National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1

Report Number: CCEVS-VR-VID11297-2023
Dated: March 14, 2023
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 Team

Jenn Dotson
Chris Thorpe
The MITRE Corporation

Farid Ahmed
Anne Gugel
Richard Toren
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Eric Isaac
Furukh Siddique
Kevin Steiner
Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 solution provided by DIGISTOR. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) 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 the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in March 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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.

The TOE is the DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). This VR 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) and the conclusions of the testing laboratory in the ETR 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). Therefore, 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target*, Version 1.7, March 2023, and analysis 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 (PP) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1
Sponsor and Developer	DIGISTOR 1000 SE Tech Center Dr Suite 160 Vancouver, WA 98683
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017.
CEM	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 5, April 2017.
Protection Profile	*collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019
ST	*DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target*, Version 1.7, March 2023

Item	Identifier
Evaluation Technical Report	*DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Evaluation Technical Report*, Version 0.6, March 2023
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Eric Isaac, Furukh Siddique, Kevin Steiner
CCEVS Validators	Farid Ahmed, Jenn Dotson, Anne Gugel, Chris Thorpe, Richard Toren

3. Architectural Information

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

The Target of Evaluation (TOE) is a solid state self-encrypting drive that provides encryption and decryption of stored user data.

3.1. Evaluated Configuration

The TOE evaluated configuration includes the DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1, which consists of the following models and versions:

Drive	Capacity	FIPS HW P/N & Version	CC/NIAP Listed HW P/N & Version	Controller	FW Version
DIGISTOR 2.5-Inch SATA SSD	128GB	DIG-SSD21286-SI	DIG-SSD21286-SI	PS3112-S12	SCPG13.0
	256GB	DIG-SSD22566-SI	DIG-SSD22566-SI		
	512GB	DIG-SSD25126-SI	DIG-SSD25126-SI		
	1024GB	DIG-SSD210006-SI	DIG-SSD210006-SI		
	2048GB	DIG-SSD220006-SI	DIG-SSD220006-SI		
DIGISTOR M.2 2280 SATA SSD	128GB	DIG-M21286-SI	DIG-M21286-SI		
	256GB	DIG-M22566-SI	DIG-M22566-SI		
	512GB	DIG-M25126-SI	DIG-M25126-SI		
	1024GB	DIG-M210006-SI	DIG-M210006-SI		
	2048GB	DIG-M220006-SI	DIG-M220006-SI		
DIGISTOR M.2 2280 NVMe SSD	256GB	DIG-M2N22566-UI	DIG-M2N22566-UI	PS5012-E12	ECPG13.0
	512GB	DIG-M2N25126-UI	DIG-M2N25126-UI		
	1024GB	DIG-M2N210006-UI	DIG-M2N210006-UI		
	2048GB	DIG-M2N220006-UI	DIG-M2N220006-UI		

Drive	Capacity	FIPS HW P/N & Version	CC/NIAP Listed HW P/N & Version	Controller	FW Version
DIGISTOR 2.5-Inch SATA SSD	128GB	DIG-SSD21286-SI	DIG-SSD212832	PS3112-S12	SCPG13.0
	256GB	DIG-SSD22566-SI	DIG-SSD225632		
	512GB	DIG-SSD25126-SI	DIG-SSD251232		
	1024GB	DIG-SSD210006-SI	DIG-SSD2100032		
	2048GB	DIG-SSD220006-SI	DIG-SSD2200032		
DIGISTOR M.2 2280 SATA SSD	128GB	DIG-M21286-SI	DIG-M212832		
	256GB	DIG-M22566-SI	DIG-M225632		
	512GB	DIG-M25126-SI	DIG-M251232		
	1024GB	DIG-M210006-SI	DIG-M2100032		
	2048GB	DIG-M220006-SI	DIG-M2200032		
DIGISTOR M.2 2280 NVMe SSD	256GB	DIG-M2N22566-UI	DIG-M2N225632	PS5012-E12	ECPG13.0
	512GB	DIG-M2N25126-UI	DIG-M2N251232		
	1024GB	DIG-M2N210006-UI	DIG-M2N2100032		
	2048GB	DIG-M2N220006-UI	DIG-M2N2200032		
DIGISTOR Ships Removable NVMe SSD	256GB	DIG-M2N22566-UI	Q80-M2N225632		
	512GB	DIG-M2N25126-UI	Q80-M2N251232		
	1024GB	DIG-M2N210006-UI	Q80-M2N2100032		
	2048GB	DIG-M2N220006-UI	Q80-M2N2200032		
	256GB	DIG-M2N22566-UI	Q80R-M2N225632		
	512GB	DIG-M2N25126-UI	Q80R-M2N251232		
	1024GB	DIG-M2N210006-UI	Q80R-M2N2100032		
	2048GB	DIG-M2N220006-UI	Q80R-M2N2200032		
DIGISTOR C Series FW M.2 2280 NVMe SSD	256GB	DIG-M2N22566-AI	DIG-M2N225633	PS5012-E12	ECPM13.1
	512GB	DIG-M2N25126-AI	DIG-M2N251233		
	1024GB	DIG-M2N210006-AI	DIG-M2N2100033		

