SEAGATE

Seagate Secure® NVMe Self-Encrypting Drives Common Criteria Configuration Guide

Version 1.2

March 7th, 2024

Revision History

Version	Date	Description	Author(s)
v1.0	01/04/2023	Initial Revision	Phison
v1.1	02/09/2023	Modified information related to Enterprise and FIPS	Phison
v1.2	03/07/2024	Modified try limit table and GenKey method information	Phison

Contents

Introduction....4

Operational Environment 4

Setup and Configuration 5

General Setup & Configuration 5

TCG Opal Setup & Configuration....5

TCG Opal Setting Try Limits....9

TCG Opal Gen Key 9

CC Operational Guidance....10

Cryptographic Symmetric Key Sizes and Key Generation 10

Power Saving States and Timing of Power Saving States 10

Cryptographic Key and Key Material Destruction (Power Management) 10

Cryptographic Key Destruction 10

Cryptographic Operation (Hash Algorithm)....10

Cryptographic Operation (Random Bit Generation)....10

Validation - Try Limits and Persistence Settings 11

Protection of Data on Disk & Specification of Management Functions 11

TCG Opal Security Mode Services 12

Non-Security Mode Services 13

Firmware Access Control and Firmware Trusted Update....19

Firmware Rollback Protection....20

Supplemental Information....20

Introduction

This Seagate Common Criteria (CC) configuration guide provides the information necessary to configure a Seagate CC certified SED drive for Common Criteria mode. Seagate SED drives communicate with a host system using the standard protocol defined by the Trusted Computing Group (TCG). TCG stands for Trusted Computing Group and is an organization sponsored and operated by companies in the computer, storage and digital communications industry.

In addition to device setup and configuration, there are Operational Environment requirements that must be met for a Seagate CC certified SED drive (storage device) to be used in Common Criteria mode.

Operational Environment

The following Operational Environment requirements must be met for a Seagate CC certified SED drive (storage device) to be used in Common Criteria mode.

Authorized administrators and users must ensure that the communication channel between the host and the storage device is sufficiently protected to prevent information disclosure. For example, extremely long unprotected interface cables from the host to the device are not permitted.

An authorized administrator must ensure that a newly provisioned or initialized storage device is free of protected data in areas not targeted for encryption.

An authorized administrator must be responsible for ensuring that the allowed passphrase authorization factors configuration conforms to the local storage device environment requirements.

Administrators must ensure that guidance is given to users regarding the amount of time it takes for the storage device volatile memory to clear after entering the Compliant power saving state (power off in this case) so memory remnant attacks are infeasible. Authorized administrators must ensure that authorized users are trained in the proper storage of external tokens that contain authorization factors and that they will be used for no other purpose than to store the external token authorization factor.

Authorized administrators and users must ensure that the storage device is used in a secure physical computing space such that an adversary is not able to make modifications to the environment or to the storage device itself.

Authorized administrators must ensure that authorized users are properly trained and follow all guidance for securing the storage device and the proper use of authorization factors.

Setup and Configuration

General Setup & Configuration

Seagate CC certified SED need to be configure to run in Common Criteria CC mode. It is the case that anyone that buys SED drives has TCG infrastructure in place to set up, control and communicate with the drives in a secure manner. The examples provided in this Configuration Guide work with Seagate NVMe SED supporting TCG Opal. Customers should treat these examples as sample code. They will have to be modified to work with any customer specific TCG Opal implementations.

TCG Opal Setup & Configuration

The following are the security rules for the initialization and operation of a CC certified Seagate SED TCG Opal drive in a CC compliant manner. The minimum pin length requirement is 8 bytes. Some CC environments may require the use of full 32 byte PIN values. Seagate supports this and it can be enforced by setting the minimum PIN length value ‘_MinPINLength’ to 32. The ‘_MinPINLength’ is not part of the TCG specification. There is a ‘_MinPINLength’ value associated with each credential and they must be set independently. At the end of these steps, the SED will be in the CC Approved Mode of operation. This can be verified with Show Status service. If the SED drive is configured with PIN length larger than 8 bytes, the CC mode bit will be set.

