owner creates a Locking Range (LR). All LRs created within the FCM must be of the Single User Mode (SUM) type. The FCM 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 FCM will be, and will remain, "SUM Locking Ranges" (SLRs). SLRs conform to the SUM feature set [7]. Each SLR is controlled and administered solely by the single User role it is associated with per [5] and [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 FIPS mode, this cooperative operation includes:

1. Creating one or more SLRs (by the Drive Owner)
   - the FCM 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))

2.7 Crypto-Erase of User Data

Because all user data written to the FCM 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 FCM supports the ability to "zeroize" all keys and CSPs, per the FIPS 140-2 key management requirement, the FCM supports the capability to "zeroize" any and all MEKs, which in turn crypto-erases all the user data encrypted with those MEKs. The FCM supports the capability to zeroize any and all MEKs whether it is in FIPS Mode or not.

It should be noted that user data stored to the FCM 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 FCM 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 2.8).

2.8 Revert via OFS

Whether in FIPS mode or not, the TCG Revert and RevertSP methods may be invoked by an appropriately authenticated Role to put the FCM into an unestablished state (non-Approved) mode. 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 FCM has to be reinitialized before it can return to a FIPS 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 [6].

3 Identification and Authentication Policies

3.1 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 FCM is in FIPS mode, see section 4.1.

3.1.1 Cryptographic Officer (CO) Roles

3.1.1.1 Drive Owner

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

3.1.1.2 Admins (1-4) in LockingSP

When in FIPS mode, these roles' Authority corresponds to the LockingSP's Admin roles as defined in Opal SSC [5].

3.1.1.3 Admin1 in AdminSP

When in FIPS mode, this role's Authority corresponds to the AdminSP's Admin1 role defined in Opal SSC [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.

3.1.2 Users (1 – 8) in LockingSP

When in FIPS mode, these roles' Authority corresponds to the LockingSP's User roles as defined in Opal SSC [5]. These roles can unlock (and also lock) the corresponding SLR in the FCM, 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.

When operating in FIPS Mode, there can be up to 8 separate Users (User IDs) and the role corresponds to the same named TCG Authority on the LockingSP. Because SUM assigns a single fixed User to a given SLR, the three SLRs supported are all associating with a given User. Because the FCM only supports three SLRs, only the three associated Users (2-4) can actually be used at present.

3.1.3 Unauthenticated Role

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

3.2 Authentication

3.2.1 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.

3.2.2 Authentication in FIPS 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 FCM 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.

3.2.3 Authentication Mechanism, Data and Strength

Operators authenticate with the FCM by providing a PIN. The provided PIN is hashed and compared to the hash non-volatilely stored when that PIN was established. Per the TCG SWG Core [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 and Persistence settings are 0 (which specifies unlimited retries) and FALSE (which means that any count of incorrect authentications will be reset on reboot), respectively. Neither the TryLimit nor the Persistence settings can be changed, both have their respective Writeable Flags permanently set to FALSE.

The PINs have a maximum length of 32 bytes. Per the policy security rules, the FCM only allows programming of PINs that are of length 8 bytes or longer (see Section 7.1's Rule 4). This PIN length results in a probability of at most $1/2^{64}$ (i.e. less than 10^{-19}) for the PIN to be guessed in a single random attempt. This far exceeds the FIPS 140-2 authentication strength requirements of less than $1/10^{6}$ (= 10^{-6}).

Each authentication attempt requires 39ms on average for the FCM 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 about $1538/2^{64} = 8 \times 10^{-17}$ which far exceeds the FIPS requirement of $1/10^{5}$ (= 10^{-5}).

3.2.4 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 32 ASCII characters long. The Security Rules (Section 7) for the FCM 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 Access Control Policy

4.1 FIPS 140-2 Services

The following tables details the FIPS 140-2 services the FCM provides when in FIPS 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 FCM is in FIPS mode.
- Not shown are the security functions which underlie the higher-level algorithms shown below (e.g. DRBG-SHA-512 as part of NDRBG)
- 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.

Table 2.1 - FIPS 140-2 Authenticated Services – FIPS mode				
Service Name	**Description**	**Operator Access Control**	**Security Function**	**Command(s)/Event(s)**
Set PIN	Change operator authentication data.	AdminSP Admin1, LockingSP Admin1- 4, User1-8, Drive Owner	SHA2-256 Hashing	TCG Set Method
Activate SLR	Allocate a SUM Locking Range (SLR)	Drive Owner	SHA2-256 Hashing	TCG Activate Method
Firmware Download	Load firmware image. If the downloaded firmware image signature checks, then the FCM will boot to the new code at next reboot	None	Digital Signature (RSA 4096 with SHA3-384) Check	NVMe Firmware Image Download
Enable / Disable AdminSP Admin	Enable / Disable the AdminSP Admin1	Drive Owner	None	TCG Set Method
Enable / Disable LockingSP Admin(s)	Enable / Disable a LockingSP Admin	LockingSP Admin1- 4	None	TCG Set Method
Set Geometry	Set the starting LBA and size of the SLR.	User1-8 (if User Ownership (Policy 0))	None	TCG Set Method
Lock / Unlock SLR for Rd/Wr	Block or allow read (decrypt) / write (encrypt) of user data in a range.	User1-8 (only one of these users is authorized for each LR created, per SUM restrictions)	Key Derivation Function (KDF)	TCG Set Method
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	None	XTS-AES-256 Decryption/ Encryption (Symmetric Key)	NVMe Read / Write Commands
Crypto-Erase of SLR	Erase user data in a SUM Locking range by changing its associated MEK	LockingSP Admin1- 4	DRBG, Symmetric Key	TCG Erase Method
		LockingSP User1-8		TCG GenKey Method, TCG Erase Method
Revert via OFS	Exit FIPS mode. Note: FCM will enter unestablished state.	Drive Owner	DRBG, Hashing, Symmetric Key	TCG LockingSPObj.Revert(), TCG AdminSPObj.Revert()
		AdminSP Admin1		TCG AdminSPObj.Revert()
		LockingSP Admin1- 4		TCG LockingSP.RevertSP()

