TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG Storage Interface Interactions Specification (SIIS)

Version 1.10
Revision 1.29
November 14, 2021

Contact:
admin@trustedcomputinggroup.com

PUBLISHED

DISCLAIMERS, NOTICES, AND LICENSE TERMS

CHANGE HISTORY

REVISION	DATE	DESCRIPTION
V1.10/R1.01	Feb. 13, 2020	• Define TPer scope at the beginning of each transport section
V1.10/R1.02	Mar. 6, 2020	• Removed extraneous whitespace • Fixed fonts to be consistent with the TCG template • Changed some if/then constructs that had extra 'and' instances • Addressed the inconsistency of style for second level entries in unordered lists: changed "A." to "A)" throughout the document • Added some xrefs to the new TPer definition sections • Corrected the spelling of "Tper" to "TPer" in a few places • Fixed bad grammar in a few places
V1.10/R1.03		• Proposed changes dealing with distinguising "TPer" and "NVM Subsystem" references appropriately
V1.10/R1.04	Apr. 23, 2020	• Incorporate the approved changes in R1.03 o TCG_SWG_SIIS_Version_1_10_Revision_1_02_20200415_WPNS_option3 • Accepted all previous approved changes • Incorporated accepted changes from the TC review of SIIS V1.09 R1.12, and accepted those changes • Globally changed 'set to zero' to 'cleared to zero' (but did not yet accept the changes)
V1.10/R1.05	June 9, 2020	• Changing the behavior of the WP after cryptographic erase or key change methods • Modify NVMe Commands Interaction section with Copy command and Lockdown command
V1.10/R1.06		• (information on this revision has been lost)
V1.10/R1.07		• (information on this revision has been lost)
V1.10/R1.08	July 22, 2020	• Moved NVMe-MI items from table 31 to table 32
V1.10/R1.09	July 29, 2020	• Group decisions on changes to the NVMe-MI items in table 32
V1.10/R1.10	August 04, 2020	• Changes in the ZNS interaction section
V1.10/R11.11	August 05, 2020	• Added comment about PCIe configuration read and write in table 32 (now table 34) • Added section 2.5 Level 0 discovery SIIS version descriptor for level 0 discovery
V1.10/R1.12	August 27, 2020	• Changes for section 2.5 level 0 discovery • Added new text for NVDIMM-N from document "TCG SIIS content for NVDIMM-N.docx" (dated July 21, 2020)
V1.10/R1.13	Sept. 01, 2020	• Fine tuning of section 2.5, making the new descriptor mandatory • Make NVMe, SCSI and ATA all match the requirements in section 2.5 • Update all references and table of contents (note: section 2.5 added 2 new tables) • Added keywords: Mandatory, Not Required and Optional • Added comments about possibly expanding the definition of 'user data removal method' to include key changing methods (including GenKen)
V1.10/R1.14	September 29, 2020	• Changes provided by Kioxia
V1.10/R1.15	October 15, 2020	• Changes in the interaction with the NVMe Verify Command
V1.10/R1.16	October 18, 2020	• Fixed formatting of all lists • Added new sections for interactions with NVMe Compare command and Verify command • Fixed 'keep with next' issues globally • Added new section/table for interactions with NVDIMM-N commands • Added new convention for Fonts • Clarified the meaning of 'ATA Security is enabled' as (i.e., ATA security state is SEC3, SEC4, SEC5, or SEC6) • Changed copyright date in footer from 2019 to 2020
V1.10/R1.17	October 20, 2020	• In the 'Locking Template interactions with the Format NVM command' changing the status returning from Invalid Security State to Operation Denied • Changing the Length field in the Level 0 Discovery – SIIS Feature Descriptor
V1.10/R1.19	December 08, 2020	• Comments received during the virtual F2F
V1.10/R1.20	January 12, 2021	• Changes in sections: 2.3, 3.6.16, 4.6.10 and 5.6.7 to include GenKey method and text around the LBA boundary on which commands are aborted during data removal method
V1.10/R1.22	January 19, 2021	• Review and agree on the changes in sections: 2.3, 3.6.16, 4.6.10 and 5.6.7 to include GenKey method and text around the LBA boundary on which commands are aborted during data removal method • Mark all comments as done
V1.10/R1.23	Feb. 16, 2021	• Added more to the Conventions section • Changed 'in process' to 'in progress' in three places • Responded to some of the TC's comments

V1.10/R1.24	March 4, 2021	• Responded to the remainder of the TC's comments (editorial and significant)
		• Changed all section xrefs to say 'see SECTION xxx'
		• Changed all 'Informative Content' to 'Informative Comment'
		• Per discussion with Storage WG:
		  ○ Kept instances of 'host SHOULD'
		  ○ Kept the word 'eradicate'
		• Added SD and TPer to the Definition of Terms section
		• Made significant structural changes to section 5.6.6 Interaction of Opal Family with Namespace Write Protection
		• Added new section 5.6.10 Interactions with the Copy command

V1.10/R1.25	March 25, 2021	• Accepted all changes, deleted all comments • Added deferred actions on updating User Data Removal methods (2.3) to the 'to do' list for SIIS 1.11 • Rechecked all 'see' references to insert 'section' as appropriate
V1.10/R1.26	June 16, 2021	• Addressed all technical and editorial comments from the TC on revision 1.25 • Deferred some issues for SIIS 1.11 to resolve
V1.10/R1.27	June 29, 2021	• Clean version after accepting all TC comments
V1.10/R1.28	Sept. 30, 2021	• Editorial update: added Ruby to definition of SSC family (accidental omission)

V1.10/R1.29	Oct. 28, 2021	• Changed paragraph style from 'TCG Header' to 'TCG Normal'
		  ○ On a blank line between sections 5.6.1.1 and 5.6.1.2; and
		  ○ On the line starting with "then execution of the Namespace...." between sections 5.6.1.3.3 and 5.6.1.3.4"
		• Changed paragraph style from 'TCG Header' to 'Caption for table 29

CONTENTS

List of Tables

1 Introduction

1.1 Document Purpose

TCG Storage specifications are intended to provide a comprehensive command architecture for putting Storage Devices under policy control as determined by the trusted platform host, the capabilities of the storage device to conform with the policies of the trusted platform, and the lifecycle state of the Storage Device (SD, see section 1.5) as a trusted peripheral (TPer). This document also serves as a specification for the TPer (see section 1.5) if that is deemed appropriate.

This document provides the essential mapping between concepts and features of the TCG Storage Architecture Core Specification, and several host/device interfaces.

1.2 Scope

The scope of this document is the interaction between the TPer and interface commands and transports. This document is written from the perspective of the Storage Device, not the host. There are no host requirements (i.e., host SHALL), but there are some host recommendations (e.g., should and may).

1.3 Intended Audience

The intended audience for this document is Storage Device and peripheral device manufacturers and developers that wish to tie Storage Devices and peripherals into trusted platforms.

1.1 Conventions

1.1.1 Key Words

The key words “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “MAY,” and “OPTIONAL” in this document normative statements are to be interpreted as described in RFC-2119, Key words for use in RFCs to Indicate Requirement Levels.

In addition to the above key words, the following are also used in this document to describe the requirements of particular features, including tables, methods, and usages thereof.

a) **Mandatory (M):** When a feature is Mandatory, the feature SHALL be implemented. A Compliance test SHALL validate that the feature is operational.
b) **Optional (O):** When a feature is Optional, the feature MAY be implemented. If implemented, a Compliance test SHALL validate that the feature is operational.
c) **Excluded (X):** When a feature is Excluded, the feature SHALL NOT be implemented. A Compliance test SHALL validate that the feature is not operational.
d) **Not Required (N)** When a feature is Not Required, the feature MAY be implemented. No Compliance test is required.

