Seagate Secure®

TCG Enterprise SSC

Self-Encrypting Drive

Non-Proprietary FIPS 140-2 Module Security Policy

Security Level 2

Rev 0.12 – November 11, 2020

Seagate Technology, LLC

Table of Contents

Table of Figures

1 Introduction

1.1 Scope

This security policy applies to the FIPS 140-2 Cryptographic Module (CM) embedded in **Seagate Secure®** **TCG Enterprise SSC Self-Encrypting Drive** products.

This document meets the requirements of the FIPS 140-2 standard (Appendix C) and Implementation Guidance (section 14.1). It does not provide interface details needed to develop a compliant application.

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

Figure 1: Nytro 3000® SSD SAS Interface

1.2 Security Levels

FIPS 140-2 Requirement Area	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interface / Electromagnetic Compatibility (EMI / EMC)	3
Self – tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

The overall security level pursued for the cryptographic modules is Security Level 2.

1.3 References

1. FIPS PUB 140-2
2. Derived Test Requirements for FIPS PUB 140-2
3. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
4. TCG Storage Security Subsystem Class: Enterprise, Specification Version 1.0, Revision 3.00, January 10, 2011
5. TCG Storage Architecture Core Specification, Specification Version 1.0, Revision 0.9, May 24, 2007
6. TCG Storage Interface Interactions Specification, Specification Version 1.0,
7. SCSI Primary Commands-4 Rev 15 (SPC-4)
8. SCSI Block Commands Rev15 (SBC-3)
9. Serial Attached SCSI-2 Rev 13 (SAS-2)

1.4 Acronyms

AES	Advanced Encryption Standard (FIPS 197)
CBC	Cipher Block Chaining, an operational mode of AES
CM	Cryptographic Module
CMAC	Cipher-Based Message Authentication Code algorithm
CO	Crypto-officer
CSP	Critical Security Parameter
CSPSK	Critical Security Parameter Sanitization Key
DRBG	Deterministic Random Bit Generator
MEK	Media Encryption Key
HDD	Hard Disk Drive
HMAC	Hash Message Authentication Code
IV	Initialization Vector for encryption operation
KDF	Key Derivation Function
LBA	Logical Block Address
LED	Light Emitting Device
MSID	Manufactured SID, public drive-unique value that is used as default PIN, TCG term
NDRNG	Non-Deterministic Random Number Generator
POR	Power-on Reset (power cycle)
POST	Power on Self-Test
PSID	Physical SID, public drive-unique value
PSK	Pre-Shared Key
RNG	Random Number Generator
SED	Self-Encrypting Drive, Seagate HDD/SSD products that provide HW data encryption.
SID	Secure ID, PIN for Drive Owner CO role, TCG term
SoC	System-on-a-Chip
SP	Security Provider or Security Partition (TCG), also Security Policy (FIPS 140-2)
SSD	Solid State Drives
XTS	The XTS-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES)

2 Cryptographic Module Description

2.1 Overview

The Seagate Secure® TCG Enterprise SSC Self-Encrypting Drive FIPS 140-2 Module is embodied in Seagate Enterprise Performance SED model disk drives. These products meet the performance requirements of the most demanding Enterprise applications. The cryptographic module (CM) provides a wide range of cryptographic services using FIPS approved algorithms. Services include hardware-based data encryption (AES-XTS), instantaneous user data disposal with cryptographic erase, independently controlled and protected user data LBA bands and authenticated FW download. The services are provided through industry-standard TCG Enterprise SSC, SCSI protocols.

The CM, whose cryptographic boundary is the full drive enclosure, has a multiple-chip embedded physical embodiment. The physical interface to the CM is a SAS connector. The logical interfaces are the industry-standard SCSI (refer to Section1.3, items 7 & 8), TCG SWG (refer to Section1.3, item 5), and Enterprise (refer to Section1.3, item 4) protocols, carried on the SAS (refer to Section1.3, item 9) transport interface. The primary function of the module is to provide data encryption, access control and cryptographic erase of the data stored on the flash drive media. The human operator of the drive product interfaces with the CM through a "host" application on a host system.

