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-VID11248-2022

Date of Activity: January 20, 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 1.1, September 16, 2022

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.1, September 16, 2022

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #1 for VID #11248 Version 1.4, January 18, 2023

Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 1.1, September 16, 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 11.4, September 16, 2022

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.1, September 16, 2022

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.1, September 16, 2022

Updated Developer Evidence:

The developer has provided sufficient supporting rationale describing the impact of each change. There are no changes to the TSF interface or hardware or the development environment. There are no changes to the existing SFRs and there was no new security feature added. There are no changes to the assumptions and objectives. Table 13 "Impact of Product Code Changes on the Developer Evidence of the Validated TOE" in the IAR lists all the changes described in the three tables detailing the changes, new features, performance improvements, and bug fixes. 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.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #1) to CCEVS for approval to add 5 firmware versions EF02, KF02, NF02, SF02, and TF02, to 14 CC certified hardware versions as shown here:

Product Name	Model #s	New Firmware
Exos 7E10 3.5" SAS HDD	ST10000NM022B ST10000NM011B ST8000NM022B ST8000NM011B ST6000NM024B ST6000NM013B ST4000NM013B ST4000NM029B ST4000NM017B	EF02 KF02 NF02
Exos 7E10 3.5" SATA HDD	ST10000NM021B ST8000NM021B ST6000NM023B ST4000NM012B ST4000NM028B	SF02 TF02

Changes to TOE:

In the updated ST, version 1.1, Table 1 "Table 1: TOE Models and Firmware Versions", was modified to show the 5 new firmware versions added to 14 CC certified hardware versions.

There were 111 non-security relevant firmware changes associated with this Assurance Continuity update. There were no changes to the TSF Hardware, to the Development Environment, or to the Security Functions. The table below is an accounting of the firmware changes made to support the new versions of firmware. It is 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. None of the code changes are security relevant.

Category	Number of Changes	Applicability to New Firmware Versions
New Features and Feature Enhancements	7	There were no new Features, and the seven Feature Enhancements were included in all the new firmware versions.
Performance Improvements	13	All 13 Performance Improvements were included in all the new firmware versions.
Bug Fixes	91	90 Bug Fixes were included in all new firmware versions. There was an error logging fix that was only included in firmware versions SF02 and TF02.

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 except to add the new hardware firmware versions.

Description of ALC Changes:

Changes to the following documents were made:

From version 1.0 to 1.1 of the Security Target

- Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.1, September 16, 2022
- Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.1, September 16, 2022

From version 1.0 to 1.1 of the Entropy Documentation

- Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 1.1, September 16, 2022

From version 11.3 to 11.4 of the Entropy Documentation

- 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 11.4, September 16, 2022

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #2) to add the 5 firmware revisions to 14 CC certified hardware versions 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 October 27, 2022, using the search terms specified below.

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
- 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

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 October 27, 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.