



## **ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Scalar and Express P-series SSD, version NV.R1900**

---

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

**Maintenance Report Number:** CCEVS-VR-VID11262-2023

**Date of Activity:** 31 March 2023

#### **References:**

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Impact Analysis Report for Scalar and Express P-series SSD, version NV.R1900, version 1.1, 27 March 2023
- Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.1, 22 February 2023
- Non-Proprietary Administrative Guidance, version 1.1, 01 January 2023
- collaborative Protection Profile for Full Drive Encryption – Encryption Engine, Version 2.0e, February 1, 2019
- collaborative Protection Profile for Full Disk Encryption – Authorization Acquisition, Version 2.0e, February 1, 2019

#### **Assurance Continuity Maintenance Report:**

UL submitted an Impact Analysis Report (IAR) for the Scalar and Express P-series SSD, version NV.R1900 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 22 February 2023. 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 updated documentation table, the minor change breakdown and the vulnerability analysis have all been pulled directly from the IAR.

**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

**Documentation updated:**

<b>Original CC Evaluation Evidence</b>	<b>Evidence Change Summary</b>
<p><b>Security Target:</b>                      Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.0, 06 June 2022</p>	<p><i>Security Target Assurance Activity changes:</i></p> <p>ASE_INT.1-8 rationale was updated to include the new form factors in the maintained TOE.</p> <p><i>Security Target Documentation Changes:</i></p> <p>ST Cover page and ST Section 1.1 changed version of ST to v1.1, and the date of document changed to ‘February 22, 2023’.</p> <p>The ‘footer’ in the ST changed ‘Version’ to “Version 1.1”.</p> <p>Sections 1.2 and 1.3.1 were updated to include the proposed models in the maintained TOE.</p> <p>Section 1.3.4. was updated to include descriptions of the proposed models in the maintained TOE, in terms of the operational environment that the proposed models are compatible with.</p>
<p><b>Design Documentation:</b>                      See Security Target and Guidance</p>	<p>No changes required</p>
<p><b>Guidance Documentation:</b>                      Non-Proprietary Administrative Guidance, version 1.0, 03 March 2022</p>	<p><i>Guidance Documentation Assurance Activity changes:</i></p> <p>AGD_PRE.1-3-PP was updated to include the new models into the rationale of the work unit.</p> <p><i>Guidance Documentation Changes:</i></p> <p>Document version changed to v1.1.</p> <p>Section 1 was updated to describe the form factors supported in the maintained TOE (mSATA and M.2 SATA).</p> <p>Section 2 was updated to fix some typos, and to reiterate the new form factors that are supported in the maintained TOE (mSATA and M.2 SATA).</p> <p>Section 3 was updated to include the new list of models proposed for the maintained TOE.</p> <p>Figures 4 through 13 were updated to include new models for the maintained TOE. Figure 14 was added to include new model.</p> <p>Section 4 was updated to include new models for the maintained TOE; clarifying the pinouts for the new form factors.</p>

**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

	<p>Section 6 was updated to fix typos.</p> <p>Section 10 was updated to include the new models of the maintained TOE.</p> <p>Section 12 was updated to fix grammar.</p> <p>Section 19 was updated to include installation instructions for new models in the maintained TOE.</p> <p>Section 26 was updated to include the new models in the maintained TOE in the existing statements regarding physical security for the TOE. Section 27 was updated to include mSATA pinout with regards to self-tests.</p> <p>Section 27 was updated to include mSATA pinout with regards to self-tests.</p> <p>Section 30 was updated to fix grammar and to update a table to include the new models.</p>
<p><b>Lifecycle:</b> None</p>	<p>No changes required.</p>
<p><b>Testing:</b> None</p>	<p>No changes required.</p> <p>All functional tests performed previously in the validated TOE were reperformed by the developer on the following models from the set of proposed models, with no testing failures:</p> <ul style="list-style-type: none"> <li>- NS361P125GCM7-1F</li> <li>- NS569P500GVM7-1F</li> </ul>
<p><b>Vulnerability Assessment:</b> None</p>	<p>The public search was updated on 3/27/2023. No public vulnerabilities exist in the product. See analysis results below.</p>

**Changes to the TOE:**

The changes are summarized below.

Major Changes

None.

Minor Changes

No changes were made to the individual products within the validated TOE.

Additional models of the hard drive are being proposed to be included in the maintained TOE.

Eleven models of storage drives are proposed for addition.

As per the previous evaluation documented in “Scalar and Express P-series SSD, version NV.R1900 Security Target, version 1.0, 06 June 2022”, together with this assurance continuity activity, the final set of claimed supported evaluated devices is:

