National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Novachips Co., Ltd

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

Report Number: CCEVS-VR-VID11262-2022
Dated: 10 June 2022
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

Acknowledgements

Validation Panel

Paul Bicknell
Linda Morison
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Oleg Andrianov
Michael C. Baron
UL Verification Services Inc.

Table of Contents

List of Tables

1 Executive Summary

This report provides an overview of the security information relevant to the Common Criteria evaluation and provides practical information about the Target of Evaluation (TOE). It is intended to assist the end-user of this product in determining the suitability of the product for their use. Potential end-users should review the Security Target (ST) for the functional requirements as well as the assumptions and threats mitigated. The Assurance Activity Report (AAR) should be consulted for detailed information about the activities performed by the Common Criteria Testing Laboratory (CCTL) which provide assurance of the TOE meeting the specified requirements.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Novachips Co., Ltd Scalar and Express P-series SSD, version NV.R1900 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was performed by UL Verification Services Inc., a Common Criteria Testing Laboratory (CCTL) in San Luis Obispo, CA, USA and assigned Validation ID (VID) 11262 by the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). Further information can be found on their web site (www.niap-ccevs.org). The evaluation was completed in June 2022.

The TOE is the Scalar and Express P-series SSD, version NV.R1900. The self-encrypting solid state drives each consist of a single ASIC controller, volatile DRAM memory chips and non-volatile NAND. The TOE is used to protect data at rest on a device that is lost or stolen while powered off. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the collaborative Protection Profile for full Drive Encryption – Authorization Acquisition Version 2.0 [CPP_FDE_AA_V2.0E] and collaborative Protection Profile for Full Drive Encryption – Encryption Engine Version 2.0 [CPP_FDE_EE_V2.0E].

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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.

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). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

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 Product Compliance 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(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Evaluation Scheme	United States NIAP Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Scalar and Express P-series SSD, version NV.R1900
Protection Profile	collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 [CPP_FDE_EE_V2.0E] collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 [CPP_FDE_AA_V2.0E]
Security Target	Scalar and Express P-series SSD Security Target, version NV.R1900, Version 1.0, June 6, 2022
Dates of Evaluation	January 2021 – June 2022
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Common Criteria Version	Version 3.1 Revision 5, April 2017
Common Evaluation Methodology (CEM) Version	Version 3.1 Revision 5, April 2017
Evaluation Technical Report (ETR)	UL13480549-ETR Rev1.2
Sponsor/Developer	Novachips Co., Ltd
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Oleg Andrianov, Michael C. Baron
CCEVS Validators	Paul Bicknell, Linda Morrison, Clare Parran

Table 1: Product Identification

3 Assumptions, Threats and Clarification of Scope

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

3.1 Threats

The following threats are countered by the TOE and/or its operational environment:

Threats	Description
T.UNAUTHORIZED_DATA_ACCESS	The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).
T.KEYING_MATERIAL_COMPROMISE	Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of keying material of equal importance to the data itself. Threat agents may look for keying material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash[, or TPMs][1].
T.AUTHORIZATION_GUESSING	Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release [BEV or DEKs][2] or otherwise put it in a state in which it discloses protected data to unauthorized users.
T.KEYSPACE_EXHAUST	Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to brute force exhaust the key space and give them unauthorized access to the data.
T.KNOWN_PLAINTEXT/EE	Threat agents know plaintext in regions of storage devices, especially in uninitialized regions (all zeroes) as well as regions that contain well known software such as operating systems. A poor choice of encryption algorithms, encryption modes, and initialization vectors

[1] "or TPMs" not in the AA Protection Profile.