2.2 Logical to Physical Port Mapping

FIPS 140-2 Interface	Module Ports
Data Input	SAS Connector
Data Output	SAS Connector
Control Input	SAS Connector
Status Output	SAS Connector, LED
Power Input	Power Connector

2.3 Product Versions

The following models and hardware versions (PNs) are validated with the following FW versions:

Product Name	Model #	FW Versions
Nytro 3730 SSD, 7mm, SAS Interface	XS1600ME10023 XS800ME10023 XS400ME10023	7A51, 0004, 0005
Nytro 3530 SSD, 7mm, SAS Interface	XS1600LE10023	7A51, 0004, 0005
Nytro 3330 SSD, 7mm, SAS Interface	XS1920SE10123 XS15360SE70143	7A51, 0004, 0005
Nytro 3130 SSD, 7mm, SAS Interface	XS3840TE10023	7A51, 0004, 0005
Nytro 3730 SSD, 15mm, SAS Interface	XS3200ME70023	7A51, 0004, 0005
Nytro 3130 SSD, 15mm, SAS Interface	XS7680TE70023	7A51, 0004, 0005
Nytro 3130 SSD, 15mm, SAS Interface	XS6400LE70023	7A51, 0004, 0005
Nytro 3731 SSD, 15mm, SAS Interface	XS3200ME70024 XS1600ME70024 XS800ME70024 XS400ME70024	0001, A001, 0002, 0003, A003, 0004
Nytro 3531 SSD, 15mm, SAS Interface	XS6400LE70024 XS3200LE70024 XS1600LE70024 XS800LE70024	0001, A001, 0002, 0003, A003, 0004
Nytro 3331 SSD, 15mm, SAS Interface	XS7680SE70024 XS3840SE70024 XS1920SE70024 XS960SE70024	0001, A001, 0002, 0003, A003, 0004
Nytro 3131 SSD, 15mm, SAS Interface	XS7680TE70024 XS3840TE70024 XS15360TE70024	0001, A001, 0002, 0003, A003, 0004
Nytro 2032 / 3032 SSD 15mm SAS Interface	XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS1920SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104 XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144	0001

Product Name	Model #	FW Versions
	XS3840SE70144 XS7680SE70144	
Nytro2032 / 3032 SSD 15mm SAS Interface	XS3840SE70104 XS960SE70104	0001, NA00

2.4 FIPS Approved Algorithms

Algorithm	Certificate Number	Modes/Key Sizes/Etc used
Hardware AES	#4843	256-bit SP800-38D GCM, SP800-38E XTS and SP800-38A CBC
Hardware RSA	#2662	FIPS 186-4 Signature verification w/ 2048-bit modulus
Hardware SHA	#3984	FIPS 180-4. 256-bit
Hardware HMAC	#3243	FIPS 198-1. 256-bit
Firmware AES	#1343	SP800-38A. 128-bit, 256-bit CBC
Firmware AES-GCM	#2841	SP800-38D. 256-bit
Firmware AES-GCM (TLS)	#3759	SP800-38D. 128-bit, 256-bit
Firmware AES CMAC	#3760	SP800-38B. 128-bit
Firmware SHA	#3304	FIPS 180-4. 256-bit, 384-bit
Firmware RSA	#2056	FIPS 186-4 Signature verification w/ 2048-bit modulus
Firmware DRBG	#1146	SP800-90A. Hash based DRBG
Firmware HMAC	#2613	FIPS 198-1. 256-bit
Firmware DHE (CVL)	#852	SP800-56Ar2. Ephemeral Mode, 2048-bit
Firmware DSA	#1390	FIPS 186-4 Key Pair Generation w/2048 bit
Firmware AES Key Wrap	#2947	SP800-38F. 256-bit
Firmware KDF (CVL)	#828	SP800-135. TLSv1.2 KDF
Firmware PBKDF	Vendor Affirmation	SP800-132. Option 2a
Firmware KAS	Vendor Affirmation	SP800-56Ar2. CVL certs. #828 and #852
Hardware NDRNG	Non approved but allowed	

SP800-132, Section 5.4 Option 2a is used and password length is a minimum of 4 bytes. The Master Key is 256 bits and decryption algorithm is AES-GCM. The keys derived from passwords are used in storage applications.

XTS-AES is only approved for use in storage applications.

There are algorithms, modes and keys that have been CAVS tested but not utilized by the module. Only the algorithms, modes and keys shown in this table are utilized by the module. AES CMAC (AES cert. #3760) was tested and has a power-on self-test, but the module does not use the algorithm as part of any service.

The module supports the TLS protocol. No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP. The module supports cipher suites from SP800-52r1, section 3.3.1. As per IG A.5, when the nonce_explicit part of the IV reaches its maximum value, the module aborts the TLS session.

