

Novachips Co., Ltd.

NS361/NS371/NS561 (2.5" & M.2) SSD FIPS 140-2 NON-PROPRIETARY SECURITY POLICY

Document Revision: V 1.0



Revision History

Version	Date	Notes
1.0	Dec 08, 2020	Initial release.

Table of Contents

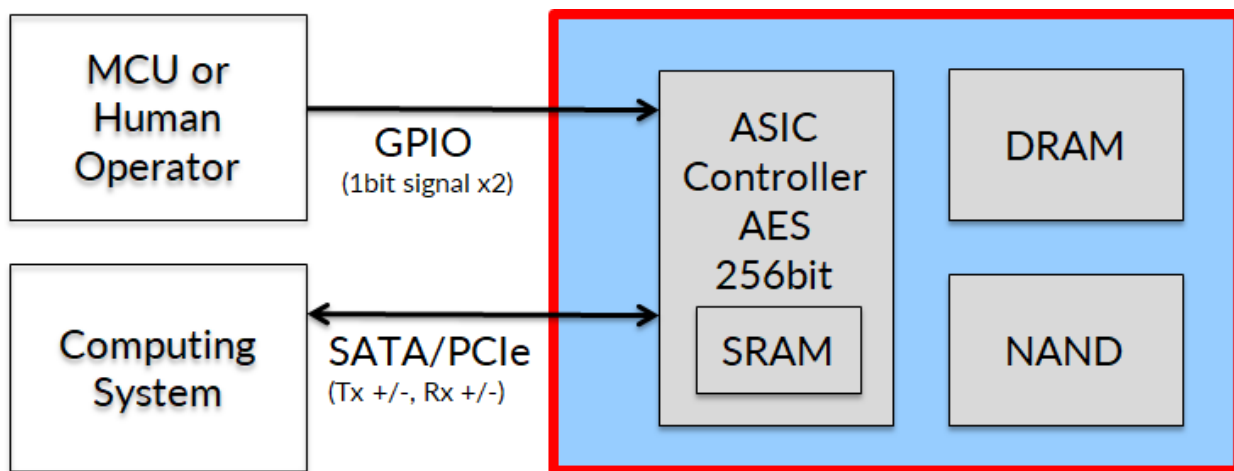
1. INTRODUCTION	4
2. CRYPTOGRAPHIC BOUNDARY	4
3. ACRONYMS	8
4. SECURITY LEVEL SPECIFICATION	9
5. PHYSICAL PORTS AND LOGICAL INTERFACES	10
6. SECURITY RULES	12
7. CRITICAL SECURITY PARAMETERS AND PRIVATE KEYS.....	15
8. IDENTIFICATION AND AUTHENTICATION POLICY	16
9. ACCESS CONTROL POLICY.....	17
10. ALGORITHMS	18
11. PHYSICAL SECURITY POLICY	19
12. MITIGATION OF OTHER ATTACKS POLICY	22
APPENDIX A: ACRONYMS	24

1. INTRODUCTION

NS361/NS371/NS561 (2.5" & M.2 SSD) module is a hardware multi-chip standalone cryptographic module designed to fulfill proprietary host key encryption.

2. CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary for the module (described by red line in Figure 1) is defined as the steel chassis for 2.5" SSD or opaque tamper-evident epoxy coating materials for M.2 SSD, which covers all integrated circuits.:




 FIPS-140-2 Cryptographic Module Boundary

Figure 1 Hardware Block Diagram of Novachips[NS361/NS371/NS561] SSD

Tested five modules are listed in Table1. Every module specified in following table are based on single NS3800 ASIC controller and different size of memory chips. NVS3800 controller has two different versions available for SATA / AHCI interface (NVS3800-39) and for PCIe / NVMe interface (NVS3800-59).

