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-VID11248-2023

Date of Activity: April 27, 2023

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, March 8, 2023

Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.2, March 8, 2023

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #2 for VID #11248 Version 1.1, April 27, 2023

Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 1.2, March 8, 2023

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 11.5, March 8, 2023

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.2, March 8, 2023

Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.2, March 8, 2023

Updated Developer Evidence:

The developer has provided sufficient supporting rationale describing the impact of each change. There are no changes to the TSF interface, no SFR changes, no new security features, and no changes to the assumptions and objectives. Two new hardware models are being added with this Assurance Maintenance: ST18000NM002D and ST20000NM005D. The new hardware versions are based on the existing certified hardware models and the hardware change is minor in scope to achieve greater storage capacity. There were no changes to the Development Environment, or to the Security Functions. Table 14 "Impact of Product Code Changes on the Developer Evidence of the Validated TOE" in the IAR lists all the changes identifying the changes; new features and enhancements (9), performance improvements (9), and bug fixes (69). It shows for each entry whether the change meets
NIAP Policies, and if it affects the Security Target, the TOE Reference, the TOE Configuration Items, the TSF Abstraction Levels, Guidance Documentation, and Assurance Activity Tests. All meet NIAP Policies and no security parameter is impacted.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #2) to CCEVS for approval to add 2 new firmware versions and 2 new hardware models. Firmware version EF04 was added to certified Exos X18 models. Two new Exos X20 models, based on existing certified hardware models, were added with the new firmware version EF03. These changes are captured in the table shown here:

Product Name	Model #	Capacity (GB)	Standard	New Firmware Version
Exos X18 3.5" SAS HDD	ST18000NM007J ST16000NM007J ST14000NM007J ST12000NM007J ST10000NM016G	18000 16000 14000 12000 10000	Enterprise SSC	EF04
Exos X20 3.5" SAS HDD	ST18000NM002D ST20000NM005D	18000 20000	Enterprise SSC	EF03

Changes to TOE:

There were 87 non-security relevant firmware changes associated with this Assurance Continuity update. There was the addition of two new hardware models (ST18000NM002D and ST20000NM005D). The new hardware versions are based on the existing certified hardware models and the hardware change is minor in scope to achieve greater storage capacity. There were no changes to the Development Environment, or to the Security Functions. The following table is an accounting of the firmware changes divided into the sub-categories: New Features and Feature Enhancements, Performance Improvements, and Bug Fixes. Detailed information regarding each of the firmware changes is provided in the IAR (Impact Analysis Report).

Category	Number of Changes	Applicability to New Firmware Versions
New Features and Feature Enhancements	9	There were no new Features, and all nine Feature Enhancements were included in the new firmware versions.
Performance Improvements	9	All nine Performance Improvements were included in the new firmware versions.
Bug Fixes	69	68 Bug Fixes were included in all new firmware versions. There was one performance improvement that was only included in firmware version EF03.

The 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 and KMD except to add the new firmware releases and the new hardware modules and to update any documentation references to the new version(s).

Description of ALC Changes:

Changes to the following documents were made:

From version 1.1 to 1.2 of the Security Target

- Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.2, March 8, 2023
- Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.2, March 8, 2023

From version 1.1 to 1.2 of the Entropy Documentation

- Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 1.2, March 8, 2023

From version 11.4 to 11.5 of the Encryption Engine Key Management Description

- 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 11.5, March 8, 2023

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #2) to add the 2 firmware revisions and 2 new hardware models listed above
- There are no security relevant code changes.
- 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:

The assurance activities performed during the original conformance and certification process remain applicable and were not repeated. Comprehensive regression testing was performed for the new firmware releases.

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)

This evaluation activity was performed on April 27, 2023, using the search terms specified below.

Seagate selected the 27 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
- ARMv6-M
- Cortex-M0
- ARM Processor
- 800-90A DRBG in Hardware
- ARMv6 AES in Firmware
- ARMv6 AES Key Wrap in Firmware
- ARMv6 GCM in Firmware
- ARMv6 HMAC in Firmware
- ARMv6 RSA in Firmware

- ARMv6 SHS in Firmware
- Janus
- drive encryption
- disk encryption
- key destruction
- key sanitization
- self encrypting drive (sed)
- Opal
- opal ssc ata security
- enterprise ssc
- Enterprise SSC ATA Security
- tcg ssc
- Exos X18
- Exos 7E10
- Exos X20

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 March 6, 2023. 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.