The modules general purpose GCM implementation (cert. #2841) uses an internally and randomly generated IV, as per IG A.5.

The length of the data unit for any instance of an implementation of XTS-AES shall not exceed 2^20 AES blocks.

The module meets the XTS-AES IG A.9 requirement.

All symmetric keys and random seeds for asymmetric key pairs are the unmodified output of the approved DRBG. The NDRNG provides a minimum of 256 bit of entropy for use in key generation.

The module supports AES Key Wrap for encrypting keys stored on the drive. The algorithm is not used for any type of key transport scheme

2.5 Self-Tests

2.5.1 Power-On Self Tests

Function Tested	Implementation	Failure Behavior
Hardware AES	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Hardware RSA	Verify KAT performed.	Enters FIPS Self Test Error State.
Hardware SHA-256	Digest KAT performed.	Enters FIPS Self Test Error State.
Hardware HMAC	Keyed-Hash Message Authentication Code constructed from SHA-256.	Enters FIPS Self Test Error State.
Hardware AES-GCM	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES-GCM	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES-GCM (large block size)	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware AES CMAC	CMAC KAT performed.	Enters FIPS Self Test Error State.
Firmware SHA-512	Digest KAT performed.	Enters FIPS Self Test Error State.
Firmware DRBG	DRBG KAT performed.	Enters FIPS Self Test Error State.
Firmware HMAC	Keyed-Hash Message Authentication Code constructed from SHA-256.	Enters FIPS Self Test Error State.
Firmware FFC Diffie Hellman Ephemeral Mode	Diffie-Hellman KAT performed.	Enters FIPS Self Test Error State.
Firmware Key Wrap	Encrypt and Decrypt KAT performed.	Enters FIPS Self Test Error State.
Firmware TLS KDF	KDF KAT performed.	Enters FIPS Self Test Error State.
Firmware PBKDF	KAT performed.	Enters FIPS Self Test Error State.
Firmware Integrity Check	Signature Verification.	Enters FW Integrity Error State.

2.5.2 Conditional Self Tests

Function Tested	Implementation	Failure Behavior
Firmware Load Check	RSA PKCS#1 signature verification of new firmware image is done before it can be loaded. Performed when new firmware is downloaded.	Incoming firmware package is not loaded and is discarded.
Firmware DRBG	Continuous Random Number Generator test (CRNGT). Newly generated random number is compared to the previously generated random number. Test fails if they are equal. Performed when a random number is generated.	Enters FIPS Self Test Error State.
Firmware DRBG Health Tests	SP800-90A Instantiate, Generate, Reseed and Uninstantiate health tests. Performed when a random number is generated,	Enters FIPS Self Test Error State.
Firmware DRBG Health Tests	SP800-90B Repetition Count and Adaptive Proportion tests are performed when a seed for the DRBG is requested.	Enters FIPS Self Test Error State.
Firmware Diffie-Hellman Assurances Tests	Conditional tests for assurances as defined in SP800-56Ar2.	Enters FIPS Self Test Error State.
Non-Approved NDRNG	Continuous Random Number Generator test (CRNGT). Newly generated random number is compared to the previously generated random number. Test fails if they are equal. Performed when a seed for a DRBG is requested.	Enters FIPS Self Test Error State.

2.6 FIPS 140-2 Approved Mode of Operation

Before the operator performs Secure Initialization steps detailed in Section 7.1, the drive will operate in a non-compliant state.

There is 1 approved mode of operation, “TCG Security”.

The module’s FIPS mode of operation is enforced through configuration and policy. Violating these ongoing policy restrictions (detailed in Section 7.2) would mean that one is no longer using the drive in a FIPS compliant mode of operation. The operator can determine if the CM is operating in a FIPS approved mode by invoking the Show Status service (refer to Section 4.1).

2.6.1 TCG Security Mode

This mode has the capability to have multiple Users with independent access control to read/write/crypto erase independent data areas (LBA ranges). Note that by default there is a single “Global Range” that encompasses the whole user data area which is the starting point from which multiple Users request their independent data areas.

In addition to the Drive Owner and User(s) roles, this mode implements a CO role (EraseMaster) to administer the above capability.

2.6.2 Entering FIPS Approved Mode of Operation

After the module is installed and configured per the Security Rules of this policy in Section 7.1, the drive is always in the Approved mode of operation except when a critical failure has been detected, causing a transition to a “Failed” state.

