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-VID11209-2023

Date of Activity: September 12, 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 1.3, August 25, 2023 [ST]

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1. 3, August 25, 2023 [ST_PUB]

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #3 Version 1.0, August 25, 2023

Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 0.4, August 25, 2023 [ENT]

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 0.6, August 25, 2023 [KMD]

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.3, August 25, 2023

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.3, August 25, 2023

Affected Developer Evidence:

No changes were made to any products, or the development environment associated with the TOE. No developer evidence is affected.

Updated Developer Evidence

No changes were made to any products, or the development environment associated with the TOE. No updates to the developer evidence are required.

Updates were made to the following documents: [ENT], [KMD], [ST], and [ST_Pub]. All the changes were to fix grammar and formatting issues and there is no assurance impact as a result of the changes.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #3) to CCEVS in order to extend the certificate for an additional year.

Changes to TOE:

No changes were made to any products, or the development environment associated with the TOE.

Description of ALC Changes:

Changes to the following documents were made:

From version 1.2 to 1.3

- Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target, Version 1.3, August 25, 2023
- Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target, Version 1. 3, August 25, 2023

From version 0.3 to 0.4

- Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 0.4, August 25, 2023

From version 0.5 to 0.6

- 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 0.6, August 25, 2023

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #3) to extend the certificate for 1 year.
- The IAR specifies the there no changes to the product.
- There are no changes to the development environment.
- There were no code changes.

Description of Regression Testing:

No changes were made to any products, or the development environment associated with the TOE. No regression testing is required.

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 August 21, 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 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.