**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

TOE developer Original Part No.	HW Ver.	Description (Form factor & Interface)	Firmware Ver.	User Capacity	Certification Sponsor Reseller Part No.
<b>Previously Validated TOE Models</b>					
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
<b>New TOE Models</b>					
NS371P01T0CC1-1F	04MN3	2.5" SATA 7mm	NV.R1900_1000	1TB	AMP2500T0T10- IM020CP
NS371P08T0CC0-1F	16MN3	2.5" SATA 9.5mm	NV.R1900_1000	8TB	AMP2500T08T0- IM020CP
NS379P16T0VC0-1F	32MN1	2.5" SATA 9.5mm	NV.R1900_1000	16TB	AMP2500T16T0- IM020CP
NS379P20T0VC0-1F	32MN1	2.5" SATA 9.5mm	NV.R1900_1000	20TB	AMP2500T20T0- IM020CP
NS361P125GCM7-1F	04MBB	M.2 2242, SATA	NV.R1900_1000	125GB	AMPW300T0125- IM020CP
NS369P250GVM7-1F	04MBA	M.2 2242, SATA	NV.R1900_1000	250GB	AMPW300T0250- IM020CP
NS369P500GVM7-1F	04MBA	M.2 2242, SATA	NV.R1900_1000	500GB	AMPW300T0500- IM020CP
NS369P01T0VE7-1F	04MB1	M.2 2280, SATA	NV.R1900_1000	1TB	AMPW500T0T10- IM020CP
NS369P01T0VA7-1F	04MB1	mSATA SATA	NV.R1900_1000	1TB	AMPV500T0T10- IM020CP
NS569P500GVM7-1F	04MBA	M.2 2242, PCIe/NVMe	NV.R1900_1000	500GB	AMPW300D0500- IM020CP
NS579P04T0VK7-1F	16SN1	M.2 22110, PCIe/NVMe	NV.R1900_1000	4TB	AMPW600D04T0- IM020CP

The table below identifies each of the eleven proposed models, the differences between the proposed models and those within the validated TOE, and a determination as to whether the differences are considered security relevant.

**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

Identifying Delta Between the Validated TOE and proposed TOE Models			
Original Part No. For the Proposed model	Description	Changes	Security Relevant Change?
NS371P01T0CC1-1F	Functionally identical to the following validated models: - NS361P500GCCR-1F - NS371P02T0CC1-1F - NS371P04T0CC1-1F	<i>Storage Capacity:</i> - Proposed model has 1TB capacity as compared to the capacity of 500GB, 2TB and 4TB of the previously validated comparable models.	No.
NS371P08T0CC0-1F, NS379P16T0VC0-1F, NS379P20T0VC0-1F	Functionally identical to the following validated model: - NS371P10T0CC0-1F	<i>Storage Capacity:</i> - Proposed models have 8TB, 16TB, and 20TB capacity as compared to the capacity of 10TB for the previously validated comparable model.	No.
NS361P125GCM7-1F, NS369P250GVM7-1F, NS369P500GVM7-1F, NS369P01T0VE7-1F	Functionally identical to the following validated models: - NS361P500GCCR-1F - NS371P02T0CC1-1F - NS371P04T0CC1-1F	<i>Storage Capacity:</i> - Proposed models have 125GB, 250GB, 500GB and 1TB capacity as compared to the capacity of 500GB, 2TB and 4TB of the previously validated comparable models.  <i>Form Factor:</i> - Proposed model's form factor is 'M.2' as opposed to 2.5"; SATA protocol is identical. (Note that M.2 2242 vs M.2 2280 just differ in physical length of the of the PCB card)	No.
NS369P01T0VA7-1F	Functionally identical to the following validated models: - NS361P500GCCR-1F - NS371P02T0CC1-1F - NS371P04T0CC1-1F	<i>Storage Capacity:</i> - Proposed model has 1TB capacity as compared to the capacity of 500GB, 2TB and 4TB of the previously validated comparable models.  <i>Form Factor:</i> - Proposed model's form factor is 'mSATA' as opposed to 2.5"; SATA protocol is identical.	No.
NS569P500GVM7-1F	Functionally identical to the following validated model: - NS561P500GCE7-1F	<i>Form Factor:</i> - Proposed model's form factor is 'M.2 2242' versus 'M.2 2280' of the validated model; SATA	No.

## CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

		protocol is identical. (Note that M.2 2242 vs M.2 2280 just differ in physical length of the PCB card)	
NS579P04T0VK7-1F	Functionally identical to the following validated model: - NS571P02T0CK7-1F	<i>Storage Capacity:</i> - Proposed model has 4TB capacity as compared to 2TB of the previously validated comparable model.	No.

### Regression Testing:

All functional tests performed previously in the validated TOE were reperformed by the developer on the following models from the set of proposed models, with no testing failures:

- NS361P125GCM7-1F
- NS569P500GVM7-1F

### NIST CAVP Certificates:

The new TOE models are covered under the original CAVP certificates.

### 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 March 27, 2023. 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

## CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

- 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.

### **Conclusion:**

The changes to the validated TOE are in form factor and/or storage capacity only. While storage capacity rarely, if ever, has security implications pertaining to Full Drive Encryption products, the form factor may have security relevant differences with regards to communication protocols between the host and device, if new protocols are introduced. However, no new protocols are introduced with the addition of the proposed models.

Testing performed in the assurance baseline covered both PCIe/NVMe and SATA; two host expansion bus protocols. The proposed models are either of PCIe/NVMe or SATA protocol.

The remaining difference between the proposed models and validated TOE pertain to storage capacity, which again, the CCTL considers to be non-security relevant in this case.

Furthermore, each of the proposed models utilize the identical microcontroller and firmware as the models within the validated TOE. There are no changes to TSF Interfaces, no hardware changes, no SFR changes, no new security features, no changes to assumptions and objectives, no ATE changes, no ALC changes, no ADV\_FSP changes, no new assurance evidence, no new non-security features and no bug fixes.

Full coverage in Functional Testing evaluation activities performed in the assurance baseline is maintained with the proposed changes.

Given this, the CCTL determined that the proposed changes are not security relevant and thus the quality of the impact is considered 'minor'.

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