



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-VID11209-2022

Date of Activity: March 9, 2022

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

Seagate Secure® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.1, February 4, 2022

Seagate Secure® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target Version 1.1, February 4, 2022

Seagate Secure® TCG SSC Self-Encrypting Drives Impact Analysis Report #1 Version 1.2, March 11, 2022

Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation Version 0.2, February 4, 2022

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 0.4, February 4, 2022

Affected Evidence:

Seagate Secure® TCG SSC Self-Encrypting Drives Proprietary Security Target Version 1.1, February 4, 2022

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 #1) to CCEVS for approval to add 18 firmware revisions to 12 CC certified hardware versions as shown here:

- add 0203 based on firmware versions 0001 and 0002
- add 0203 based on firmware versions 0001 and 0002
- add CF06 based on firmware versions CK01 and CF04
- add CF06 and NF06 based on firmware versions CKF1 and NF04
- add 1002, RPE4, LXMA, LXF1, and LXF2 based on firmware versions SDM2, RXE2, RXE3, LXM7, RPE2, and 0001
- add NF06 based on firmware versions SCF2 and NF04
- add CF06 and CS11 based on firmware versions CS10 and CF04
- add EF04 based on firmware versions EF01 and EFA2
- add NF04 based on firmware versions EF01 and NFA2
- add SF04 based on firmware versions SF01 and SFA2
- add SF04 based on firmware versions TF01 and TFA2
- add TF04 based on firmware versions EF01, EF02, and EF03

The table below shows the model numbers and the new firmware version.

Changes to TOE:

In the updated ST, version 1, Table 1 was updated to show the 18 new firmware versions to 12 CC certified hardware versions.

These code changes did not impact the crypto software and, therefore, did not require update to the CAVP certificates. There were no changes to the EAR except to add the new hardware firmware versions.

The products, models, and firmware versions are shown in the table below. The new firmware versions added are shown in bold and italics in the validated firmware versions column.

Product Name	Model Number	Validated Firmware Versions
Nytro® 2032 SSD, 15mm, SAS Interface	XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	0001, 0002, 0203
Nytro® 3032 SSD, 15mm, SAS Interface	XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104 XS7680TE70104	0001, 0002, 0203
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0166 ST600MP0156	CK10, CF04, CF06
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0126 ST600MP0026	CKF1, NF04, CF06, NF06
BarraCuda Pro 2.5", SATA Interface	ST1000LM050 ST500LM035	SDM2, RXE2, RXE3, LXM7, RPE2, 0001, 1002, RPE4, LXMA, LXF1, LXF2
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST1200MM0069	CSF2, NF04, NF06
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST2400MM0149 ST1800MM0149 ST1200MM0149	CS10, CF04, CF06, CS11
Exos™ 7E8, SAS Interface	ST4000NM014A ST8000NM010A ST6000NM033A	EF01, EFA2, EF04
Exos™ 7E8, SAS Interface	ST4000NM015A ST3000NM005A	EF01, NFA2, NF04
Exos™ 7E8, SATA Interface	ST4000NM012A ST8000NM008A	SF01, SFA2, SF04

Product Name	Model Number	Validated Firmware Versions
	ST6000NM025A	
Exos™ 7E8, SATA Interface	ST3000NM004A ST4000NM013A	TF01, TFA2, TF04
Exos™ 16, SAS Interface	ST1000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	EF01, EF02, EF03, EF04

Changes to the development environment of the validated TOE were made to support the new versions of firmware. These changes include bug fixes, performance improvements and feature requests; in this case most of the changes were fixes for incorrect error/sense data reporting, smart error, protocol violation, command (I/O), assert (Flash LED), log page errors, and drive hangs, and for performance optimization.

Section 2.3. “Assurance Impact Determination” of the IAR specifies that there are a number of changes to the validated TOE, and none of the changes impact the secure operation of the TOE. The assurance impact of these changes is minor. There are no changes to the TSF interface, no hardware changes, no SFR changes, no new security features, no changes to assumptions and objectives, no changes that require updates to assurance evidence, and no new non-security features. There is one security relevant fix to allow commands to retrieve drive state information in the case where the security files have been corrupted. This change does not affect the underlying security architecture. All other fixes are not security relevant.

