

# **Novachips Co., Ltd.**

## **Scalar and Express P-series SSD**

### **Non-Proprietary Administrative Guidance**

Document Revision: V 1.0

**Revision History**

Version	Date	Notes
1.0	Mar 3 <sup>rd</sup> , 2022	Initial release.

---

## TABLE OF CONTENTS

1. INTRODUCTION .....	5
2. PRODUCT DESCRIPTION .....	5
3. TOE EVALUATED CONFIGURATION AND PICTURES .....	7
4. PORTS AND LOGICAL INTERFACES .....	12
5. TOE OPERATION PRIOR HOST KEY ACTIVATION.....	15
6. POWER STATES.....	16
7. ZEROIZE, IMMEDIATE KEY DESTRUCTION, AND MILITARY ERASE PROTOCOL.....	17
8. KEY RECOVERY .....	19
9. PRODUCT IDENTIFICATION .....	19
10. PRODUCT PART NUMBER .....	20
11. SCOPE OF EVALUATION .....	21
12. OPERATING ENVIRONMENT.....	22
13. OPERATING ENVIRONMENT ASSUMPTION AND REQUIREMENTS.....	22
14. UNATTENDED OPERATION.....	23
15. STATE OF TOE AT FRESH OUT OF BOX.....	23
16. SOFTWARE UTILITY.....	24
17. COMMAND INTERFACE .....	25
18. CHANGING THE PASSWORD (HOST KEY) AFTER CONFIGURATION .....	26
19. INSTALLATION OF TOE .....	27
20. CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS .....	29
21. ROLES.....	31
22. HOST KEY FAILED ATTEMPTS PENALTY .....	32
23. FIRMWARE UPDATE .....	32
24. ACCESS CONTROL POLICY .....	35
25. ALGORITHMS .....	36
26. PHYSICAL SECURITY .....	37
27. SERVICE READY ONLY AFTER PASSING SELF-TEST AND ERROR STATE.....	40
28. ELECTROMAGNETIC INTERFACE CAPABILITY .....	41
29. MITIGATION OF OTHER ATTACKS POLICY .....	41
30. SECURITY GUIDANCE SUMMARY .....	41

---

<b>APPENDIX A: KEY MATERIALS .....</b>	<b>44</b>
<b>APPENDIX B: ACRONYMS.....</b>	<b>45</b>
<b>APPENDIX C: REFERENCE DOCUMENT &amp; SUPPORT DOCUMENTATION.....</b>	<b>46</b>

## 1. INTRODUCTION

This document provides administrative guidance for Scalar 2.5" SATA (NS361/NS371) and Express M.2 and U.2 (NS561/NS571) P-series Solid State Drive (hereafter, also referred to as Target of Evaluation, TOE). The document describes expected physical and logical status of Fresh Out Of the Box product, necessary steps to initiate secure configuration of the TOE, and other important guidance to achieve designated Security Target which is based on the Collaborative Protection Profiles (cPPs) for Full Drive Encryption (FDE): Authorization Acquisition (AA) and Encryption Engine (EE) v2.0, January 2, 2019. The document is intended for use by the Crypto Officer (CO) (hereafter, also referred to as administrator) responsible for configuring the product prior to field deployment by setting up initial password (hereafter, also referred to as Host Key) to establish complete key chain.

The terms, TOE, administrator, and password in cPP FDE, stand for Scalar and Express P-series SSD, Crypto Office (CO), and Host Key, respectively, and the document uses each terms interchangeably.

## 2. PRODUCT DESCRIPTION

Scalar and Express P-series are encrypted secure solid-state drives, which is multi-chip standalone cryptographic module consists of single ASIC controller and different size of memory chips of volatile DRAM and non-volatile NAND. Those cryptographic modules are designed to fulfill non-proprietary Host Key encryption, and compatible to use at industry standard form factor such as 2.5" SATA hard drive or NVMe M.2 & U.2 SSD slot.

Since administrator or CO activates initial Security Mode in accordance with "[30. INITIALIZATION AND GUIDANCE SUMMARY](#)", 256MB Shadow Disk is appearing to host as Login State at powering-up. Only after successful user authentication with correct password, Shadow Disk will disappear and full capacity User Disk will be re-appearing to host automatically without user intervention as showing in following diagram.

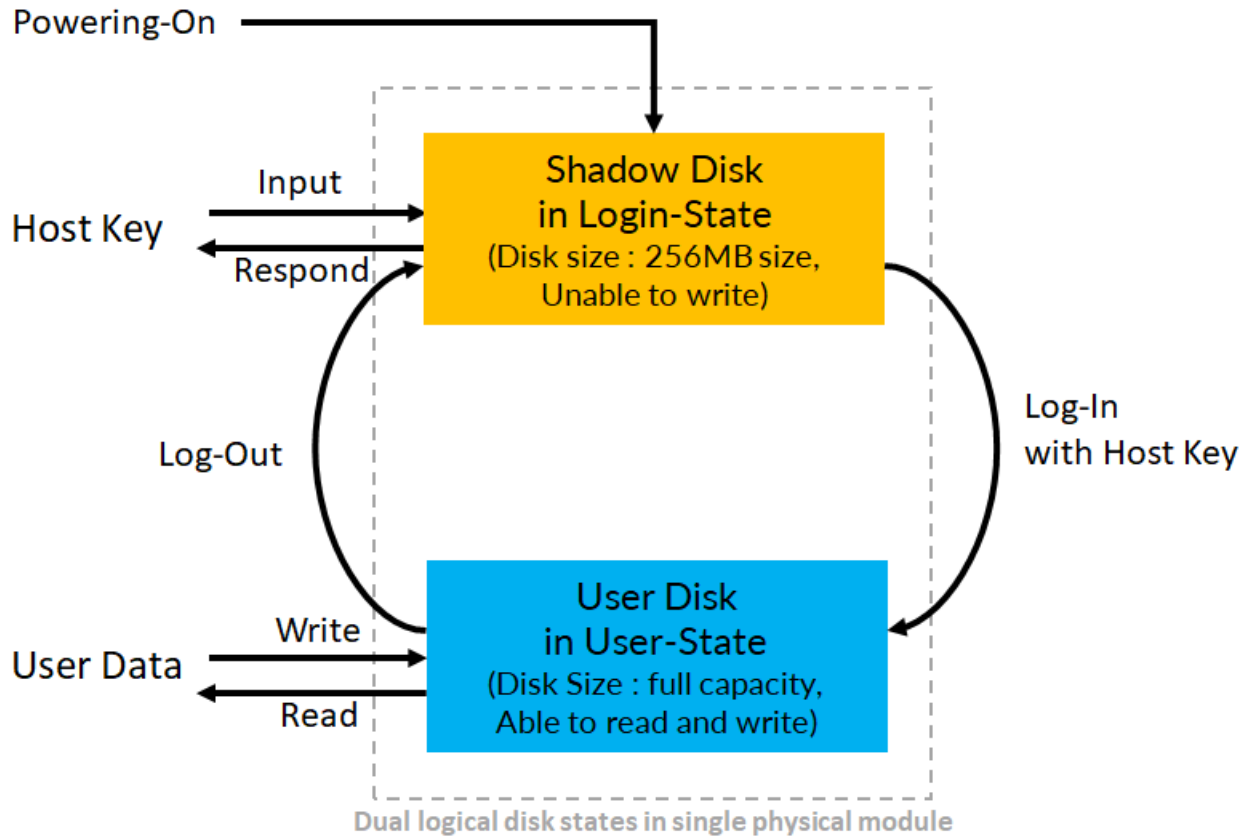


Figure 1 Simplified Diagram of TOE operation in CC compliant mode.

Unlike most of other secure solid state drive products, Novachips Host Key encryption does not depend on a TPM module, TCG, or OPAL to implement security. Instead, Novachips SSD module implements security using hardware-based AES-256 XTS encryption and key management techniques that are using standard ATA or NVM commands. These techniques provide superior and flexible solutions for mission critical defense applications and commercial enterprise environment, and have no requirements for any 3rd party software.

### 3. TOE EVALUATED CONFIGURATION AND PICTURES

The Novachips is providing reference GUI-based admin tool which enables user to send Host Key password from host computing system to TOE easily by manually typing in Windows OS environment.

However, the user should take into account that Novachips admin tool was not used for evaluating configuration, because software tool is not the part of TOE. Instead, evaluated configuration was tested per ATA / NVM command guidance document and the configuration instructions which is mandated by ST.

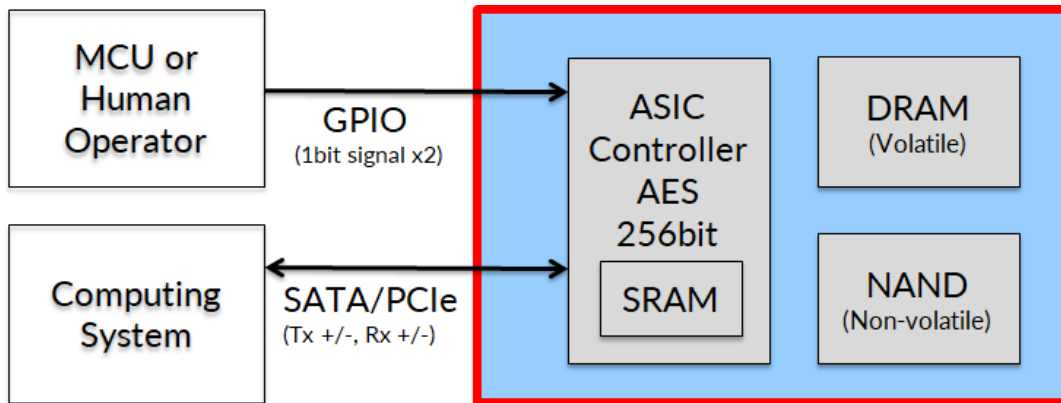
Additionally, Security Target is based on FDE cPPs: AA and EE to protect 'Data At Rest' on a device that is lost or stolen while powered off without any prior access by an adversary. So the scope of evaluation is not covering the security of any 3<sup>rd</sup> party or vendor software tool. During the evaluation, TOE is not evaluated nor tested with the use of other cryptographic engines. If there are multiple cryptographic engines installed in the host system, it is up to the user to ensure that data is being sent to the TOE for encryption. If the TOE is the only storage medium in the host system, there should be no need for user intervention to ensure that data is sent to the TOE for encryption.

The TOE evaluation covers following models with specified hardware and firmware version.