In some of these exit scenarios (e.g. repeated POST failure), the drive cannot be restored to FIPS mode and does not provide any FIPS services.

2.7 User Data Cryptographic Erase Methods

Since all user data is encrypted / decrypted by the CM for storage on / retrieval from the drive media, the data can be erased using cryptographic methods. The data is erased by zeroizing the LBA Range Media Encryption Key (MEK).

Other FIPS services can be used to erase all the other private keys and CSPs (see Section 2.8).

2.8 Revert-SP Method

The TCG Revert-SP method may be invoked to transition the CM back to the manufactured state (uninitialized). This corresponds to the Exit FIPS Mode service and is akin to a "restore to factory defaults" operation. This operation also provides a means to zeroize keys and CSPs. Subsequently, the CM has to be re-initialized before it can return to a FIPS compliant mode of operation. This Revert-SP method is invoked as an unauthenticated service by virtue of the use of a public credential (PSID).

2.9 Show Status

Show status service can be used to determine if the drive is operational under the security constraints of FIPS. For this purpose TCG Level 0 Discovery mechanism is utilized. TCG Level 0 Discovery mechanism maybe invoked by the operator to know if drive is in "use" or security "fail" state. If the Drive Security Life Cycle State is 0x80 then drive is in Use State i.e. security is operational. If the Drive Security Life Cycle State is 0xFF the drive is in security Fail State i.e. drive is not operational in terms of FIPS services.

The LED indicates the drive is powered on. Drive activity is indicated by blinking of the LED. No other status is indicated through LED.

3 Identification and Authentication (I&A) Policy

3.1 Operator Roles

Note: The following identifies the CO and User roles with a *general* description of the purposes. For further details of the services performed by each role in each FIPS mode, see section 4.1.

3.1.1 Crypto Officer Roles

3.1.1.1 Drive Owner

This CO role corresponds to the SID (Secure ID) Authority on the Admin SP as defined in Enterprise SSC [4]. This role is used to download a new FW image. Note: only a FIPS validated firmware version can be loaded to the module. Otherwise, the module is not operating in FIPS mode.

3.1.1.2 EraseMaster (TCG Security Mode)

This CO role corresponds to the same named role as defined in Enterprise SSC [refer to Section1.3, item 4]. This role is used to enable/disable User roles, and erase the user data region (LBA band).

3.1.2 User Roles

3.1.2.1 BandMasters (0-15) (TCG Security Mode)

This user role corresponds to the same named role as defined in Enterprise SSC [refer to Section1.3, item 4]. This role is used to lock/unlock and configure a user data band ("LBA band") for read/write access.

A CM can be configured to support up to 16 user data bands, which are controlled by their respective BandMaster credentials. By default 2 user bands are enabled. BandMasters are enabled/disabled using the EraseMaster role. An operator is authenticated to the BandMaster role with identity-based authentication. If a user data band is erased (EraseMaster service) then the BandMaster PIN is reset to MSID.

3.1.3 Unauthenticated Role

This role can perform the Show Status service.
If the operator has physical access to the drive, this role can also reset the module with a power cycle (which results in POSTs). This role can also use the public PSID value to invoke the Exit FIPS Mode service. See section 4.1 for details.

3.2 Authentication

3.2.1 Authentication Types

Operator roles have identity-based authentication. For example, the Drive Owner has only one ID and one PIN. In TCG Security Mode, the CM has up to 16 User operators. Each of these operators is assigned a unique ID to which a PIN is associated, thus this provides identity-based authentication.

For some services the authentication is performed in a separate associated service; e.g. the Read Unlock service is the authentication for subsequent User Data Read service. If the User Data Read service is attempted without prior authentication then the command will fail.

3.2.2 Authentication in TCG Security Mode

Operator authentication is provided within a TCG session. The host application can have only a single session open at a time. Authentication of an operator, using the TCG interface, uses the Authenticate method to authenticate to a role after a session has been started. Authentications will persist until the session is closed.

Another method of authentication uses the StartTLS method in order to setup a secure TLS tunnel. Note that this method is only available after the PSKs have been set, which requires the operator to first authenticate using the method described in the preceding paragraph.

During a session the application can invoke services for which the authenticated operator has access control. Note that a security rule of the CM is that the host must not authenticate to more than one operator (TCG authority) in a session.