Table 2.2 - FIPS 140-2 Unauthenticated Services – FIPS mode				
Service Name	**Description**	**Operator Authentication Required**	**Security Function**	**Command(s)/Event(s)**
Cold Boot	Firmware integrity check on boot	None	RSA-4096/ SHA3-384 signature	Power On Reset
Unblock PIN	Resets password attempt counters	None	None	Power On Reset
Reset Module	Runs all POSTs and zeroizes keys & CSPs in RAM	None	None	Power On Reset, NVMe reset (NSSR)
FIPSmode?	Reports whether, from a drive perspective, the drive is in FIPS mode	None	None	NVMe Identify: Controller Identify, bytes 3600-3607 (set to “FIPSmode”?)
FIPScode?	Reports whether the code level in operation was FIPS validated	None	None	NVMe Identify: Controller Identify, bytes 3616-3623 (set to “FIPScode”?)
DRBG Generate Bytes	Returns a SP800-90A DRBG Random Number of # of bytes requested up to 50	None	DRBG	TCG Random()
Revert via OFS	Exit FIPS mode. Note: FCM will enter unestablished state.	None (e.g. by use of PSID)	DRBG, Hashing, Symmetric Key	AdminSP.RevertSP(), AdminSPObj.Revert()

4.2 Non-FIPS Mode Services

In the unestablished state, the FCM supports the following services:

1. The ability to transition the FCM to FIPS Mode of operation
2. The ability to update firmware
3. The ability to crypto-erase user data
4. The ability to reset the FCM via NVMe Reset (NSSR) or Power On Reset
5. The ability to report status.

All cryptographic algorithms used in FIPS Mode of operation are also available in this security unestablished state.

4.3 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
- The Set PIN service is shown in this table though it is generally only used at FCM setup
- All non-volatile storage of keys and CSPs is internal to the FCM and to which there is no logical or physical access from outside of the FCM
- The FCM uses a SP 800-90A DRBG and adopts the Hash_DRBG mechanism
- Non-critical security parameters are not shown in this table
- Read access of private values is kept internal to the FCM and so are not represented in this table.
- There is no audit feature supported which is security-relevant.

Table 3 - Key Management					
Name	**Description / Non-volatile Storage**	**Type (Pub / Priv, key / CSP (e.g. PIN)), size**	**Operator Role**	**Services Used In**	**How accessed**
SID (Security Identifier), a.k.a. Drive Owner PIN	Auth. Data / Hash	Secret, PIN, 32 bytes	Drive Owner	Set PIN, Activate SLR, Enabl / Disbl AdminSP Admin(s), Revert via OFS	Entered into FCM (in plaintext)
LockingSP Admin1-4 Passwords	LockingSP Admins Auth. Data / Hash	Secret, PIN, 32 bytes	LockingSP Admins	Set PIN, Enabl / Disbl LockingSP Admin(s), Crypto-erase of SLR, Revert via OFS	Entered into FCM (in plaintext)
AdminSP Admin1 Passwords	AdminSP Admin Auth. Data / Hash	Secret, PIN, 32 bytes	AdminSP Admin	Set PIN, Revert via OFS	Entered into FCM (in plaintext)
User1-8 Passwords	Users Auth. Data / Hash	Secret, PIN, 32 bytes	LockingSP User	Set PIN, Set Geometry, Lock/Unlock SLR for Rd/Wr	Entered into FCM (in plaintext)
LBA Range Root Key (unmodified DRBG Output)	Root Key / Obfuscated	Secret, AES Key, 256 bits	LockingSP Admins, Users	Encrypt / Decrypt User Data	Use allowed during Execution only
LBA Range MEKs (each 'MEK' is comprised of two 256-bit keys)	Media Encryption Key / No*	Secret, 2 AES keys, 2 x 256 bits	LockingSP Admins, Users	Encrypt / Decrypt User Data	Use allowed during Execution only
DRBG Entropy Input String	String of bits that contains entropy, input to a SP 800-90A DRBG / No*	Private, 128 bytes (providing full entropy)	None	Services which use the DRBG (e.g. crypto-erase)	Use allowed during Execution only
DRBG Seed	String of bits that is used as input to a SP 800-90A DRBG / No*	Private, 888 bits**, seed	None	Services which use the DRBG (e.g. crypto-erase)	Use allowed during Execution only
DRBG Internal State	Collection of stored information about a SP	Private, DRBG intermediate values V and	None	Services which use the DRBG (e.g. crypto-erase)	Use allowed during Execution only