TOE developer Original Part No.	HW Ver.	Description (Form factor & Interface)	Firmware Ver.	User Capacity	Certification Sponsor Reseller Part No.
NS361P500GCCR-1F	04MB3	2.5" SATA 7mm MLC 500GB	NV.R1900_1000	500GB	AMP25T500-IM02AI
NS371P02TOCC1-1F	08MN3	2.5" SATA 7mm MLC 2TB	NV.R1900_1000	2TB	AMP25TT20-IM02AI
NS371P04TOCC1-1F	16MN3	2.5" SATA 7mm MLC 4TB	NV.R1900_1000	4TB	AMP25TT40-IM02AI
NS371P10TOCC0-1F	16MN3	2.5" SATA 9.5mm MLC 10TB	NV.R1900_1000	10TB	AMP25TT10-IM02AI
NS561P500GCE7-1F	02MB3	M.2 2280 PCIe/NVMe MLC 500GB	NV.R1900_1000	500GB	AMPW5D500-IM02AI
NS571P02TOCK7-1F	16SN3	M.2 22110 PCIe/NVMe MLC 2TB	NV.R1900_1000	2TB	AMPW6DT20-IM02AI
NS571P08TOCC0-1F	16MN3	2.5" PCIe/NVMe (U.2) MLC 8TB	NV.R1900_1000	8TB	AMP2UDT80-IM02AI

Table 1 Cryptographic Module Configuration

The physical boundary of the TOE is disk metal enclosure for 2.5" SATA and U.2 or opaque tamper-evident epoxy coating materials for M.2 SSD, which covers all integrate circuits.




 Physical Boundary of the TOE

Figure 2 Hardware Block Diagram of Novachips [NS361/NS371/NS561/NS571] SSD

Following are pictures of evaluated TOE modules, and every module is based on same single NVS3800 ASIC controller and different size of memory chips. NVS3800 controller has two different versions of hardware fusing option available for SATA / ATA interface (NVS3800-39) and for PCIe / NVMe interface (NVS3800-59).





Figure 3 NS361P500GCCR-1F, NS371P02TOCC1-1F, NS371P04TOCC1-1F 2.5" SATA 7mm SSD Module



Figure 4 NS371P10TOCC0-1F 2.5" SATA 9.5mm SSD Module

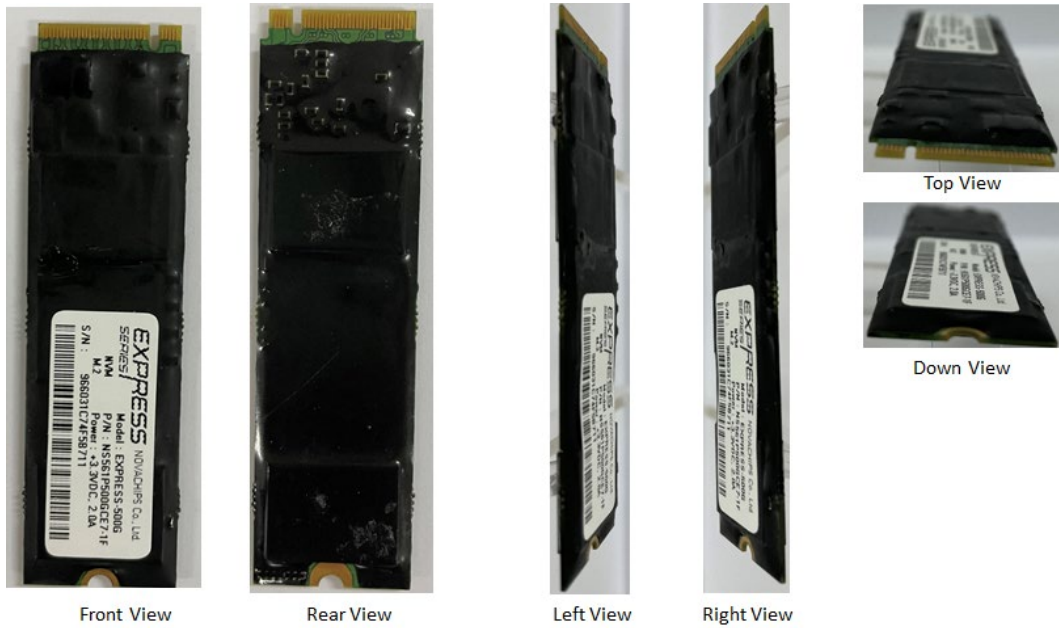


Figure 5 NS561P500GCE7-1F M.2 2280 PCIe/NVMe SSD Module

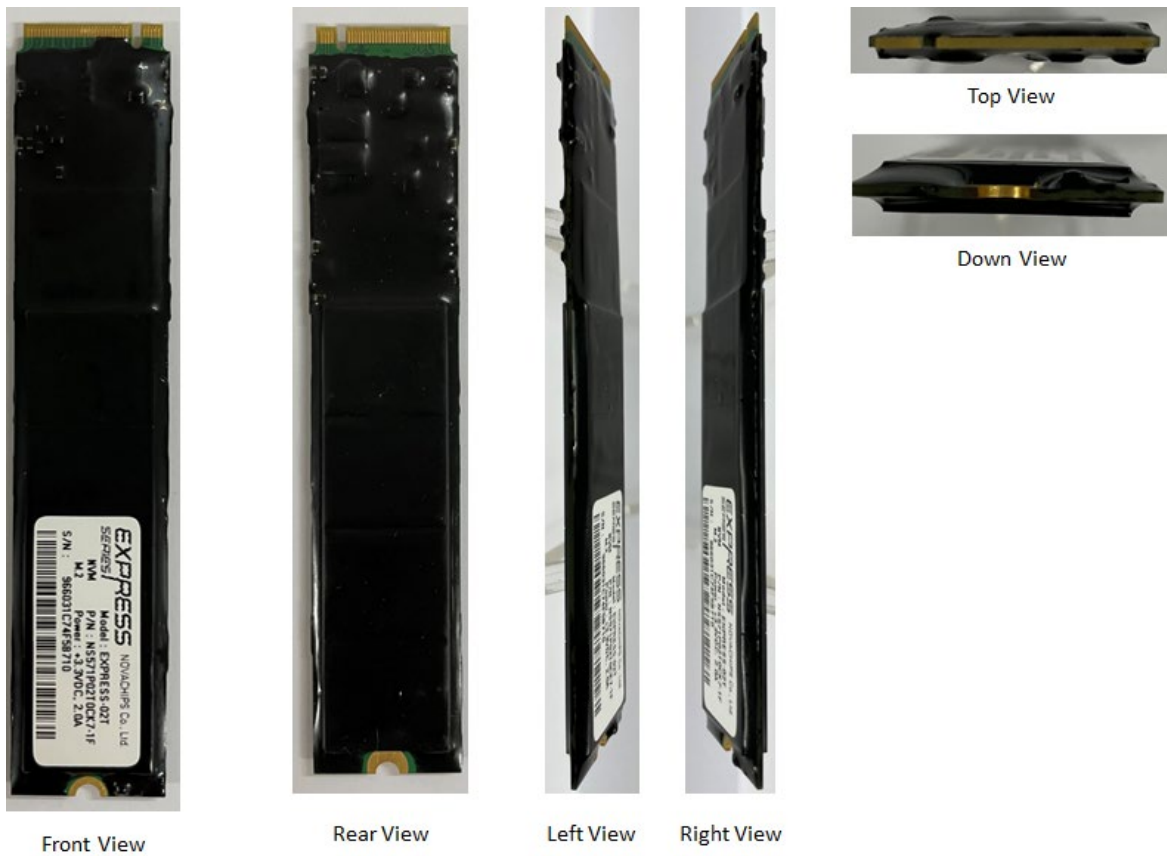


Figure 6 NS571P02T0CK7-1F M.2 22110 PCIe/NVMe SSD Module



Figure 7 NS571P08T0CC0-1F U.2 (2.5") PCIe/NVMe SSD Module

## 4. PORTS AND LOGICAL INTERFACES

For SATA-based TOEs (part numbers: NS361P500GCCR-1F, NS371P02T0CC1-1F, NS371P04T0CC1-1F, and NS371P10T0CC0-1F), the design of mechanical dimension and connector pinout conforms to the industry standard 2.5" form factor (SFF-8201), and the applicable ports and interfaces are:

PHYSICAL PORT	LOGICAL INTERFACE
SATA power (P1~P15)	Status Output, Power Input, Control input (Optional)
SATA signal (S1~S7)	Data input, Data output, Status output, Control input
GPIO	Control input

Table 2 Specification of Scalar (SATA products) Cryptographic Module Physical Ports and Logical Interfaces

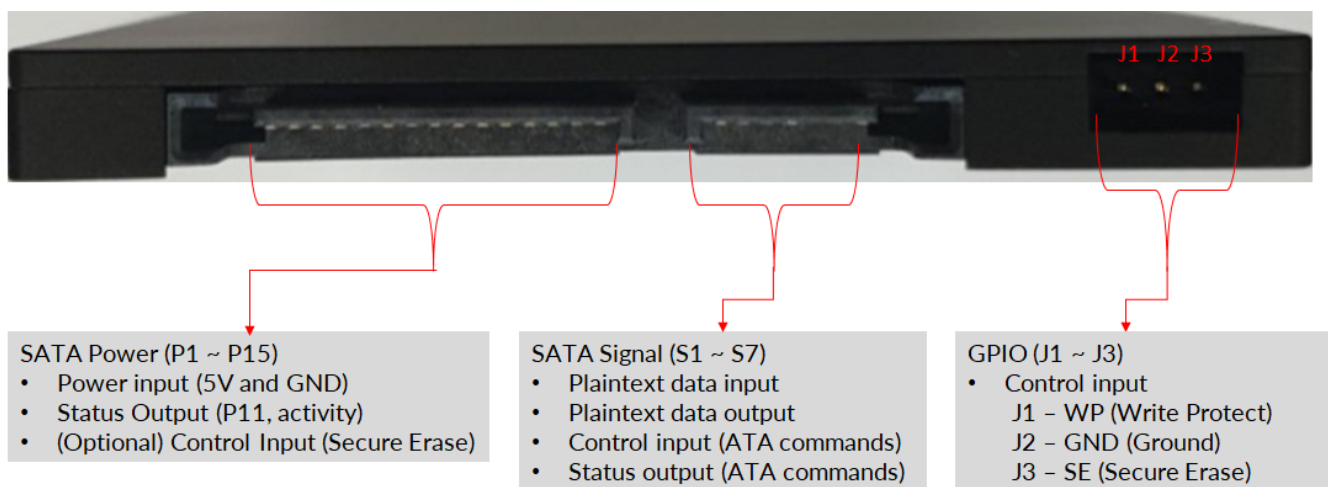
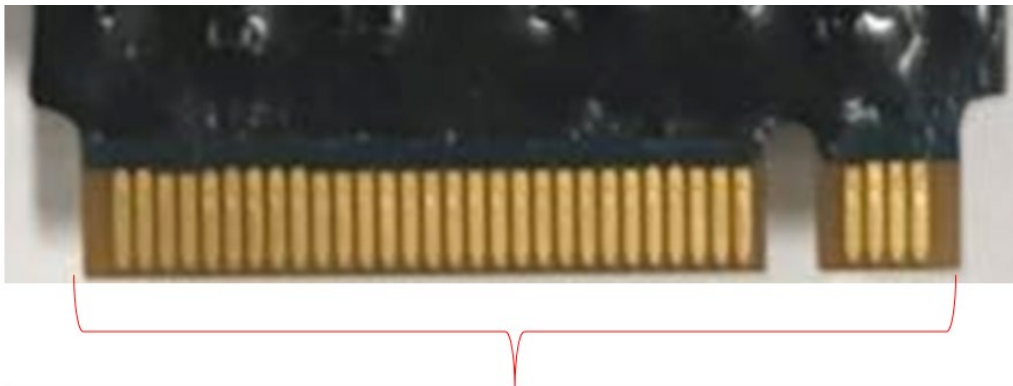