1.1.2 Fonts

Names of methods and SP tables are in Courier New font (e.g., the `Set` method, the `Locking` table). This requirement does not apply to method and table names appearing in headings or captions.

1.1.3 Statement Type

Please note a very important distinction between different sections of text throughout this document. There are two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, it can be considered a kind of normative statements.

EXAMPLE: Start of informative comment

This is the first paragraph of 1–n paragraphs containing text of the kind *informative comment* ...

This is the second paragraph of text of the kind *informative comment* ...

This is the nth paragraph of text of the kind *informative comment* ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

End of informative comment

1.1.4 Lists

1.1.4.1 Lists overview

Lists are associated with an introductory paragraph or phrase, and are numbered relative to that paragraph or phrase (i.e., all lists begin with an a) or 1) entry).

Each item in a list is preceded by an identification with the style of the identification being determined by whether the list is intended to be an ordered list or an unordered list.

If the item in a list is not a complete sentence, the first word in the item is not capitalized. If the item in a list is a complete sentence, the first word in the item is capitalized.

Each item in a list ends with a semicolon, except the last item, which ends in a period. The next to the last entry in the list ends with a semicolon followed by an “and” or an “or” (i.e., “…; and”, or “…; or”). The “and” is used if all the items in the list are required. The “or” is used if only one or more items in the list are required.

1.1.4.2 Unordered lists

An unordered list is one in which the order of the listed items is unimportant (i.e., it does not matter where in the list an item occurs as all items have equal importance). Each list item shall start with a lower case letter followed by a close parenthesis. If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an upper case letter followed by a close parenthesis.

The following is an example of an unordered list with a nested unordered list:

EXAMPLE - The following are the items for the assembly:
a) a box containing:
    A) a bolt;
    B) a nut; and
    C) a washer;
b) a screwdriver; and
c) a wrench.

1.1.4.3 Ordered lists

An ordered list is one in which the order of the listed items is important (i.e., item n is required before item n+1). Each listed item starts with a Western-Arabic numeral followed by a close parenthesis. If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an upper case letter followed by a close parenthesis.

The following is an example of an ordered list with a nested unordered list:

EXAMPLE - The following are the instructions for the assembly:

1) remove the contents from the box;
2) assemble the item;
   A) use a screwdriver to tighten the screws; and
   B) use a wrench to tighten the bolts;
   and
3) take a break.

1.1.5 Numbering

A binary number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 and 1 immediately followed by a lower-case b (e.g., 0101b). Underscores or spaces may be included between characters in binary number representations to increase readability or delineate field boundaries (e.g., 0 0101 1010b or 0_0101_1010b).

A hexadecimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 and/or the upper-case English letters A through F immediately preceded by "0x". Underscores or spaces may be included between characters in hexadecimal number representations to increase readability or delineate field boundaries (e.g., 0xFD8C FA23 or 0x0B_FD8C_FA23). Hexadecimal numbers are in Courier New font.

A decimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 not immediately followed by a lower-case b or lower-case h (e.g., 25). This standard uses the following conventions for representing decimal numbers:

a) the decimal separator (i.e., separating the integer and fractional portions of the number) is a period;
b) the thousands separator (i.e., separating groups of three digits in a portion of the number) is a space; and
c) the thousands separator is used in both the integer portion and the fraction portion of a number.

A decimal number represented in this standard with an overline under one or more digits following the decimal point is a number where the overlined digits are infinitely repeating (e.g., 666. $\overline{6}$ means 666.666 666… or 666 2/3, and 12. $\overline{142857}$ means 12.142 857 142 857… or 12 1/7).

1.1.6 Bit conventions

Name (n:m), where n is greater than m, denotes a set of bits (e.g., Feature (7:0)).

1.1.7 Number range convention

p..q, where p is less than q, represents a range of numbers (e.g., words 100..103 represents words 100, 101, 102, and 103).

1.4 References to Other Documents

1.4.1 Document Precedence

If there is a conflict between this specification and an approved reference (see section 1.4.2) or a reference under development (see section 1.4.3), then the precedence is:

1. this specification;
2. references under development; and
3. approved references.

1.4.2 Approved References

[1] IETF RFC 2119, 1997, “Key words for use in RFCs to Indicate Requirement Levels”

[2] INCITS 447-2008, "Information technology - SCSI Architecture Model - 4 (SAM-4)". Available from https://webstore.ansi.org/

[3] INCITS 513-2015, "Information technology - SCSI Primary Commands - 4 (SPC-4)". Available from https://webstore.ansi.org/

[4] INCITS 514-2014, "Information technology - SCSI Block Commands - 3 (SBC-3)". Available from https://webstore.ansi.org/

[5] INCITS 482-2012, "Information technology - ATA/ATAPI Command Set - 2 (ACS-2)". Available from https://webstore.ansi.org/

[6] INCITS 451-2008, "Information technology - AT Attachment – 8 ATA/ATAPI Architecture Model (ATA8-AAM)". Available from https://webstore.ansi.org/

[7] INCITS 481-2011, "Information technology - Fibre Channel Protocol for SCSI, Fourth Version (FCP-4)". Available from https://webstore.ansi.org/

[8] INCITS 417-2006, "Information technology - Serial Attached SCSI - 1.1 (SAS-1.1). Available from https://webstore.ansi.org/

[9] INCITS 471-2010, Information technology - USB Attached SCSI (UAS). Available from https://webstore.ansi.org/

[10] Universal Serial Bus Mass Storage Class USB Attached SCSI Protocol (UASP), Revision 1.0. Available from https://www.usb.org/

[11] Universal Serial Bus Mass Storage Class Bulk-Only Transport (USBBOT), Revision 1.0. Available from https://www.usb.org/

[12] NVM Express Specification version 1.4. Available from https://www.nvmexpress.org/

[13] NVM Express over Fabrics, Revision 1.0. Available from https://www.nvmexpress.org/

[14] JESD84-B50 *e*•MMC Specification version 5.0. Available from https://www.jedec.org/

[15] JESD220B UFS Specification version 2.0. Available from https://www.jedec.org/

[16] PCI Express® Base Specification Revision 3.0. Available from https://www.pcisig.com/

[17] Trusted Computing Group (TCG), “TCG Storage Architecture Core Specification”, Version 2.01

[18] INCITS 529, "Information technology - ATA/ATAPI Command Set - 4 (ACS-4)". Available from https://webstore.ansi.org/

[19] INCITS 537, "Information technology - Zoned Device ATA Command Set (ZAC)", Available from https://webstore.ansi.org/

[20] INCITS 536, "Information technology - Zoned Block Commands (ZBC)", Available from https://webstore.ansi.org/

[21] JESD248A DDR4 NVDIMM-N Design Specification. Available from https://www.jedec.org/.

[22] JESD245C Byte Addressable Energy Backed Interface. Available from https://www.jedec.org/.