	800-90A DRBG / No*	C (888 bits each)			
FW Verification Key	Firmware Load Test Signature Verify Key / hardcoded in firmware	Public, RSA-4096 key, 4096 bits	None	FW Download	Use allowed during Execution only

* Not stored non-volatilely

** per https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf; Table 2, seedlen

5 Physical Security

5.1 Mechanisms

The FCM has the following physical security:

1. Built of production-grade components which have standard passivation
2. Four opaque tamper-evident labels (TELs) on the FCM. Two of the TELs are on the top (lid) of the FCM. Additionally there is one TEL on each the front and back of the FCM. 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 Assembly cover removal for access to or visibility of the solid-state memory
4. Exterior of the FCM 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

5.1.1 Figure 1 – TEL1 and TEL2

Figure shows TEL1 (black Agency Label) and TEL2 (blue Counterfeit Label)

5.1.2 Figure 2 – TEL3

Figure shows TEL3, the BSMI label

5.1.3 Figure 3 – TEL4

Figure shows TEL4, the Warrantee Label

5.2 TELs on ends of FCM

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

5.2.1 Figure 4 – tampered TEL1

Showing tamper-evidence on TEL1

Where the folding and general distress are seen, and the TEL's shape has been distorted.

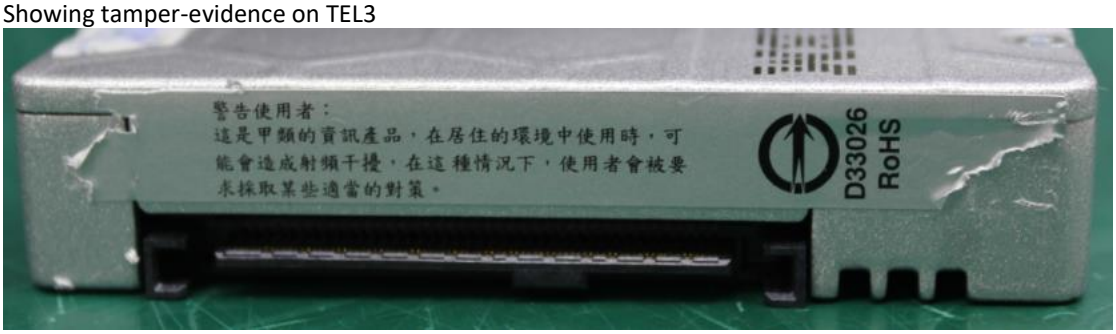
5.2.2 Figure 5 – tampered TEL2

Showing tamper-evidence on the holographic TEL2

Where the folding and general distress are seen, and the TEL's shape has been distorted.

5.2.3 Figure 6 – tampered TEL3

Showing tamper-evidence on TEL3



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

5.2.4 Figure 7 – tampered TEL4

Showing tamper evidence of TEL4

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

5.3 Operator Requirements

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

- Flaking, folding, or ripping of TELs or metal case
  - Figures 4 illustrates tamper evidence on TEL3
- 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
- General distress or discoloration of the TELs
  - Figures 5 illustrates tamper evidence on TEL4
- FCM assembly lid does not sit evenly or looks deformed

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

6 Operational Environment

The FCM operates in a "non-modifiable operational environment" and so the FIPS 140-2, Section 6, Operational Environment requirements do not apply. Specifically, the operational environment cannot be modified while the FCM 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 FCM will boot to it following the next cold boot and so will begin operating with the new firmware image.

7 Security Rules

7.1 Establishing FIPS mode and exit conditions

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

The following are the security rules for establishment and operation of the FCM in a FIPS 140-2 Approved manner. Further detail is available in the appropriate sections of this document.

1. Cryptographic Officer(s): 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 FCM'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: At installation, determine if the FCM 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.
5. Transition the FCM to FIPS mode: The Drive Owner invokes the Activate method for each SLR to be created
6. Cryptographic Officers and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 8 bytes length by use of FIPS mode: Drive Owner, Admins, and Users
7. Cryptographic Officers (specifically LockingSP Admins) to operate in FIPS 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.
8. Use the "FIPSmode?" service to assure the firmware sees itself as being in FIPS mode.
9. Drive Owner: At installation, disable the "Makers" authority by use of the TCG Set method.
10. After secure establishment is complete, do a power-on reset to clear authentications established during establishment.
11. Users: do a GenKey of each SLR's Media Encryption Key (MEK)

If all of these steps are followed correctly, the FCM will be in FIPS Mode of operation. It should be noted that all of the conditions detailed above must continue to be met to remain in FIPS mode.

7.2 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.

8 Mitigation of Other Attacks Policy

The FCM does not claim to mitigate against any other attacks relevant to FIPS 140-2 validation.