Figure 8 Ports description of 2.5" SATA products

For PCIe-based M.2 form factor TOEs (part numbers: NS561P500GCE7-1F and NS571P02T0CK7-1F), the design of mechanical dimension and connector pinout confirms to the industry standard M.2 form factor specification (PCIe M.2 Electromechanical Specification Rev1.0 Final), and the applicable ports and interfaces are:

PHYSICAL PORT	LOGICAL INTERFACE
PCIe M.2 Edge Card Input	Data input, Data output, Status output, Control input, and Power Input

Table 3 Specification of PCIe M.2 SSD module Cryptographic Module Physical Ports and Logical Interfaces



- PCIe M.2 (Pin1 ~ Pin75)
- Power input (3.3V and GND)
  - Plaintext data input/output
  - Status output (NVM commands)
  - Status output (Pin# 10, Toggle, High, Low to show device activity status)
  - Control input (NVM commands)
  - Control input (Pin# 50, PCIe Reset)
  - (Optionally) Control input (Secure Erase on Pin# 26, 48)
  - (Optionally) Control input (Write Protect on Pin# 24, 46)

Figure 9 Ports description of PCIe M.2 SSD module (NS561P500GCE7-1F and NS571P02T0CK7-1F)



For PCIe-based U.2 form factor TOE (part numbers: NS571P08TOCC0-1F), the design of mechanical dimension and connector pinout confirms to the industry standard U.2 form factor specification (Enterprise SSD Form Factor Version 1.0a SFF8639), and the applicable ports and interfaces are:

PHYSICAL PORT	LOGICAL INTERFACE
U.2 SFF8639 (P1~P15)	Power Input, Status Output, Control Input
U.2 SFF8639 (E1~E6)	Control Input
U.2 SFF8639 (E7~E39)	Data input, Data output, Status output, Control input
GPIO	Control input

Table 4 Specification of PCIe U.2 SSD module Cryptographic Module Physical Ports and Logical Interfaces

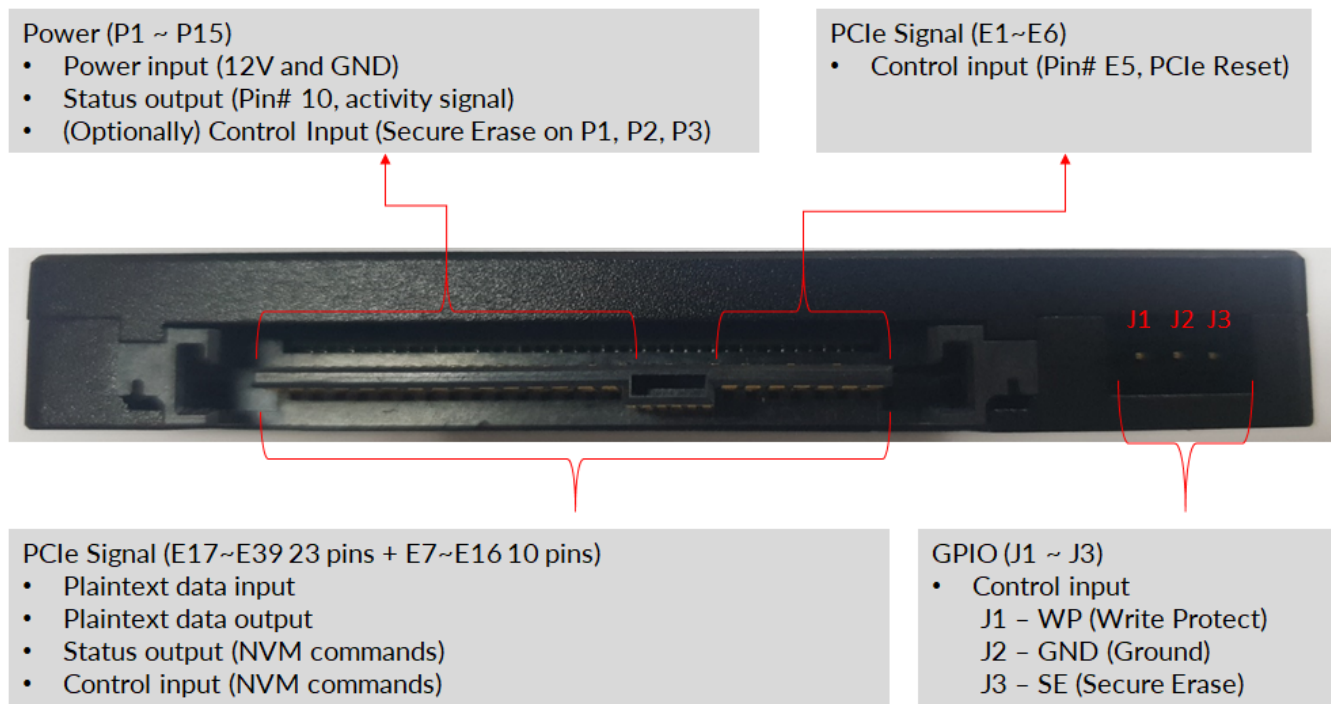


Figure 10 Ports description of PCIe U.2 SSD module (NS571P08TOCC0-1F)

## 5. TOE OPERATION PRIOR HOST KEY ACTIVATION

The TOE will be in Uninitialized State at Fresh Out of the Box. The administrator is required to complete initial Host Key activation before field deployment. Prior to initial Host Key activation, TOE responds to standard ATA commands normally as defined the ATA specification. In the Uninitialized State, the key chain for TOE is not completed, and all written data in Uninitialized state will be automatically erased at Host Key activation by establishing complete key chain.

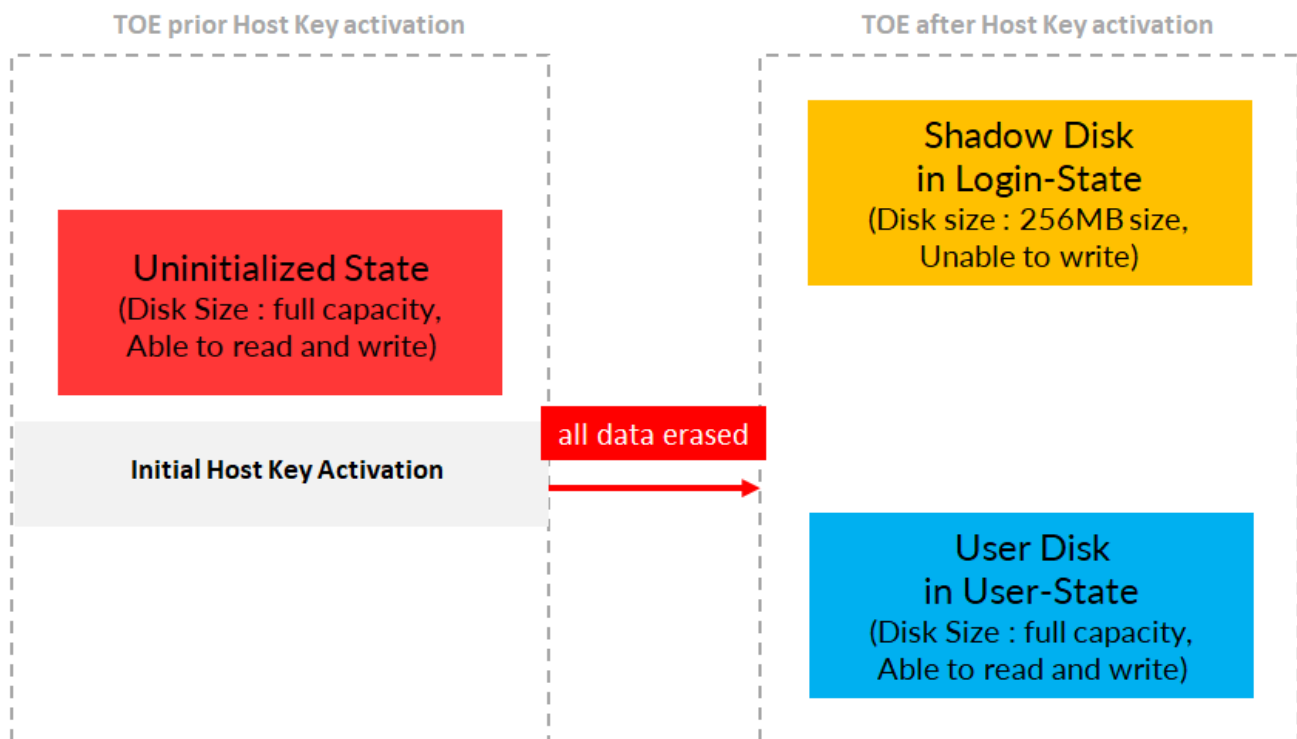


Figure 11 Simplified Diagram of TOE operation at security activation

## 6. POWER STATES

The TOE does not allow the administrators or users to manage or configure the Compliant power saving states. The TOE automatically enforces operation in ACPI device power states D0 and D3. Specifically, D0 is defined as the fully on, active state, and D3 (cold) is the state where the device is fully powered off. The TOE does not support any other power saving states.

From a power-on cycle, the TOE enters power state D0, and requires Host Key at Login State. When authentication completes successfully with the correct Host Key, TOE converts into User Disk. Only power state D0 allows to input Host Key to Shadow Disk and to access plaintext data in User Disk.

When power is removed from the TOE, the TOE enters power state D3 (cold), a fully powered-off condition. Since SSDs never receive warning of imminent power loss, the design of the TOE assures that there are no scenarios where an unexpected power loss can result in the TOE entering a non-compliant power state.

Operating system power control button will result in changing TOE state as below.