The IAR shows the FW Version(s) in Table 8, Validated TOE Product Code Changes. For each FW change, the FW Version(s) cell lists the FW releases that include the change. Many of the changes are included in all 18 releases. In other cases, the change is only relevant to SATA devices and in the remaining cases, the change is only relevant to SAS devices. As Table 8 indicates, none of the changes in this update are security relevant. All changes are to address non-security issues. For further detail, see table below.

#	Change Description	Security Relevant?	Comments	FW Version(s)
1	Update the Extent/HatArrayBasePTR in MCMT (Media Cache Management Table) buffer when loading second MCMT copy	N	Fix for Assert (Flash LED)	LXMA 1002 RPE4 LXF1 LXF2

#	Change Description	Security Relevant?	Comments	FW Version(s)
2	Add support for spin-up to detect bad heads	N	Fix to detect bad heads and come ready without them.	LXMA 1002 RPE4 LXF1 LXF2
3	NCQ (Native Command Queuing) read/write in STX_NODEUNLOADSTRESS	N	Fix for (I/O) timeout	LXMA 1002 RPE4 LXF1 LXF2
4	IOEDC (Input / Output Error Detection Code) error on read command after SMART warning occurs during a read stream	N	Fix for incorrect error/sense code	EF04 NF04
5	High Load Unload Count with Host Read Device Statistics Log	N	Fix for error detection failure	EF04 SF04 TF04
6	IOEDC error on Read with encryption drive	N	Ensure HW does not pre-fetch data beyond current command boundary	EF04 NF04
7	Incorrect model number reported in boot mode	N	Fix inquiry / identify device error	EF04 NF04
8	Unrecoverable write error logged in write LogPage for NVC (Non-Volatile Cache) write back IOEDC error	N	Fix for log page error	EF04 CF04 SF04 NF04 TF04 NF06 CS11
9	Long latency in random writes mixed with some large writes test	N	Performance optimization	EF04 SF04
10	Command timeouts across multiple drives with infinite max burst size	N	Fix for command (I/O) timeout	EF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
11	Stale data mis-compare on read-write access pattern	N	Fix for mis-compare	EF04
12	Pin 11 activity LED not functioning if pin 11 is pulled low at power on	N	Fix for specification violation	EF04
13	Drive does not spin up on power up after PHY (Physical Layer) initialization is complete	N	Fix for drive not spinning up	EF04
14	Allow set sector configuration command when drive is in format corrupt	N	Fix to allow set sector commands when drive is in format corrupt mode	EF04 NF04 SF04
15	Change the SMART temperature attribute threshold to 0	N	Default SMART temperature threshold to 0	EF04
16	Drive goes into format corrupt mode on 4160 sector size	N	Update max LBA for specific 4160 sector size	EF04
17	Format corrupt caused by incorrect information in checksum error	N	Fix for incorrect error / sense code	EF04 NF04 SF04 TF04
18	Disable background DIC (Data Integrity Check) task	N	Performance optimization	EF04 NF04
19	Sequential write performance lower than expected	N	Performance optimization	EF04 NF04 SF04 TF04
19	IBT (In Bus Trace) log pull (0x400 sectors) aborts unexpectedly	N	Fix for incorrect error / sense code	EF04
20	Command timeout with repeated FReD (Field Reader Depopulation) error recovery	N	Fix for command (I/O) timeout	EF04
21	Servo flaws are not cleared in Sanitize overwrite pass	N	Fix for incorrect error / sense data reporting	EF04 NF04 SF04 TF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
				CS11
22	EMAP (Electronic Mapping) track offset not restored	N	Fix for log page error	EF04
23	IOPS (Input / Output Operations) drop when running extended (multi-day) tests	N	Performance optimization	EF04 NF04 TF04
24	Internal event improperly reported as an assert	N	Fix for incorrect error sense data reporting	EF04 NF04 SF04 TF04 CS11
25	03/16 errors on drives with degraded reader after certain download sequences	N	Fix for incorrect error / sense code reporting	EF04
26	Parity collection skipped for auto-reallocation requests	N	Fix for parity collection logic error	EF04
27	Assert after DOS (Direct Offline Scan) rewrites the last user track	N	Fix for Assert (Flash LED)	EF04 CS11
28	Assert seen during performance testing	N	Fix for Assert (Flash LED)	EF04 CS11
29	Unrecoverable read error seen following highly localized write intensive workload	N	Fix for incorrect error / sense data reporting	EF04 SF04
30	Command timeouts due to DOS and Media Cache cleaning	N	Fix for command (I/O) timeout	EF04
31	SMART attribute 10h counter incremented incorrectly	N	Fix for SMART counter error	EF04
32	DOS refresh counts are incremented on partial track refresh	N	Fix for specification violation	EF04