[23] TCG Opal SSC Feature Set: Opal Feature Set: Single User Mode, Version 1.00

[24] TCG Opal SSC Feature Set: Configurable Namespace Locking version 1.00 revision 1.00

[25] TCG Storage Opal Family Feature Set: Shadow MBR for Multiple Namespaces, Version 1.00, revision 1.21

1.4.3 References under development

[26] T10/BSR INCITS 502, "Information technology - SCSI Primary Commands - 5 (SPC-5)". Available from https://t10.org/

[27] T10/BSR INCITS 506, "Information technology - SCSI Block Commands - 4 (SBC-4)". Available from https://t10.org/

[28] *e*•MMC Security Extension version 1.0 Available from https://www.jedec.org/

[29] UFS Security Extension version 1.0 Available from https://www.jedec.org/

[30] TCG Opal SSC Feature Set: Configurable Namespace Locking version 1.00 revision 1.00

[31] T13/BSR INCITS 558, "Information technology - ATA Command Set - 5 (ACS-5)". Available from https://www.t13.org/

[32] INCITS 549, "Information technology - Zoned Device ATA Command Set -2 (ZAC-2)", Available from https://www.t13.org/

[33] NVM Express Specification version 1.4. Available from https://www.nvmexpress.org/

1.5 Definition of Terms

Term	Definition
IF-RECV	An interface command used to retrieve security protocol data from the TPer
IF-SEND	An interface command used to transmit security protocol data to the TPer
Opal family	Any of: Opal SSC, Opalite SSC, Ruby SSC, or Pyrite SSC
Locking SP	A security provider that incorporates the Locking Template as described in the Core Spec
Locking SP is owned	A condition in which specific modifications (see section 2.2) of an SP have been made
SD	Storage Device
SSC	Security Subsystem Class. SSC specifications describe profiled sets of TCG functionality
TCG Reset	A high-level reset type defined in the Core Spec
TPer	The TCG security subsystem within a Storage Device
Trusted Peripheral	A TPer

2 Overview

2.1 Summary

This document defines for each interface:

- Mapping of interface events to TCG resets
- Mapping of IF-SEND, IF-RECV
- Handling of common TPer errors
- Discovery of security capabilities
- Miscellaneous Items

2.2 Locking SP Ownership

For the Opal family, the Locking SP is owned if:

a) an SP exists that incorporates the Locking Template; and
b) an SP that incorporates the Locking Template is not in the Manufactured-Inactive state.

For the Enterprise SSC, the Locking SP is owned if:

a) the EraseMaster C_PIN credential is not equal to MSID;
b) any BandMaster C_PIN credential is not equal to MSID; or
c) for any Locking object:
    A) the value of the WriteLockEnabled column is TRUE;
    B) the value of the ReadLockEnabled column is TRUE;
    C) the value of the RangeStart column is not equal to zero; or
    D) the value of the RangeLength column is not equal to zero.

2.3 User data removal method

A user data removal method is a method that may change the contents of user data read by the host.

For the Opal SSC family, the following methods are user data removal methods:

a) AdminSP.Revert,
b) LockingSP.Erase,
c) LockingSP.GenKey; and
d) LockingSP.RevertSP.

2.4 Additional Methods Status Code

The Core Specification defines the status codes that are returned by the TPer in response to method invocations and other operations (see [17]). This specification adds a status code as described in Table 1:

Table 1 - Additional TPer Status Code

Code	Value
INCOMPATIBLE_MBR_FORMAT	0x13
WP_DATA_REMAIN	0x14

2.5 Level 0 Discovery - SIIS Feature Descriptor (M)

An SD that supports this standard SHALL return the SIIS feature descriptor described in this subclause. It is Not Required (NR) for versions of this standard prior to Version 1.10.

Table 2 - Level 0 Discovery – SIIS Feature Descriptor

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB) Feature Code							
1								(LSB)
2	Data Structure Version				Reserved			
3	Length							
4	SIIS Revision Number							
5	Reserved							KEY CHANGE ZONE BEHAVIOR
6..15	Reserved							

A compliant SD that returns this descriptor SHALL return the following:

- Feature Code = 0x0005
- Data Structure Version = 0x1
- Length = 0x0C
- SIIS Revision Number = As specified in Table 3
- KEY CHANGE ZONE BEHAVIOR = VU

Table 3 - SIIS Versions

SIIS Major Version	Standard Referenced
x00	TCG Storage Interface Interactions Specification v1.00 r1.00
x01	TCG Storage Interface Interactions Specification v1.01 r1.00
x02	TCG Storage Interface Interactions Specification v1.02 r1.00
x03	TCG Storage Interface Interactions Specification v1.03 r1.00
x04	TCG Storage Interface Interactions Specification v1.04 r1.00
x05	TCG Storage Interface Interactions Specification v1.05 r1.00
x06	TCG Storage Interface Interactions Specification v1.06 r1.00
x07	TCG Storage Interface Interactions Specification v1.07 r1.00
x08	TCG Storage Interface Interactions Specification v1.08 r1.00
x09	TCG Storage Interface Interactions Specification v1.09 r1.00
x0A	TCG Storage Interface Interactions Specification v1.10 r1.00
All others	Reserved

The KEY CHANGE ZONE BEHAVIOR bit specifies whether or not cryptographic erase or key change methods (e.g., `GenKey` or `Revert`) affect the write pointer of a zoned device. For details, see section 3.6.7, section 4.6.3, and section 5.6.8.

3 SCSI Interface

See [2], [26], [27], [7], [8], [20], and [18] for details on SCSI architecture, commands and transports.

See [5] for details on ATAPI commands.

See [9], [10] and [11] for details on UAS and USB.

See [15] and [29] for details on UFS.

3.1 TPer scope

In the context of the SCSI interface, the scope of the TPer is a Logical Unit that provides access to user data. See section 3.6.3 for additional details.

3.2 Mapping of Resets

Table 4 – SAS Resets Mapped to TCG reset_type (single port)

SAS Event	Maps to TCG reset_type
Power on reset	Power cycle
I_T Nexus Loss	(none)
ABORT TASK task management function	(none)
ABORT TASK SET task management function	(none)
CLEAR TASK SET task management function	(none)
CLEAR ACA task management function	(none)
I_T NEXUS RESET task management function	(none)
LOGICAL UNIT RESET task management function	Hardware Reset
Link Reset Sequence	(none)
Link reset sequence with hard reset	Hardware Reset

Table 5 – SAS Resets Mapped to TCG reset_type (dual port)

SAS Event	Maps to TCG reset_type
Power on reset	Power cycle
I_T Nexus Loss	(none)
ABORT TASK task management function	(none)
ABORT TASK SET task management function	(none)
CLEAR TASK SET task management function	(none)
CLEAR ACA task management function	(none)
I_T NEXUS RESET task management function	(none)
LOGICAL UNIT RESET task management function	Hardware Reset
Link Reset Sequence	(none)
Link reset sequence with hard reset	Hardware Reset

Table 6 – Fibre Channel Resets Mapped to TCG reset_type

FC Event	Maps to TCG reset_type	Other Comments
Power on reset	Power cycle	
I_T Nexus Loss	(none)	
ABORT TASK task management function	(none)	
ABORT TASK SET task management function	(none)	
CLEAR TASK SET task management function	(none)	
CLEAR ACA task management function	(none)	
I_T NEXUS RESET task management function	(none)	
LOGICAL UNIT RESET task management function	Hardware Reset	
LIP(AL_PD,AL_PS)	Hardware Reset	LIP directed reset

LIP(FF,AL_PS)	Hardware Reset	LIP Global reset
Port Login	(none)	
Process Login	(none)	

Table 7 – ATAPI Resets Mapped to TCG reset_type

ATAPI Event	Maps to TCG reset_type
Power on reset	Power cycle
Hardware reset	PATA: Hardware Reset SATA: If Software Settings Preservation is enabled, then COMRESET is not a TCG Hardware Reset. If Software Settings Preservation is disabled, then COMRESET is a TCG Hardware Reset.
Software reset	(none)
DEVICE RESET command	(none)

