CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Seagate Secure ® TCG SSC Self-Encrypting Drives (CPP FDE EE V2.0E)

Maintenance Report Number: CCEVS-VR-VID11209-2022-2

Date of Activity: June 10, 2022

References:

Common Criteria Evaluation and Validation Scheme Publication #6 "Assurance Continuity: Guidance for Maintenance and Re-evaluation" Version 3.0, September 12, 2016

NIAP Policy #12 "Acceptance Requirements of a product for NIAP Evaluation." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" Version 2.1, June 2012

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

Supporting Document, Mandatory Technical Document – Full Drive Encryption: Encryption Engine, CCDB-2019, Version 2.0 + Errata 20190201, February 2019

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.2, May 20, 2022

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.2, May 20, 2022

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #2 Version 1.1, May 20, 2022

Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 0.3, May 20, 2022

Seagate Secure ® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description Version 0.5, May 20, 2022

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.2, May 20, 2022

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.2, May 20, 2022

Updated Developer Evidence:

Code change did not have any impact on the developer evidence of the validated TOE.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #2) to CCEVS for approval to add 2 firmware revisions to 4 CC certified hardware versions as shown here:

- add ***NF08*** based on firmware versions CSF2, NF04, and NF06
- add ***CF08*** based on firmware versions CS10, CF04, CF06, and CS11

The table below shows the model numbers and the new firmware version.

Changes to TOE:

In the updated ST, version 1.2, Table 1 was updated to show the 2 new firmware versions to 4 CC certified hardware versions.

These code changes did not impact the crypto software and, therefore, did not require update to the CAVP certificates. There were no changes to the EAR except to add the new hardware firmware versions.

The products, models, and firmware versions are shown in the table below. The new firmware versions added are shown in bold and italics in the validated firmware versions column.

Product Name	Model Number	Validated Firmware Versions
Nytro® 2032 SSD, 15mm, SAS Interface	XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	0001, 0002, 0203

Product Name	Model Number	Validated Firmware Versions
Nytro® 3032 SSD, 15mm, SAS Interface	XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104	0001, 0002, 0203
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0166 ST600MP0156	CK10, CF04, CF06
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0126 ST600MP0026	CKF1, NF04, CF06, NF06
BarraCuda Pro 2.5", SATA Interface	ST1000LM050 ST500LM035	SDM2, RXE2, RXE3, LXM7, RPE2, 0001, 1002, RPE4, LXMA, LXF1, LXF2
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST1200MM0069	CSF2, NF04, NF06, ***NF08***
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST2400MM0149 ST1800MM0149 ST1200MM0149	CS10, CF04, CF06, ***CF08***, CS11
Exos™ 7E8, SAS Interface	ST4000NM014A ST8000NM010A ST6000NM033A	EF01, EFA2, EF04
Exos™ 7E8, SAS Interface	ST4000NM015A ST3000NM005A	EF01, NFA2, NF04
Exos™ 7E8, SATA Interface	ST4000NM012A ST8000NM008A ST6000NM025A	SF01, SFA2, SF04
Exos™ 7E8, SATA Interface	ST3000NM004A ST4000NM013A	TF01, TFA2, TF04
Exos™ 16, SAS Interface	ST10000NM010G ST12000NM008G	EF01, EF02, EF03, EF04

Product Name	Model Number	Validated Firmware Versions
	ST14000NM012G ST16000NM009G	

There were no changes to the Development Environment.

Section 2.3. “Assurance Impact Determination” of the IAR specifies that there are a number of changes to the validated TOE, and none of the changes impact the secure operation of the TOE. The assurance impact of these changes is minor.

There are no changes to the TSF interface, no hardware changes, no SFR changes, no new security features, no changes to assumptions and objectives, and no new non-security features. The only changes that required updates to assurance evidence were the 1) update to the vulnerability assessment (AVA) and the 2) Security Target (ST) update to add the new firmware releases. Changes were also made to the KMD and EAR to add the new firmware releases and update any documentation references to the new version(s).