33	Assert due to divide-by-zero calculation	N	Fix for assert (Flash LED)	EF04 CS11
34	Rebuild Assist cannot select heads beyond 16	N	Fix for specification violation	EF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
35	Unrecoverable read errors seen during post margin testing	N	Performance optimization to address read errors	EF04
36	Drives goes format corrupt if certain NVC metadata is not saved on a power cycle	N	Fix for incorrect error / sense data reporting	EF04
37	Format failed with resident DST (Drive Self Test) full	N	Fix for incorrect error / sense data reporting	EF04 CS11
38	Assert when drive is initializing after hardware reset	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04
40	04/09/00/9C during write recovery sequence near end of track	N	Fix for incorrect error / sense data reporting	EF04 NF04 SF04 TF04
41	Activity LED stops functioning after code download	N	Fix for incorrect LED behavior	EF04 SF04 TF04
42	Format between same internal sector size but different host sector size fails	N	Fix to correct MaxLBA logic	EF04
43	Assert when cleaning Media Cache	N	Fix for assert (Flash LED)	EF04
44	Drive does not report that it has entered idle A	N	Fix to bounds checking to prevent underflow	EF04 NF04 SF04 TF04 CS11
45	Assert during head depopulation test	N	Fix for assert (Flash LED)	EF04
46	10+ second timeout on low performance command due to cache flush	N	Fix for command (I/O) timeout	EF04
47	Read command timeout when RevertSP operation interrupted by power cycle	N	Fix for command (I/O) timeout	EF04 NF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
				SF04 TF04 CS11
48	IOEDC error after uncorrectable error	N	Fix for incorrect error / sense data reporting	EF04 SF04
49	WFI (Wait for Interrupt) on NCQ (Native Command Queuing) ZACManagementOut following sequential reads / writes	N	Fix for command (I/O) timeout	EF04
50	Wrong sense data for first non-identity command after inner signature error	N	Fix for incorrect error / sense data reporting	EF04 NF04 SF04 TF04 CS11
51	Incorrect "under pressure" sense code	N	Fix for SMART error	EF04 NF04 SF04 TF04 CS11
52	Improve logging capability for IDD (In-Drive Diagnostics) feature	N	Improve system level error reporting	EF04
53	Drive assert due to mDRAM cleaning state machine problem	N	Fix for assert (Flash LED)	EF04 SF04
54	Assert in WCD (Write Cache Disabled) environment with NVC cache space constrained and hard resets	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04
55	Host unable to open session after power cycle interrupted crypto scramble	N	Fix for specification violation	EF04
56	Assert during creating of ISP (Intermediate Super Parity) node	N	Fix for assert (Flash LED)	EF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
57	Incorrect sense code reporting after a read error during DIC operation	N	Fix for incorrect error / sense data reporting	EF04 NF04 CS11
58	Unexpected transition from Sanitize SD4 to SD0 state on soft reset	N	Fix for protocol violation	EF04 NF04 SF04 TF04
59	I/O timeout reallocating on write pass of WRITE AND VERIFY	N	Fix for command (I/O) timeout	EF04 NF04 SF04 TF04 CS11
60	Flash LED on write same when media cache cleaning is active	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04
61	Assert during format when interrupted with resets	N	Fix for assert (Flash LED)	EF04 SF04
62	Assert during PVT (Parity Validity Table) scan on track with partial reallocated sector	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04 CS11
63	Assert on Write Command due to failure to get ISP resources	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
64	Resolve intermittent drive hang on READ/WRITE FPDMA (First Parity Direct Media Access)	N	Fix for drive hang	EF04
65	Format command with FMTDATA set to zero and FMTPINFO set to non-zero not aborted by drive	N	Fix for specification violation	EF04 NF04 CS11
66	IOPS loss during write workload	N	Performance optimization	EF04
67	Assert after initiating IDD Long Test as a background task	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04 CS11
68	Read command timeout during mixed write/read overlapped workload	N	Fix for command (I/O) timeout	EF04
69	Drive hang during SAS error injection testing	N	Fix for drive hang	EF04 CS11
70	Persistent reservation does not persist on a download	N	Fix for specification violation	EF04 CS11
71	Assert during Sanitize command	N	Fix for assert (Flash LED)	EF04
72	Drive hand during recovery of corrupted system file	N	Fix for drive hang	EF04
73	Run-to-run performance variation in random write workload	N	Performance optimization	EF04