Table 8 – UAS Events Mapped to TCG reset_type

Event	Maps to TCG reset_type	Reference
Device Power Cycle	Power cycle	[11]
ABORT TASK task management function	(none)	[26]
ABORT TASK SET task management function	(none)	[26]
CLEAR TASK SET task management function	(none)	[26]
CLEAR ACA task management function	(none)	[26]
I_T NEXUS RESET task management function	(none)	[26]
LOGICAL UNIT RESET task management function	Hardware Reset	[26]
USB VBus Power Cycle	Power cycle	[11]
USB Port Reset	(none)	[11]
USB Set Configuration with wValue cleared to zero	(none)	[11]
USB Set Configuration with wValue set to non-zero value that is not equal to the current value of bConfiguration	(none)	[11]
USB Set Configuration with wValue set to non-zero value that is equal to the current value of bConfiguration	(none)	[11]
USB Bulk-Out Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-Out pipe of the Mass Storage Interface)	(none)	[11]
USB Bulk-In Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-In pipe of the Mass Storage Interface)	(none)	[11]
USB Suspend	Hardware Reset	[11]
USB Resume	Hardware Reset	[11]

Table 9 – USB Events Mapped to TCG reset_type

Event	Maps to TCG reset_type	Reference
Device Power Cycle	Power cycle	[11]
USB VBus Power Cycle	Power cycle	[11]
USB Port Reset	(none)	[11]
USB Set Configuration with wValue cleared to zero	(none)	[11]
USB Set Configuration with wValue set to non-zero value that is not equal to the current value of bConfiguration.	(none)	[11]
USB Set Configuration with wValue set to non-zero value that is equal to the current value of bConfiguration.	(none)	[11]
USB Bulk-Out Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-Out pipe of the Mass Storage Interface)	(none)	[11]
USB Bulk-In Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-In pipe of the Mass Storage Interface)	(none)	[11]
USB Interface Reset (Also known as the BBB Bulk Only Mass Storage Reset Request x 21 FF with wIndex addressing the bInterfaceNumber of the Mass Storage Interface)	(none)	[11]
USB Suspend	Hardware Reset	[11]
USB Resume	Hardware Reset	[11]

Table 10 – UFS Events Mapped to TCG reset_type

Event	Maps to TCG reset_type	Reference
Power-on	Power cycle	[15]
HW Pin Reset	Hardware Reset	[15]
EndPoint Reset	Hardware Reset	[15]
ABORT TASK task management function	(none)	[26]
ABORT TASK SET task management function	(none)	[26]
CLEAR TASK SET task management function	(none)	[26]
LOGICAL UNIT RESET task management function	(none)	[26]
Host System UniPro Reset	Hardware Reset	[15]

3.3 Mapping of IF-SEND and IF-RECV

3.3.1 IF-SEND

IF-SEND SHALL be implemented with the SECURITY PROTOCOL OUT [26] command, with additional requirements on the CDB as described in Table 11.

Table 11 – IF-SEND CDB field contents (SCSI)

SECURITY PROTOCOL	SECURITY PROTOCOL SPECIFIC	INC_512	TRANSFER LENGTH
0x00	Security Protocol 0x00 is not defined for IF-SEND		
0x01	a ComID	1 [a]	Non-zero [b] number of 512-byte data units.
0x02	a ComID	1 [a]	Non-zero [b] number of 512-byte data units.
0x06	a ComID	0	Number of bytes of data.

[a] If the INC_512 field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see section 3.4).

[b] If the TRANSFER LENGTH field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see section 3.4).

3.3.2 IF-RECV

IF-RECV SHALL be implemented with the SECURITY PROTOCOL IN [26] command, with additional requirements on the CDB as described in Table 12.

Table 12 – IF-RECV CDB field contents (SCSI)

SECURITY PROTOCOL	SECURITY PROTOCOL SPECIFIC	INC_512	ALLOCATION LENGTH
0x00	(See [26] for details)	0 or 1	INC_512=0: Number of bytes of data. INC_512=1: Number of 512-byte data units.
0x01	a ComID	1 [a]	Non-zero [b] number of 512-byte data units.
0x02	a ComID	1 [a]	Non-zero [b] number of 512-byte data units.
0x06	a ComID	0	Number of bytes of data.

[a] If the INC_512 field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see section 3.4).

[b] If the ALLOCATION LENGTH field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see section 3.4), even though SPC-4 allows the ALLOCATION LENGTH field to be zero.

3.4 Handling Common TPer Errors

There are some common errors detected by the TPer. Table 13 describes how they are reported via the SCSI interface.

Table 13 – TPer Errors (SCSI)

TPer Error ID	Status	Sense Key	ASC/ASCQ	Comments
Good	GOOD	NO SENSE	NO ADDITIONAL SENSE INFORMATION	Normal command completion.
Invalid Security Protocol ID parameter	CHECK CONDITION	ILLEGAL REQUEST	INVALID FIELD IN CDB	No data SHALL be transferred.
Invalid Transfer Length parameter on IF-SEND	CHECK CONDITION	ILLEGAL REQUEST	INVALID FIELD IN CDB	No data SHALL be transferred.
Other Invalid Command Parameter	CHECK CONDITION	ILLEGAL REQUEST	INVALID FIELD IN CDB	No data SHALL be transferred.
Synchronous Protocol Violation	CHECK CONDITION	ILLEGAL REQUEST	COMMAND SEQUENCE ERROR	No data SHALL be transferred.
Data Protection Error	CHECK CONDITION	DATA PROTECT	ACCESS DENIED– NO ACCESS RIGHTS	No user data SHALL be transferred.

3.5 Discovery of Security Capabilities

3.5.1 Security Protocol 0x00

See the description of SECURITY PROTOCOL IN [26] for information on Security Protocol `0x00`.

3.6 Miscellaneous

3.6.1 Queued Commands

The TPer requires that for a given ComID the order of the IF-SEND and IF-RECV command completion be the same as the order in which the host application sent the commands.

Some transport protocols MAY NOT guarantee ordering of delivery or ordering of IF-SEND and IF-RECV command completion. Therefore, the host application communicating with the TPer should ensure that a prior IF-SEND or IF-RECV has completed prior to issuing another, or use mechanisms in the interface protocol to ensure ordering (e.g. ORDERED Task Attribute for SCSI Transport protocols).

Begin Informative Comment

The following definition of synchronous behavior does not affect the queuing behavior (if any) of the device interface. On queuing devices, synchronicity is enforced at the time IF-SEND/RECV commands are dequeued for processing by the SD. For non-queuing devices, synchronicity is enforced at the time the IF-SEND/RECV command is initially received by the device. If queuing behavior is supported, the host should use Ordered Queuing for IF-SEND/RECV commands or indeterminate behavior may result.

It is assumed that the SD can only process one IF-SEND/RECV interface command at a time.

