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-VID11248-2023-2

Date of Activity: February 15, 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 1.4, January 12, 2024

Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.4, January 12, 2024

Seagate Secure ® TCG SSC Self-Encrypting Drives Impact Analysis Report #3 for VID #11248 Version 1.1, January 22, 2024

Seagate Secure ® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 1.3, December 22, 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 11.6, December 22, 2023

Affected Evidence:

Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.4, January 12, 2024

Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.4, January 12, 2024

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 new security features, and no changes to the assumptions and objectives. There was a change to the ST to correct the bits for RSA Signature Services from 2048 to 3072 bits. Five 5 new firmware release versions, EF03, TF03, SF03, NF03, and KF03, are being added to the certified Exos 7E10 models with this Assurance Maintenance release. The new firmware versions are based on existing certified firmware versions. There are 6 security relevant firmware changes and 55 non-security relevant firmware changes associated with this Assurance Maintenance release. There were no changes to the Development Environment, or to the Security Functions. Table 15 "Impact of Product Code Changes on the Developer Evidence of the Validated TOE" in the IAR lists all the changes identifying the security relevant fixes (6), the feature enhancements (3), performance improvements (3), and bug fixes (49). 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 #3) to CCEVS for approval to add 5 new firmware release versions, EF03, KF03, NF03, SF03, and TF03, to the certified Exos 7E10 models. These changes are captured in the table shown here:

Product Name	Model #	Capacity (GB)	Standard	New Firmware Version
Exos 7E10 3.5" SAS HDD	ST10000NM022B ST10000NM011B ST8000NM022B ST8000NM011B ST6000NM024B ST6000NM013B ST4000NM013B ST4000NM029B ST4000NM017B	10000 10000 8000 8000 6000 6000 4000 4000 4000	Enterprise SSC	**EF03** **KF03** **NF03**

Product Name	Model #	Capacity (GB)	Standard	New Firmware Version
Exos 7E10 3.5" SATA HDD	ST10000NM021B ST8000NM021B ST6000NM023B ST4000NM012B ST4000NM028B	10000 8000 6000 4000 4000	Enterprise SSC	**SF03** **TF03**

Changes to TOE:

There were 6 security relevant fixes and 55 non-security relevant firmware changes associated with this Assurance Maintenance update. The 5 new firmware versions are based on existing certified firmware versions. The assurance impact of these changes is minor and even though there are 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 table is an accounting of the firmware changes divided into the sub-categories: Security Relevant Fixes, 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
Security Relevant Fixes	6	Security relevant Fixes were included in all new firmware versions.
Feature Enhancements	3	There were no new Features and all 3 Feature enhancements were included in the new firmware versions
Performance Improvements	3	All three Performance Improvements were included in the new firmware versions.
Bug Fixes	49	45 Bug Fixes were included in all new firmware versions.

The code changes did not impact the cryptographic software and, therefore, did not require update to the CAVP certificates. The Security Target was changed to update ST Table 5: 'Cryptographic Functions' to show RSA: 3072 bits, from 2048, for Cryptographic signature services and to remove the superfluous CAVP A1086. CAVP A1093, which was already included, supports RSA: 3072 bits for Cryptographic signature service as required.

There were changes to the Security Target (ST) to update the TOE Models and Firmware Versions with the new firmware releases. The ST Cryptographic (Signature Verification) FCS_COP.1(a)) section changed to say RSA Digital Signature Algorithm with a key size (modulus) of 3072 from 2048 bit. Certificate #A1086 was removed. The Assurance Activity Report (AAR) was changed to specify the new firmware releases and firmware validation using a 3072-bit instead of 2048-bit public key and to remove CAVP A1086. The Common Criteria Evaluated Configuration Guide (AGD) was updated to new firmware release and to specify RSA Digital Signature Algorithm with a key size of 3072 from 2048 bits. There were no changes to the EAR and KMD except to add the new firmware releases and to update any documentation references to the new version(s).

Description of ALC Changes:

Changes to the following documents were made:

From version 1.2 to 1.4 of the Security Target

- Seagate Secure ® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.4, January 12, 2024
- Seagate Secure ® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.4, January 12, 2024

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 1.3, December 22, 2023

From version 11.5 to 11.6 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 11.6, December 22, 2023

From version 1.0 to 1.1 of the Common Criteria Evaluated Configuration Guide (AGD)

- Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Evaluated Configuration Guide, Version 1.1, 16 January 2024

From version 1.0 to 1.1 of the Assurance Activity Report

- Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Assurance Activity Report, Version 1.1, 11 January 2024

From version 1.0 to 1.1 of the Evaluation Technical Report

- Evaluation Technical Report for Seagate Secure® TCG SSC Self-Encrypting Drives (Seagate Proprietary), Version 1.1, 17 January 2024

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #3) to add 5 new firmware release versions, EF03, KF03, NF03, SF03, and TF03, to the certified Exos 7E10 models based on existing certified firmware 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.

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. As noted above, the changes did not require additional evaluator testing.

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 February 9th, 2024, 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 February 9th, 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 6 security relevant firmware changes to the validated TOE but these are minor and do not require a new certification.
>
> 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 firmware versions identified above and to update ST, including Table 5: Cryptographic Functions, to show RSA: 3072 bits, from 2048 bits, for Cryptographic signature services. Retesting wasn't required for the SFR change as the CAVP A1093 certificate covered 3072 as well as 2048 bits for RSA Signature Services. Further, none of the non-certificate related SFRs were impacted by that change or required retesting. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.