74	Asserts after WCE (Write Cache Enabled)=1 random writes with flush and power cycles	N	Fix for assert (Flash LED)	EF04
75	Assert storm during download sequence	N	Fix for assert (Flash LED)	EF04
76	Assert during repopulation operation	N	Fix for assert (Flash LED)	EF04 SF04 TF04
77	SAS IDD not completing as expected	N	Fix for incorrect status reporting	EF04
78	0B/09/04/00 error reported by the drive after a power cycle	N	Correct logic error when drive checking for failed heads	EF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
79	Reduce amount of read look-ahead performed when drive is idle	N	Performance optimization	EF04 NF04 SF04 TF04 CF06 NF06 CS11
80	Disable Internal Write to Write Verify Conversion feature	N	Performance optimization	EF04 NF04
81	Long IO latency in random mixed read-write with unaligned workload	N	Performance optimization	EF04
82	Device statistics reported uncorrectable and SMART attribute 187 out-of-sync	N	Fix for log page error	EF04
83	Drive taken offline during hot plug	N	Fix for protocol violation	EF04 NF04 CS11
84	Log Page 3A download tag shows incorrect microcode level	N	Fix for incorrect log page error	EF04 NF04 SF04 TF04
85	Optimize some LPC (Lap Rate Control) commands	N	Performance optimization	EF04
86	Support internal flush mirror cache when drive goes idle	N	Performance optimization	EF04 SF04
87	EMAP (Electrical Map) number of LBAs to EMAP input error	N	Fix for incorrect log page error	EF04
88	Log page 08 information incorrect when EPC (Extended Parity Check) is disabled	N	Fix for incorrect log page error	EF04 SF04 TF04
89	IOPs drop during frequent SMART commands sent during MC (Media Cache) mirror random writes	N	Performance optimization	EF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
				NF04 SF04 TF04
90	PHY resets are slow to complete	N	Fix for command (I/O) timeout	EF04 NF04 SF04 TF04
91	Command timeout during DOS scan of the alternate sector region	N	Fix for command (I/O) timeout	EF04
92	Incorrect value of bits in the ZAC2 (Zoned Device ATA Command) capabilities flag in ID log page 3	N	Fix for specification violation	EF04
93	Write fault scan is not triggering with the required urgency	N	Fix to write fault scans with urgency	EF04
94	IDD log reporting g-list entries when they are no longer needed	N	Remove the g-list entry from the IDD log	EF04
95	Do not run Write/Read DST after code download	N	Performance optimization	EF04
96	Disable intermediate parity scan	N	Reduce read amplification	EF04 NF04 SF04 TF04 CS11
97	Assert when performing depop sequence	N	Fix for assert (Flash LED)	EF04
98	MDRAM (Mirrored DRAM) cleaning running with sweep seeks	N	Restrict MDRAM cleaning schedules during idle1 time	EF04 NF04
99	Format corrupt detected	N	Fix for assert (Flash LED)	EF04 NF04
100	Issue with processing grown defect list	N	Fix inconsistency in grown defect list following T10 fast format	EF04 NF04 SF04 TF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
101	Security commands aborted after security files are corrupted	Y	Allow the commands to retrieve drive state in case of security files corruption. Does not affect the underlying security architecture.	EF04 SF04 TF04
102	Assert during write transfer with reallocated blocks	N	Fix for assert (Flash LED)	EF04
103	Logged user write counts (log page 0x37) are incorrect after format	N	Fix for log page error	EF04
104	IOECC incorrectly injected recoverable error in a log page	N	Fix for log page error	EF04
105	Assert during write transfer with multiple reallocated blocks	N	Fix for assert (Flash LED)	EF04
106	Performance drop on random write workload	N	Performance optimization	EF04
107	Large IOPS (Input / Output Operations per Second) drop after a block size switch from 1K to 4K during random writes	N	Performance optimization	EF04
108	Device statistics counters incorrectly updated during certain power transitions	N	Fix for log page error	EF04
109	Assert encountered during Send Diag command with Rebuild Assist	N	Fix for assert (Flash LED)	EF04
110	Reserved bytes of IBT data are not zero	N	Fix for specification violation	EF04
111	Asserts reported on drives with degraded NAND	N	Fix for assert (Flash LED)	CF06
112	Assert during Write Same command processing	N	Fix for assert (Flash LED)	CF06 NF06 CS11
113	Drive becomes unresponsive following Hard Reset during Write command workload	N	Fix for incorrectly scheduled disc write operation	CF06 NF06 CS11
114	Aligned write command timeout due to dynamic WCD streaming	N	Fix for command (I/O) timeout	CF06 CS11
115	Drive asserts when processing write same commands	N	Fix for assert (Flash LED)	CF06 NF06 CS11