End Informative Comment

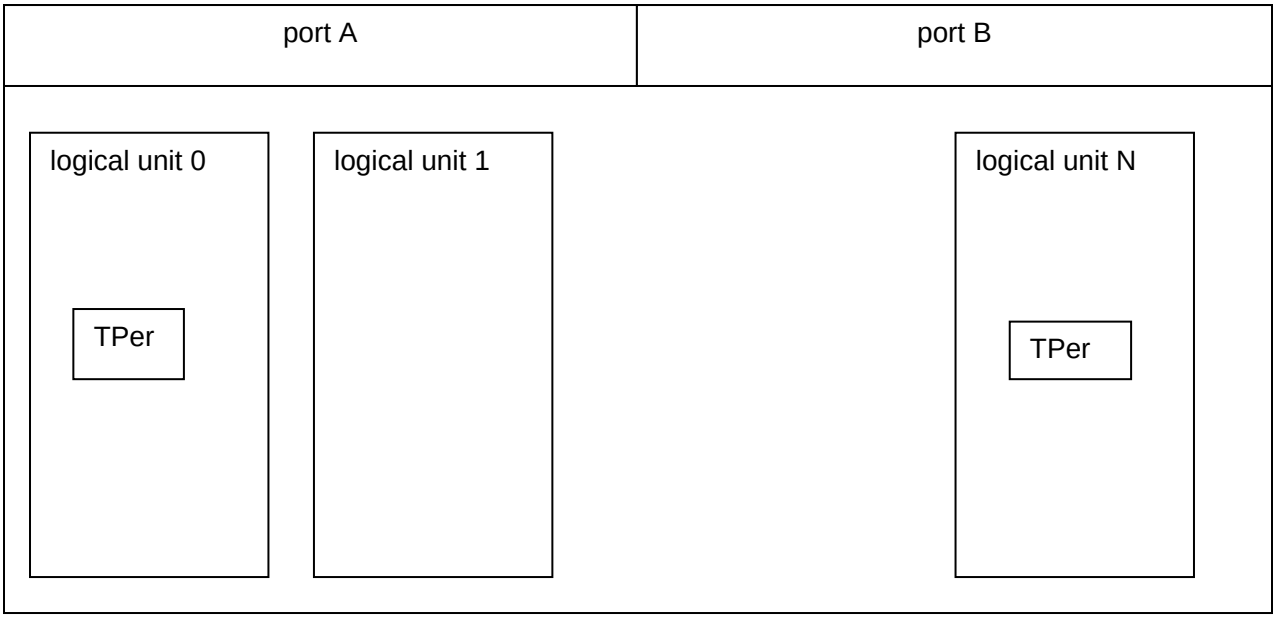
3.6.2 MBR Interactions

The LUN associated with the MBR is the boot LUN.

3.6.3 Logical Unit usage

A target that has multiple logical units MAY have multiple TPers (see section 3.1). Each TPer SHALL be associated with a different logical unit. Every logical unit on a device is not required to have a TPer, but logical units that support the TCG Core specification commands and functionality SHALL have a TPer. A TPer SHALL be associated with exactly one logical unit.

Figure 1 – SCSI target: port, Logical Unit, and TPer relationships



3.6.4 Interaction of the Opal family with the SANITIZE command

If the Locking SP is not owned (see section 2.2) in an Opal family TPer, then the SD MAY support SANITIZE commands.

If the Locking SP is owned (see section 2.2) in an Opal family TPer, then the SD:

a) SHALL NOT support SANITIZE commands; or
b) SHALL:
    A) report that SANITIZE commands are supported; and
    B) terminate SANITIZE commands with a Data Protection Error (see section 3.4).

3.6.5 Interaction of an Enterprise SSC with the SANITIZE command

If the Locking SP is not owned (see section 2.2) in an Enterprise SSC TPer, then the SD MAY support SANITIZE commands.

If the Locking SP is owned (see section 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a SANITIZE command with a Data Protection Error (see section 3.4).

A successful SANITIZE command SHALL eradicate all Locking SP media encryption keys and generate new media encryption keys.

3.6.6 Special Locking SP command interactions

For an SD implementing the Opal family or the Enterprise SSC, the SD SHALL terminate the:

a) READ LONG(10); and
b) READ LONG(16)

commands with CHECK CONDITION status and the sense key set to ILLEGAL REQUEST, and the additional sense code:

a) SHOULD be set to INVALID FIELD IN CDB; or
b) MAY be set to INVALID COMMAND OPERATION CODE.

For an SD implementing the Opal family or the Enterprise SSC, the SD SHALL terminate the:

a) WRITE LONG(10), (WR_UNCOR = 0); and
b) WRITE LONG(16), (WR_UNCOR = 0)

commands with CHECK CONDITION status and the sense key set to ILLEGAL REQUEST, and the additional sense code:

a) SHOULD be set to INVALID FIELD IN CDB; or
b) MAY be set to INVALID COMMAND OPERATION CODE.

3.6.7 Interactions with Zoned Block devices

If the device is not a zoned block device (see [20]), then this subclause does not apply. This subclause applies to zoned block devices only.

If the KEY CHANGE ZONE BEHAVIOR bit (see Table 2) is set to one, then cryptographic erase or key change methods (e.g., `GenKey` or `Revert`) SHALL:

a) reset the write pointer of all zones in the affected range; and
b) change the state of those Zones to Empty state (i.e. ZSE:Empty state).

If the KEY CHANGE ZONE BEHAVIOR bit is cleared to zero, then cryptographic erase or key change methods SHALL NOT:

a) change the write pointer of any zones in the affected range; and
b) change the state of those Zones.

The fields in the Geometry Reporting Feature Descriptor SHALL be set to the following values:

a) Align field = 1;
b) LogicalBlockSize = logical block size for the device;
c) AlignmentGranularity = zone size for the device; and
d) LowestAlignedLBA = 0.

3.6.8 Interactions with the FORMAT UNIT command

If the Locking SP is owned and a FORMAT UNIT command is sent to the device:

a) to change the number of logical blocks per physical block, then the SD SHALL terminate that FORMAT UNIT command with a Data Protection Error (see section 3.4); or
b) to change the size of a logical block without changing the number of logical blocks per physical block, then the SD SHALL NOT modify:
    A) the `Locking` table; or
    B) any `Datastore` tables.

3.6.9 Interactions with Verify commands

When BYTCHK is set to 1, the host provides input data and the SD verifies whether or not the data on the SD matches the input data. This allows the host to gather information about the data on the SD and should not be allowed unless the host can retrieve the data directly

3.6.10 Interactions with Extended Copy Operations

For the EXTENDED COPY command:

a) if the SD is the copy source, then the portion of the EXTENDED COPY command that operates on the SD is a read command (see [17]); and
b) if the SD is the copy destination, then the portion of the EXTENDED COPY command that operates on the SD is a write command (see [17])).

For the POPULATE TOKEN command, if the SD is the copy source, then the POPULATE TOKEN command is a read command.

For the WRITE USING TOKEN command, if the SD is the copy destination, then the WRITE USING TOKEN command is a write command.

3.6.11 Interactions with Unmap Operations

An UNMAP command shall return a Data Protection Error (see section 3.4) if:

a) the parameter list specifies an LBA range that is included in one or more Locking objects; and
b) the values of the WriteLockEnabled column and WriteLocked column are TRUE for at least one of the Locking objects that contains at least part of any LBA range specified.

3.6.12 Interaction of the Opal family with the REMOVE ELEMENT AND TRUNCATE command

If the Locking SP is not owned (see section 2.2) in an Opal family TPer, then the SD MAY support the REMOVE ELEMENT AND TRUNCATE command.

If the Locking SP is owned (see section 2.2) in an Opal family TPer, then the SD:

a) SHALL NOT support the REMOVE ELEMENT AND TRUNCATE command; or
b) SHALL:
    A) report that the REMOVE ELEMENT AND TRUNCATE command is supported; and
    B) terminate REMOVE ELEMENT AND TRUNCATE commands with a Data Protection Error (see section 3.4).

3.6.13 Interaction of an Enterprise SSC with the REMOVE ELEMENT AND TRUNCATE command

If the Locking SP is not owned (see section 2.2) in an Enterprise SSC TPer, then the SD MAY support the REMOVE ELEMENT AND TRUNCATE command.

If the Locking SP is owned (see section 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a REMOVE ELEMENT AND TRUNCATE command with a Data Protection Error (see section 3.4).

3.6.14 Interaction of the Opal family with the RESTORE ELEMENT AND REBUILD command

If the Locking SP is not owned (see section 2.2) in an Opal family TPer, then the SD MAY support the RESTORE ELEMENT AND REBUILD command.

If the Locking SP is owned (see section 2.2) in an Opal family TPer, then the SD:

a) SHALL NOT support the RESTORE ELEMENT AND REBUILD command; or
b) SHALL:

A) report that the RESTORE ELEMENT AND REBUILD command is supported; and
B) terminate RESTORE ELEMENT AND REBUILD commands with a Data Protection Error (see section 3.4).