[2] "BEV" in the AA Protection Profile, "DEKs" in the EE Protection Profile.

	along with known plaintext could allow an attacker to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.CHOSEN_PLAINTEXT/EE	Threat agents may trick authorized users into storing chosen plaintext on the encrypted storage device in the form of an image, document, or some other file A poor choice of encryption algorithms, encryption modes, and initialization vectors along with the chosen plaintext could allow attackers to recover the effective DEK, thus providing unauthorized access to the previously unknown plaintext on the storage device.
T.UNAUTHORIZED_UPDATE	Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software [and/or firmware][3] that bypasses the intended security features and provides them unauthorized to access to data.
T.UNAUTHORIZED_FIRMWARE_UPDATE/EE	An attacker attempts to replace the firmware on the SED via a command from the AA or from the host platform with a malicious firmware update that may compromise the security features of the TOE.
T.UNAUTHORIZED_FIRMWARE_MODIFY/EE	An attacker attempts to modify the firmware in the SED via a command from the AA or from the host platform that may compromise the security features of the TOE.

Table 2: Threats

3.2 Assumptions

These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumptions	Description
A.TRUSTED_CHANNEL	Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.

[3] Not in the EE Protection Profile.

A. INITIAL_DRIVE_STATE	Users enable Full Drive Encryption on a newly provisioned [or initialized][4] storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media until after provisioning. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, unpartitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE preauthentication software) contain no protected data.
A.TRAINED_USER/AA	Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
A.TRAINED_USER/EE	Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.
A.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
A.POWER_DOWN/AA	The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a "hibernation mode".
A.POWER_DOWN /EE	The user does not leave the platform and/or storage device unattended until the device is in a Compliant power saving state or has fully powered off. This properly clears memories and locks down the device. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen or sleep state). Users power the platform and/or storage device

[4] Not in the EE Protection Profile

	down or place it into a power managed state, such as a "hibernation mode".
A.STRONG_CRYPTO	All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.
A.SECURE_STATE/AA	Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
A.SINGLE_USE_ET/AA	External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
A.PASSWORD_STRENGTH/AA	Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
A.PLATFORM_I&A/AA	The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the Operating system's login interface, but it will not change or degrade the functionality of the actual interface.
A.PHYSICAL	The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform's correct operation.

Table 3: Assumptions

3.3 Organizational Security Policies

There are no organizational security policies addressed by the cPPs or the ST.

3.4 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 above. Furthermore, it is likely that any assumptions not upheld by the TOE environment will create new unmitigated threats.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within the Protection Profiles cited.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

4 Architectural Information

The TOE is the Scalar and Express P-series SSD, version NV.R1900. The self-encrypting solid state drives, each consists of a single ASIC controller, volatile DRAM memory chips and non-volatile NAND. The SSDs are compatible with industry standard form factors such as 2.5" SATA hard drive or NVMe M.2 & U.2 SSD slot.

5 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.

- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TSF

5.1 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:

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

Table 4: Cryptographic Algorithms

5.2 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.

5.3 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.

5.4 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.

6 Documentation

The following guidance documents were provided by the vendor with the TOE for evaluation:

- Non-Proprietary Administrative Guidance, version 1.0, March 3, 2022
- ATA/NVM Command Guidance, version 1.0, March 3, 2022

Any additional documentation provided with the product, or that is 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 the documentation from the NIAP website to ensure the device is configured as evaluated.

7 Evaluated Configuration

The TOE is identified as Scalar and Express P-series SSD, version NV.R1900. The specific part numbers and HW and FW versions are shown in the following table:

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	NV.R1900_1000	500GB	AMP25T500-IM02AI
NS371P02T0CC1-1F	08MN3	2.5" SATA 7mm	NV.R1900_1000	2TB	AMP25TT20-IM02AI
NS371P04T0CC1-1F	16MN3	2.5" SATA 7mm	NV.R1900_1000	4TB	AMP25TT40-IM02AI
NS371P10T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000	10TB	AMP25TT10-IM02AI
NS561P500GCE7-1F	02MB3	M.2 2280 PCIe/NVMe	NV.R1900_1000	500GB	AMPW5D500-IM02AI
NS571P02T0CK7-1F	16SN3	M.2 22110 PCIe/NVMe	NV.R1900_1000	2TB	AMPW6DT20-IM02AI
NS571P08T0CC0-1F	16MN3	2.5” PCIe/NVMe (U.2)	NV.R1900_1000	8TB	AMP2UDT80-IM02AI

Table 5: TOE Models

The specific part numbers that make up the various TOE configurations including the hardware version, firmware version and related properties is in Table 4 above. To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation identified above in Section 0. The evaluation of security functionality for this product was limited to the configuration contained in the guidance.