Part Number	HW Version	Physical Form Factor	Host Interface	Firmware Source	PCB	User Capacity
NS361F500GCC1-1F	04MB3	2.5" SATA 7mm	SATA / AHCI	NV.R1800_1200	2.5"_legacy_single_side	500GB
NS371F04T0CC1-1F	16MN3	2.5" SATA 7mm	SATA / AHCI	NV.R1800_1200	2.5"_HLsingle_PCB	4TB
NS371F08T0CC0-1F	16MN3	2.5" SATA 9.5mm	SATA / AHCI	NV.R1800_1200	2.5"_HLdual_PCB	8TB
NS361F500GCE7-1F	04MB3	M.2 2280 (B+M)	SATA / AHCI	NV.R1800_1200	M.2_legacy_SATA	500GB
NS561F500GCE7-1F	02MB3	M.2 2280 (M)	PCIe / NVMe	NV.R1800_1200	M.2_legacy_PClE	500GB

Table 1 Cryptographic Module Configuration

Follows are images of tested five modules from different angles of view.



Figure 2 NS361F500GCC1-1F 2.5" SATA 7mm SSD Module



Figure 3 NS371F04TOCC1-1F 2.5" SATA 7mm SSD Module



Figure 4 NS371F08TOCC0-1F 2.5" SATA 9.5mm SSD Module

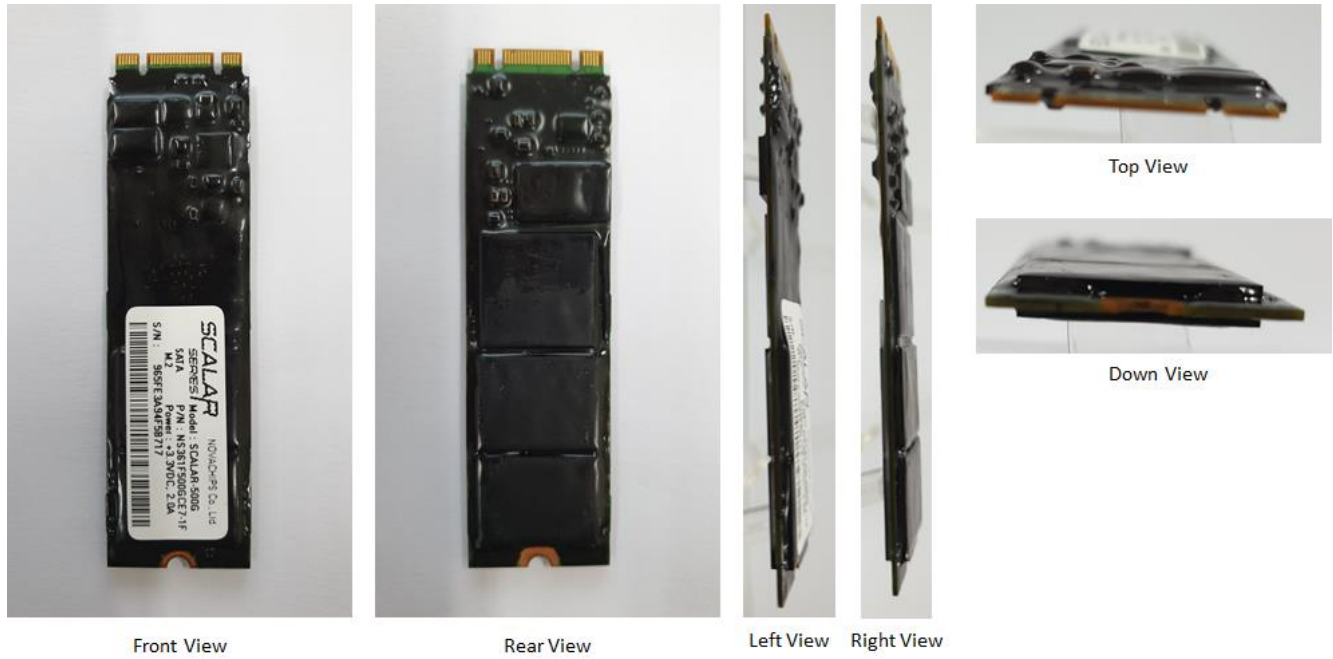


Figure 5 NS361F500GCE7-1F M.2 SATA SSD Module

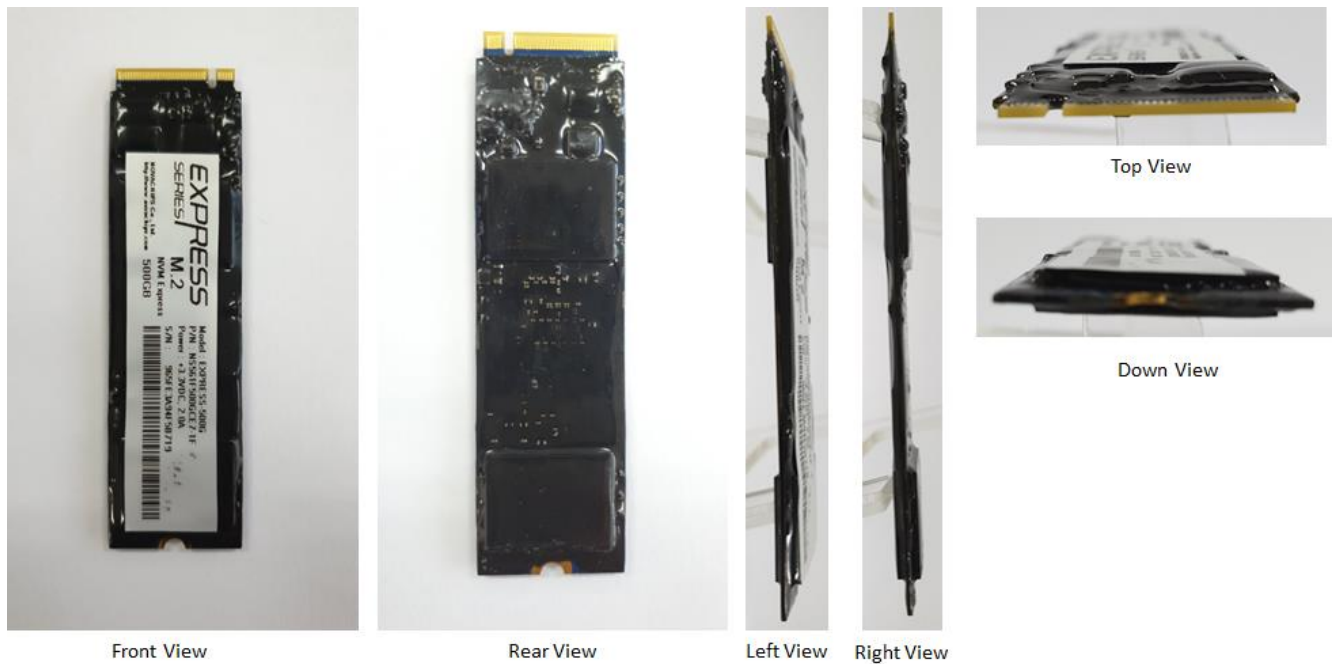


Figure 6 NS561F500GCE7-1F M.2 PCIe SSD Module

3. ACRONYMS

mode	state	Description
Security Mode Disabled	Uninitialized state	SSD is not activated Host Key encryption. Any user can access full range of SSD.
Security Mode Enabled	After enabling Host Key security mode, only authorized user can access User LBA range after passing verification.	
	Crypto Officer State	Crypto Officer is activating Host Key encryption by published API or service software after verifying physical security of SSD module.
	Self-Test State	SSD is running self-test of each encryption module.
	Login State	SSD is waiting for Host Key input from host. Only accessible to Shadow LBA range.
	User State	SSD is verified correct Host Key, and available service for User LBA range.
Exception mode	SSD is out of service to any host command.	
	Error State	SSD is out of service. It requires manual process of power cycle, or to be shipped back to manufacturer.
	Erase State	SSD is progressing zeroize process. SSD is out of service until zeroize process completion.