Steps:

1. **Transition to TCG Opal security operating mode by executing the activate method of the Locking SP.**

   Commands to run the Locking SP activate method

   ```
   admin_sp.do_session_activate_locking()            # run Locking SP activate method
   ```

2. **Set drive owner SID credential to private value of 32 bytes in length.**

   Commands to set Drive Owner (SID) credential

```
sid=admin_sp.get_credential("C_PIN", "SID")       # get SID object
admin_sp.open_session(write=True)                 # admin sp - open session – enable writes
admin_sp.call_authenticate(“SID”)                 # authenticate to SID
sid.call_set(("PIN",                              # set new SID PIN value
"321SRQPONMLKJIHGFEDCBA9876543210"))
sid.call_set(("_MinPINLength”, 32))               # set minimum pin length to 32 bytes
admin_sp.end_session()                            # admin sp - end session
```

3. **Optionally set User1 PIN length to 32 bytes (Needs to be done for each credential)**

   Commands to set User 1 credential minimum pin length to 32 bytes

```
u1=locking_sp.get_credential("C_PIN", "User1")    # get User1 object
locking_sp.open_session(write=True)               # locking sp - open session - enable writes
locking_sp.do_batch_authenticate(u1)              # authenticate to User1
u1.call_set(("_MinPINLength”, 32))                # set minimum pin length to 32 bytes
locking_sp.end_session()                          # locking sp - end session
```

4. **Set User credentials to private value(s) of 32 bytes in length. We will use User1 in this example.**

   Commands to set User1 credential

```
u1=locking_sp.get_credential("C_PIN", "User1")    # get Admin1 object
locking_sp.open_session(write=True)               # locking sp - open session – enable writes
locking_sp.do_batch_authenticate(am)              # authenticate to Admin1
am.call_set(("_MinPINLength”, 32))                # set minimum pin length to 32 bytes
am.call_set(("PIN",                               # set new Admin1 PIN value
"321SRQPONMLKJIHGFEDCBA9876543210"))
locking_sp.end_session()                          # locking sp - end session
```

5. **Set Admin1 credential to private value of 32 bytes in length**

   Commands to set Admin1 credential

```
am=locking_sp.get_credential("C_PIN", "Admin1")   # get Admin1 object
locking_sp.open_session(write=True)               # locking sp - open session – enable writes
locking_sp.do_batch_authenticate(am)              # authenticate to Admin1
am.call_set(("_MinPINLength”, 32))                # set minimum pin length to 32 bytes
am.call_set(("PIN",                               # set new Admin1 PIN value
"321SRQPONMLKJIHGFEDCBA9876543210"))
```

```
locking_sp.end_session()                          # locking sp - end session
```

6. **Set Locking Range credentials to private value(s) of 32 bytes in length. We will use Locking Range 1 in this example.**

   Commands to set Locking Range 1 credential

```
r1 = locking_sp.get_lba_locking range                # get Range 1 object
("Locking_Range1")
auth =                                               # get auth obj
locking_sp.get_minimum_authorities_to_access(r1,
method_identifier="Set")
auth = auth[0]                                       # we want the first authority
cred = auth.linked_credential                        # get credential for authority
locking_sp.open_session(write=True)                  # locking sp - open session – enable writes
locking_sp.call_authenticate(auth
credential=”321SRQPONMLKJIHGFEDCBA9876543210”)
cred.call_set(("PIN",
"321SRQPONMLKJIHGFEDCBA9876543210"))
locking_sp.end_session()                             # locking sp - end session
```

7. **Disable the Makers authority**

   Commands to disable makers authority

```
admin_sp.open_session(write=True)                    # admin sp - open session - enable writes
makers_auth = admin_sp.get_authority("Makers")       # get makers authority
admin_sp.call_authenticate("SID",
credential="321SRQPONMLKJIHGFEDCBA9876543210")
makers_auth.do_set_enabled_field(enabled=False)      # disable makers authority
admin_sp.end_session()                               # admin sp - end session
```

8. **Set firmware download port to lock on reset**

   Commands to set firmware download port to lock on reset

```
admin_sp.open_session(write=True)                    # admin sp - open session – enable writes
port=admin_sp.get_port("FWDownload")                 # get port object
admin_sp.call_authenticate("SID",
credential="321SRQPONMLKJIHGFEDCBA9876543210")
port.call_set(("LockOnReset", [0]))                  # set firmware download port to lock on
                                                     reset
admin_sp.end_session()                               # admin sp - end session
```

9. Lock firmware download port

Commands to lock firmware download port

```
admin_sp.open_session(write=True)                        # admin sp - open session - enable writes
port=admin_sp.get_port("FWDownload")                     # get port object
admin_sp.call_authenticate("SID",
credential="321SRQPONMLKJIHGFEDCBA9876543210")
port.call_set(("PortLocked", 1))                         # lock firmware download port
admin_sp.end_session()                                   # admin sp - end session
```