Drive	Capacity	FIPS HW P/N & Version	CC/NIAP Listed HW P/N & Version	Controller	FW Version
	2048GB	DIG-M2N220006-AI	DIG-M2N2200033		
DIGISTOR Ships Removable C Series FW NVMe SSD	256GB	DIG-M2N22566-AI	Q80-M2N225633		
	512GB	DIG-M2N25126-AI	Q80-M2N251233		
	1024GB	DIG-M2N210006-AI	Q80-M2N2100033		
	2048GB	DIG-M2N220006-AI	Q80-M2N2200033		
	256GB	DIG-M2N22566-AI	Q80R-M2N225633		
	512GB	DIG-M2N25126-AI	Q80R-M2N251233		
	1024GB	DIG-M2N210006-AI	Q80R-M2N2100033		
	2048GB	DIG-M2N220006-AI	Q80R-M2N2200033		

3.2. TOE Architecture

The TOE provides full drive encryption to protect data at rest on a lost or stolen device. The Encryption Engine (EE) ensures that the data is encrypted using FIPS-validated algorithms. It manages the encryption and decryption of the stored data, policy enforcement, and key management.

3.3. Physical Boundary

The physical boundary of the TOE encompasses the DIGISTOR Secure SSD firmware running on the SEDs. The TOE hardware is delivered to customers via trusted courier with the firmware preinstalled.

The TOE models support either NVMe PCIe or SATA III interfaces. All TOE models incorporate an ARM Cortex-R5 processor (ARMv7-R microarchitecture).

3.4. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- Authorization Acquisition. KLC CipherDrive v1.2.2 software installed on a 128 MB read-only Shadow MBR partition on the SED. This supplies the Border Encryption Value (BEV) for locking and unlocking the drives. The KLC software provides the GUI used for performing the security management functions described within this ST.
- Protected OS. The TOE supports protection of commonly used operating systems, such as Linux Operating Systems/Linux based Hypervisors and Windows Operating Systems.

- Computer Hardware. Intel based UEFI booted systems that supports Intel Secure Key Technology. CC Testing performed using CPUs:
    - Intel Core i3-8100
    - Intel Core i5-8400
    - Intel Core i5-9600
    - Intel Core i7-3770K

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Cryptographic Support

The TOE ensures key material used for storage encryption is properly generated and protected from disclosure. It also implements cryptographic key and key material destruction during transitioning to a Compliant power saving state, or when all keys and key material are no longer needed.

The TOE performs cryptographic operations as shown in relevant Cryptographic Algorithm Validation Program (CAVP) certificates.

4.2. User Data Protection

The TOE enables encryption and decryption of user data on a SED to protect it from unauthorized disclosure.

4.3. Security Management

The TOE enables management of its security functions, including:

i) Changing and erasing the DEK

ii) Updating the TOE firmware

4.4. Protection of the TSF

The TOE ensures the authenticity and integrity of firmware updates through digital signatures using RSA 2048 with SHA-256. The TOE supports the D3 compliant power saving state dependent on the OS parameters or user-initiated request.

The TOE ensures its integrity and operation by performing self-tests.

5. Assumptions and Clarification of Scope

5.1. Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

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

That information has not been reproduced here and CPP_FDE_EE_V2.0E should be consulted if there is interest in that material.

5.2. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_EE_V2.0E as described for this TOE in the ST. Other functionality provided by the devices was not assessed as part of this evaluation. All other functionality 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 in accordance with the assurance activities specified in the CPP_FDE_EE_V2.0E and performed by the Evaluation team.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide identified in Section 6, additional customer documentation for the specific 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 CPP_FDE_EE_V2.0E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, functionality defined in Section 3.2 is not covered by this evaluation.

6. Documentation

The following guidance documents were available with the TOE for evaluation:

- *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Common Criteria Guide,* Version 1.3, January 2023

This document is the only documentation that should be trusted to set-up, administer, or use the product in the evaluated configuration. Additional documentation was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

7. IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 FDE Encryption Engine Test Plan*, which is not publicly available. The *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Assurance Activities Report*, Version 0.8, March 2023 provides an overview of testing and the prescribed assurance activities.

7.1. Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA lab in Baltimore, MD from April 2, 2022, until February 27, 2023. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. Remote testing

Remote testing was conducted at the Phison facility located in Jhunan, Miaoli, Taiwan. Phison representatives conducted the testing. The Evaluation team directed and observed remote testing for the DIG-M2N22566-AI, DIG-SSD22566-SI, DIG-M2N25126-UI, and DIG-M21286-SI TOE models for the FCS_CKM.1(c), FCS_CKM.4(b) and FDP_DSK_EXT.1 test activities. This was performed over a recorded remote session and participation included the CCTL, NIAP and the Validation team on November 28, 2022. Prior approval was granted by NIAP. Prior to testing, the Evaluation team confirmed the TOE models were running the correct firmware and were physically and logically separated from each other and other hardware in the test facility.