For the Show Status the host application will authenticate to the "Anybody" authority which does not have a private credential. Therefore this operation is effectively an unauthenticated service.

3.2.3 Authentication Mechanism, Data and Strength

Operator authentication by means of the respective CO/User roles PIN is implemented. This mechanism also applies to the respective User roles associated with PSKs. The PINs have a retry attribute ("TryLimit") that controls the number of unsuccessful attempts before the authentication is blocked. The "TryLimit" has an unmodifiable value of 1024. The PINs have a maximum length of 32 bytes (256 bits). The PSKs have a maximum length of 64 bytes (512 bits).

Per the policy security rules, the minimum PIN/PSK length is 4 bytes (32 bits) (Rule 2 in Section 7.1). This gives a probability of $1/2^{32}$ of guessing the PIN/PSK in a single random attempt. This easily meets the FIPS 140-2 authentication strength requirements of less than 1/1,000,000.

In TCG interface, each failed authentication attempt for PINs takes a minimum of 15ms to complete. Thus a theoretical maximum of {(60*1000)/15} attempts can be processed in one minute. Thus the probability of multiple random attempts to succeed in one minute is $4000/2^{32}$. This is significantly lower than the FIPS requirement of 1/100,000. In addition, since the "TryLimit" is unmodifiable, only 1024 attempts can be processed in one minute before the authorities are locked out.

In TCG interface, each authentication attempt for PSKs takes a minimum of 500ms to complete. Thus a theoretical maximum of {(60*1000)/500} attempts can be processed in one minute. Thus the probability of multiple random attempts to succeed in one minute is $120/2^{32}$. This is significantly lower than the FIPS requirement of 1/100,000.

3.2.4 Personalizing Authentication Data

The initial value for SID and various other PINs is a manufactured value (MSID). This is a device-unique, 32-byte, public value. The Security Rules (Section 7) for the CM requires that the PIN values must be "personalized" to private values using the "Set PIN" service.

The initial value for PSKs are empty and disabled. For Drive Owner PSKs, "personalized" to private values by Drive Owner role using the "Set TLS PSK" service. For EraseMaster PSK, "personalized" to private values by EraseMaster role using the "Set TLS PSK" service. For BandMaster PSKs, "personalized" to private values by respective BandMasters role using the "Set TLS PSK" service.

4 Access Control Policy

4.1 Services

The following tables represent the FIPS 140-2 services for each FIPS Approved Mode in terms of the Approved Security Functions and operator access control. Note the following:

- Use of the services described below is only compliant if the module is in the noted Approved mode.
- Underlying security functions used by higher level algorithms are not represented (e.g. hashing as part of asymmetric key)
- Operator authentication is not represented in this table.
- Some security functions listed are used solely to protect / encrypt keys and CSPs.
- Service input and output details are defined by the TCG and SCSI standards.
- Unauthenticated services (e.g. Show Status) do not provide access to private keys or CSPs.
- Some services have indirect access control provided through enable / disable or lock / unlock services used by an authenticated operator; e.g. User data read / write.

4.1.1 Authenticated Services – TCG Security Mode

Service Name	Description	Operator Access Control	Command(s) Event(s)
Set PIN	Change operator authentication data.	EraseMaster, BandMasters, Drive Owner	TCG Set Method
Firmware Download	Enable / Disable FW Download and load complete firmware image. If the self-test of the code load passes then the device will run with the new code.	Drive Owner **	TCG Set Method, SCSI Write Buffer
Enable / Disable BandMasters	Enable / Disable a User Authority.	EraseMaster	TCG Set Method
Set Range Attributes	Set the location, size, and locking attributes of the LBA range.	BandMasters	TCG Set Method
Lock / Unlock User Data Range for Read and/or Write	Block or allow read (decrypt) / write (encrypt) of user data in a range.	BandMasters	TCG Set Method
User Data Read / Write	Encryption / decryption of user data to/from a LBA range. Access control to this service is provided through Lock / Unlock User Data Range.	None*	SCSI Read, Write Commands
Cryptographic Erase	Erase user data in an LBA range by cryptographic means: changing the Media encryption key (MEK). BandMaster PIN is also reset.	EraseMaster	TCG Erase Method
Set TLS PSK	Set PSK for Secure Messaging.	EraseMaster, BandMasters, Drive Owner	TCG Set Method