Table 2 Specification of Acronyms and their Descriptions

4. SECURITY LEVEL SPECIFICATION

SECURITY REQUIREMENTS AREA	LEVEL
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 3 Security Level Table

5. PHYSICAL PORTS AND LOGICAL INTERFACES

For part numbers NS361F500GCC1-1F, NS371F04T0CC1-1F and NS371F08T0CC0-1F, the applicable ports and interfaces are:

PHYSICAL PORT	LOGICAL INTERFACE
SATA	Data input, Data output, Control input, Status output, and Power Input
GPIO	Control input

Table 4 Specification of Cryptographic Module Physical Ports and Logical Interfaces

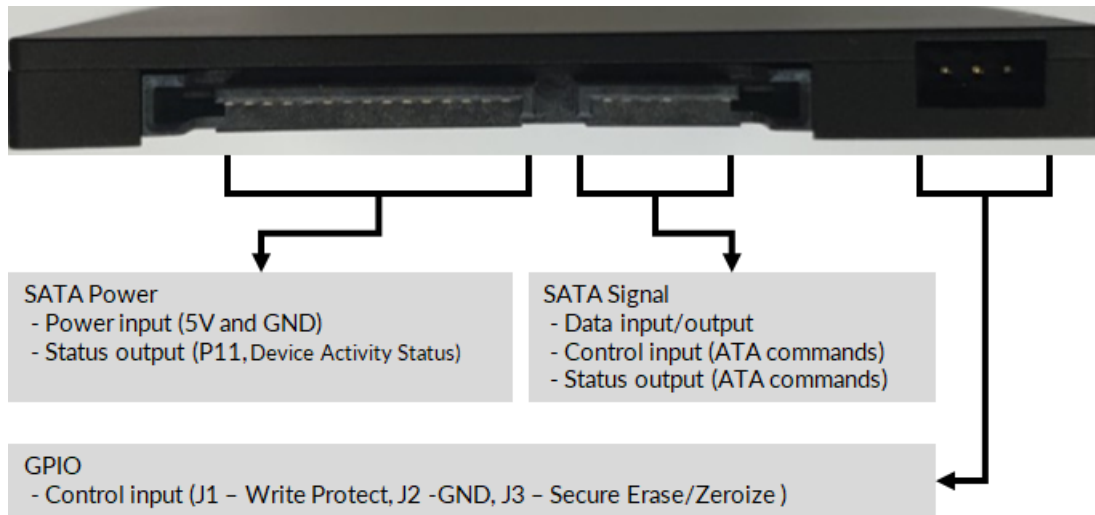


Figure 7 Physical Port of NS361F500GCC1-1F, NS371F04T0CC1-1F and NS371F08T0CC0-1F

For part number NS361F500GCE7-1F, the applicable ports and interfaces are:

PHYSICAL PORT	LOGICAL INTERFACE
SATA	Data input, Data output, Control input, Status output, and Power Input

Table 5 Specification of Cryptographic Module Physical Ports and Logical Interfaces

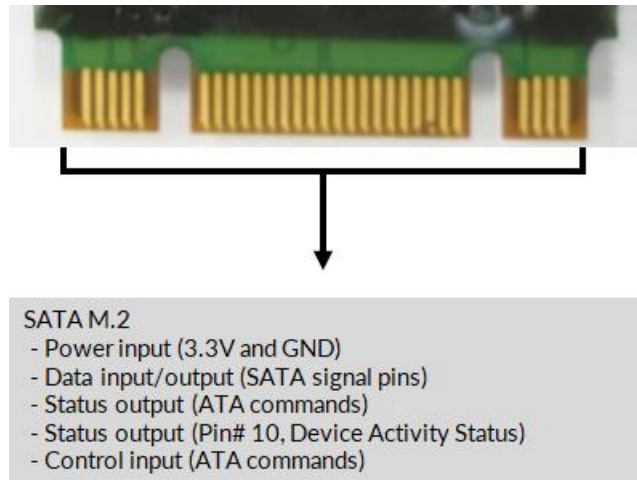


Figure 8 Physical Port of NS361F500GCE7-1F

For part number NS561F500GCE7-1F, the applicable ports and interfaces are:

PHYSICAL PORT	LOGICAL INTERFACE
PCIe	Data input, Data output, Control input, Status output, and Power Input

Table 6 Specification of Cryptographic Module Physical Ports and Logical Interfaces

