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-VID10857-2019-4

Date of Activity: 21 October 2019

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 #4 Version 1.1, August 30, 2019

Seagate Secure ® TCG SSC SED Security Target Version 5.0, Proprietary August 30, 2019

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 5.0 August 30, 2019

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 5.0 August 30, 2019

Affected Evidence:

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 5.0, Proprietary August 30, 2019

Updated Developer Evidence:

Assurance Continuity Maintenance Report:

Seagate Technology, LLC. submitted an Impact Analysis Report (IAR #4-2) to CCEVS for approval to update the code on twenty-nine Common Criteria certified Seagate product models including fourteen new product models. The twenty-nine modified models including the fourteen new models have five new firmware versions based on existing Common Criteria certified versions. The hardware change is minor in scope to achieve a more compact physical PCB layout. No components were changed or swapped.

The IAR describes code changes the vendor specifies as security relevant. One firmware change fixed a TCG specification violation due to reporting incorrect sense data. The issue "Drive reports good status for write command during Sanitize" (#28) occurred due to the status of an active low-priority command being returned instead of the expected failure status of an aborted sanitize operation. This firmware change is included in all new firmware versions submitted in this IAR. None of these changes impact the security functional requirements (SFR) against which the product was evaluated.

The ACMR is intended to satisfy requirements outlined in

- 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 1.0, February 2004.

In accordance with those requirements, the ACMR describes the changes made to the certified TOE, the evidence that was updated because of those changes, and the security impact of those changes.

Changes to TOE:

The TOE has been updated in the following ways.

- There are a relatively small number of changes to the validated TOE and only one of the changes has an indirect effect on the secure operation of the TOE. The assurance impact of these changes is minor. The issue "Incorrect sense data return after invoke sanitize follow by power-cycle" occurred due to an omitted variable check after the sanitization had completed successfully that treated the completion state the same as 'sanitization in progress'. (Change #28)
- The security relevant change submitted in this IAR fix a TCG specification violation due to reporting incorrect sense data, which did not impact the underlying security architecture.
- Additionally, there is one hardware change associated with a new product being added to this certification. This hardware change is minor, encompassing a PCB physical layout change only, and therefore does not present a risk to the security architecture that would necessitate further testing.

- The security relevant fixes and the minor hardware change therefore do not require any updates to developer evidence.

Twenty-nine Common Criteria certified Seagate product models have one of the new firmware versions that are based on existing Common Criteria certified versions

- Firmware version 0003 is based on the certified firmware revision 0002
- firmware versions EF01 is based on certified firmware revision NF04
- firmware versions NF01 are based on certified firmware revision NF04
- firmware versions SF01 is based on certified firmware revision CF04
- firmware versions TF01 is based on certified firmware revision CF04.

Of the 29 product models with one of the new firmware versions, 14 are new and the other 15 are existing hardware. See table below.

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

Model	New Firmware	Model Vintage
ST10000NM010G	EF01	New
ST12000NM008G	EF01	New
ST14000NM012G	EF01	New
ST16000NM009G	EF01	New
ST3000NM004A	TF01	New
ST3000NM005A	NF01	New
ST4000NM012A	SF01	New
ST4000NM013A	TF01	New
ST4000NM014A	EF01	New
ST4000NM015A	NF01	New
ST6000NM025A	SF01	New
ST6000NM033A	EF01	New
ST8000NM008A	SF01	New
ST8000NM010A	EF01	New
XS15360TE70024	0003	Existing
XS1600LE70024	0003	Existing
XS1600ME70024	0003	Existing
XS1920SE70024	0003	Existing
XS3200LE70024	0003	Existing
XS3200ME70024	0003	Existing
XS3840SE70024	0003	Existing
XS3840TE70024	0003	Existing
XS400ME70024	0003	Existing
XS6400LE70024	0003	Existing

XS7680SE70024	0003	Existing
XS7680TE70024	0003	Existing
XS800LE70024	0003	Existing
XS800ME70024	0003	Existing
XS960SE70024	0003	Existing

IAR 4-2 also specifies 20 existing hardware models that do not use one of the new processors based on certified firmware identified in this IAR. Some use firmware that was the basis of the new firmware.

Model	Firmware
ST500LM035	SDM2, RXE2, RXE3, LXM7, RPE2, 0001
ST1000LM050	SDM2, RXE2, RXE3, LXM7, RPE2, 0001
ST1200MM0149	CS10, CF04
ST1800MM0149	CS10, CF04
ST2400MM0149	CK10, CF04
ST1200MM0069	CSF2, NF04
ST600MP0156	CK10, CF04
ST900MP0166	CK10, CF04
ST600MP0026	SSM1, NF04
ST900MP0126	SSM1, NF04
XS400ME10023	7539, 0004, 0005
XS800ME10023	7539, 0004, 0005
XS1600ME10023	7539, 0004, 0005
XS6400LE70023	7539, 0004, 0005
XS1600LE10023	7539, 0004, 0005
XS1920SE10123	7539, 0004, 0005
XS3840TE10023	7539, 0004, 0005
XS7680TE70023	7539, 0004, 0005
XS15360SE70143	7539, 0004, 0005
XS3200ME70023	7539, 0004, 0005

Vendor Conclusion:

The IAR indicates that there are no changes to the development environment of the validated TOE. The IAR further indicates that there are a number of minor code changes to the product associated with the validated TOE. Of these, one is security relevant and does not affect the underlying security architecture.

Additionally, there is one hardware change associated with a new product added to this certification. This hardware change is minor, encompassing a PCB physical layout change only, and therefore does not present a risk to the security architecture that would necessitate further testing.
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 incorporate the updated and new model numbers and to add the new firmware versions identified above. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.