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-VID10857-2020

Date of Activity: 3 June 2020

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." March 20, 2013

Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements" Version 1, February 2004

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #6 Version 1.0 February 15, 2020

Seagate Secure ® TCG SSC SED Security Target Version 7.0, Proprietary February 15, 2020

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 7.0 February 15, 2020

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 7.0 February 15, 2020

Affected Evidence:

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 7.0 Proprietary February 15, 2020

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 #6) to CCEVS for approval to add six new versions of firmware, based on an existing Common Criteria certified version, to twenty-five Common Criteria certified Seagate product models. Firmware versions A003 and 0004 are both based upon existing firmware revision 0003. Firmware versions TFA2, NFA2, SFA2, and EFA2 are each based on existing firmware revisions TF01, NF01, SF01, and EF01, respectively.

The IAR specifies-that there are two security relevant firmware changes; both firmware changes fixed incorrect reporting issues related to the security subsystem but did not impact the underlying security architecture. The issue “Incorrect status/error reporting when drive is locked” (#60) occurred due to an incorrect status being sent when the drive is in a locked state. The issue “Activity LED is still driven after Crypto Erase” (#69) occurred due to an incorrect LED status not being reset after a crypto erase operation had completed.-Neither of these security relevant changes impacted the underlying security architecture or rendered drives into an insecure or vulnerable state. These changes did not impact the crypto software and, therefore, did not require update to the CAVP certificates.

Changes to TOE:

Firmware versions A003 and 0004 are both based upon existing firmware revision 0003. Firmware versions TFA2, NFA2, SFA2, and EFA2 are each based on existing firmware revisions TF01, NF01, SF01, and EF01, respectively.

The hardware models use the firmware versions as shown in the following table.

Validated Hardware Versions	New Firmware Versions
XS800LE70024, XS1600LE70024, XS3200LE70024, XS6400LE70024, XS400ME70024, XS800ME70024, XS1600ME70024, XS3200ME70024, XS960SE70024, XS1920SE70024, XS3840SE70024, XS7680SE70024, XS7680TE70024, XS3840TE70024, XS16360TE70024	A003 0004
ST3000NM004A, ST4000NM013A	TFA2
ST3000NM005A, ST4000NM015A	NFA2
ST4000NM012A, ST8000NM008A, ST6000NM025A	SFA2
ST4000NM014A, ST6000NM033A, ST8000NM010A	EFA2

Description of ALC Changes:

Changes to the following documents were made, going from version 6.0 to 7.0:

- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 7.0 Proprietary February 15, 2020
- Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 7.0 Public February 15, 2020

- Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 7.0 Dated: February 15, 2020
- 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 Report Version 7.0 Dated: February 15, 2020

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR) for the twenty-five Common Criteria certified models listed above
- The IAR specifies-that there are two security relevant firmware changes; both firmware changes fixed incorrect reporting issues related to the security subsystem but did not impact the underlying security architecture. There are no changes to the development environment.
- Code change did not have any impact on the developer evidence of the validated TOE.
- The changes to the ST and other documents were limited to document version with the addition of the new firmware version.

Description of Regression Testing:

For all storage products, Seagate performs 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 21 days to complete. Regression testing was conducted for these firmware releases starting January 17, 2020 and ending February 7, 2020.

Vulnerability Assessment:

Seagate searched 3 vulnerability databases, 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) for a large number of terms, on February 13, 2020. No new vulnerabilities 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 this IAR further indicates that there are a number of minor code changes to the product associated with the validated TOE. Of these, two are security relevant but neither impact the underlying security architecture.

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 concur 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, the Entropy Document, and the Key Management Description were only changed to add the new firmware version identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.