3.6.15 Interaction of an Enterprise SSC with the RESTORE ELEMENT AND REBUILD command

If the Locking SP is not owned (see section 2.2) in an Enterprise SSC TPer, then the SD MAY support the RESTORE ELEMENT AND REBUILD command.

If the Locking SP is owned (see section 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a RESTORE ELEMENT AND REBUILD command with a Data Protection Error (see section 3.4).

3.6.16 Interface command interactions with user data removal methods

If a user data removal method (see section 2.3) is in progress on an LBA range, then the SD shall terminate all supported SCSI commands affecting that LBA range with a Synchronous Protocol Violation (see section 3.4), except for the following:

a) SECURITY PROTOCOL IN commands (see [26]);
b) SECURITY PROTOCOL OUT commands (see [26]);
c) INQUIRY commands (see [26]);
d) LOG SENSE commands that specify the Temperature log page (see [26]);
e) MODE SENSE commands that specify (see [26]):
    A. the Informational Exceptions Control mode page;
    B. the Caching mode page;
    C. the Control mode page;
    D. the Protocol Specific Port mode page; or
    E. the Protocol Specific Logical Unit mode page
f) READ CAPACITY (16) commands (see [26]);
g) REPORT LUNS commands (see [26]);
h) REPORT SUPPORTED OPERATION CODES commands (see [26]);
i) REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS commands (see [26]);
j) REPORT ZONES commands (see [20]) with:
    A. the ZONE START LBA field cleared to zero;
    B. the REPORTING OPTIONS field set to 3Fh;
    C. the PARTIAL bit set to one; and
    D. the ALLOCATION LENGTH field set to a value less than or equal to 64;
k) REQUEST SENSE commands (see [26]); and
l) TEST UNIT READY command; and
m) vendor specific commands that do not affect or retrieve user data.

3.6.17 Interactions with the FORMAT WITH PRESET command

If the Locking SP is owned and a FORMAT WITH PRESET command is sent to the device:

a) to change the number of logical blocks per physical block, then the SD SHALL terminate that FORMAT WITH PRESET command with a Data Protection Error (see section 3.4); or
b) to change the size of a logical block without changing the number of logical blocks per physical block, then the SD SHALL NOT modify:
    A) the `Locking` table; or
    B) any `Datastore` tables.

3.6.18 Interactions with other SCSI commands

Table 32 specifies the interactions of SCSI commands not already described by other subclauses.

4 ATA Interface

See [5] and [6] for details on ATA architecture, commands and transports.

4.1 TPer scope

In the context of the ATA interface, the scope of the TPer is the ATA device.

4.2 Mapping of Resets

Table 14 – ATA Resets Mapped to TCG reset_type

ATA Event	**Maps to TCG** reset_type
Power on reset	Power Cycle
Hardware reset	PATA: Hardware Reset SATA: If Software Settings Preservation is enabled, then COMRESET is not a TCG Hardware Reset. If Software Settings Preservation is disabled, then COMRESET is a TCG Hardware Reset.
Software reset	(none)

4.3 Mapping of IF-SEND and IF-RECV

4.3.1 IF-SEND

IF-SEND SHALL be implemented with either the TRUSTED SEND or TRUSTED SEND DMA commands, with additional requirements on the inputs as described in Table 15:

Table 15 – IF-SEND command fields (ATA)

SECURITY PROTOCOL	SP SPECIFIC	TRANSFER LENGTH
0x00	Security Protocol 0x00 is not defined for IF-SEND	
0x01	a ComID	Non-zero [a] number of 512-byte data units.
0x02	a ComID	Non-zero [a] number of 512-byte data units.
0x06	Protocol 0x06 is not defined for ATA.	
[a] If the Transfer Length parameter is zero, then the TPer SHALL report Other Invalid Command Parameter (see section 4.4).		

4.3.2 IF-RECV

IF-RECV SHALL be implemented with either the TRUSTED RECEIVE or TRUSTED RECEIVE DMA commands, with additional requirements on the inputs as described in Table 16:

Table 16 – IF-RECV command fields (ATA)

SECURITY PROTOCOL	SP SPECIFIC	TRANSFER LENGTH
0x00	(See [5])	Non-zero number of 512-byte data units.
0x01	a ComID	Non-zero [a] number of 512-byte data units.
0x02	a ComID	Non-zero [a] number of 512-byte data units.
0x06	Protocol 0x06 is not defined for ATA.	
[a] If the Transfer Length parameter is zero, then the TPer SHALL report Other Invalid Command Parameter (see section 4.4).		

4.4 Handling Common TPer Errors

There are some common errors detected by the TPer. This section describes how they are reported via the ATA interface.

See [5] for information about the Sense Data Reporting (SDR) feature set and the SENSE DATA AVAILABLE (SDA) bit (i.e., ATA STATUS field bit 1).

Table 17 describes common TPer errors if:

a) SDR is not supported;
b) SDR is supported and SDR is disabled; or
c) SDR is supported and SDR is enabled and SENSE DATA AVAILABLE (SDA) is cleared to zero.

Table 18 describes common TPer errors if:

a) SDR is supported and SDR is enabled and SENSE DATA AVAILABLE is set to one.

Table 17 – TPer Errors (ATA) – Without Sense Data Reporting (SDA=0)

TPer Error ID	ATA Status Field	ATA Error Field	Comments
Good	0x50	0x00	Normal command completion.
Invalid Security Protocol ID parameter	0x51	0x04	No data SHALL be transferred.
Invalid Transfer Length parameter on IF-SEND	0x51	0x04	No data SHALL be transferred.
Other Invalid Command Parameter	0x51	0x04	No data SHALL be transferred.
Synchronous Protocol Violation	0x51	0x04	No data SHALL be transferred.
Data Protection Error	0x51	0x04	No user data SHALL be transferred.

Table 18 – TPer Errors (ATA) – With Sense Data Reporting (SDA=1)

TPer Error ID	ATA Status Field Bit 1	Sense Key	ASC/ASCQ	Comments
Good	1	NO SENSE	NO ADDITIONAL SENSE	Normal command completion.
Invalid Security Protocol ID parameter	1	ILLEGAL REQUEST	INVALID FIELD IN CDB	No data SHALL be transferred.
Invalid Transfer Length parameter on IF-SEND	1	ILLEGAL REQUEST	INVALID FIELD IN CDB	No data SHALL be transferred.
Other Invalid Command Parameter	1	ILLEGAL REQUEST	INVALID FIELD IN CDB	No data SHALL be transferred.
Synchronous Protocol Violation	1	ILLEGAL REQUEST	COMMAND SEQUENCE ERROR	No data SHALL be transferred.
Data Protection Error	1	DATA PROTECT	ACCESS DENIED– NO ACCESS RIGHTS	No user data SHALL be transferred.

4.5 Discovery of Security Capabilities

4.5.1 IDENTIFY DEVICE

The IDENTIFY DEVICE command (see [5]) indicates whether the device has support for the ATA Security feature set or the Trusted Computing feature set. See IDENTIFY DEVICE data words 48, 82, and 128 for further information.

4.5.2 Security Protocol 0x00

The TRUSTED RECEIVE command (see [5]) describes Security Protocol `0x00`.

4.6 Miscellaneous

4.6.1 Feature set interactions

4.6.1.1 Trusted Computing feature set

The Trusted Computing feature set SHALL be supported by the device.

4.6.1.2 Sense Data Reporting feature set

If the Sense Data Reporting (SDR) feature set is supported and enabled, then common TPer errors are reported as Sense Codes instead of as regular ATA errors. (See [5] and section 4.4).