8 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.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the [ST] for a product claiming conformance to the protection profiles. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in supporting documentation of the protection profiles. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in the Evaluation Technical Report.

8.3 Vulnerability Analysis

The evaluation team performed each AVA_VAN.1 CEM work unit (as refined by the SD) and each AVA_VAN evaluation activities defined in the SD. A vulnerability analysis was performed following the processes described in the PP. The vulnerability analysis included a public domain search for potential vulnerabilities. This search was performed on May 20, 2022. The following public vulnerability repositories were utilized:

- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
- National Vulnerability Database: https://nvd.nist.gov/
- US-CERT http://www.kb.cert.org/vuls/html/search

The following search terms were utilized:

- Novachips
- ASIC
- Scalar and Express
- NVS3800
- drive encryption
- disk encryption
- “SED”
- NVMe
- NV.R1900
- SSD
- self-encrypting

The search resulted in no vulnerabilities that are applicable to the TOE. No residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

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 performed each TSS assurance activity and ASE CEM work unit as specified in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E. 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 Scalar and Express P-series SSD version NV.R1900 TOE that is consistent with the Common Criteria, and product security function descriptions that support the requirements.

9.2 Development (ADV)

The evaluation team performed each ADV assurance activity and ADV CEM work unit as specified in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence.

9.3 Guidance Documents (AGD)

The evaluation team performed each AGD assurance activity and AGD CEM work unit as specified in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE and how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

9.4 Life-cycle Support (ALC)

The evaluation team performed each ALC assurance activity and ALC CEM work unit as specified in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E. The evaluation team found that the TOE was identified, and a method of timely updates was described.

9.5 Tests (ATE)

The evaluation team performed each ATE assurance activity and ATE CEM work unit as specified in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E. The evaluation team ran the set of tests specified by the Assurance Activities in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E, and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

9.6 Vulnerability Assessment (AVA)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and validated that the vendor fixed all findings with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

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 test activities 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 performed the Evaluation Activities in the CPP_FDE_EE_V2.0E and CPP_FDE_AA_V2.0E, 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 the *Non-Proprietary Administrative Guidance, version 1.0, March 3rd, 2022 and ATA/NVM Command Guidance, version 1.0, March 3rd, 2022*.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Scalar and Express P-series SSD Security Target, version NV.R1900, Version 1.0, June 6, 2022.

13 Terms

13.1 Acronyms

Acronym	Meaning
CC	Common Criteria
CSP	Critical Security Parameters
FIPS	Federal Information Processing Standards Publication 140-2
NIST	National Institute of Standards and Technology
PP	Protection Profile
SD	Supporting Document
SED	Self Encrypting Drive
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 6: Acronyms

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[5] collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019.

[6] Supporting Document Mandatory Technical Document Full Drive Encryption: Encryption Engine, Version 2.0 + Errata 20190201, February 2019.

[7] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

[8] Supporting Document Mandatory Technical Document Full Drive Encryption: Authorization Acquisition, Version 2.0 + Errata 20190201, February 2019.

[9] Non-Proprietary Administrative Guidance, version 1.0, March 3rd, 2022

[10] ATA/NVM Command Guidance, version 1.0, March 3rd, 2022

[11] Scalar and Express P-series SSD Security Target, version NV.R1900, Version 1.0, June 6, 2022.

[12] Scalar and Express P-series SSD, version NV.R1900 Assurance Activity Report, UL13480549-AAR Rev1.2, June 2, 2022

[13] Common Criteria Evaluation Technical Report UL13480549-ETR Rev1.2, June 2, 2022