National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Scalar and Express P-series SSD, version NV.R1900

Report Number:	**CCEVS-VR-VID11567-2025**
Dated:	**May 15, 2025**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGMENTS

Validation Team

Randy Heimann
Chris Thorpe
Lisa Mitchell
Clare Parran
Linda Morrison

The MITRE Corporation

Common Criteria Testing Laboratory

Dylan Lyman

Brad Mitchell

Oleg Andrianov

UL Verification Services Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation Team of the evaluation of the Scalar and Express P-series SSD, version NV.R1900 by Novachips Co., Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by UL Verification Services Inc., a Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, CA, United States of America, and was completed in May 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by UL Verification Services Inc. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019, collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

The TOE is the Scalar and Express P-series SSD, version NV.R1900, firmware version NV.R1900_1000 and NV.R1900_1002. Under prior approval from NIAP, testing of the TOE was performed at a Novachips' location at 46 Sujeong-gu, Dallaenae-ro, Seongnam-si, Gyeonggi-do, 13516, Republic of Korea under remote control and observation of the Evaluator using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). The CCTL submitted a formal request for remote testing and was granted approval by NIAP on January 27, 2025. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The Validation Team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation Team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). The Validation Team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from Novachips Co., Ltd. For the Scalar and Express P-series SSD, version NV.R1900 Security Target, Version 1.8, May 15, 2025 and analysis was performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Scalar and Express P-series SSD
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019
Security Target	Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.8, May 15, 2025
Common Criteria Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Rev 5, April 2017
Common Evaluation Methodology (CEM) Version	CC3.1 Revision 5, April 2017
Conformance Result	CC Part Extended, CC Part 3 Extended
Evaluation Technical Report (ETR)	UL15482093-ETR V1.2
Sponsor/Developer	Novachips Co., Ltd
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc. San Luis Obispo, CA
CCEVS Validators	Randy Heimann, Chris Thorpe, Lisa Mitchell, Clare Parran, Linda Morrison

Table 1: Product Identification

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE description

The TOE is the Scalar and Express P-series SSD, version NV.R1900. The TOE is a multi-chip standalone cryptographic module consisting of a single ASIC controller and different sizes of memory chips of volatile DRAM and non-volatile NAND. The SSDs are compatible with industry standard form factors, such as a 2.5” SATA hard drive, a mini-SATA (mSATA), an M.2 SATA, or an NVMe M.2 & U.2 SSD slot, in addition to ruggedized connection types (R-SATA and RMM).

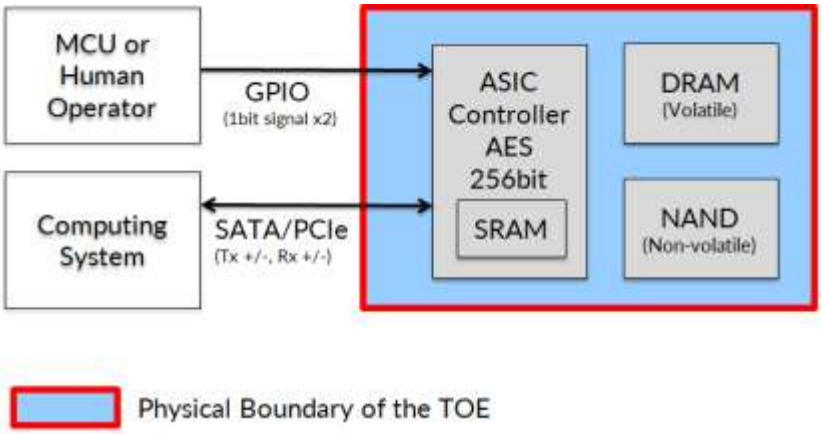
3.2 TOE Evaluated Platforms

This evaluation covers the TOE only in its evaluated configuration. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation identified in Section 5. The evaluation of security functionality for this product was limited to physical enclosure of the device.

The security target contains a list of evaluated models and firmware revisions applicable to those models. Details regarding the evaluated configuration are provided in Section 8 below.