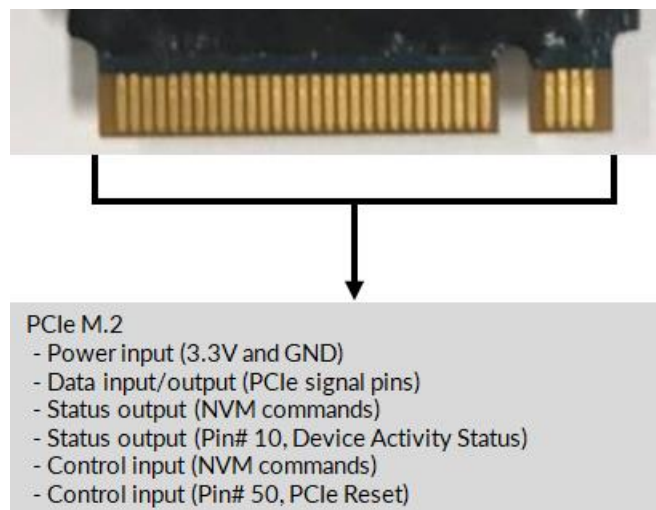


Figure 9 Physical Port of NS561F500GCE7-1F

6. SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

- The module only supports a FIPS Approved Mode of Operation.
- The module supports the following power-up self-tests:
 - Firmware image verified by SHA-256 hash tag
 - SHA-256 KAT
 - SP800-90A HASH DRBG KAT
 - SP800-90A HASH DRBG Section 11.3 Health Test
 - AES-XTS Encrypt KAT
 - AES-XTS Decrypt KAT
 - NDRNG Repetition Count Test
 - NDRNG Adaptive Proportion Test
- The module supports the following conditional self-tests:
 - Continuous RNG test on Approved SP800-90A HASH DRBG
 - Continuous RNG test on non-Approved NDRNG
 - NDRNG Repetition Count Test
 - NDRNG Adaptive Proportion Test
- The module will be at Uninitialized State after connecting it with host PC at fresh-out-of-box status.
- Crypto Officer can initialize and activate FIPS Approved Mode of Operation by following the next procedures:
 1. Inspect module as per section "[PHYSICAL SECURITY POLICY](#)".
 2. Power-on the module.
 3. Module shall appear to the host as uninitialized; this confirms all power-up self-tests successfully passed.
 4. Execute service "**Show Status**" ATA command Identify Device (Command OP code : ECh) or NVM admin Identify command (Command OP code : 06h). Confirm the module Hardware Part Number and Firmware Version is an approved configuration as listed in section "[CRYPTOGRAPHIC BOUNDARY](#)".
 5. Execute service "**Set Host Key (PIN)**" to set a Host Key(PIN). This is a one-time operation.
 6. Module will automatically reboot, and run power-up self-tests again.
If all power-up self-tests pass, the module SSD capacity will appear to the host as 256MB, which means that security is enabled.
 7. Module is now in a Login State.

8. Execute service "**Show Status**" ATA command Identify Device and verify module status specifies (FIPS-compliant, Security Enabled). (See below for more information on FIPS Approved Mode indicator)
 9. Module is now in the FIPS Approved Mode of Operation.
- The FIPS Approved Mode indicator can be obtained by executing "**Show Status**" ATA command Identify Device or NVM admin Identify command.

Part Number	Show Status command	FIPS Descriptor Address	FIPS Approved Mode Expected Indicator
NS361F500GCC1-1F	ATA Identify Device	Word 137	0x0023 (FIPS-compliant, Security Enabled)
NS371F04T0CC1-1F	ATA Identify Device	Word 137	0x0023 (FIPS-compliant, Security Enabled)
NS371F08T0CC0-1F	ATA Identify Device	Word 137	0x0023 (FIPS-compliant, Security Enabled)
NS361F500GCE7-1F	ATA Identify Device	Word 137	0x0023 (FIPS-compliant, Security Enabled)
NS561F500GCE7-1F	NVM admin Identify	Byte 3092~3093	0x0023 (FIPS-compliant, Security Enabled)

- The power-on self-tests can be performed on-demand by power-cycling the module.
- If the module fails any power-up tests or conditional tests, then the module will enter a hard error state. During a hard error state, the module is not available for any services, and it inhibits all data output. Error indicator is:
 - Module will not show up to host.
 - Module will output constant toggle signal via Activity signal pin. Pin location identified below per part number:

Part Number	Pin
NS361F500GCC1-1F	SATA P11
NS371F04T0CC1-1F	SATA P11
NS371F08T0CC0-1F	SATA P11
NS361F500GCE7-1F	M.2 Pin# 10
NS561F500GCE7-1F	M.2 Pin# 10

- If the module passed all self-test items, then the module will show up to the host and it is available to start servicing commands.
- The module inhibits all data output during self-tests.
- At Login State, authentication is always required.