#	Change Description	Security Relevant?	Comments	FW Version(s)
116	Single SAS port becomes unresponsive during error injection testing	N	Fix for command (I/O) timeout	CF06 NF06 CS11
117	Assert on Write command with data frame error	N	Fix for assert (Flash LED)	CF06 NF06
118	Assert during Write Same command processing	N	Fix for assert (Flash LED)	CF06 NF06 CS11
119	Non-medium access command times out after Start immed=1 command	N	Fix for assert (Flash LED)	CF06 NF06 CS11
120	Assert when during IT Nexus Loss event	N	Fix for assert (Flash LED)	CF06 NF06
121	Ensure Attribute Worst case values do not get set to 0	N	Fix for SMART log error	CF06 NF06
122	Drive hang after NAND hybrid program or erase error	N	Fix for drive hang	CF06
123	Unexpected flash programming errors caused SMART warning (01/0B/04/00)	N	Fix for SMART log error	CF06
124	Servo positional error information is invalid in UDS	N	Fix for UDS log error	CF06 NF06 CS11
125	Forced Sweep Seek performance enhancements	N	Performance optimization	CF06 NF06 CS11
126	Assert while processing write command when DOS is active	N	Fix for assert (Flash LED)	CF06 NF06 CS11

#	Change Description	Security Relevant?	Comments	FW Version(s)
127	Assert on overlapping Read FUA (Forced Unit Access) commands	N	Fix for assert (Flash LED)	CF06 NF06
128	Incorrect use of encoding seed during internal write to parity sectors	N	Fix for assert (Flash LED)	CF06 NF06
129	Timeout on Read that overlaps with cached mirror data	N	Fix for command (I/O) timeout	CF06 NF06
130	Assert when adjusting read for ROA (Read On Arrival)	N	Fix for assert (Flash LED)	CF06 NF06
131	Internal calculation error after reallocation during merge Write operation	N	Fix for specification violation	CF06
132	Drive hang during sequential writes when interrupted by resets	N	Fix for drive hang issue	CF06
133	Assert during concurrent Read and Destroy MFR Credentials operations	N	Fix for assert (Flash LED)	CF06 NF06
134	Incorrectly scheduling commands that are not ready for transfer	N	Fix for assert (Flash LED)	CF06 NF06
135	Assert when running a SMART DST (Drive Self Test)	N	Fix for assert (Flash LED)	CF06 NF06
136	500MB partition random Read with hybrid cache hits disabled via ModePage	N	Performance optimization	CF06
137	Improve response times of Log Sense, Inquiry, and Test Unit Ready commands	N	Performance optimization	CF06 NF06
138	SMART warning reported multiple times	N	Fix for SMART error	CF06
139	Assert during Read commands in mixed workloads	N	Fix for assert (Flash LED)	CF06 NF06
140	04/44/F2/xx error reported during random Write Read test	N	Fix for incorrect error / sense data reporting	CF06 NF06
141	Disable intermediate parity scan	N	Performance optimization	CF06 NF06