10. Set LockingRange1 and enable lock on reset

Commands Set LockingRange1 and enable lock on reset

```
cred =locking_sp.get_linked_credential("Admin1")         # get credential obj for authority
locking_session = locking_sp.open_session(write=True)    # locking sp - open session – enable writes
locking_sp.call_authenticate("Admin1",
credential=”321SRQPONMLKJIHGFEDCBA9876543210”)
locking range 1= locking_sp.get_lba_ locking
range("Locking_Range1")
locking range1.do_set_locking range (rangestart=0,
rangelength=400)
locking range1.do_set_lock_state(state=0)
locking range1.do_set_lock_enabled_state(state=1)        # Set lock enabled to True for
                                                         LockingRange1
locking_sp.end_session()                                 # locking sp - end session
```

11. Power cycle the device.

TCG Opal Setting Try Limits

TCG Opal products allow the Try Limit to be set for some TCG Opal mode credentials. The following code is an example of how to set a new Try Limit value for the 'Admin1' credential. See the ' Validation - Try Limits and Persistence Settings' section below for the list of TCG Opal credentials where the Try Limit is settable.

Steps:

Transition to TCG Opal security operating mode by executing the activate method of the Locking SP.

Commands to set Drive Owner (SID) credential

```
u1=locking_sp.get_credential("C_PIN", "Admin1")
locking_sp.open_session(write=True)
locking_sp.do_batch_authenticate(u1)
u1.call_set(("TryLimit", 1024))                   #1024 is the new try limit value
locking_sp.end_session()"'
```

TCG Opal Gen Key

TCG Opal products allow the user to issue Gen Key(Change DEK). The following code is an example of how to issue crypto erase for the 'Admin1' credential.

Commands Set LockingRange1 and enable lock on reset

```
cred =locking_sp.get_linked_credential("Admin1")          # get credential obj for authority
locking_session=locking_sp.open_session(write=True)       # locking sp - open session – enable writes
locking_sp.call_authenticate("Admin1",
credential="321SRQPONMLKJIHGFEDCBA9876543210")
locking range 1= locking_sp.get_lba_ locking
range("Locking_Range1")
locking range1.do_gen_key()
locking_sp.end_session()                                  # locking sp - end session
```

CC Operational Guidance

Cryptographic Symmetric Key Sizes and Key Generation

Seagate TCG Opal SSD SED drives internally generate all AES keys necessary for the operation of the device. The size of the AES keys is not configurable. Intermediate AES keys are always 256 bits and the AES XTS data encryption key is always 512 bits in length.

Power Saving States and Timing of Power Saving States

The TOE supports a single Compliant power state of device full off (D3). The TOE SEDs have two possible transitions: power off to on; and on to off. Only the transition from on to off applies to this requirement. The device changes to off when the system removes power to the drive. This can happen immediately or when the user initiates a system shutdown request. After power is removed, it takes approximately 2 seconds for DRAM volatile memory and about 30 mS for SRAM volatile memory to completely power down.

Cryptographic Key and Key Material Destruction (Power Management)

All Seagate Self Encrypting Drives support only two power states power ON and power OFF. When an SED drive transitions from power ON to power OFF all cryptographic key material in volatile memory (DRAM and SRAM) is cleared automatically as the RAMs lose power. It is not possible for a Seagate Self Encrypting Drive to end up in a non-compliant power saving state.

Cryptographic Key Destruction

Seagate TCG Opal SSD SED drives implement a NAND flash wear leveling algorithm. And this algorithm is not effect key store in NAND. Because after change key the old key value in the original block will be erase directly.

Cryptographic Operation (Hash Algorithm)

All Seagate Self Encrypting Drives use the SHA-2 256, SHA-2 512 hash algorithm. It is not configurable.

Cryptographic Operation (Random Bit Generation)

All Seagate SED drives automatically instantiate an 800-90A compliant DRB that is seeded with entropy from an 800-90B compliant entropy system. Neither the DRBG or the entropy system are configurable.

Validation - Try Limits and Persistence Settings

Seagate SED drives have a separate counter for each credential which keeps track of the number of unsuccessful authentication attempts for each credential. The Try Limit sets an upper bound to this counter. This becomes the number of times the drive will accept an invalid password before shutting the drive down against further attacks.

