
**CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT**

**ASSURANCE CONTINUITY MAINTENANCE REPORT FOR**

---

**Seagate Secure ® TCG SSC Self-Encrypting Drives (CPP FDE EE v2.0)**

**Maintenance Report Number:** CCEVS-VR-VID10857-2018

**Date of Activity:** 14 November 2018

**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 Version 1.4, November 19, 2018

Seagate Secure ® TCG SSC SED Security Target Version 2.0 Public July 31, 2018

Seagate Secure ® TCG SSC SED Security Target Version 2.0 Proprietary July 31, 2018

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 1.0, Public April 4, 2018

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 1.0, Proprietary April 4, 2018

Seagate Secure ® TCG SSC SED CC Configuration Guide version 2.0 July 31, 2018

Seagate Secure ® TCG SSC SED CC Configuration Guide version 1.0 February 15, 2018

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 2.0 July 31, 2018

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 1.2 April 4, 2018

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 2.0 July 31, 2018

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 0.14 April 5, 2018

**Affected Evidence:**

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 1.0, Public April 4, 2018

Seagate Secure® TCG SSC Self-Encrypting Drives Security Target, Version 1.0, Proprietary April 4, 2018

Seagate Secure ® TCG SSC SED CC Configuration Guide version 1.0 2018-02-15

**Updated Developer Evidence:**

Seagate Secure ® TCG SSC SED Security Target version 2.0 Public 2018-07-31

Seagate Secure ® TCG SSC SED CC Configuration Guide version 2.0 2018-07-31

**Assurance Continuity Maintenance Report:**

Seagate Technology, LLC. submitted an Assurance Continuity Maintenance Report (ACMR) to CCEVS for approval to add two new versions of firmware to Common Criteria certified Seagate product models ST1000LM050 and ST500LM035.

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.

1. Two new versions of firmware have been added to Common Criteria certified Seagate product models ST1000LM050 and ST500LM035.
2. Each model number uses the same two new firmware revision numbers. The new firmware version numbers are RXE3 and LXM7.
3. Both RXE3 and LXM7 are based on the existing CC certified firmware revision RXE2.
    a. Two separate firmware revisions are required because these are unique customer configurations that have different compile time flags enabled.
    b. These compile time flags are minimal and mostly involve customer identification information.
    c. There are zero security related differences based on customer unique flags.
4. There are a total 28 firmware code changes that make up the two new CC firmware revisions. Of these, only one is security relevant. The item "Enable Block SID Feature" is security relevant and while it does not affect the developer evidence directly, if used incorrectly, it can prevent the drive from entering FIPS or CC mode, since SID authentication is required for CC mode. Because of this interaction, the vendor has added new developer evidence and information to the "Seagate Secure® TCG Enterprise and TCG Opal SSC Self-Encrypting Drive Common Criteria Configuration Guide" to instruct administrators and users on how to avoid this issue.
5. The updated Security Target, the Entropy Document, and the Key Management Description were only changed to incorporate the new firmware version, RXE3 and LXM7.

**Vendor Conclusion**:

The 'Description of Changes' section of this 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 28 code changes to the product associated with the validated TOE. Of these, none are security relevant. There is one 'Block SID Enable' change that blocks SID authentication and if used incorrectly by an administrator, can prevent the device from entering CC mode of operation, since SID authentication is required for CC mode. Seagate has mitigated this by adding language to the Common Criteria Guidance documentation instructing administrators on how to avoid this scenario. Based on this and other information from within the 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 new firmware version, RXE3 and LXM7. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.