4.6.1.3 Locking Template interactions with the ATA Security feature set

If the lifecycle state of the Locking SP changes from the Manufactured-Inactive state to the Manufactured state, then:

1) the TPer SHALL save the current value of:
   A) IDENTIFY DEVICE, word 82, bit 1;
   B) IDENTIFY DEVICE, word 85, bit 1; and
   C) IDENTIFY DEVICE, word 128;

   and

2) the TPer SHALL change the value of IDENTIFY DEVICE, word 82, bit 1 to zero.

If the lifecycle state of the Locking SP is in the Manufactured state, then IDENTIFY DEVICE commands processed by the device SHALL indicate that the ATA Security feature set is not supported.

If the lifecycle state of the Locking SP changes from the Manufactured state to the Manufactured-Inactive state, then the TPer SHALL restore the value of the IDENTIFY DEVICE data to the values that were saved when the TPer changed the state from Manufactured-Inactive to Manufactured:

a) IDENTIFY DEVICE, word 82, bit 1;
b) IDENTIFY DEVICE, word 85, bit 1; and
c) IDENTIFY DEVICE, word 128.

If there is no Locking SP or the lifecycle state of the Locking SP is in the Manufactured-Inactive state, IDENTIFY DEVICE commands processed by the device MAY indicate that the ATA Security feature set is supported.

When ATA Security is enabled (i.e., ATA security state is SEC3, SEC4, SEC5, or SEC6), the TPer SHALL prohibit issuance of an SP that incorporates the Locking Template, and SHALL prohibit a SP that incorporates the Locking Template from transitioning out of the Manufactured-Inactive state.

4.6.1.4 Interaction of the Opal family with the ATA Sanitize Device feature set

If the Locking SP is not owned in an Opal family TPer (see section 2.2), then the SD MAY support (i.e., IDENTIFY DEVICE, word 59, bit 12 = 1) the ATA Sanitize Device feature set.

If the Locking SP is owned in an Opal family TPer, the SD SHALL:

a) report that the ATA Sanitize Device feature set is not supported (i.e., IDENTIFY DEVICE, word 59, bit 12 = 0); or
b) perform the following operations:
   A) report that the ATA Sanitize Device feature set is supported (i.e., IDENTIFY DEVICE word 59, bit 12 = 1); and
   B) terminate the following commands with a Data Protection Error (see section 4.4):
      a) CRYPTO SCRAMBLE EXT command;
      b) OVERWRITE EXT command;
      c) BLOCK ERASE EXT command;
      d) SANITIZE ANTIFREEZE LOCK EXT command; and
      e) SANITIZE FREEZE LOCK EXT command.

4.6.1.5 Interaction of an Enterprise SSC with the ATA Sanitize Device feature set

If the Locking SP is owned (see section 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate the following commands with a Data Protection Error (see section 4.4):

a) CRYPTO SCRAMBLE EXT command;
b) OVERWRITE EXT command;
c) BLOCK ERASE EXT command;
d) SANITIZE ANTIFREEZE LOCK EXT command; and
e) SANITIZE FREEZE LOCK EXT command,

A successful SANITIZE command SHALL eradicate all Locking SP media encryption keys and generate new media encryption keys.

4.6.1.6 Interaction of the Opal family Activate method with the ATA Security feature set

An Activate Error condition occurs when the `Activate` method is not successful.

If the `Activate` method is invoked on the Locking SP while ATA Security is enabled (i.e., ATA security state is SEC3, SEC4, SEC5, or SEC6), then the method invocation SHALL fail with a status of FAIL.

4.6.2 Special Locking SP command interactions

If:

a) an SD implements the Opal family or the Enterprise SSC; and
b) the Sense Data Reporting feature is supported and is enabled,

then the SD SHALL terminate the following ATA commands with the Sense Key set to ILLEGAL REQUEST and the additional sense set to INVALID COMMAND OPERATION CODE:

a) READ LONG;
b) WRITE LONG;
c) SCT READ LONG; and
d) SCT WRITE LONG.

If:

a) an SD implements the Opal family or the Enterprise SSC; and
b) the Sense Data Reporting feature is not supported or is not enabled,

then the SD SHALL return command aborted for the following ATA commands:

a) READ LONG;
b) WRITE LONG;
c) SCT READ LONG; and
d) SCT WRITE LONG.

4.6.3 Interactions with Zoned Block devices

If the device is not a zoned block device (see [18]), then this subclause does not apply. This subclause applies to zoned block devices only.

If the KEY CHANGE ZONE BEHAVIOR bit is set to one, then cryptographic erase or key change methods (e.g., `GenKey` or `Revert`) SHALL:

a) reset the write pointer of all zones in the affected range; and
b) change the state of those Zones to Empty state (i.e. ZSE:Empty state).

If the KEY CHANGE ZONE BEHAVIOR bit (see Table 2) is cleared to zero, then cryptographic erase or key change methods SHALL NOT:

a) change the write pointer of any zones in the affected range; and
b) change the state of those Zones.

The fields in the Geometry Reporting Feature Descriptor SHALL be set to the following values:

a) Align field = 1;
b) LogicalBlockSize = logical block size for the device;
c) AlignmentGranularity = zone size for the device; and
d) LowestAlignedLBA = 0.

4.6.4 Interactions with SET SECTOR CONFIGURATION EXT

If the Locking SP is owned and a SET SECTOR CONFIGURATION EXT command is sent to the device:

a) to change the number of logical blocks per physical block, then the SD SHALL terminate that SET SECTOR CONFIGURATION EXT command with a Data Protection Error (see section 3.4); or
b) to change the size of a logical block without changing the number of logical blocks per physical block, then the SD SHALL NOT modify:
    A) the `Locking` table; or
    B) any `Datastore` tables.

4.6.5 Interactions with DATA SET MANAGEMENT commands

If the device processes:

a) a DATA SET MANAGEMENT EXT command with the TRIM bit set to one;
b) a DATA SET MANAGEMENT XL command with the TRIM bit set to one; or
c) a SEND FPDMA QUEUED command with the SUBCOMMAND field set to DATA SET MANAGEMENT and the TRIM bit set to one,

then the device SHALL return a Data Protection Error (see section 4.4) for that command if:

a) the DATA SET MANAGEMENT Request Data specifies an LBA range that is included in one or more Locking objects; and
b) the values of the WriteLockEnabled column and WriteLocked column are TRUE for at least one of the Locking objects that contains at least part of any LBA range specified.

4.6.6 Interaction of the Opal family with the REMOVE ELEMENT AND TRUNCATE command

If the Locking SP is not owned (see section 2.2) in an Opal family TPer, then the SD MAY support the REMOVE ELEMENT AND TRUNCATE command.

If the Locking SP is owned (see section 2.2) in an Opal family TPer, then the SD:

a) SHALL NOT support the REMOVE ELEMENT AND TRUNCATE command; or
b) SHALL:
    A) report that the REMOVE ELEMENT AND TRUNCATE command is supported; and
    B) terminate REMOVE ELEMENT AND TRUNCATE commands with a Data Protection Error (see section 4.4).

4.6.7 Interaction of an Enterprise SSC with the REMOVE ELEMENT AND TRUNCATE command

If the Locking SP is not owned (see section 2.2) in an Enterprise SSC TPer, then the SD MAY support the REMOVE ELEMENT AND TRUNCATE command.

If the Locking SP is owned (see section 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a REMOVE ELEMENT AND TRUNCATE command with a Data Protection Error (see section 4.4).