The Persistence setting determines whether the count persists through a power cycle. If the counter does not persist through a power cycle, it will be reset to zero on power cycle and another round of authentication attempts can be made until the Try Limit is once again reached. If the count persists through a power cycle it is not reset to zero on power cycle and once the Try Limit is reached, the drive will lock out all further authentication attempts whether the drive is power cycled or not. Regardless of the Persistence setting, if a successful authentication is made at any time before the Try Limit is reached, the counter is reset to zero.

Credential Name / Firmware	Credential Type	Try Limit		Persistent
		Retry-count	Settable	
SID (SE4SA530)	TCG Opal	5	YES	NO
SID (SGEBHG02)	TCG Opal	100	YES	YES
PSID (SE4SA530)	TCG Opal	5	YES	NO
PSID (SGEBHG02)	TCG Opal	100	YES	YES
Locking SP Admin 1-4 Passwords (BEV) (SE4SA530)	TCG Opal	5	YES	NO
Locking SP Admin 1-4 Passwords (BEV) (SGEBHG02)	TCG Opal	100	YES	YES
Admin SP Admin 1-4 Passwords (BEV) (SE4SA530)	TCG Opal	5	YES	NO
Admin SP Admin 1-4 Passwords (BEV) (SGEBHG02)	TCG Opal	100	YES	YES
User 1-9 Passwords (BEV) (SE4SA530)	TCG Opal	5	YES	NO
User 1-9 Passwords (BEV) (SGEBHG02)	TCG Opal	100	YES	YES

Protection of Data on Disk & Specification of Management Functions

All Seagate Self Encrypting Drives (SED) Drives are manufactured and delivered with the encryption on and the drive unlocked. The initial value for SID and various other PINs is a 32- byte manufactured SID (MSID), a fixed value when fresh out of the box that is used as the default PIN. The drives also include a physical SID (PSID) public drive unique 32-byte value on the drive label. The drive must be “personalized” to change the initial value of the SID to private values. Once the administrator takes ownership of the drive the SID value is set to the administrator configured value. Names of Authentication PINs are tied to Opal SSC self-encrypting drives. This applies to all user PINs (Admins and Users). The PSIDs and MSIDs are never going to be a BEV.

An SED gets Authentication PIN from host Authorization Acquisition (AA) component, which could be whatever form or content the AA allows. The Seagate SEDs support Authentication PINs with length up to 32 bytes. This is the password that allows the SED drive to be accessible. All of the drives are open-access until this key and the locking settings are established.

Seagate SEDs support subdividing user storage using logical block addressing (LBA). The storage ranges are called locking ranges and can be configured to support up to 9 user locking ranges. Each locking range is secured with its own authentication key. User roles have identity-based authentication. For example, the Drive Owner has only one ID and one PIN. In TCG Security Mode, the SED can support up to 9 User operators. Each of these operators is assigned a unique ID to which a PIN is associated, thus this provides identity-based authentication. After power is removed from drive or a user locks the locking range, the Password/ TCG Pin is no longer needed and is removed from volatile memory.

Since all user data is encrypted / decrypted for storage on / retrieval from the drive media, the data can be erased using cryptographic methods. The data is erased by zeroizing the data encryption key (DEK). Seagate terminology refers to the DEK as the Media Encryption Key (MEK)

TCG Opal Security Mode Services

The following tables represent the CC Security services for each CC Approved Mode in terms of the Approved Security Functions and operator access control. Note the following:

- Use of the services described below is only compliant if the module is in the noted Approved mode.
- Underlying security functions used by higher level algorithms are not represented (e.g., hashing as part of asymmetric key)
- Operator authentication is not represented in this table.
- Some security functions listed are used solely to protect / encrypt keys and CSPs.

- Service input and output details are defined by the TCG standards.
- Unauthenticated services (e.g., Show Status) do not provide access to private keys or CSPs.
- Some services have indirect access control provided through enable / disable or lock / unlock services used by an authenticated operator; e.g., User data read / write.
- If the Operator value contains “optional” then the access is dependent on the module setup.

Non-Security Mode Services

In the uninitialized state, the module supports the following services:

- Services required to transition the SED to TCG Opal Security mode of operation.
- Services related to firmware update.
- Services related to unauthenticated encryption/decryption of user data.
- Services related to cryptographic erase of user data.
- Module reset.
- Services related to status reporting.

All cryptographic algorithms used in TCG Opal security operating modes are also available in the security uninitialized state.