#	Change Description	Security Relevant?	Comments	FW Version(s)
142	Intermittent CCT (Constant Clearance Tests) spikes / performance drops during Read streaming	N	Performance optimization	CS11
143	Flash LED reported during sequential write	N	Fix for assert (Flash LED)	CS11
144	Link reset response time exceeds 3 seconds	N	Fix for command (I/O) timeout	CS11
145	Excessive Servo flaws during write retry sequence	N	Fix to address excessive Servo flaws during write retries	CS11
146	Single Reader error recovery SMART counters incorrect	N	Fix for SMART log error	CS11
147	16K Q16 WCD random write performance lower than expected	N	Performance optimization	CS11 EF04 NF04 SF04 TF04
148	Improvement to FReD2 channel reload	N	Fix for assert (Flash LED)	CS11
149	Assert FLED 8A1C when repeat write of last user LBA track	N	Fix for assert (Flash LED)	CS11
150	After G2P pad, some grown defects are not padded	N	Fix for SMART log error	CS11
151	Temperature PZT (Piezoelectric Transducer) calculation not run at the aggressive schedule	N	Fix to ensure PXT calculations run every 10 seconds when temperature changes	CS11
152	Enable Single Reader Retry Feature	N	Enable feature (single reader retry)	CS11
153	Unrecoverable Read errors due to early Write timing	N	Fix for parity (CRC) error	CS11
154	Assert encountered during WCS sequential write	N	Fix for assert (Flash LED)	CS11
155	Short DST reports false failures during Read Verify operation	N	Fix for incorrect error / sense data reporting	CS11
156	Full format encountered an assert	N	Fix for assert (Flash LED)	CS11
157	Assert due to mismatch in Mode Page settings	N	Fix for assert (Flash LED)	CS11
158	Drive hang during recovery of a corrupted system file	N	Fix for drive hang when drive's file system becomes corrupted	CS11
159	FLED 76AD observed when going from FReD2 enabled code to FReD2 disabled code	N	Fix for assert (Flash LED)	CS11

#	Change Description	Security Relevant?	Comments	FW Version(s)
160	Assert due to FReD accessing RAP	N	Fix for assert (Flash LED)	CS11
161	Possible assert during DST	N	Fix for assert (Flash LED)	CS11
162	Unexpected reservation conflict status after new firmware download	N	Fix for protocol violation	CS11
163	Unexpected 03/11 errors on Read Long commands	N	Fix for incorrect error / sense data reporting	CS11 EF04 NF04 SF04 TF04
164	SAS drive fails to sync up when failing to next lower rate during Train_Rx-SNW	N	Fix for protocol violation	CS11
165	Corrupted location not found by background parity scan in time	N	Fix for incorrect error sense data reporting	CS11
166	SAS drive fails speed negotiation and stops responding to COMINIT	N	Fix to detect when controller is stuck in a "speed negotiation" failure and transition to idle state	CS11
167	New Diagnostic error for Read/Write failure to generate super block parity on clean	N	Fix for absent error / sense data reporting	CS11
168	Super parity recovery fails if there is ALT (Accelerated Life Testing) at the last sector	N	Fix for incorrect error / sense data	CS11
169	Timeout event when running offline DST	N	Fix for command (I/O) timeout	CS11
170	Timeout during read sequences	N	Fix for command (I/O) timeout	CS11
171	Read command received unexpected good status during error injection test	N	Fix for incorrect error sense data reporting	CS11
172	IDD (In Drive Diagnostics) SAS BER calculations incorrect	N	Fix for incorrect error sense data reporting	CS11
173	Drive offline after entering stop-state	N	Fix for log page error	CS11
174	If BER is invalid do not report value	N	Fix for incorrect error sense data reporting	CS11
175	SMART trip is not being reported when Reman is enabled	N	Fix for SMART error not being reported	CS11
176	Attribute information mismatch	N	Fix to ensure SMART attribute and FARM log data are in sync	CS11