3.3 TOE Physical Boundaries

The physical boundary of the TOE is a disk metal enclosure for 2.5” SATA and U.2 or opaque tamper-evident epoxy coating materials for mSATA and M.2 SSD, which covers all integrated circuits. The TOE communicates with a host computing system through these interfaces. The TOE has two GPIO lines through which either a machine, represented by a Microcontroller Unit (MCU), or operator can use to write protect or zeroize the TOE data written by the host.



The specific part numbers that make up the various TOE configurations including the hardware version, firmware version and related properties are listed in section 8. The TOE is delivered by the customer’s trusted carrier or Novachips FEDEX/DHL account, and the tracking number is provided to the customer after arranging the shipment. The TOE is encapsulated by a CNC/aluminum enclosure with either tamper label or epoxy coating to detect any tamper evidence. Upon initialization, the admin or user should check for tamper evidence.

4 Security Policy

This section contains the product security features and services and contains the policies or rules that the TOE must comply with and/or enforce.

4.1 *Cryptographic Support*

The drive utilizes the following cryptographic algorithms that are approved for use by NIST FIPS 140-3 per SP 800-140C and SP 800-140D.

Table 2: Entropy Source

Algorithm	Standard	Use	ESV Cert. #
Entropy Source	NIST 800-90B	Entropy Source	E80

Table 3: Cryptographic Algorithms

Algorithm	Standard	Use	CAVP Cert. #
AES-KW	SP800-38F	Symmetric key wrapping	A897
AES-XTS-256	FIPS 197 SP800-38E	User data encryption and decryption	C448
DRBG	SP800-90A	Key, nonce and IV generation	C463
PBKDF	SP800-132	Key derivation using PBKDF option 2a	A897
SHA-256	FIPS 180-4	Used in DRBG and HMAC	C411
SHA-384	FIPS 180-4	Message Digest, Digital Signature	A897
HMAC-SHA-256	FIPS 198-1	Used in PBKDF	A897
ECDSA P-384	FIPS 186-4	Firmware image authentication using signature verification	A897

4.2 *User Data Protection*

The device uses XTS-AES-256 (SP800-38E) IEEE Std. 1619-2007 XTS-AES-256 algorithm to encrypt all user data on the drive.

4.3 *Security Management*

The TOE allows authorized users to change the data encryption key (DEK), erase the DEK, initiate firmware updates, erase user data, and change passwords.

4.4 *Protection of the TSF*

The TOE protects itself by running a suite of self-tests at power-up and before using certain functions, authenticating firmware and by not providing any mechanism to export any key values.

5 Assumptions and Clarification of Scope

5.1 Secure Usage Assumptions

The Security Problem Definition, including the assumptions and threats, may be found in the following documents:

- collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019
- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019

That information has not been reproduced here and the Protection Profiles should be consulted if there is interest in that material.

5.2 Clarification of Scope

The evaluation of security functionality and scope are inherently tied to the specific assurance activities performed and the defined scope of the evaluation methodology. This evaluation provides no assurance that the TOE counters any threats which are not identified in the above PPs. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents are provided with the product by the developer to the consumer and were evaluated along with the TOE:

- Novachips Co., Ltd. Scalar and Express P-series Non-Proprietary Administrative Guidance, v.1.43, May 08, 2025
- Novachips Co., Ltd. Scalar and Express P-series SSD ATA/NVM Command Guidance, v.1.42, March 10, 2025

Any additional documentation provided with the product or may be available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download documentation from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

The Evaluation Team configured the TOE according to the vendor-provided guidance documentation and performed the tests specified in the [PP]. These results are summarized in the evaluation Assurance Activity Report with the approach summarized here.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities of this product.

7.2 Evaluation Team Independent Testing

The CCTL evaluation team created the test plan.

The functional testing was performed by CCTL evaluation team. The evaluation team was present at the vendor’s manufacture site and performed evaluation activities. The CCTL evaluation team generated the Detailed Test Report using the evidence collected by the CCTL evaluation team during the testing.

Testing was performed on both firmware revisions and on the following selected TOE models. An equivalency argument for the tested devices can be found in Section 1.1 of the AAR.