TCG Opal Security Mode Authenticated Services

Service Name	**Description**	**Operator Access Control**	**Security Function**	**Command(s)/Event(s)**
Set PIN	Change operator authentication data. Note: Locking SP Admins can set PINs for any non-SUDR User or Locking SP Admin.	Locking SP Admin1-4, User1-9 (unless previously disabled by “Disable User Set PIN”), Drive Owner	PBKDF, Symmetric Key	TCG Set Method

Disable User Set PIN	Disable a non-SUDR User's ability to change its own PIN.	Locking SP Admin1-4	None	TCG Set Method
Enable / Disable Single User Data Range (SUDR)	Enable / Disable Single User Data Range (SUDR) classification for a data range	Locking SP Admin1-4	None	TCG Reactivate Method
Lock / Unlock FW Download	Enable / Disable FW Download Service	Drive Owner	None	TCG Set Method
Firmware Download	Load complete firmware image. If the self-test of the code load passes then the device will run with the new code.	None**	Asymmetric Key	FIRMWARE IMAGE DOWNLOAD Command, FIRMWARE IMAGE
Enable / Disable Admin SP Admin(s)	Enable / Disable an Admin SP Admin.	Drive Owner	None	TCG Set Method
Enable / Disable Locking SP Admin(s), non- SUDR User(s)	Enable / Disable a Locking SP Admin or non-SUDR User Authority.	Locking SP Admin1-4	None	TCG Set Method
Set Range Attributes for non-SUDR	Set the location, size, locking and User access rights of the non-SUDR.	Locking SP Admin1-4	None	TCG Set Method

Set Range Geometry for SUDR	Set the location and size of the SUDR.	User1-9 (if User Ownership) , Locking SP Admin1-4 (if Admin Ownership)	None	TCG Set Method
Lock / Unlock User Data Range for Read and/or Write	Block or allow read (decrypt) / write (encrypt) of user data in a range.	User1-9, Locking SP Admin1-4 (for non- SUDRs)	None	TCG Set Method
User Data Read / Write	Encryption / decryption of user data to/from a LBA range. Access control to this service is provided through Lock / Unlock User Data Range.	None*	Symmetric Key	Read / Write Commands
Cryptographic Erase of non- SUDR	Erase user data in a non-Single User Data Range by cryptographic means: changing the	User1-9, Locking SP Admin1-4	RNG, Symmetric Key	TCG GenKey Method
Cryptographic Erase of SUDR	Erase user data in a Single User Data Range by cryptographic means: changing the	Locking SP Admin1-4, User1-9	RNG, Symmetric Key	TCG Erase Method TCG GenKey Method, TCG Erase Method

	encryption key.cnging the encryption key.			
Exit CC Security Mode	Exit TCG Opal Security Mode. Note: CM will enter uninitialized state.	Drive Owner	RNG, PBKDF, Symmetric Key	TCG LockingSPObj.Revert() , TCG AdminSPObj.Revert()
		Admin SP Admin1-4		TCG AdminSPObj.Revert()
		Locking SP Admin1-4		TCG LockingSP.RevertSP()
Lock / Unlock User Data Range for Read and/or Write	Block or allow read (decrypt) / write (encrypt) of user data in a range.	User1-9, Locking SP Admin1-4 (for non- SUDRs)	None	TCG Set Method
User Data Read / Write	Encryption / decryption of user data to/from a LBA range. Access control to this service is provided through Lock / Unlock User Data Range.	None*	Symmetric Key	Read / Write Commands
Cryptographic Erase of non- SUDR	Erase user data in a non-Single User Data Range by cryptographic means:	User1-9, Locking SP Admin1-4	RNG, Symmetric Key	TCG GenKey Method

	changing the encryption key.			
Cryptographic Erase of SUDR	Erase user data in a Single User Data Range by cryptographic means: changing the encryption key.	Locking SP Admin1-4, User1-9	RNG, Symmetric Key	TCG Erase Method TCG GenKey Method, TCG Erase Method
Exit CC Security Mode	Exit TCG Opal Security Mode. Note: CM will enter uninitialized state.	Drive Owner	RNG, PBKDF, Symmetric Key	TCG LockingSPObj.Revert() , TCG AdminSPObj.Revert()
		Admin SP Admin1-4		TCG AdminSPObj.Revert()
		Locking SP Admin1-4		TCG LockingSP.RevertSP()

