ASSURANCE CONTINUITY MAINTENANCE REPORT FOR DIGISTOR TCG OPAL SSC FIPS SSD Series, Firmware Version SCPG13.0/ECPG13.0/ECPM13.1/ECPM15.0

DIGISTOR TCG OPAL SSC FIPS SSD Series, Firmware Version SCPG13.0/ECPG13.0/ECPM13.1/ECPM15.0

Maintenance Report Number: CCEVS-VR-VID11297-2025

Date of Activity: 14 January 2025
References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- DIGISTOR TCG OPAL SSC FIPS SSD Series, Firmware Version SCPG13.0/ECPG13.0/ECPM13.1/ECPM15.0 Impact Analysis Report, Version 1.2, January 2025
- collaborative Protection Profile for Full Drive Encryption – Encryption Engine, v2.0 + Errata 20190201

Original Documentation:

- DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target, Version 1.7, March 2023
- DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Common Criteria Guide, Version 1.3, January 2023

Revised Documentation:

- DIGISTOR TCG OPAL SSC FIPS SSD Series, Firmware Version SCPG13.0/ECPG13.0/ECPM13.1/ECPM15.0 Security Target, v2.0, October 2024
- DIGISTOR TCG OPAL SSC FIPS SSD Series, Firmware Version SCPG13.0/ECPG13.0/ECPM13.1/ECPM15.0 Common Criteria Guide, v2.0, October 2024

Assurance Continuity Maintenance Report:

Lightship submitted an Impact Analysis Report (IAR) for the DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 3 December 2024. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target, the Administrator's Guide, and the Impact Analysis Report (IAR). The ST, Admin Guide, and IAR were updated.

The information below has all been pulled from the IAR, updated ST and updated AGD provided for this assurance maintenance action.

Documentation updated:

Original CC Evaluation Evidence	**Evidence Change Summary**
DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target, Version 1.7, March 2023	The ST has been revised to update the following sections: Title Page, ST Reference, TOE Reference, Guidance document versions and Added TOE Hardware/Firmware to include the new TOE models and firmware version.
Design Documentation: See Security Target and Guidance	See Security Target and Guidance changes in this table
Guidance Documentation: DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Common Criteria Guide, Version 1.3, January 2023	The AGD has been revised to update the following sections: Title Page, TOE Reference and Added TOE Hardware/Firmware to include the new TOE models and firmware version.
Lifecycle: None	No changes required.
Testing: None	No changes required. DIGISTOR performed a series of CC tests on the new drive models running the ECPM15.0 firmware. Lightship Security has reviewed the test evidence and confirms that the TOE operates as expected and maintains the same results as the tests conducted by the Evaluator during the previous evaluation. The Developer performed the following regression testing related to SFRs: • FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key) • FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware)

	• FDP_DSK_EXT.1 - Protection of Data on Disk
Vulnerability Assessment: None	Lightship Security performed a search of public information for potential vulnerabilities on January 14, 2025. The search was in accordance with Labgram #116/Valgram #135 - Vulnerability Evidence. See more details including search terms below.

Changes to the TOE:
The changes are summarized below.

Major Changes

None.

Minor Changes

The following changes have been made to the certified TOE:

a. Hardware. Two drive models were introduced. The DIGISTOR C Series Advanced NVMe SSD and the DIGISTOR Ships Removable C Series Advanced NVMe SSD.
b. Firmware. To support the new drive models the ECPM15.0 firmware was added.

Hardware Changes and Impact
There are no changes to hardware components. The same controller module used for the ECPM13.1 firmware (Controller PS5012-E12) is supported for the new drive/firmware composition. Addition of the new hardware models (drives) is for the purpose of identification. Only the hardware part numbers have changed to uniquely identify the drives supporting the ECPM15.0 firmware.

Firmware Changes and Impact:
The new ECPM15.0 firmware adds support and configuration for Bit Cost Scalable 5 (BiCS5) storage technology. BiCS5 increases storage capacity per unit and improves performance in NAND Flash. Due to the larger physical block size of BiCS5, code changes were made to support Redundant Array of Independent Disks Error Correction Code (RAIDECC) functionality.

The changes to the TOE firmware are assessed as MINOR for the following reasons:

- BiCS5 is a performance enhancement and has no impact on the cryptographic functionality. Cryptographic functionality is provided by the controller, which has not changed.
- The type of NAND supported has not changed (TLC and SLC).
- The most significant code change was support for RAIDECC. RAID is unevaluated functionality that is not touched in any way by the CC testing of SFRs.

As per the previous evaluation documented in “DIGISTOR TCG OPAL SSC FIPS SSD Series, firmware version SCPG13.0/ECPG13.0/ECPM13.1 Security Target, Version 1.7, March 2023”, together with this assurance continuity activity, the final set of claimed supported evaluated devices is:

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		
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-SSD2100032		
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		

Drive	Capacity	FIPS HW P/N & Version	CC/NIAP Listed HW P/N & Version	Controller	FW Version
	2048GB	DIG-M220006-SI	DIG-M2100032		
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-M2N2100032		
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		
	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		
	256GB	DIG-M2N22566-AX	DIG-M2N225633	PS5012-E12	ECPM15.0

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

Developer Testing

DIGISTOR performed a series of CC tests on the new drive models running the ECPM15.0 firmware. Lightship Security has reviewed the test evidence and confirms that the TOE operates as expected and maintains the same results as the tests conducted by the Evaluator during the previous evaluation.

The Developer performed the following regression testing related to SFRs:

- FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key)
- FCS_CKM.4(b) Cryptographic Key Destruction (TOE-Controlled Hardware)
- FDP_DSK_EXT.1 - Protection of Data on Disk

Assurance Activity Requirements

No changes were made to the Security Functional Requirements or Security Assurance Requirements, therefore no updates to the Assurance Activities were necessary.

NIST CAVP Certificates:

No changes to CAVP certificates.

Vulnerability Analysis:

Lightship Security performed a search of public information for potential vulnerabilities. The search was in accordance with Labgram #116/Valgram #135 - Vulnerability Evidence. The following public sources were searched on January 14, 2025.

- NIST National Vulnerability Database: https://nvd.nist.gov

- MITRE CVE Search: https://cve.mitre.org/cve/search_cve_list.html

The search terms listed below were used from the initial evaluation:

- 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 following search terms were added due to the updated TOE:

- DIGISTOR C Series Advanced NVMe SSD
- DIGISTOR Ships Removable C Series Advanced NVMe SSD
- ECPM15.0

The search of the public domain using the search sources above returned a number of vulnerabilities. No new vulnerabilities were found that are applicable to the TOE since February 28, 2023 when the vulnerabilities were last searched for the Validated TOE.

All known public security vulnerabilities are mitigated in the TOE version.

Digistor asserts that there are no known exploitable public vulnerabilities in the changed TOE as of the publication date of this IAR.

Conclusion:

The evaluation evidence consists of the Security Target and CC-specific Guidance Documentation. Both the Security Target and Guidance Documentation were revised to include the additional TOE models and firmware version. The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims.

There are no changes to TSF Interfaces, no hardware changes, no SFR changes, no SAR changes, no changes to assumptions threats or objectives, no CAVP changes and no new assurance evidence. Regression testing was done and was considered adequate based on the scale and types of changes made. The vulnerability search also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. The impact of all TOE changes on the assurance baseline is assessed to have an impact of minor severity and is within the parameters of the Assurance Continuity Framework.

Therefore, CCEVS agrees that the original assurance is maintained for the product.