- “Log off”, “Switch User”, “Lock”, or “Restart” keeps supplying the power to the TOE, so the security state of TOE will NOT be changed.
- “Sleep”, “Hibernate”, or “Shut Down” removes the power supply to the TOE, so the security state of TOE will be changed to Login State automatically without user logout command.



## 7. ZEROIZE, IMMEDIATE KEY DESTRUCTION, AND MILITARY ERASE PROTOCOL

The TOE performs the zeroize operation that erases the wrapped DEK and other key materials at one of following conditions.

- When User or CO triggers hardware Secure Erase signal by connecting SE pin with nearby GND pin. Please see [4. PORTS AND LOGICAL INTERFACES](#)
- When User or CO sends Zeroize commands to TOE by using specified ATA/NVM command or using admin tool. Please see [24. ACCESS CONTROL POLICY](#)
- When the maximum number of failed attempt counts exceeded. Failed attempt counts is not configurable and fixed as 10.

The TOE design is based on single ASIC controller which includes built-in hardware AES encryption engine and controls all memory components directly. This architecture design allows ASIC controller initiate zeroize service without any delay factor to destroy key and key materials immediately via specified ATA/NVM command or GPIO signal input, regardless of ongoing operation such as garbage collection, wear-levelling, bad block management, or any other ATA command operation including TRIM. During progressing zeroize, TOE does not respond to any host command except activity signal output indicator. After completing zeroize process, TOE will appear to host in Uninitialized State with all user data erased.

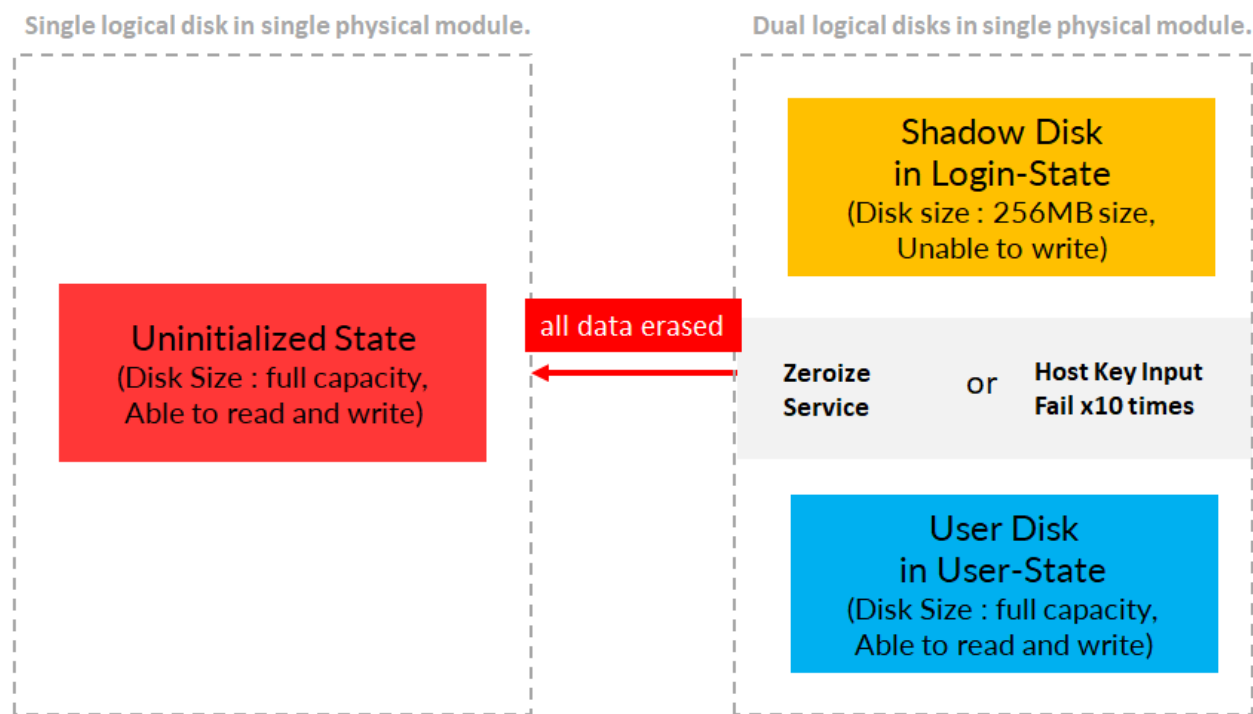


Figure 12 Simplified Diagram of TOE operation at zeroization

Additionally, the TOE supports various types of advanced military secure erase protocols as shown at Table 5 List of available Military Secure Erase protocols. This eases administrator to perform clean and purge storage disk as specified protocol automatically by itself without host PC equipment or control software. Any of listed secure erase protocols performs zeroize service first to destroy all keys and key materials prior to proceeding next steps. Processing time of each secure erase protocol varies as required step workload and disk raw capacity from several minutes to several hours. During performing military secure erase, the module shuts down all logical interfaces except transmitting output signal via activity signal pin, and keeps resuming erase process automatically even when power supply is interrupted until full process completion. Administrator is required to give power cycling to the module when erase protocol process is completed to make the module appear to host PC.

Secure Erase Protocol	STEP1	STEP2	STEP3	STEP4
Military Fast Erase	Erase only	-	-	-
DoD 5220 22-M NISPOM, Sup 1	Erase + Prog (0x53)	Erase + Prog (0xAC)	Erase + Prog (random)	-
RCC-TG IRIG 106-07	Erase + Prog (0x55)	Erase + Prog (0xAA)	Erase only	-
NSA/CSS 130-2	Erase + Prog (random)	Erase + Prog (random)	Erase + Prog (0xAA)	-
NISPOMSUP Chap 8, Sect. 8-501	Erase + Prog (0x66)	Erase + Prog (0x99)	Erase + Prog (random)	-
Army AR 380-19	Erase + Prog (rand)	Erase + Prog (0x65)	Erase + Prog (0x9A)	-
Navy NAVSO P-5239-26	Erase + Prog (0x65)	Erase + 2min delay	Erase + Prog (random)	Verify100%
Air Force AFSSI 5020	Erase + Prog (0x00)	Erase + Prog (0xFF)	Erase + Prog (random)	Verify10% + Erase + Prog (0x55)
NSA/CSS 9-12	Erase + Prog (0xAA)	Verify 0.1%	-	-
Gutmann Method	Erase + Prog (random)	STEP1 x Repeat 35 times	-	-

Table 5 List of available Military Secure Erase protocols

This advanced military erase is not covered by the cPP, and the scope of the evaluation does not include this function. This function is neither evaluated nor tested during TOE valuation.

## 8. KEY RECOVERY

The TOE contains no mechanism to allow export or recovery of keys or key materials.

## 9. PRODUCT IDENTIFICATION

It is important to verify that the product received from Novachips has not been tampered with or replaced with a similar but non-compliant product during shipment. Novachips is sending carrier tracking number and shipping document after arranging the shipment from factory. For additional fee, Novachips can ship the product using special carrier service such as Fedex Custom Critical services.

The administrator responsible for configuring the product prior to field deployment is required to ensure authenticity and integrity of the reviewed TOE as below.

- The main label of the TOE contains the product part number. Referring to the [10. PRODUCT PART NUMBER](#) section of this document, verify that the part number on the main label matches one of the part number list in the table, and also matches what was ordered from Novachips.
- Verify that the Firmware version (FW) printed on the main label matches the following: "NV.R1900\_1000"
- The main label contains a Common Criteria validation report number. Verify that the validation report number (VR#) matches the number listed on the CC certificate on the NIAP website.
- Use SATA or NVM Identify command, admin tool, or Novachips NCSMART utility to verify that TOE reports Firmware revision number NV.R1900\_1000.
- Inspect the TOE to verify that the product received matches the images in [3. TOE EVALUATED CONFIGURATION AND PICTURES](#).
- Inspect bending of enclosure, removal or disfiguration of TE label, or any scratches, gouges, scrapes, deformations on Urethane/Epoxy Coating as per section [26. PHYSICAL SECURITY](#).

## 10. PRODUCT PART NUMBER

The CC compliant part numbers are shown as below.

Part Number	Part number suffix option description
NS361P500GCCR-XY	<p><b>Option Field X (Hardware Secure Erase Protocol Setting)</b></p> <ul style="list-style-type: none"> <li>1 - Military Fast Erase (Default)</li> <li>2 - DoD 5220 22-M NISPOM, Sup 1</li> <li>3 - RCC-TG IRIG 106-07</li> <li>4 - NSA/CSS 130-2</li> <li>5 - NISPOMSUP Chap 8, Sect. 8-501</li> <li>6 - Army AR 380-19</li> <li>8 - Navy NAVSO P-5239-26</li> <li>A - Air Force AFSSI 5020</li> <li>B - NSA/CSS 9-12</li> <li>E - Gutmann Method</li> <li>F - Crypto Erase</li> </ul> <p><b>Option Field Y (Hardware Secure Erase Pin Location Setting)</b></p> <ul style="list-style-type: none"> <li>F - Hardware Secure Erase pin is not allocated (Default)</li> <li>1 - SATA Pin1 is allocated for Hardware Secure Erase</li> <li>2 - SATA Pin2 is allocated for Hardware Secure Erase</li> <li>3 - SATA Pin3 is allocated for Hardware Secure Erase</li> <li>B - SATA Pin11 is allocated for Hardware Secure Erase</li> <li>D - SATA Pin13 is allocated for Hardware Secure Erase</li> <li>E - SATA Pin14 is allocated for Hardware Secure Erase</li> </ul>
NS371P02TOCC1-XY	Same option as NS361P500GCCR-1F
NS371P04TOCC1-XY	Same option as NS361P500GCCR-1F
NS371P10TOCC0-XY	Same option as NS361P500GCCR-1F
NS561P500GCE7-XY	<p><b>Option Field X (Hardware Secure Erase Protocol Setting)</b></p> <p>Same option as NS361P500GCCR-XY</p> <p><b>Option Field Y (Hardware Secure Erase Pin Location Setting)</b></p> <ul style="list-style-type: none"> <li>F - Hardware trigger is not allocated (Default)</li> <li>1 - M.2 (M-Keying) Pin 24 (WP) and Pin 26 (SE) are allocated.</li> <li>2 - M.2 (M-Keying) Pin 46 (WP) and Pin 48 (SE) are allocated.</li> </ul>
NS571P02TOCK7-XY	Same option as NS561P500GCE7-XY
NS571P08TOCC0-XY	<p><b>Option Field X (Hardware Secure Erase Protocol Setting)</b></p> <p>Same option as NS361P500GCCR-XY</p> <p><b>Option Field Y (Hardware Secure Erase Pin Location Setting)</b></p> <ul style="list-style-type: none"> <li>F - Hardware trigger is not allocated (Default)</li> <li>1 - SFF8639 P1 is allocated for Hardware Secure Erase.</li> <li>2 - SFF8639 P2 is allocated for Hardware Secure Erase.</li> <li>3 - SFF8639 P3 is allocated for Hardware Secure Erase.</li> </ul>

Table 6 Product part number and available suffix option

## 11. SCOPE OF EVALUATION

The TOE was evaluated to verify the security functional requirement specified in the Security Target document. The TOE does not depend on a TPM or TCG Opal specification to provide security. Instead, the TOE supports Host Key encryption mode which conforms to the requirements of the Collaborative Protection Profile for Full Drive Encryption – Encryption Engine, v.2.0 dated January 2, 2019 and the Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v 2.0 dated January 2, 2019.