4.1.2 Unauthenticated Services – TCG Security Mode

Service Name	Description	Operator Access Control	Command(s) Event(s)
Enable Secure Messaging	Set up secure communication with CM.	None	TCG StartTLS Method
Show Status	Reports if the CM is operational in terms of FIPS services and approved mode of operation value.	None	TCG Level 0 Discovery, TCG Get Method FIPS Operating Mode indicator (Byte 30, bit 0) = 1.
Reset Module	Runs POSTs and zeroizes key & CSP in RAM.	None	POR
DRBG Generate Bytes	Returns an SP800-90A DRBG Random Number.	None	TCG Random()
Exit FIPS Mode	Exit Approved Mode of Operation. Note: CM will enter non-compliant state.	None (using PSID)	TCG AdminSP.RevertSP()
FIPS 140 Compliance Descriptor	Reports FIPS 140 Revision, Overall Security Level, Hardware and Firmware revisions and Module name.	None	SCSI SECURITY PROTOCOL IN – Protocol 0

*Security has to be Unlocked
**FW Download Port has to be Unlocked

4.2 Cryptographic Keys and CSPs

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

- The use of PIN CSPs for authentication is implied by the operator access control.
- The Set PIN service is represented in this table even though generally it is only used at module setup.
- All non-volatile storage of keys and CSPs is in the system area of the drive media to which there is no logical or physical access from outside of the module.
- The module uses SP 800-90A DRBG and adopts Hash_DRBG mechanism.
- Read access of private values are internal only to the CM and are thus not represented in this table.
- There is no security-relevant audit feature.

4.2.1 Key Management

Name	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access **(W, X)
SID (Secure ID), aka Drive Owner PIN	Auth. Data	Private, PIN, 32-256 bits	Drive Owner	Set PIN	W
EraseMaster	EraseMaster Auth Data	Private, PIN, 32-256 bits	EraseMaster	Set PIN	W
				Cryptographic Erase	X
BandMaster Passwords	Users Auth. Data (up to 16 are supported)	Private, PIN, 32-256 bits	BandMasters	Set PIN	W
				Lock/Unlock User Data	X
LBA Range MEKs	MEK (per LBA band)	Private, AES Key, 256 bits	BandMasters	Lock/Unlock User Data	X
				Cryptographic Erase	W
Entropy Input String	*Input to a DRBG mechanism of a string of bits that contains entropy	Private, 256 bits	None	Reset Module	W
				Services which uses the DRBG (cryptographic erase, SetPIN)	X
Seed	*String of bits that is used as input to a DRBG mechanism	Private, Hash seed, 440 bits	None	Reset Module	W
				Services which uses the DRBG (cryptographic erase, SetPIN)	X
Internal State	*Collection of stored information about DRBG instantiation	Private, V and C 440 bits	None	Reset Module	W
				Services which uses the DRBG (cryptographic erase, SetPIN)	X
ORG 0-0 - ORG 0-1	Power On Integrity & Firmware Load Test Signature Verification Keys	Public, RSA Key, 2048 bits	Drive Owner	FW Download	X
MEKEK	This key is used to wrap the MEK	Private, AES Key, 256 bits	BandMasters, EraseMaster	Lock/Unlock User Data, Cryptographic Erase, Set PIN	W,X
Master Key	This key is used to protect the MEKEK	Private, AES Key, 32 bytes	Drive Owner, BandMasters, EraseMaster	Unlock User Data, Cryptographic Erase, Set PIN	W,X
CSPSKs	Critical Security Parameter Sanitization Keys, used within PBKDF	Private, AES Key, 256 bits	BandMasters, EraseMaster	Lock/Unlock User Data, Cryptographic Erase, SetPIN	W, X
Drive Owner PSKs	Pre-Shared secret value used for TLS handshake (up to 4 are supported)	Private, Pre-Shared Key, 32-512 bits	Drive Owner	Set TLS PSK	W
EraseMaster PSK	Pre-Shared secret value used for TLS handshake	Private, Pre-Shared Key, 32-512 bits	EraseMaster	Set TLS PSK	W
BandMaster PSKs	Pre-Shared secret value used for TLS handshake (16 are supported)	Private, Pre-Shared Key, 32-512 bits	BandMaster	Set TLS PSK	W
Diffie-Hellman Key Pair	Key Pair used during TLS handshake	Private, Diffie-Hellman Key Pair, 2048 bits/224 bits	EraseMaster, BandMasters, Drive Owner	Enable Secure Messaging	W,X
Secure Messaging Premaster Secret	TLS Premaster Secret value derived during TLS handshake	Private, 384 bits	EraseMaster, BandMasters, Drive Owner	Enable Secure Messaging	W,X