The IAR shows the there is one security relevant bug fix to allow commands to retrieve drive state information in the case where the security files have been corrupted. This change does not affect the underlying security architecture. All other fixes are not security relevant.

The only change to the TOE Environment was a minor maintenance action which required retesting but nothing more.

Description of ALC Changes:

Changes to the following documents were made:

From version 1.1 to 1.12

- Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target, Version 1.2, May 20, 2022
- Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target, Version 1.2, May 20, 2022

From version 0.2 to 0.3

- Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 0.3, May 20, 2022.

From version 0.4 to 0.5

- Seagate Secure ® TCG Enterprise SSC Self-Encrypting Drive and TCG Opal SSC Self-Encrypting Drive Common Criteria Full Drive Encryption – Encryption Engine Key Management Description, Version 0.5, May 20, 2022.

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #2) to add the 2 firmware revisions to 4 CC certified hardware versions listed above
- The IAR specifies the there is one security relevant bug fix to allow commands to retrieve drive state information in the case where the security files have been corrupted. This change does not affect the underlying security architecture. All other fixes are not security relevant.
- There are no changes to the development environment.
- Product level code change did not have any impact on the developer evidence of the validated TOE.

Description of Regression Testing:

For all storage products, Seagate performs a lengthy and rigorous suite of regression tests before releasing any firmware revisions. Regression testing performs a comprehensive set of security and non-security related test cases, including tests for device I/O throughput and performance, device read/write verification, servo performance, shock and vibration, environmental, secure port locking, firmware updates, secure boot signature verification and roll back protection. In addition, secure SED and FIPS or CC certified secure storage products are tested for all aspects of security including all TCG commands, ATA commands, FDE encryption modes, credentials, retry limits, band creation and deletion, and FIPS and CC mode testing. The entire regression test process takes about 3 weeks to complete. Regression testing was conducted for these firmware releases. Refer to the following table for the test intervals for these releases.

Product Name	Model Numbers	Firmware Version	Test Completion Date
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST1200MM0069	NF08	03/16/2022
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST2400MM0149 ST1800MM0149 ST1200MM0149	CF08	03/17/2022

Vulnerability Assessment:

Seagate searched the Internet for potential vulnerabilities in the TOE using the three web sites listed below.

- National Vulnerability Database (NVD, https://nvd.nist.gov/),
- MITRE Common Vulnerabilities and Exposures (CVE, http://cve.mitre.org/cve/), and

- United States Computer Emergency Readiness Team (US-CERT, http://www.kb.cert.org/vuls/html/search)

Seagate selected the 26 search key words based upon the vendor's name, the product name, and key platform features the product leverages. The search terms used were:

- Seagate
- Seagate Secure TCG Opal SSC
- Seagate Secure TCG Enterprise SSC
- ARMv7
- ARM Cortex-R
- ARM Processor
- 800-90 DRBG 1.0 Firmware
- ARMv7 AES in Firmware
- ARMv7 AES Key Wrap in Firmware
- ARMv7 GCM in Firmware
- ARMv7 HMAC in Firmware
- ARMv7 RSA in Firmware
- ARMv7 SHS in Firmware
- Hash Based DRBG 2.0 Firmware
- Balto
- Cheops
- Myna
- drive encryption
- disk encryption
- key destruction
- key sanitization
- self-encrypting drive
- sed
- opal
- enterprise ssc
- tcg ssc

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. This search was performed on May 18, 2022. No vulnerabilities applicable to the TOE were found.

Vendor Conclusion:

The 'Description of Changes' section (Chapter 2) of the IAR indicates that there are no changes to the development environment of the validated TOE. The 'Description of Changes' section of the IAR further indicates that there are no security relevant firmware changes to the validated TOE.

Based on this and other information from within this IAR document, the assurance impact of these changes is minor.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are minor, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The updated Security Target changed to add the new hardware models and the new firmware version identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.