TOE supports CC-compliant mode as following table, and no other key management modes were evaluated during the course of the CC-evaluation.

mode	state	Description
<b>Security Mode Disabled</b> (Fresh out of box state)	<b>Uninitialized State</b>	TOE is NOT activated Host Key encryption. Any user can access full range of unprotected area. Security is not claimed at this state.
<b>Security Mode Enabled</b> (Compliant modes of operation)	<b>Crypto Officer State</b>	Crypto Officer is activating Host Key encryption by admin tool, or other 3 <sup>rd</sup> party tool after verifying physical security of SSD module.
	<b>Self-Test State</b>	At powering-on, TOE is running self-test of each security functions. TOE is not available to provide any service to host until passing all self-test items. If any item fails during self test, TOE will go Error State.
	<b>Login State</b>	TOE is waiting for Host Key input from host by appearing to host as 256MB Shadow Disk. This 256MB capacity is used only for indicator, so the user can't write any data to this 256MB capacity.
	<b>User State</b>	With DEK loaded after verifying correct Host Key input, TOE is available to access to protected area by appearing full capacity User Disk. Now user can access protected area.
<b>Exception mode</b> (TOE is out of service to any host command except activity signal pin output signal.)	<b>Erase State</b>	TOE is progressing zeroize process. TOE is out of service until zeroize process completion. It may require manual power cycle to make TOE re-appear to the host system. In Erase State, TOE outputs repeating pattern 01010101 in 0.1 ~ 2.0 Hz via Activity signal pin. (0 – signal low, 1 – signal high)
	<b>Error State</b>	TOE is out of service. It requires manual process of power cycle, or to be shipped back to manufacturer, if TOE remains in Error State after several times of manual power cycling. In Error State, TOE outputs repeating pattern 01010000 in 0.1 ~ 2.0 Hz via Activity signal pin. (0 – signal low, 1 – signal high)

Table 7 CC Compliant modes

## 12. OPERATING ENVIRONMENT

SATA-based Scalar P-series SSD is compliant and compatible with the industry standard Serial ATA 3.1 specification and conforms to the ATA-8 specification and command set. Scalar P-series SSD will function correctly in all host system that include a standard SATA interface and are compliant to the SATA and ATA8 specification.

PCIe-based Express P-series SSD is compliant and compatible with the industrial standard PCIe Base Specification Rev 2.0 and conforms to the NVMe specification and command set. Express P-series SSD will function correctly in all host system that include a standard PCIe interface and are compliant to the PCIe and NVMe specification.

## 13. OPERATING ENVIRONMENT ASSUMPTION AND REQUIREMENTS

The guidance for the TOE makes the following assumption:

- The TOE encrypts all user data with AES-256 XTS. There are no configuration options or support for different key sizes.
- The TOE is not dependent on the operational environment to perform DEK purging or memory clear operations. All operations that perform clear and purge operations, once triggered, operate independently from the host SATA or PCIe interface.
- The TOE does not support TCG Opal, or require a trusted platform module for secure operation.
- The TOE is located in secure environment during initial secure configuration.
- The administrator or CO connects TOE to host system that includes electrical and software interface support necessary to implement an industry standard SATA interface as defined by Serial ATA specification, revision 3.1 (for Scalar P-series), or PCIe Base specification revision 2.0 (for Express P-series).
- The TOE does not interfere with or change the normal platform identification and authentication functionality such as the operating system login.
- When configuring the TOE by using custom designed utility, administrator or CO shall verify that the custom utility configures the TOE to the same configuration described by the ATA / NVM command guidance document.
- The administrator and system designer shall implement application techniques, safeguards, and/or procedures to assure that power is removed from the TOE, state D3 (cold), when the host system is left unattended. On removal of power, the TOE purges the DEK and enters a full-off state in less than 20 milliseconds.
- The administrator shall verify that TOE users are trained on how to power-off the host system and TOE per section [6. POWER STATES](#).
- The TOE accepts passwords length minimum 10 bytes up to 64 bytes. The administrator shall enforce complexity to provide suitable security strength.

- After enabling security mode of the TOE, the administrator will verify that the TOE is operating in CC-compliant Security Mode Enabled states. Please see ATA / NVM command guidance document to determine the SATA or NVM commands required to verify this information.
- The TOE is compliant to the AA and EE protection profiles. It is assumed that the external interface providing the password to the AA portion of the TOE, is in close enough proximity to the TOE during operation that a threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
- The administrator or CO understands that Novachips supplies the TOE in Security Mode Disabled (or Uninitialized State). The TOE contains no data when delivered by Novachips. The administrator or CO shall not store information on the TOE until after completing the initial security configuration procedure.
- The administrator or CO shall implement methods and procedures to assure that the host system is free of malware that could interfere with the correct operation and power-off procedures of the host system connected to the TOE.
- The administrator or CO is responsible for completing the initial secure configuration of the TOE and for generating Host Key values that meet strength requirements of the AA and EE protection profiles.
- The administrator CO shall train any users involved in the provisioning of the TOE in the methods and procedures to properly handle, store, and secure the Host Key values. For example, the Host Key value should be stored separately from the TOE.

## 14. UNATTENDED OPERATION

The TOE is compliant to the ATA specification and NVM specification. The ATA and NVM specification defines a set of commands the host system uses to write/read data to/from the TOE. Since the TOE cannot independently initiate communication with the host, the TOE has no mechanism to determine when a host system is unattended, or for example, in a lock-screen or sleep state. For this reason, the CO and system designers must implement host system application techniques, safeguards, and/or procedures that remove power or run logout command from the TOE whenever the host platform is left unattended. Upon removal of power or logout, the TOE purges the DEK and moves to a complete power-off state in less than 20 milliseconds.

## 15. STATE OF TOE AT FRESH OUT OF BOX

For simplicity of initial setup at customer site, TOE ships from Novachips fully erased and in Security Mode Disabled (or Uninitialized State). The administrator or CO, after taking possession of factory delivered TOEs, must perform initial secure configuration of each TOE to place the TOE into Security Mode Enabled (or Login State) prior to deployment.

## 16. SOFTWARE UTILITY

The initial secure configuration of the TOE can be accomplished by using GUI or CLI-based admin tool. When using admin tool for configuration, connect the TOE into a host computer using standard SATA/Power cables or standard M.2/U.2 slots, then launch the admin tool to begin configuration.

Windows admin tool utility runs on standard Windows OS version including but not limited to Windows 8.1, Windows 10, and Windows 11. After GUI-based admin tool opens, it is necessary to press “Scan”. Use the cursor to select to a specific TOE and press each function buttons to perform the service from selected TOE.

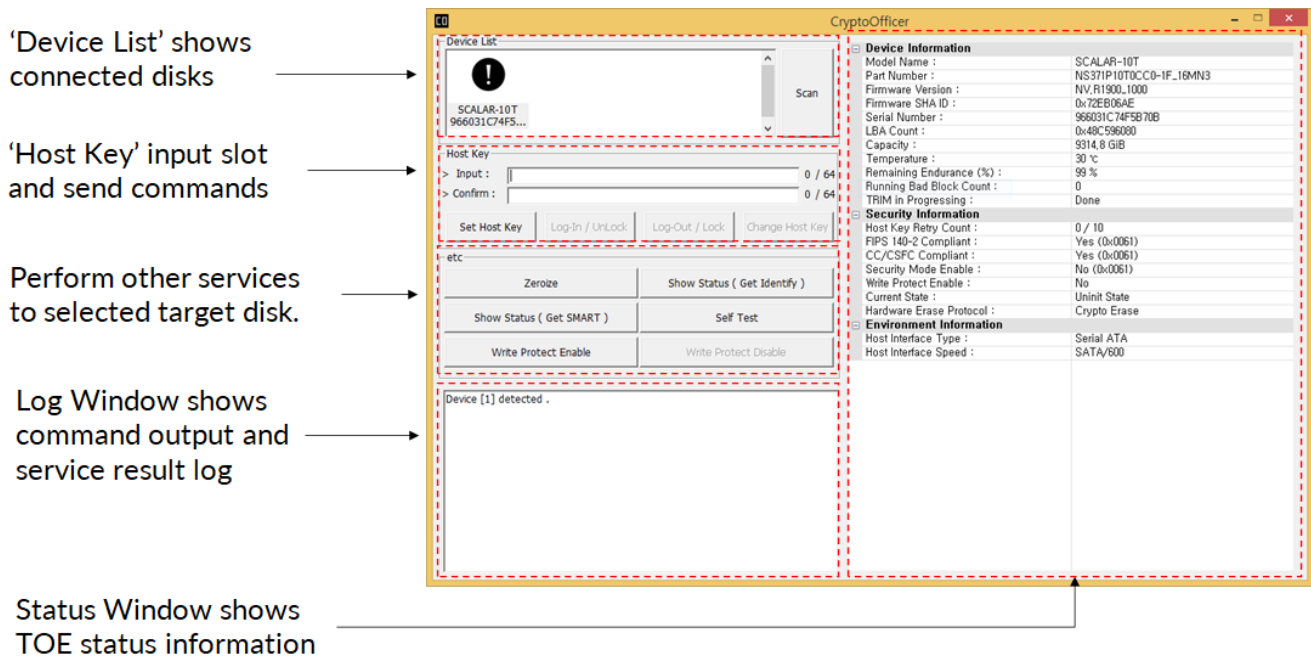


Figure 13 Screenshot of admin tool

For each function buttons, they can be also performed by using non-proprietary open-source software tool such as hdparm and nvme-cli. Details of command syntax and parameters are described in ATA/NVM command guidance document.



## 17. COMMAND INTERFACE

The TOE supports two logical command interfaces to activate security as below.