Ref	TOE developer Original Part No.	HW Ver.	Description (Form factor & interface)	Firmware Ver.	User Capacity	Certification Sponsor Reseller Part. No.
A	NS371P10T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000	10TB	AMP25TT10-IM02AI
B	NS369P500GVR4-1F	04MB4	Removable Memory Module	NV.R1900_1002	500GB	4119625G001/ G002
C	NS561P500GCE7-1F	02MB3	M.2 2280 PCIe/NVMe	NV.R1900_1000	500GB	AMPW5D500-IM02AI
D	NS571P02T0CK7-1F	16SN3	M.2 22110 PCIe/NVMe	NV.R1900_1002	2TB	AMPW6DT20-IM02AI

8 Evaluated Configuration

The TOE includes several models as shown in the table below:

Table 4: TOE Models

TOE developer Original Part No.	HW Ver.	Description (Form factor & Interface)	Firmware Ver.[1]	User Capacity	Certification Sponsor Reseller Part No.
NS361P500GCCR-1F	04MB3	2.5" SATA 7.0mm	NV.R1900_1000 or NV.R1900_1002	500GB	AMP25T500-IM02AI
NS371P01T0CC1-1F	04MN3	2.5" SATA 7.0mm	NV.R1900_1000 or NV.R1900_1002	1TB	AMP2500T0T10-IM020CP
NS371P02T0CC1-1F	08MN3	2.5" SATA 7.0mm	NV.R1900_1000 or NV.R1900_1002	2TB	AMP25TT20-IM02AI
NS371P04T0CC1-1F	16MN3	2.5" SATA 7.0mm	NV.R1900_1000 or NV.R1900_1002	4TB	AMP25TT40-IM02AI
NS371P08T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000 or NV.R1900_1002	8TB	AMP2500T08T0-IM020CP
NS371P10T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000 or NV.R1900_1002	10TB	AMP25TT10-IM02AI
NS379P16T0VC0-1F	32MN1	2.5" SATA 9.5mm	NV.R1900_1000 or NV.R1900_1002	16TB	AMP2500T16T0-IM020CP
NS379P20T0VC0-1F	32MN1	2.5" SATA 9.5mm	NV.R1900_1000 or NV.R1900_1002	20TB	AMP2500T20T0-IM020CP
NS361P250GCC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1002	250GB	AMP2500F0250-IM020CP
NS361P500GCC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1002	500GB	AMP2500F0500-IM020CP
NS369P01T0VC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1002	1TB	AMP2500F0T10-IM020CP
NS369P02T0VC0-1S	04MB3	2.5" SATA 9.5mm R-SATA	NV.R1900_1002	2TB	AMP2500F0T20-IM020CP
NS361P125GCM7-1F	04MBB	M.2 2242, SATA	NV.R1900_1000 or NV.R1900_1002	125GB	AMPW300T0125-IM020CP
NS369P250GVM7-1F	04MBA	M.2 2242, SATA	NV.R1900_1000 or NV.R1900_1002	250GB	AMPW300T0250-IM020CP
NS369P500GVM7-1F	04MBA	M.2 2242, SATA	NV.R1900_1000 or NV.R1900_1002	500GB	AMPW300T0500-IM020CP
NS361P125GCR3-1F	04MBB	Removable Memory Module	NV.R1900_1000 or NV.R1900_1002	125GB	2026640-003
NS369P250GVR3-1F	04MBA	Removable Memory Module	NV.R1900_1000 or NV.R1900_1002	250GB	2026640-003
NS369P500GVR3-1F	04MBA	Removable Memory Module	NV.R1900_1000 or NV.R1900_1002	500GB	2026640-003
NS361P125GCR4-1F	04MB4	Removable Memory Module	NV.R1900_1002	125GB	4119625G001, 4119625G002
NS369P250GVR4-1F	04MB4	Removable Memory Module	NV.R1900_1002	250GB	4119625G001, 4119625G002
NS369P500GVR4-1F	04MB4	Removable Memory Module	NV.R1900_1002	500GB	4119625G001, 4119625G002