*Data Range has to be Unlocked

**FW Download Port has to be Unlocked

TCG Opal Security Mode Unauthenticated Services

Service Name	Description	Operator Access Control	Security Function	Command(s)/Event(s)
Unblock PIN	Resets password attempt counters.	None	None	POR
Show Status	Reports if CM satisfies Security Rules	None	None	TCG Level 0 Discovery: CC Security Mode Operating Mode Indicator (Byte 30, Bit 0) = 1
Reset Module	Runs POSTs and zeroizes keys & CSPs in RAM	None	None	POR
DRBG Generate Bytes	Returns a SP800-90 DRBG Random Number of 32 bytes	None	None	TCG Random()

Exit CC Security Mode	Exit TCG Opal Security Mode. Note: CM will enter uninitialized state.	None (using PSID)	None	AdminSP.RevertSP()
				AdminSPObj.Revert()

Firmware Access Control and Firmware Trusted Update

Seagate SED drives provide authorized users with the ability to query the current version of the SED firmware, the ability to initiate the SED firmware updates, and the ability to verify updates (prior to installing those updates) using the RSA digital signature algorithm (with a key size (modulus) of 4096 bits) provided by Seagate.

For NVMe SED drives the SED firmware version is queried with the NVMe Identify Controller command.

This section assumes that the firmware download port is in the locked state. Seagate drives all ship with the firmware download port in the unlocked state. The firmware download port is placed into the locked state as part of the steps to enable the CC operating mode.

The SEDs Firmware Access Control requires the administrator to unlock the firmware download port. This requires authentication with the SID credential (password) in order for the firmware update to proceed. To enable firmware download an administrator performs the following steps:

1. Open session to Admin SP.
2. Authenticate with SID credential (password).
3. Set FW download _PortLocking Object PortLocked Column to FALSE.
4. Close Session.

To perform a firmware download, an administrator performs the following steps:

1. Unlock firmware download port.
2. Obtain a genuine Seagate Secure firmware update package from: https://www.seagate.com/support-home
3. The signed firmware package is downloaded to the drive. It is received by the drive
4. firmware and placed into DRAM.
5. The signature is verified using PKCS #PSS, v2.1 RSA signature algorithm and public key in ROM. If the verification fails an error is returned and the update is not performed. The RSA key/modulus size for all current generation Seagate products is 4096 bits.
6. The firmware update package is written to flash. This overwrites the original firmware.
7. The FW performs a soft reset which loads and runs the new firmware.
8. At this point the firmware download port is unlocked. It can be locked by either performing a power on reset or by resetting the _PortLocking Object PortLocked Column to TRUE.

An error code is returned if any part of the firmware update process fails. The SED only allows installation of an update if the digital signature has been successfully verified.

The firmware can only be updated using the authenticated update mechanism by an authorized user where the authorized source that signs the firmware updates is Seagate. The SED firmware authenticates the source of the firmware update using the RSA digital signature algorithm: with a key size (modulus) of 4096 bits. The mechanism uses the RTU Key Store that contains the public key to verify the signature on an update image.   An error code is returned if any part of the firmware update process fails. The SED only allows installation of an update if the digital signature has been successfully verified.

Firmware Update Error Messages:

Error Status	When	Message

StatusType = 1h
StatusCode = 07h
	Download	“Invalid Firmware Image”

NONE	Boot	“Flash boot code Digital Signature Verification failure!”

Firmware Rollback Protection

The evaluator ensures that a description is provided on how the user should interpret the error codes.

The SED supports the functional capability to assure that downgrading to a lower security version number is not possible. With this mechanism if a flaw in FW 1 is found then FW 2 is generated and downloaded to the drive. Using the firmware rollback mechanism, FW 1 will no longer be compatible with the drive and cannot be downloaded.

If a firmware update package is downloaded to the drive with an invalid firmware revision number, the rollback protection firmware in the SED generates and returns the error code below and the firmware update package is rejected

Roll back Error Message

Error State	Message

StatusType = 1h;
StatusCode = 07h
	“Invalid Firmware Image”

Supplemental Information

CC Self-Encrypting Drive Configuration Guide, Version 1.2

For more information, see the following documents:

1. More information regarding TCG Opal can be found at: https://trustedcomputinggroup.org/work-groups/storage/
2. More information regarding the NVMe command set can be found at: https://nvmexpress.org/wp-content/uploads/NVM-Express-1_4-2019.06.10-Ratified.pdf