7.4. TOE Test Environment Configuration

The TOE testing environment components are identified in the tables.

Table 2: Devices in the Testing Environment

TOE model	Platform	Controller	Firmware	SFRs
DIG-M2N25126-UI	Windows 10 Pro, Intel i5-9600	PS5012-E12	ECPG13.0	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1
DIG-M2N25126-AI	Windows 10 Pro, Intel i5-9600	PS5012-E12	ECPM13.1	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1
DIG-SSD22566-SI	Windows 10 Pro, Intel i5-9600	PS3112-S12	SCPG13.0	FCS_VAL_EXT.1 FMT_SMF.1 FPT_TUD_EXT.1
DIG-M2N22566-AI	Ubuntu 20.04.2 LTS, Intel i5-8400	PS5012-E12	ECPM13.1	FCS_CKM.1(c) FCS_CKM.4(b) FDP_DSK_EXT.1
DIG-SSD22566-SI	Ubuntu 16.04 LTS, Intel i7-3770K	PS3112-S12	SCPG13.0	FCS_CKM.1(c) FCS_CKM.4(b) FDP_DSK_EXT.1
DIG-M2N25126-UI	Ubuntu 20.04.2, Intel i3-8100	PS5012-E12	ECPG13.0	FCS_CKM.1(c) FCS_CKM.4(b) FDP_DSK_EXT.1
DIG-M21286-SI	Ubuntu 16.04 LTS, Intel i3-8100	PS3112-S12	SCPG13.0	FCS_CKM.1(c) FCS_CKM.4(b) FDP_DSK_EXT.1

Table 3: Tools Used for Testing

Tool name	Version	Description
KLC CipherDrive	v1.2.2	This tool provides GUI access to the TOE to be able to perform management functions
Phison Test Utility for SCPG drives	0.9.01.33	This tool was used to test the deletion and generation of key as well as provide dumps

Tool name	Version	Description
		of the entire drive to verify evidence
Phison Test utility for ECPG & ECPM drives	1.10.01.01_FIPS_Digistor	This tool was used to test the deletion and generation of key as well as provide dumps of the entire drive to verify evidence
DLMC Tool for Trusted Update	ECPG13.0, ECPM13.1, SCPG13.0	This tool was used for updating the firmware on the TOE for trusted update tests.
HxD	2.5.0.0	This tool was used to verify binary file dumps with key contents

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 to be Part 2 extended, and to meet the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in CPP_FDE_EE_V2.0E.

8.1. Evaluation of Security Target (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 DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CPP_FDE_EE_V2.0E related to the examination of the information contained in the TOE Summary Specification (TSS).

The Validation 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.

8.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. 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 guidance in describing how to securely administer the TOE. All of 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 requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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.

8.5. Evaluation of Test Documentation and the Test Activity (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 CPP_FDE_EE_V2.0E and recorded the results in the DTR, summarized in the AAR.

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.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 CPP_FDE_EE_v2.0E Vulnerability Assessment*, Version 0.7, February 2023, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on February 28, 2023, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- US-CERT: http://www.kb.cert.org/vuls/html/search

The Evaluation team performed a search using the following keywords:

- Digistor
- Trusted Computing Group (TCG)
- Digistor Secure SSD

- Self Encrypting Drive (SED)
- Digistor 2.5-Inch SATA SSD
- PS3112-S12
- SCPG13.0
- Digistor M.2 2280 SATA SSD
- Digistor M.2 2280 NVMe SSD
- PS5012-E12
- ECPG13.0
- Digistor Ships Removable NVMe SSD
- Digistor C Series FW M.2 2280 NVMe SSD
- Digistor Ships Removable C Series FW NVMe SSD
- ECPM13.1
- Drive encryption
- Disk encryption
- Key destruction
- Key sanitization
- OPAL
- ARM Cortex-R5 processor
- ARMv7-R microarchitecture
- Phison TCG OPAL SSC SSD solutions

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.

8.7. 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 followed the procedures defined in the CEM and performed the Assurance Activities in the CPP_FDE_EE_V2.0E and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this VR. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE models or Firmware versions, either earlier or later, were evaluated.

10. Annexes

Not applicable.

11. Security Target

DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target, Version 1.7, March 2023.

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Full Drive Encryption – Encryption Engine*, Version 2.0e + Errata 20190201, February 1, 2019
6. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target*, Version 1.7, March 2023 (ST)
7. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Common Criteria Guide*, Version 1.3, January 2023 (AGD)
8. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Assurance Activity Report,* Version 0.8, March 2023 (AAR)
9. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 CPP_FDE_EE_v2.0E Vulnerability Assessment,* Version 0.7, February 2023
10. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Evaluation Technical Report*, Version 0.6, March 2023 (ETR)
11. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 FDE Encryption Engine Test Plan*, Version 0.5, March 2023 (DTR)
12. *DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 FDE Encryption Engine Test Plan Evidence*, Version 0.5, March 2023 (DTR)