NS369P01T0VE7-1F	04MB1	M.2 2280, SATA	NV.R1900_1002	1TB	AMPW500T0T10-IM020CP
NS369P01T0VA7-1F	04MB1	mSATA SATA	NV.R1900_1002	1TB	AMPV500T0T10-IM020CP
NS569P500GVM7-1F	04MBA	M.2 2242, PCIe/NVMe	NV.R1900_1002	500GB	AMPW300D0500-IM020CP
NS561P500GCE7-1F	02MB3	M.2 2280 PCIe/NVMe	NV.R1900_1000 or NV.R1900_1002	500GB	AMPW5D500-IM02AI
NS571P02T0CK7-1F	16SN3	M.2 22110 PCIe/NVMe	NV.R1900_1002	2TB	AMPW6DT20-IM02AI
NS579P04T0VK7-1F	16SN1	M.2 22110, PCIe/NVMe	NV.R1900_1002	4TB	AMPW600D04T0-IM020CP
NS571P01T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000 or NV.R1900_1002	1TB	AMP2U00D0T10-IM020CP
NS571P02T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000 or NV.R1900_1002	2TB	AMP2U00D0T20-IM020CP
NS571P04T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000 or NV.R1900_1002	4TB	AMP2U00D0T40-IM020CP
NS571P08T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000 or NV.R1900_1002	8TB	AMP2UDT80-IM02AI

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5. The evaluation was successful and provides a level of assurance that the TOE meets the Security Functional Requirements identified in the Security Target. This assurance comes from the performance of the work units associated with the Security Assurance Requirements. A detailed description of those Assurance Requirements as well as the details of how the product meets each of them can be found in the Security Target. A more detailed account of the evaluation assurance activities and the results obtained can be found in the Assurance Activity Report.

9.1 Security Target Evaluation (ASE)

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the target PPs.

The Validator Team reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation was justified.

9.2 TOE Development (ADV)

The evaluation team applied each ADV CEM work unit as refined by the target PPs. This activity is considered implicitly resolved.

9.3 Guidance Documents (AGD)

The Evaluation Team applied each AGD CEM work units as refined by the target PPs. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the target PPs.

The Evaluation Team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation Team ensured the adequacy of the administrator's guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation Team reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation Team was justified.

9.4 TOE Life Cycle Support (ALC)

The Evaluation Team applied each ALC CEM work unit. The Evaluation Team found that the TOE was identified.

The Validation Team reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

9.5 TOE Tests (ATE)

The Evaluation Team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the target PPs and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The Validation Team reviewed the work of the Evaluation Team and found that sufficient evidence was provided by the Evaluation Team to show that the evaluation activities addressed the test activities in the target PPs and that the conclusion reached by the Evaluation Team was justified.

9.6 Vulnerability Assessment (AVA)

The Evaluation Team applied each AVA CEM work unit as refined by the target PPs. The Evaluation Team performed a public search for vulnerabilities, performed vulnerability testing, and did not discover any issues with the TOE. A list of search terms, databases searched, and evaluation findings may be found in the AAR. The Evaluation Team also performed additional Assurance Activities as required by the target PPs and documented that in the AAR

The Validation Team reviewed the work of the Evaluation Team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the target PPs and that the conclusion reached by the Evaluation Team was justified.

9.7 Summary of Evaluation Results

The Evaluation Team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team’s testing also demonstrated the accuracy of the claims in the ST.

The Validation Team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation Team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in Novachips Co., Ltd. Scalar and Express P-series Non-Proprietary Administrative Guidance, v.1.43, May 08, 2025 and the Novachips Co., Ltd. Scalar and Express P-series SSD ATA/NVM Command Guidance, v.1.42, March 10, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by SFRs claimed in the ST. All other functionality provided by the TOE, including Military Secure Erase protocols, need to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. Evaluation activities are strictly bound by the assurance activities described in the NDcPP22e and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.8, May 15, 2025.

13 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
AAR	Assurance Activities Report
SSD	Solid State Drive

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, Version 3.1, Revision 5, April 2027.

[5] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 2019020, February 1, 2019.

[6] collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 2019020, February 1, 2019.

[7] Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.8, May 14, 2025. (ST)

[8] Novachips Co., Ltd. Scalar and Express P-series SSD Non-Proprietary Administrative Guidance, Version 1.43. (AGD)

[9] Novachips Co., Ltd. Scalar and Express P-series SSD ATA/NVM Command Guidance, v.1.42, March 10, 2025.

[10] Scalar and Express P-series SSD, version NV.R1900, Version 1.3, May 15, 2025. (AAR)

[11] Common Criteria Evaluation Technical Report, UL15482093-ETR V1.2, May 14, 2025. (ETR)