- Vendor-specific ATA or NVM command  
: Host Key is transported from user to TOE via vendor-specific ATA or NVM command. Additional ATA/NVM command guidance document is available to provide detailed register-level information describing how to use security commands/services supported by the TOE. User or admin can create their own version of security utility by using this document as a reference manual.
- ATA SECURITY SET PASSWORD command  
: Not only vendor-specific command, Host Key is also transported from user to TOE via standard ATA password command which is widely used in SATA HDDs. This command is useful for the user of SATA-based TOE who wants to use BIOS password or legacy system ATA password as Host Key. .

When administrator or CO activates security in BIOS or by using other 3<sup>rd</sup> party software via ATA SECURITY SET PASSWORD command, it is important to preserve same host environment in field deployment or end-user environment, because each system can use different padding policy or character format. It is needed to know that ATA security password is expanded from original ATA command specification to send up to 64 bytes size password per cPP FDE requirement as shown at ATA/NVM command Guidance document.

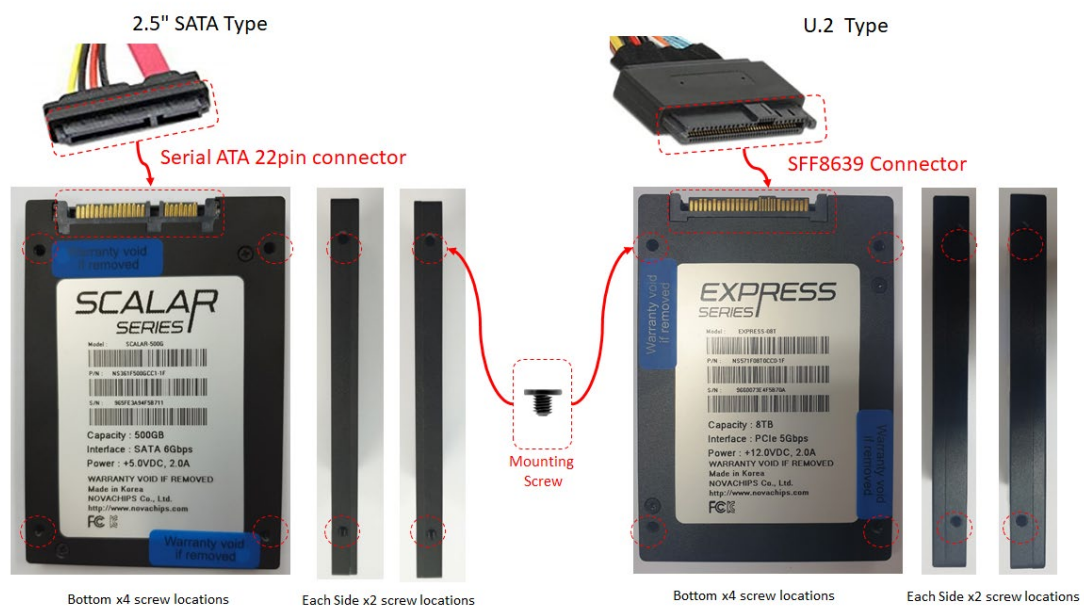
## 18. CHANGING THE PASSWORD (HOST KEY) AFTER CONFIGURATION

The TOE verifies that incoming Host Key is identical with the one filled during the initial secure configuration procedure. In order to change to a new Host Key, original Host Key is required to fill in first to enter User State in which authorized user can change to new Host Key by using “Change Host Key” service. When “Change Host Key” service performs successfully in User State, the TOE reappears to host in Login State. Now only new Host Key is valid for authentication, and old Host Key is neither usable nor traceable. When user changes Host Key in BIOS or by using other 3<sup>rd</sup> party software, it is important to preserve same host environment at next use, because each system can apply different padding policy.

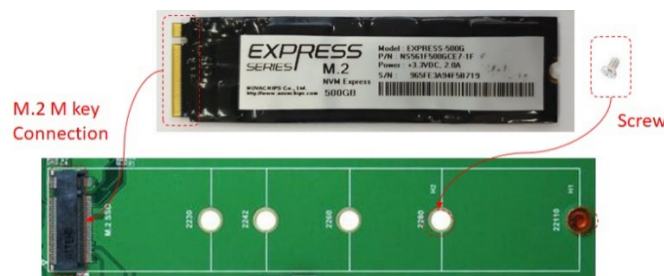
## 19. INSTALLATION OF TOE

Novachips recommends to follow industry standard specification of 2.5inch SATA, PCIe M.2 or NVMe U.2 (SFF-8639), and below is standard example of installing TOE hardware module into standard computing system.

- Configure host connector and prepare screws per TOE hardware form factor type.
  1. 2.5" SATA and U.2 SFF-8639 SSD is using M3 standard screws (height less than 3.5mm) for four mounting screw locations on bottom side and two mounting screw locations along each side edges.



2. PCIe M.2 SSD is using CM2x3-3.3 screw for single mounting screw location at the opposite edge from host connector. Screw type and size can vary per host design.



- Shut down host computer and remove the power cable or battery power source.
- Discharge residual power and ground yourself.
- Disassemble the computing system and find corresponding host receptacle or host cable per TOE hardware physical ports and size as shown at [4. PORTS AND LOGICAL INTERFACE](#).

- Connect TOE with host cable, or insert TOE into host receptacle slot carefully.
- Tighten the fastening screws on the side of the unit securely per TOE.
- Assemble the computing system and powering-on the system to configure TOE.

Novachips SSD utilized ESD production circuitry to mitigate damage caused by severe electro-static discharge, and Novachips recommends to follow industry standard ESD precautions and procedures when handling TOEs.

As an ordering option, the TOE is available to support Secure Erase pin assignment in reserved SATA, M.2, or U.2 pinouts as specified in section [10. PRODUCT PART NUMBER](#). In case of using industry standard SATA or M.2 connectors with those optional products, it is important to isolate those pins not to trigger SE procedure unintentionally.

## 20. CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS

CSP & KEY	Description/Usage	Storage
<b>DRBG Internal State (V, C)</b>	<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 with complying SP800-90B.</p> <p>Random numbers generated by the NDRNG are used as seeding values for the FIPS Approved Deterministic Random Bit Generator (SP800-90A HASH DRBG). At each power cycling, DRBG Internal State (V, C) values are newly generated by re-instantiation process without storing them to non-volatile memory.</p> <ul style="list-style-type: none"> <li>• Generation: Internally using the SP800-90 HASH DRBG</li> <li>• Entry: N/A</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize</li> </ul> <p>Continuous RNG tests are performed on the outputs of the NDRNG and on the outputs of the Approved SP800-90A DRBG. <i>Note: the minimum number of bits of entropy generated by the module for use in key generation is 256.</i></p>	SRAM
<b>IV</b>	<p>This value is generated from DRBG and truncated to 128bits to use as input for Key Wrapping and Key Encryption.</p> <ul style="list-style-type: none"> <li>• Generation: DRBG</li> <li>• Entry: N/A</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize</li> </ul>	SRAM/ NAND
<b>KEK</b>	<p>SSD module uses an AES 256-bit encryption to protect key materials. The AES 256-bit key is generated by using approved DRBG.</p> <ul style="list-style-type: none"> <li>• Generation: DRBG</li> <li>• Entry: N/A</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize</li> </ul>	SRAM/ NAND
<b>Salt</b>	<p>This 256bit value is generated by DRBG to as input for PBKDF, and protected by Key Encryption.</p> <ul style="list-style-type: none"> <li>• Generation: DRBG</li> <li>• Entry: N/A</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize</li> </ul>	SRAM/ NAND
<b>Host Key (password)</b>	<p>User sets minimum of 10 characters and maximum 64 characters. Single character can be any 8-bit value including upper case, lower case, numbers and other special characters.</p>	SRAM

	<p>SSD module performs Password-based Key Derivation Functions in accordance with specified cryptographic algorithm HMAC-SHA-256 with 1000 iterations to make output 256bit Key Wrap Key.</p> <p>SSD module supports only one Host Key code.</p> <ul style="list-style-type: none"> <li>• Generation: Externally generated by CO/User</li> <li>• Entry: Directly entered from the host in plaintext</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize</li> </ul>	
<b>KWK</b>	<p>KWK is generated from approved PBKDF function with input of 512bit Host Key and 256bit salt. This KWK is used to unwrap DEK after verifying user authentication by comparing with hashed 384 bits of KWK output.</p> <ul style="list-style-type: none"> <li>• Generation: Externally generated by CO/User</li> <li>• Entry: Directly entered from host in plaintext</li> <li>• Output: N/A</li> <li>• Zeroization: Set Host Key, Zeroize</li> </ul>	SRAM
<b>KWK hashed value</b>	<p>This 384bits of KWK hashed value is used to verify user authentication.</p> <ul style="list-style-type: none"> <li>• Generation:</li> <li>• Entry: N/A</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize, Change Host Key</li> </ul>	SRAM/ NAND
<b>DEK</b>	<p>SSD module uses two AES 256-bit keys for XTS mode operation to encrypt/decrypt User Disk data. The AES 256-bit keys are generated by approved DRBG, and protected by KWK.</p> <ul style="list-style-type: none"> <li>• Generation: DRBG</li> <li>• Entry: N/A</li> <li>• Output: N/A</li> <li>• Zeroization: Zeroize</li> </ul>	SRAM/ NAND
<b>Public Key hashed value</b>	<p>This 384bits of public key hashed output is hard-coded and used for Root of Trusted Update.</p> <ul style="list-style-type: none"> <li>• Generation: Externally generated by manufacturer.</li> <li>• Entry: Directly entered via Fuse pin and JTAG by manufacturer.</li> <li>• Output: N/A</li> <li>• Zeroization: N/A</li> </ul>	SRAM/ FUSEBOX

Table 8 Critical Security Parameters

## 21. ROLES

The TOE supports role-based authentication for a Crypto Officer and a single user as below. The TOE does not support multiple concurrent roles. When changing from one role to another, the characteristics and capabilities of the new role replace the capabilities of the previous role.