- Any invalid attempts to authenticate to the module will result in status output "Password Failure" (Fail=1h, key retry count value). Module does not provide any other feedback to the operator and mitigates brute force attacks as described in section "[IDENTIFICATION AND AUTHENTICATION POLICY](#)".
- The module does not support manual key entry or any other type of key entry/output.
- The module supports zeroization to destroy all critical security parameters.
- The module logically inhibits the data output interface when performing key generation and zeroization processes.
- Host Key is only supported for single entity. The module does not support concurrent operators.
- The cryptographic module satisfies the requirements of FIPS 140-2 IG A.9 (i.e. key_1 ≠ key_2).

7. CRITICAL SECURITY PARAMETERS AND PRIVATE KEYS

CSP & KEY	Description/Usage	Storage
Host Key (PIN)	<p>10 ~ 32 bytes PIN, authentication data for CO/User. SSD module supports only one Host Key code, and rejects command if input key size is smaller than 10 bytes.</p> <ul style="list-style-type: none"> • Generation: Externally generated by CO/User • Entry: Directly entered from host in plaintext • Output: N/A • Zeroization : Set Host Key, Zeroize 	SRAM / NAND
DRBG Internal State (Values of Entropy Input, Seed, V and C)	<p>SSD module contains a non-deterministic hardware random number generator (NDRNG) that uses an internal, unpredictable physical source of entropy that is outside of human control. Random numbers generated by the NDRNG are used as seeding values for the FIPS Approved Deterministic Random Bit Generator (SP800-90A HASH DRBG). The values of Entropy Input, Seed, V and C of HASH DRBG mechanism</p> <ul style="list-style-type: none"> • Generation: Internally using the SP800-90A HASH DRBG • Entry: N/A • Output: N/A • Zeroization: Zeroize <p>Continuous RNG tests are performed on the outputs of the NDRNG and on the outputs of the Approved SP800-90A DRBG. Note: the minimum number of bits of entropy generated by the module for use in key generation is 256.</p>	SRAM / NAND
AES Master Key	<p>SSD module uses an AES 256-bit XTS to encrypt/decrypt data to/from secure range of internal memory. The AES 256-bit key is generated by using cryptographic module which is FIPS Approved deterministic random bit generator (SP800-90A HASH DRBG).</p> <ul style="list-style-type: none"> • Generation: Internally using the SP800-90A HASH DRBG • Entry: N/A • Output: N/A • Zeroization : Zeroize 	SRAM / NAND

Table 7 Critical Security Parameters

8. IDENTIFICATION AND AUTHENTICATION POLICY

ROLE	Role Description	AUTHENTI CATION TYPE	AUTHENTI CATION DATA
CO (Crypto Officer)	<p>SSD module shall be provided to Crypto Officer for first time use, and Crypto Officer shall be in charge of below procedures.</p> <ul style="list-style-type: none"> CO inspects the module as per section "PHYSICAL SECURITY POLICY". CO initializes and activates the FIPS Approved Mode of Operation. CO ensures proper handling of the module when in a hard Error State. May require manual process of power cycle, or to be shipped back to manufacturer. 	Role-based	PIN
User	<p>SSD module shall be provided to User after Crypto Officer state, and user shall follow rules set forth in this Security Policy.</p> <ul style="list-style-type: none"> User shall change Host Key before initial use. User shall contact Crypto Officer when SSD is in Error State. 	Role-based	PIN