#	Change Description	Security Relevant?	Comments	FW Version(s)
177	Add Read polarity flips to the SMART frame	N	Add data to FARM log	CS11
178	Multi-signal magnetic recording reader select by region	N	Add method to select multi-signal magnetic recording reader by region	CS11
179	02/04/1A on StartStop unit	N	Fix for command (I/O) timeout	CS11
180	Drive hangs during write workload or on a format, stop unit or download	N	Fix for system hang	0203
181	Drive fails to come ready after a FW download	N	Fix for system hang	0203
182	SMART trip followed by >256 block READ with media error asserts	N	Fix for assert (Flash LED)	0203
183	Drive does not properly abort some commands following a code download	N	Fix for command (I/O) timeout	0203
184	Incorrect sense code reported after some LUN (Logical Unit Number) resets	N	Fix for incorrect error / sense data reporting	0203
185	Command timeouts on Inquiry 0xC3 commands	N	Fix for incorrect error / sense data reporting	0203
186	LOGICAL UNIT RESET task management function stalls for OPEN REJECT on another port	N	Fix for command (I/O) timeout	0203
187	LOGICAL UNIT RESET task management function stalls for OPEN REJECT (No Dest) on other port	N	Fix for command (I/O) timeout	0203
188	Command timeout on report LUNs	N	Fix for command (I/O) timeout	0203
189	Spin-up failure when bus reset occurs while using Power Primitives	N	Fix PWR_GRANT receipt logic so it will try again correctly	0203
190	Spin-up failure using Power Primitives	N	Add protections to avoid sending PWR_REQ on both PHYs	0203
191	Command timeout	N	Fix for command (I/O) timeout – clear memory registers when correctable SPAM error	0203
192	“Task Set Full on Unmap” commands cause an assert	N	Fix for assert (Flash LED)	0203
193	Command timeout running verify commands	N	Fix for command (I/O) timeout	0203
194	Drive can report INVALID_FRAME instead of QFULL with PI enabled	N	Fix for incorrect error / sense data reporting	0203
195	Drive never comes ready after a power cycle	N	Fix for drive hang – address message timing issue	0203

#	Change Description	Security Relevant?	Comments	FW Version(s)
196	Drive hangs in excessive read error condition	N	Fix for drive hang – ensure one of the resources is available	0203
197	Add Flash Error Log to UDS	N	Add Flash Error Log to UDS	0203
198	LED continues to blink after Sanitize Crypto Erase command	N	Fix to address incorrect LED behavior	0203
199	IOEDC error on read command after SMART warning occurs during a read stream	N	Fix for incorrect error / sense data reporting	EF04
200	SAS drive can miss HARD_REST primitive sequence	N	Fix for protocol violation	EF04 NF04
201	Command timeout during sequential write workload with large write burst configuration	N	Fix for command (I/O) timeout	EF04 NF04
202	Disable the background DIC (Data Integrity Check) task	N	Background DIC feature determined to be unnecessary	EF04
203	SAS hard reset workaround may fail with some SAS controllers / expanders	N	Fix for protocol violation	EF04 NF04
204	IBT log pull (0x400 sectors) aborts unexpectedly	N	Fix to ensure sufficient DRAM cache is available for the IBT log pull	EF04 NF04 SF04 TF04
205	Unrecoverable read errors seen post highly localized write intensive workload	N	Fix to ensure DOS scans will run during highly localized write intensive workload	EF04 NF04 TF04
206	Unexpected timeout on commands that run into device fault after power on	N	Fix for command (I/O) timeout	EF04 NF04 SF04 TF04
207	Assert on WCD spaced writes with write error recovery	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
208	Improve mDRAM mirror idle cleaning	N	Performance improvement	EF04 TF04
209	Assert when trying to clean Media Cache	N	Fix for assert (Flash LED)	EF04 SF04
210	Incorrect parity setup leads to drive assert	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04
211	Timeout on TUR (Test Unit Ready) issued after hard reset	N	Fix for command (I/O) timeout	EF04 SF04
212	Unexpected response to last host after drive reset	N	Fix for incorrect error / sense data reporting	EF04 NF04
213	Assert when write error encountered while cleaning media cache data	N	Fix for assert (Flash LED)	EF04 SF04
214	Assert after a reallocation when drive is low on spares	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04
215	Add humidity reporting to FARM log	N	Add humidity data to FARM log	EF04 NF04 SF04 TF04
216	Assert observed during IDD test	N	Fix for assert (Flash LED)	EF04 NF04 SF04 TF04
217	Write cache state set by SCT (SMART Command Transport) not consistent after system reboot	N	Fix for protocol violation	SF04 TF04