ROLE	Role Description	AUTHENTICATION	
		TYPE	DATA
CO (Crypto Officer)	<p>The CO or administrator responsible for configuring the product prior to field deployment is required to ensure authenticity and integrity of the reviewed TOE. TOE shall be provided to CO for first time use, and CO shall be in charge of below procedures.</p> <ul style="list-style-type: none"> <li>• CO inspects the module as per section "<a href="#">PHYSICAL SECURITY POLICY</a>".</li> <li>• CO initializes and activates the CC Approved Mode of Operation by typing in a unique Host Key password for initial configuration.</li> <li>• 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.</li> </ul>	Role-based	PIN
User	<p>The TOE shall be provided to the User after Crypto Officer state, and the User shall follow rules set forth in this guidance document.</p> <ul style="list-style-type: none"> <li>• The User shall change the initial Host Key password to a new Host Key password after taking ownership of TOE from CO. The User does not need to change this initial Host Key password when the private user is performing the roles of CO and User together.</li> <li>• The User shall contact Crypto Officer when SSD is in Error State.</li> </ul>	Role-based	PIN

*Table 9 Roles and Required Identification and Authentication*

## 22. HOST KEY FAILED ATTEMPTS PENALTY

Authentication Method	STRENGTH OF MECHANISM	Probability
<b>Password (Host Key) based authentication</b>	<p>The probability of guessing a password (Host Key) in a single attempt with a 10 characters password is <math>1/2^{80}</math> in a single random attempt, considering single byte is <math>2^8</math> and 10 bytes length is total <math>(2^8)^{10}</math> different possible input. This probability is less than authentication strength requirements <math>1/1,000,000</math>.</p> <p>To protect SSD from brute-force attack, module implements a Key Retry count or current password fail count ("N"). The Key Retry count or current password fail count will increase, whenever Host Key (password) 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. Key Retry count is reset to zero when correct key input is verified. Hence, in a one-minute period, the probability that a random attempt will succeed, or false acceptance will occur, is <math>10/(2^{80})</math> which is less than 1 in 100,000.</p>	<p>Minimum PIN length is 10 bytes with a maximum length of 64 bytes, and Key Retry count is persistent during power-cycle.</p>

*Table 10 Strength of Authentication Mechanisms*

## 23. FIRMWARE UPDATE

The TOE supports a service to update the internal firmware after an authentication to verify the digital signature of the new firmware. The signature validation process verifies that the new firmware was signed by and originated from Novachips. The process uses ECDSA with a P-384 prime curve. The TOE performs signature verification before accepting new firmware, and firmware update tool is only single executable file, NCMPTool.exe.

Firmware update tool is required to run as admin authority mode in authorized Windows OS condition. When update tool is turned on, update tool shows "Ready" message, and click "Rescan Disk" to mount compliant module. Then target modules will show as "Connected" status.



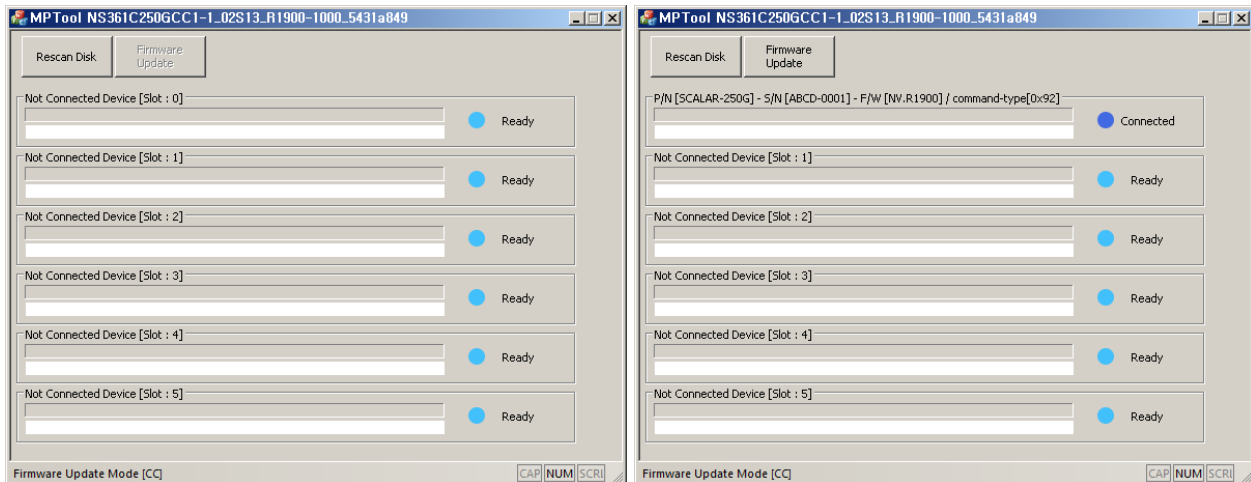


Figure 14 Firmware Update Tool Screenshot : Ready (Left) and Connected (Right)

After confirming target module information, “Firmware Update” button can be clicked to initiate firmware update process. Firmware update process will be completed within several seconds until showing “firmware updated” log message. After firmware update process completion, TOE is required to power-off, and it operates with updated firmware since next powering-on. If firmware update process is failed, then the tool shows “firmware update failed” message with error code at status text.

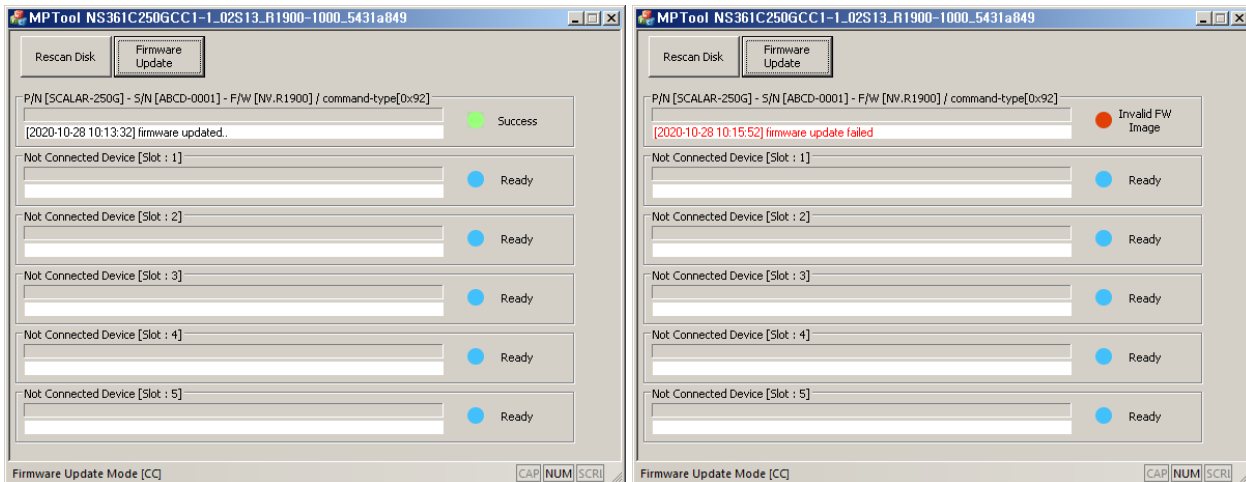


Figure 15 Firmware Update Tool Result Screenshot : Success (Left) and Failed (Right)

Each error message stands for below failed situation.

- **Backward update error:** Backward firmware update is not allowed to comply FPT\_RBP\_EXT.1 Rollback Protection from cPP FDE-EE. Firmware update can be proceeded only to newer firmware version which is using higher numbering than older version. In case of attempting backward firmware update to lower numbering version, update tool shows error message code such as “Backward update error”.
- **Invalid FW image:** TOE proceeds firmware update process only after comparing hash value of public key and passing firmware image digital signature verification. Any error or failure comes out during the process, the tool shows “Invalid FW Image” message.
- **Not user state:** Since completing key establishment via initial security activation, TOE supports firmware update service only in User State, and will show “Not User State” message, if firmware update process is requested in other state.

Novachips provides firmware update tool to customers via Novachips support site with a unique user name and password. This support site is managed by Novachips directly. Please contact your Novachips sales representative to have a support site login name and password generated.

## 24. 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, W = Write, Z = Zeroize, N/A = Not applicable,)

Service	Description	CO	User	U/A	Type of Access	Cryptographic Keys and CSPs
<b>Write Data to User Disk</b>	Receive plaintext data from host, outside of the cryptographic boundary, AES encrypt data and program into secured range of internal memory.	○	○		R	DEK
<b>Read Data from User Disk</b>	AES decrypt data from secured range of internal memory. Output plaintext to host, outside of the cryptographic boundary.	○	○		R	DEK
<b>Set Host Key (PIN)</b>	Set Initial Host Key (PIN).	○	○		W W W W W	IV KEK Salt KWK Hashed DEK
<b>Change Host Key (PIN)</b>	Change Host Key (PIN).	○	○		R W	Salt KWK Hashed
<b>Login/Unlock</b>	Unlock secured range of internal memory.	○	○		R R R R	IV KEK Salt KWK Hashed
<b>Logout/Lock</b>	Lock-up secured range of internal memory.	○	○	○	N/A	N/A
<b>Show Status</b>	Status Outputs. (ATA command Identify Device and other status information)	○	○	○	N/A	N/A
<b>Self-Test</b>	Module automatically performs required self-tests of the module after power-on.	○	○	○	N/A	N/A
<b>Set Write Protect<sup>1</sup></b>	Set the device to read-only mode by one of below methods. <ul style="list-style-type: none"> <li>ATA or NVM command</li> <li>GPIO External trigger</li> </ul>	○	○	○	N/A	N/A
<b>Zeroize</b>	Destroy all CSPs. This service can be triggered by one of below methods. <ul style="list-style-type: none"> <li>ATA standard command (SATA)<sup>2</sup></li> <li>NVM admin command (PCIe)<sup>3</sup></li> <li>GPIO External trigger</li> </ul>	○	○	○	Z Z Z Z Z	IV KEK Salt KWK Hashed DEK
<b>Trusted Update</b>	Update firmware image	○	○		R	Public Key Hashed

Table 11 Roles, Services, CSPs, Types of Access

<sup>1</sup> This Write Protect function is not covered by the cPP, and the scope of the evaluation does not include this function. This function is neither evaluated nor tested during TOE valuation. Please see ATA and NVM Command Guidance file for the operating details and commands guidance of this function.

<sup>2</sup> CRYPTO SCRAMBLE EXT (B4h/0011h) or SECURITY ERASE UNIT (F4h). The operator can send this command outside the scope of the boundary.

<sup>3</sup> NVM admin command (CDW0\_07:00b - 81h / CDW10\_15:08b - C0h / CDW10\_23:16b - FDh). The operator can send this command outside the scope of the boundary.