Table 8 Roles and Required Identification and Authentication

Authentication Method	Probability	STRENGTH OF MECHANISM
Host Key (PIN) based authentication	<p>Minimum PIN length is 10 bytes with a maximum length of 32 bytes, and Key Retry count is persistent during power-cycle.</p>	<p>The probability of guessing a Host Key (PIN) in a single attempt with a 10 characters password is $1/2^{80}$ in a single random attempt, considering single byte is 2^8 and 10 bytes length is total $(2^8)^{10}$ different possible input. This probability is less than FIPS 140-2 authentication strength requirements 1/1,000,000.</p> <p>To protect SSD from brute-force attack, module implements a Key Retry count ("N"). The Key Retry count will increase, whenever Host Key verification fails. This Key Retry count record is non-volatile even after power cycling. When key retry count is greater than 10, SSD will proceed zeroization process automatically, then the state will be changed to Uninitialized state. Key Retry count is reset to zero when correct key input is verified.</p>

		Hence, in a one-minute period, the probability that a random attempt will succeed, or false acceptance will occur, is $10/(2^{80})$ which is less than 1 in 100,000.
--	--	--

Table 9 Strength of Authentication Mechanisms

9. ACCESS CONTROL POLICY

The cryptographic module supports two roles: Crypto Officer(CO) and User. The type of services corresponding to each of the supported roles is described as below.

(U/A = Unauthenticated, R = Read/Execute, W = Write, Z = Zeroize, N/A = Not applicable,)

Service	Description	CO	User	U/A	Type of Access	Cryptographic Keys and CSPs
Write Data (to Shadow LBA)	Receive plaintext data from host. Write data to non-secured range of internal memory.	○	○	○	N/A	N/A
Read Data (from Shadow LBA)	Output plaintext data to host. Read data from non-secured range of internal memory.	○	○	○	N/A	N/A
Write Data (to User LBA)	Receive plaintext data from host, outside of the cryptographic boundary, AES encrypt data and program into secured range of internal memory.	○	○		R	AES Master Key
Read Data (from User LBA)	AES decrypt data from secured range of internal memory. Output plaintext to host, outside of the cryptographic boundary.	○	○		R	AES Master Key
Set Host Key (PIN)	Set or Change Host Key (PIN).	○	○		W W W	Host Key AES Master Key DRBG Internal State
Login/Unlock	Unlock secured range of internal memory.	○	○		R R	Host Key AES Master Key
Logout/Lock	Lock-up secured range of internal memory.	○	○	○	N/A	N/A
Show Status	Status Outputs. (ATA command Identify Device and other status information)	○	○	○	N/A	N/A
Self-Test	Module automatically performs required self-tests of the module after power-on.	○	○	○	N/A	N/A
Set Write Protect	Set the device to read-only using GPIO.	○	○	○	N/A	N/A

	(SATA 2.5" Form Factor only) ¹					
Zeroize	Destroy all CSPs. This service can be triggered by one of below methods. <ul style="list-style-type: none"> ATA CRYPTOSCRAMBLE ² ATA SET SECURITY ERASE ³ GPIO External trigger (SATA 2.5" Form Factor only) ⁴ 	O	O	O	Z Z Z	Host Key AES Master Key DRBG Internal State

Table 10 Roles, Services, CSPs, Types of Access

10. ALGORITHMS

APPROVED ALGORITHMS

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTHS, CURVES, OR MODULUS	USE
AES 3962 ⁵	AES	FIPS 197 SP 800-38A	AES ECB	256	Prerequisite only for AES XTS
C448	AES	FIPS 197 SP 800-38E	XTS	256	Data Encryption/ Decryption for storage applications only
Vendor Affirmed	CKG	SP800-133			Cryptographic Key Generation. The key generation is performed as per the "Direct Generation" of Symmetric Keys which is an Approved key generation method.
C463	DRBG	SP 800-90A	HASH_DRBG SHA-256		Deterministic Random Bit Generation
C411	SHS	FIPS 180-4	SHA-256		Message Digest

Table 11 Table of Approved Algorithms

¹ Please see Figure 7 "Physical Port of NS361F500GCC1-1F, NS371F04TOCC1-1F and NS371F08TOCC0-1F"

² The operator can send this command using software outside the scope of the boundary.

³ The operator can send this command using software outside the scope of the boundary.

