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-VID11209-2023-2

Date of Activity: February 21, 2024

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 1.5, January 25, 2024 [ST]

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.5, January 25, 2024 [ST_PUB]

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #4 Version 1.1, February 16, 2024

Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 0.6, January 25, 2024 [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 0.8, January 30, 2024 [KMD]

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.5, January 25, 2024

Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.5, January 25, 2024

Updated Developer Evidence:

The Security Target [ST], the Public ST [ST_Pub], Key Management Description [KMD], and Entropy Documentation [ENT] were updated to add the new products (5), new model numbers (21), and new firmware versions (2). No changes were made to the development environment associated with the TOE. No changes related to the Security Functional Requirements (SFRs), or Security Assurance Requirements (SARs) were made to the products or development environment associated with the validated TOE. No new assurance activity is required.

Affected 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. There were new hardware components: 5 new products, 21 new models, and 2 new firmware versions, SDM1 and 0204.

New FW version SDM1 was incorporated into 2 existing products and 5 existing models. The 30 changes of FW version SDM1 included 9 non-security bug fixes, 10 non-security new features, removal of 2 non-security features, 4 reliability improvements, and 5 performance optimizations.

New FW version 0204 was incorporated into 5 new products and 21 new models. FW version 0204 included 128 non-security relevant changes. The majority of the non-security relevant changes were described as fixes for 2 non-security bugs, 4 Log Page Errors, 9 Drive Hang - Power Cycle fixes, 2 System Hangs, 8 Incorrect Error/Sense Data Reports, 9 Assert (Flash LED), 14 Command (I/O) Timeouts, 7 Spec Violations, 10 Performance Impacts, 2 SMART changes, 6 Spec Updates, and 2 Log Page Updates. The remaining 53 non-security relevant changes covered a broad range of areas. There were also 2 security relevant fixes. The first one dealt with the need to guarantee that the security hardware is initialized before read/write commands are allowed to prevent mis-compare errors by initializing security read/write hardware earlier. The second modified the error reporting of entropy failures while all error conditions remain unchanged. Both of these changes were minor and had minor impact on the assurance of the TOE. As any change to the security code could cause unknown or unintended consequences, Seagate conducted code reviews and regression testing to mitigate any unintended consequences.

Description of ASE Changes:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #4) to CCEVS in order to add 5 new products, 21 new models, and 2 new firmware versions, SDM1 and 0204, to the existing Common Criteria certified Seagate product models. The new firmware versions are based on

existing certified firmware versions. These changes are captured in the table shown here, with the **bold text** indicating a new version:

Product Name	Model Number	New Firmware Version
BarraCuda 2.5", SATA Interface	ST2000LM010 ST1000LM038 ST500LM033	**SDM1** SDM2 RSE3 (1D) RDE3 (2D) RTE2 REE2
BarraCuda Pro 2.5", SATA Interface	ST1000LM050 ST500LM035	**SDM1** SDM2 RXE2 RXE3 LXM7 RPE2 0001 1002 RPE4 LXMA LXF1 LXF2
Nytro® 3750 SSD, 15mm, SAS Interface	**XS400ME70065** **XS800ME70065** **XS1600ME70065** **XS3200ME70065**	**0204**
Nytro® 3550 SSD, 15mm, SAS Interface	**XS800LE70065** **XS1600LE70065** **XS3200LE70065** **XS6400LE70065** **XS3840LE70065**	**0204**
Nytro® 3350 SSD, 15mm, SAS Interface	**XS960SE70065** **XS1920SE70065** **XS3840SE70065** **XS7680SE70065** **XS15360SE70065**	**0204**
Nytro® 2550 SSD, 15mm, SAS Interface	**XS960LE70105** **XS1920LE70105** **XS3840LE70105**	**0204**
Nytro® 2350 SSD, 15mm, SAS Interface	**XS960SE70105** **XS1920SE70105** **XS3840SE70105** **XS7680SE70155**	**0204**

Changes to TOE:

There were 30 non-security relevant changes for FW version SDM1 and 130 changes for FW version 0204, of these only 2 were security relevant. Both updated FW versions are based on existing certified firmware versions. The assurance impact of these changes is minor and even though there are 2 security-relevant changes included in this update, they are minor and do not require a new certification. There were no changes to the Development Environment, or to the Security Functions. The following is an accounting of the firmware changes, by updated FW version, divided into the sub-categories as shown in the table. Detailed information regarding each of the firmware changes is provided in the IAR (Impact Analysis Report).

Firmware Version	Category	Number of Changes
SDM1	Non-Security Relevant Bug Fixes	9
SDM1	Additional Non-Security Features	10
SDM1	Non-Security Features Removed	2
SDM1	Reliability Improvements	4
SDM1	Performance Optimization Updates	5
0204	Log Page Errors	4
0204	Drive Hang - Power Cycle fixes	9
0204	Incorrect Error/Sense Data Reports	8
0204	System hang fixes	2
0204	Assert (Flash LED)	9
0204	Command (I/O) Timeouts	14
0204	7 Spec Violations	7
0204	Performance Optimization Updates	10
0204	SMART changes	2
0204	Spec Updates	6
0204	Non-Security Relevant Bug Fixes and other non-security relevant changes	55

The code changes did not impact the cryptographic software and, therefore, did not require update to the CAVP certificates.

Description of ALC Changes:

Changes to the following documents were made:

From version 1.3 to 1.5

- Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.5, January 25, 2024
- Seagate Secure ® TCG SSC Self-Encrypting Drives Public Security Target Version 1.5, January 25, 2024

From version 0.4 to 0.6

- Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 0.6, January 25, 2024 [ENT]

From version 0.6 to 0.8

- 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 0.8, January 30, 2024 [KMD]

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #4) to add 5 new products, 21 new models, and 2 new firmware versions based on existing Common Criteria certified versions.
- There are security relevant fixes but they are minor and do not required a new certification.
- 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.
- There were no changes that required the evaluators to do any additional testing beyond regression testing.

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 three weeks to complete. Regression testing was conducted for the new product models with 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)

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 February 16, 2024. 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, Entropy Document, and Key Management Description were only 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.