## 25. ALGORITHMS

### APPROVED ALGORITHMS

CAVP CERT	ALGORITHM	STANDARD	MODE/METHOD	KEY LENGTHS, CURVES, OR MODULUS	USE
AES 3962	AES	FIPS 197 SP 800-38A	AES ECB AES CBC	256	Prerequisite only for AES XTS, Key Encryption, Key Wrapping
C448	AES	FIPS 197 SP 800-38E	XTS	256	User Data Encryption/ Decryption
Vendor Affirmed	CKG	SP800-133			Cryptographic Key Generation
C463	DRBG	SP 800-90A	HASH_DRBG SHA-256		Deterministic Random Bit Generation
C411	SHS	FIPS 180-4	SHA-256		Prerequisite only for DRBG, HMAC
A897	HMAC	FIPS 198-1	SHA-256		Prerequisite only for PBKDF
A897	PBKDF	SP800-132	HMAC SHA-256		Option 2a for protecting DEK
A897	Key Wrap	SP800-38F	AES CBC	256	Key protection
A897	SHS	FIPS 180-4	SHA-384		Message Digest, Digital Signature
A897	ECDSA	FIPS 186-4	P-384	384	Trusted update

Table 12 Table of Approved Algorithms

### ALLOWED ALGORITHMS

ALGORITHM	CAVEAT	USE
NDRNG	Only used for generating seed materials for the Approved HASH_DRBG. Minimum security strength is 256 bits, and SP800-90B compliant	Non-deterministic Random Number Generator

Table 13 Table of Allowed Algorithms

## 26. PHYSICAL SECURITY

2.5" SSD is covered by CNC/Aluminum enclosure and enclosure screws are sealed by tamper evident labels. Tamper evident labels are applied at manufacturing. 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.

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"> <li>• Bending of enclosure</li> <li>• Removal of TE label</li> </ul>
Tamper Evident Seals	On initial receipt of the device and in accordance with Crypto Officer organizational security policy. It is recommended to inspect the seals once a year.	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"> <li>• Peeling will result in a residue on the enclosure and/or an inability to reapply the label</li> <li>• Solvent attacks will result in the TE label being physically disfigured</li> <li>• Temperature attacks will result in the TE label being disfigured</li> </ul>
Urethane/Epoxy Coating	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.	Inspect for scratches, gouges, scrapes, deformations, and any other suspicious signs of malice and tampering. If any evidence of tampering exists, the Crypto Officer is required to cease use of the cryptographic module immediately.

Table 14 Inspection/Testing of Physical Security Mechanisms



Figure 16 Enclosure and Tamper-evident label locations



Figure 17 Tamper-evident label detached



*Figure 18 Urethane/Epoxy Coating*

---

## 27. SERVICE READY ONLY AFTER PASSING SELF-TEST AND ERROR STATE

The following specifies self-test which the TOE module shall operate:

- The module supports the following power-up self-tests:
  - Firmware image verified by SHA-384 hash tag
  - SHA-256 KAT
  - HMAC SHA-256
  - PBKDF2
  - Key Wrap Key
  - 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
  - SHA-384 KAT
  - ECDSA (P-384)
- 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 inhibits all data output during self-tests.
- If the module fails any power-up self-tests or conditional tests specified in this section, 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 01010000 repeating pattern in 0.1 ~ 2.0 Hz via Activity signal pin. (0 – signal low, 1 – signal high). Activity signal pin. (SATA P11 or M.2 Pin#10)
- If the module passed all self-test items, then the module will appear to the host and it is available to start providing service listed in section [ACCESS CONTROL POLICY](#).



## 28. ELECTROMAGNETIC INTERFACE CAPABILITY

The TOE successfully completed EMI/EMC testing and conforms to the EMI/EMC requirement specified by FCC Part 15B Class B.

## 29. MITIGATION OF OTHER ATTACKS POLICY

The TOE does not mitigate attacks outside of the scope of CC.

## 30. INITIALIZATION AND GUIDANCE SUMMARY

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

- The module meets security target only when the module is enabled Security Mode under operating environment and assumption as described in section [13. OPERATING ENVIRONMENT ASSUMPTION AND REQUIREMENTS](#).
- 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 Security Mode by executing service buttons with admin tool in Windows or by running equivalent commands with non-proprietary software such as hdparm and nvme-cli in Linux as following the next procedures:
  1. Inspect module as per section [26. PHYSICAL SECURITY](#).
  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 button “**Show Status**” or run equivalent **Identify** command. Confirm the module Part Number and Firmware Version is an approved configuration as listed in section “[3. TOE EVALUATED CONFIGURATION AND PICTURES](#)”.
  5. Execute service button “**Set Host Key (PIN)**”, or run equivalent **Activate** command. This is a one-time operation. TOE does not accept Host Key password length smaller than 10 characters.
  6. Module will automatically reboot, and run power-up self-tests again.
    - a. 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 button “**Show Status**” or run equivalent **Identify** command to verify module status specifies Security Mode Enabled. See below for more information on Security Mode indicator.
  9. Module is now in the Security Mode Enabled.
- The Security Mode indicator can be obtained by executing “**Show Status**” or by running **Identify** command. For SATA, CC descriptor information can be found at Word **137** address from returned data, and expected output is 0x0063 (CC-compliant, Security Enabled, Unlocked) or 0x0067 (CC-compliant, Security Enabled, Locked). For PCIe / NVMe, CC descriptor information will be shown at **Byte 3092~3093** address from returned data, and expected output is 0x0063 (CC-compliant, Security Enabled, Unlocked) or 0x0067 (CC-compliant, Security Enabled, Locked).

TOE developer Original Part No.	Show Status / Identify command	CC Descriptor Address	CC Approved Mode Expected Indicator
NS361P500GCCR-1F	ATA Identify Device	Word 137	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)
NS371P02T0CC1-1F	ATA Identify Device	Word 137	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)
NS371P04T0CC1-1F	ATA Identify Device	Word 137	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)
NS371P10T0CC0-1F	ATA Identify Device	Word 137	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)
NS561P500GCE7-1F	NVM admin Identify	Byte 3092~3093	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)
NS571P02T0CK7-1F	NVM admin Identify	Byte 3092~3093	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)
NS571P08T0CC0-1F	NVM admin Identify	Byte 3092~3093	0x0063 (Security Enabled, Unlocked) 0x0067 (Security Enabled, Locked)

Table 15 TOE CC Descriptor Indicator

- At Login State (Security Enabled, Locked), the authentication is always required.
- The module changes automatically by itself from Login State to User State (Security Enabled, Unlocked) by executing “**Log-In / Unlock**” button or by running **Login** command successfully with loading correct Host Key (password).
- Any invalid attempts to authenticate to the module will result in status output “Password Failure” (Fail=1h). If the incorrect Host Key password input is counted over than 10 (Non-volatile count), then TOE will delete all keys and key materials, zeroize all user data, and change its state to Uninitialized state. Please see details at [HOST KEY FAILED ATTEMPTS PENALTY](#).

- The module does not support manual key entry or any other type of key entry/output. The TOE uses a hardware-based NDRNG and a DRBG algorithm to self-generate a random DEK. The CO or user does not require to configure DRBG.
- The module supports zeroization to destroy all critical security parameters via specified **Zeroize** commands or direct GPIO signal input.
- 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.

## Appendix A: Key Materials

CSP & KEY	Description/Usage	Generation	Entry	Output	Zeroization	Storage
DRBG Internal State	Values of V and C of HASH DRBG mechanism	Internally using the SP800-90 HASH DRBG	N/A	N/A	N/A	SRAM
IV	Initialization vector for Key Encryption & Key Wrapping	DRBG	N/A	N/A	Zeroize	SRAM/ NAND
KEK	Protecting key materials	DRBG	N/A	N/A	Zeroize	SRAM/ NAND
Salt	Input for PBKDF	DRBG	N/A	N/A	Zeroize	SRAM/ NAND
Host Key (PIN)	10 ~ 64 bytes PIN. User authentication.	Externally generated by CO/User	Directly entered from host in plaintext	N/A	N/A	SRAM
KWK	Protecting DEK	PBKDF	N/A	N/A	N/A	SRAM
KWK Hashed	User Authentication	SHA	N/A	N/A	Zeroize	SRAM/ NAND
DEK	AES XTS 256-bit use to encrypt/decrypt data to/from secure range of internal memory.	DRBG	N/A	N/A	Zeroize	SRAM/ NAND
Public Key Hashed	Root Trusted Update to verify public key authentication.	In factory	N/A	N/A	N/A	SRAM/ FUSE

Table 16 List of Critical Security Parameters

## Appendix B: Acronyms

TERM	Description
SSD	Solid State Drive
MCU	Microcontroller Unit
2.5"	2.5 inch disk form factor
LBA	Logical Block Address
TOE	Target Of Evaluation
ST	Security Target
FDE	Full Disk Encryption
cPP	Collaborative Protection Profile
M.2	Computer Expansion Card Disk form factor
GUI	Graphic User Interface
CLI	Command Line Interface
AES	Advanced Encryption Standard (FIPS-197)
IV	Initialization Vector
ECB	Electronic Code Book
CBC	Cipher Block Chaining
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher
GPIO	General Purpose Input Output
SATA	Serial Advanced Technology Attachment
PCIe	PCI Express
CPU	Central Processing Unit
BIOS	Basic Input/Output System
SRAM	Static Random-Access Memory
DRAM	Dynamic Random-Access Memory
NAND	NAND flash memory
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
KWK	Key Wrapping Key
KEK	Key Encryption Key
DEK	Data Encryption Key
ECDSA	Elliptic Curve Digital Signature Algorithm
PBKDF	Password-Based Key Derivation Function
SHA	Secure Hash Algorithms
SHS	Secure Hash Standard
TPM	Trusted Platform Module
KAT	Known Answer Test
LED	Light Emitting Diode

Table 17 Acronyms

## Appendix C: Reference Document & Support documentation

Category	Description
cPP	<ul style="list-style-type: none"> <li>• Collaborative Protection Profile for Full Drive Encryption - Encryption Engine v2.0 January 2, 2019.</li> <li>• Collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition v2.0, January 2, 2019.</li> </ul>
ST	<ul style="list-style-type: none"> <li>• Security Target for Novachips</li> </ul>
NIST (FIPS & SP)	<ul style="list-style-type: none"> <li>• NIST, <i>Security Requirements for Cryptographic TOEs</i></li> <li>• NIST 800-38F Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping</li> </ul>
SATA/ATA	<ul style="list-style-type: none"> <li>• Serial ATA: High-speed serialized AT attachment</li> <li>• SATA 3.1 GOLD</li> <li>• ATA-8 ACS2 (T13/2015-D, Revision 4)</li> <li>• SFF-8201</li> </ul>
PCIe/NVMe	<ul style="list-style-type: none"> <li>• NVMe Revision 1.1a</li> <li>• PCIe Base Specification Revision 2.0</li> <li>• PCIe_M.2_Electromechanical_Spec_Rev1.0_Final</li> <li>• Enterprise SSD Form Factor Version 1.0a</li> </ul>
Product Datasheet	<ul style="list-style-type: none"> <li>• Scalar P-series Datasheet rev1.0</li> <li>• Express P-series Datasheet rev1.0</li> </ul>
User Guide Document	<ul style="list-style-type: none"> <li>• Scalar and Express P-series Administrative Guidance rev1.0</li> <li>• Scalar and Express P-series ATA/NVM Command Guidance rev1.0</li> </ul>

*Table 18 Reference Document & Support documentation*