#	Change Description	Security Relevant?	Comments	FW Version(s)
218	Low read performance on IOzone test	N	Performance improvement	SF04 TF04
219	SCT Write Same command timeout	N	Fix for command (I/O) timeout	SF04 TF04
220	Set Sector Configuration: Maximum LBA is beyond the capacity after depop/repop	N	Fix for protocol violation	SF04
221	Enable SATA set sector config command while in format corrupt	N	Change allows drive to execute set sector config command while drive is in format corrupt	SF04 TF04
222	Unrecoverable read error found during ATI (Adjacent-Track Interference) beat-up test	N	Fix for incorrect error / sense data reporting	NF04 TF04

Description of ALC Changes:

Changes to the following documents were made:

From version 1.0 to 1.1

- Seagate Secure® TCG SSC Self-Encrypting Drives Proprietary Security Target, Version 1.0, February 4, 2022
- Seagate Secure® TCG SSC Self-Encrypting Drives Non-Proprietary Security Target, Version 1.1, February 4, 2022

From version 0.1 to 0.2

- Seagate Secure® TCG Opal SSC and Seagate Secure TCG Enterprise SSC Self-Encrypting Drive Entropy Documentation, Version 0.2, February 04, 2022.

From version 0.3 to 0.4

- 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 0.4, February 4, 2022.

Assurance Continuity Maintenance Report:

- Seagate submitted an Impact Analysis Report (IAR #1) to add the 18 firmware revisions to 12 CC certified hardware versions. listed above

- The IAR specifies that there is one security relevant fix to allow commands to retrieve drive state information in the case where the security files have been corrupted. This change does not affect the underlying security architecture. All other fixes are not security relevant.
- There are a number of changes to the validated TOE, and none of the changes impact the secure operation of the TOE. The assurance impact of these changes is minor.
- 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.

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 3 weeks to complete. Regression testing was conducted for these firmware releases, and table 13 shows the test intervals for these releases.

Product Name	Model Numbers	Firmware Version	Test Completion Date
Nytr0® 2032 SSD, 15mm, SAS Interface	XS960LE70144 XS1920LE70144 XS3840LE70144 XS960SE70144 XS1920SE70144 XS3840SE70144 XS7680SE70144	0203	12/22/2021
Nytr0® 3032 SSD, 15mm, SAS Interface	XS400ME70104 XS800ME70104 XS1600ME70104 XS3200ME70104 XS800LE70104 XS1600LE70104 XS3200LE70104 XS3840LE70104 XS6400LE70104 XS960SE70104 XS1920SE70104 XS3840SE70104 XS7680SE70104 XS15360SE70104 XS3840TE70104	0203	12/22/2021

Product Name	Model Numbers	Firmware Version	Test Completion Date
	XS7680TE70104		
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0166 ST600MP0156 ST900MP0126	CF06	06/27/2021
Exos™ 15E900, 2.5-Inch, 15K-RPM, SAS Interface	ST900MP0126 ST600MP0026	CF06	06/27/2021
		NF06	06/24/2021
BarraCuda Pro 2.5", SATA Interface	ST1000LM050 ST500LM035	1002	12/09/2020
		RPE4	03/26/2021
		LXMA	03/12/2021
		LXF1	03/12/2021
		LXF2	02/03/2021
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST1200MM0069	NF06	04/21/2021
Exos™ 10E2400, 2.5-Inch, 10K-RPM, SAS Interface	ST2400MM0149 ST1800MM0149 ST1200MM0149	CF06	04/21/2021
		CS11	04/21/2021
Exos™ 7E8, SAS Interface	ST4000NM014A ST8000NM010A ST6000NM033A	EF04	07/24/2021
Exos™ 7E8, SAS Interface	ST4000NM015A ST3000NM005A	NF04	01/12/2022
Exos™ 7E8, SATA Interface	ST4000NM012A ST8000NM008A ST6000NM025A	SF04	01/12/2022
Exos™ 7E8, SATA Interface	ST3000NM004A ST4000NM013A	TF04	01/12/2022
Exos™ 16, SAS Interface	ST10000NM010G ST12000NM008G ST14000NM012G ST16000NM009G	EF04	10/20/2021

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 March 9, 2022. 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 security relevant firmware 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 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 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.