Name	Description	Type (Pub / Priv, key / CSP (e.g. PIN)), size	Operator Role	Services Used In	Access **(W, X)
Secure Messaging Master Secret	TLS Master Secret value derived during TLS handshake	Private, 384 bits	EraseMaster, BandMasters, Drive Owner	Enable Secure Messaging	W,X
Secure Messaging Session Key	Derived session unique key	Private, AES Key, 128 or 256 bits	EraseMaster, BandMasters, Drive Owner	Enable Secure Messaging	W,X
HMAC Keys	Key used for HMAC implementations	Private, HMAC Key, 256 bits	EraseMaster, BandMasters, Drive Owner	Lock/Unlock User Data, Enable Secure Messaging, Set PIN	W,X

* Source: Section 4 Terms and Definitions of NIST Special Publication 800-90A
** W- Write access is allowed, X – Execute access is allowed

5 Physical Security

5.1 Mechanisms

The CM has the following physical security:

- Production-grade components with standard passivation
- Two tamper-evident security labels applied by Seagate manufacturing prevent top and bottom cover removal for access or visibility to the media
- Exterior of the drive is opaque
- The tamper-evident labels cannot be penetrated or removed and reapplied without tamper-evidence
- The tamper-evident labels cannot be easily replicated with a low attack time
- Security label on sides of drive provide tamper-evidence of top and bottom cover removal

Figure 2: Top view of tamper-evidence label on sides of Nytro 3000® SAS Interface module

Figure 3: Left-side view of tamper-evidence label on left side Nytro 3000® SAS Interface module

Figure 4: Right-side view of tamper-evidence label on right side of Nytro 3000® SAS Interface module

5.2 Operator Requirements

The operator is required to inspect the CM periodically for one or more of the following tamper evidence:

- Checkerboard pattern on security label
- Security label cutouts do not match original
- Security label over PCBA screws not penetrated

Upon discovery of tamper evidence, the module should be removed from service.

Figure 5: Nytro 3000® 7mm Top Cover Tamper Evidence

Figure 6: Nytro 3000® 7mm Label lifted off

Figure 7: Nytro 3000® 15mm Top Cover Tamper Evidence

Figure 8: Nytro 3000® 15mm Label lifted

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the CM operates in a "non-modifiable operational environment". That is, while the module is in operation the operational environment cannot be modified and no code can be added or deleted. FW can be upgraded (replaced) with a signed FW download operation. If the code download is successfully authenticated then the module will begin operating with the new code image.

7 Security Rules

7.1 Secure Initialization

The following are the security rules for initialization and operation of the CM in a FIPS 140-2 compliant manner. Reference the appropriate sections of this document for details.

1. Users: At installation and periodically examine the physical security mechanisms for tamper evidence.
2. COs and Users: At installation, set all operator PINs applicable for the FIPS mode to private values of at least 4 bytes (32 bits) length:
    - TCG Security: Drive Owner, EraseMaster and BandMasters
3. Drive Owner: At installation, disable the "Makers" authority[1]
4. At installation, the value of LockOnReset[1] for FW Download must be set to "Power Cycle" and it must not be modified.
5. At installation, the value of PortLocked[1] for FW Download must be set to "TRUE".

At the end of these steps, the CM will be in a FIPS Approved Mode of operation. This can be verified with Show Status service (refer to Section 4.1).

7.2 Ongoing Policy Restrictions

1. Prior to assuming a new role, close the current Session and start a new Session, or do a power cycle, so that the previous authentication is cleared.
2. User Data Read/Writes shall be an authenticated service[2]. Therefore, set ReadLockEnabled[1] and WriteLockEnabled[1] to "True" (the default value is "False"). If a band is configured with a value of "False" then the band is to be considered excluded from the module boundary.
3. Set all PSKs (Drive Owner PSKs, EraseMaster PSK, BandMaster PSKs) applicable for the FIPS mode to private values of at least 4 bytes (32 bits) length.

8 Mitigation of Other Attacks Policy

The CM does not make claims to mitigate against other attacks beyond the scope of FIPS 140-2.

[1] Refer Section 1.3, Item 5
[2] Refer to Section 4.1, Table 1.1