⁴ Please see Figure 7 "Physical Port of NS361F500GCC1-1F, NS371F04TOCC1-1F and NS371F08TOCC0-1F"

⁵ Module does not implement AES-CBC; Latent Functionality.

ALLOWED ALGORITHMS

The module supports the following non-Approved but allowed algorithms:

ALGORITHM	CAVEAT	USE
NDRNG	Only used for generating seed materials for the Approved HASH_DRBG. Minimum security strength is 256 bits.	Non-deterministic Random Number Generator
PBKDF	No Security Claimed as per FIPS-140-2 IG section 1.23	Used for obfuscation of PIN, considered as plaintext.

Table 12 Table of Allowed Algorithms

11. PHYSICAL SECURITY POLICY

2.5" SSD is covered by CNC/Aluminum enclosure and enclosure screws are sealed by tamper evident labels. Two tamper evident labels are applied at manufacturing, please see figure 10 2.5" SATA enclosure and tamper evident label locations. Furthermore, 2.5" SSD PCBA is encapsulated with a hard, opaque, tamper-evident Urethane/Epoxy Coating.

M.2 SSD is encapsulated with a hard, opaque, tamper-evident Urethane/Epoxy Coating. This coating functions as the physical security boundary of the device. M.2 SSD is not applied tamper evident label.

PHYSICAL SECURITY MECHANISMS	RECOMMENDED FREQUENCY OF INSEPTION/TEST	INSPECTON/TEST GUIDANCE DETAILS
CNC/Aluminum enclosure	On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the enclosure once a year.	Inspect for evidence of prying or removal <ul style="list-style-type: none"> • Bending of enclosure • Removal of TE label. If any evidence of tampering exists, the Crypto Officer is required to cease use of the cryptographic module immediately.
Tamper Evident Seals	On initial receipt of the device and in accordance with Crypto Officer organizational	Inspect labels for evidence of a removal attempt. In all cases the label will not be able to be reapplied. <ul style="list-style-type: none"> • Peeling will result in a residue on the

	<p>security policy. It is recommended to inspect the seals once a year.</p>	<p>enclosure and/or an inability to reapply the label</p> <ul style="list-style-type: none"> • Solvent attacks will result in the TE label being physically disfigured • Temperature attacks will result in the TE label being disfigured. <p>If any evidence of tampering exists, the Crypto Officer is required to cease use of the cryptographic module immediately.</p>
Urethane/Epoxy Coating	<p>On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the Epoxy Coating once a year.</p>	<p>Inspect for scratches, gouges, scrapes, deformations, and any other suspicious signs of malice and tampering.</p> <p>If any evidence of tampering exists, the Crypto Officer is required to cease use of the cryptographic module immediately.</p>

Table 13 Inspection/Testing of Physical Security Mechanisms



Figure 10 2.5" SATA enclosure and tamper evident label locations



Figure 11 Tamper-evident labels detached



Figure 12 SATA 2.5" and M.2 Urethane/Epoxy Coating

12. MITIGATION OF OTHER ATTACKS POLICY

OTHER ATTACKS	MITIGATION MECHANISM	SPECIFIC LIMITATIONS
N/A	N/A	N/A

Table 14 Table of Mitigation of Other Attacks

The Module has not been designed to mitigate attacks outside of the scope of FIPS 140-2. This area is noted as not being applicable.

Appendix A: Acronyms

TERM	Description
2.5"	2.5 inch disk form factor
M.2	Computer Expansion Card Disk form factor
AES	Advanced Encryption Standard (FIPS-197)
GPIO	General Purpose Input Output
SATA	Serial Advanced Technology Attachment
PCIe	PCI Express
CPU	Central Processing Unit
DRAM	Dynamic Random-Access Memory
NAND	NAND flash memory
SSD	Solid State Drive
CO	Crypto Officer
CSP	Critical Security Parameter
PIN	Personal Identification Number
FIPS	Federal Information Processing Standard Publication
ASIC	Application-Specific Integrated Circuit
RNG	Random Number Generator
NDRNG	Non-Deterministic Random Number Generator
DRBG	Deterministic Random Bit Generator
SHA	Secure Hash Algorithms
SHS	Secure Hash Standard
KAT	Known Answer Test

Table 15 Acronyms