4.6.8 Interaction of the Opal family with the RESTORE ELEMENT AND REBUILD command

If the Locking SP is not owned (see section 2.2) in an Opal family TPer, then the SD MAY support the RESTORE ELEMENT AND REBUILD command.

If the Locking SP is owned (see section 2.2) in an Opal family TPer, then the SD:

a) SHALL NOT support the RESTORE ELEMENT AND REBUILD command; or
b) SHALL:
    A) report that the RESTORE ELEMENT AND REBUILD command is supported; and
    B) terminate RESTORE ELEMENT AND REBUILD commands with a Data Protection Error (see section 4.4).

4.6.9 Interaction of an Enterprise SSC with the RESTORE ELEMENT AND REBUILD command

If the Locking SP is not owned (see section 2.2) in an Enterprise SSC TPer, then the SD MAY support the RESTORE ELEMENT AND REBUILD command.

If the Locking SP is owned (see section 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a RESTORE ELEMENT AND REBUILD command with a Data Protection Error (see section 4.4).

4.6.10 Interface command interactions with user data removal methods

If a user data removal method (see section 2.3) is in progress on an LBA range, then the device SHALL terminate all supported ATA commands affecting that LBA range with a Synchronous Protocol Violation (see section 4.4), except for the following:

a) TRUSTED RECEIVE command (see [18]);
b) TRUSTED RECEIVE DMA command (see [18]);
c) TRUSTED SEND command (see [18]);
d) TRUSTED SEND DMA command (see [18]);
e) TRUSTED NON-DATA command (see [18]);
f) CHECK POWER MODE command (see [18]);
g) IDENTIFY DEVICE command (see [18]);
h) IDLE IMMEDIATE command with UNLOAD (see [18]);
i) READ LOG EXT command (see [18]) or READ LOG DMA EXT command (see [18]) if one of the following log addresses is requested:
    A) 10h (i.e., NCQ Command Error log);
    B) 30h (i.e., IDENTIFY DEVICE data log); or
    C) E0h (i.e., SCT Command/Status log);
j) REPORT ZONES EXT command (see [19]) with:
    A) the ZONE LOCATOR field cleared to zero;
    B) the REPORTING OPTIONS field set to 3Fh (i.e., conventional zones);
    C) the RETURN PAGE COUNT field set to 0001h; and
    D) the PARTIAL bit set to one;
k) REQUEST SENSE DATA EXT command (see [18]);
l) SANITIZE STATUS EXT command (see [18]);
m) SET FEATURES PUIS feature set device spin-up sub command (see [18]);
n) SMART READ LOG command (see [18]) if one of the following log addresses is requested:
    A) 30h (i.e., IDENTIFY DEVICE data log); or
    B) E0h (i.e., SCT Command/Status log);
o) SMART RETURN STATUS command (see [18]); and
p) vendor specific commands that do not affect or retrieve user data.

4.6.11 Interactions with the MUTATE EXT commands

If the Locking SP is owned and a MUTATE EXT command is sent to the device:

a) to change the number of logical blocks per physical block, then the SD SHALL terminate that MUTATE EXT command with a Data Protection Error (see section 3.4); or
b) to change the size of a logical block without changing the number of logical blocks per physical block, then the SD SHALL NOT modify:
    A) the `Locking` table; or
    B) any `Datastore` tables.

4.6.12 Interactions with other ATA commands

Table 33 specifies the interactions of ATA commands not already described by other subclauses.

5 NVM Express Interface

See [12] for details on NVM Express architecture, commands and transports.

5.1 TPer scope

In the context of the NVMe interface, the scope of the TPer is the NVM subsystem, except for namespaces that are permanently write protected (see the Namespace Write Protection feature in [12] and section 5.6.1).

5.2 Mapping of Resets

If bit 0 of the CMIC field in the Identify Controller data structure is:

a) cleared to zero (i.e., the NVM subsystem contains only one NVM subsystem port), then use Table 19; and
b) set to one (i.e., the NVM subsystem may contain more than one NVM subsystem port), then use Table 20.

Table 19 – NVM Express over PCIe Resets Mapped to TCG reset_type (single port)

NVM Express Event	**Maps to TCG** reset_type	**Reference**
Main Power loss / PCIe cold reset	Power Cycle	[16]
PCIe hot reset	None	[16]
PCIe warm reset	Hardware Reset	[16]
PCIe transaction layer Data Link Down status	None	[16]
NVMe subsystem reset	Hardware Reset	[12]
NVMe Controller reset (CC.EN transitions from 1 to 0)	None	[12]
NVMe Function level (PCI) reset	None	[12]
NVMe Queue level reset	None	[12]
NVMe-MI Reset Command with Reset Type = Reset NVM Subsystem	Hardware Reset	[12]

Table 20 – NVM Express over PCIe Resets Mapped to TCG reset_type (multiple ports)

NVM Express Event	**Maps to TCG** reset_type	**Reference**
Main Power loss / PCIe cold reset	Power Cycle	[16]
PCIe hot reset	None	[16]
PCIe warm reset	None	[16]
PCIe transaction layer Data Link Down status	None	[16]

NVMe subsystem reset	Hardware Reset	[12]
NVMe Controller reset (CC.EN transitions from 1 to 0)	None	[12]
NVMe Function level (PCI) reset	None	[12]
NVMe Queue level reset	None	[12]
NVMe MI Reset Command with Reset Type = Reset NVM Subsystem	Hardware Reset	[12]

5.3 Mapping of IF-SEND and IF-RECV

5.3.1 IF-SEND

IF-SEND SHALL be implemented with the Security Send command, with additional requirements on the inputs as described in Table 21:

Table 21 – IF-SEND command parameters (NVM Express)

Security Protocol	**SP Specific** [b]	**Transfer Length**	**Namespace Identifier**
0x00	Security Protocol 0x00 is not defined for IF-SEND		Is not used [a]
0x01	SPSP0 = ComID (7:0) SPSP1= ComID (15:8)	Number of bytes to transfer.	Is not used [a]
0x02	SPSP0 = ComID (7:0) SPSP1= ComID (15:8)	Number of bytes to transfer.	Is not used [a]
0x06	Security Protocol 0x06 is not defined for NVMe.		

[a] See [12] for behavior when the Namespace Identifier (NSID) field is not used.

[b] Starting with NVMe Revision 1.2a, the SP Specific (SPSP) field was split into two fields (SPSP0 and SPSP1).

5.3.2 IF-RECV

IF-RECV SHALL be implemented with the Security Receive command, with additional requirements on the inputs as described in Table 22:

Table 22 – IF-RECV command parameters (NVM Express)

Security Protocol	SP Specific [b]	Allocation Length	Namespace Identifier
0x00	See [12]	Number of bytes to transfer.	Is not used [a]
0x01	SPSP0= ComID (7:0) SPSP1= ComID (15:8)	Number of bytes to transfer.	Is not used [a], except as specified in the Configurable Namespace Locking Feature set (see [30]) for Namespace Level 0 Discovery.
0x02	SPSP0= ComID (7:0) SPSP1= ComID (15:8)	Number of bytes to transfer.	Is not used [a]
0x06	Security Protocol 0x06 is not defined for NVMe.		

[a] See [12] for behavior when the Namespace Identifier (NSID) field is not used.

[b] Starting with NVMe Revision 1.2a, the SP Specific (SPSP) field was split into two fields (SPSP0 and SPSP1).

5.4 Handling Common TPer Errors

There are some common errors detected by the TPer. This section describes how they are reported via the NVM Express interface.

Common TPer errors are reported in the NVM Express Admin Completion Queue, Status Field (see [12]). The Status Code Type (SCT) field, the Status Code (SC) field, and the Do Not Retry bit SHALL indicate and map the TPer error as in Table 23.

Table 23 – TPer Errors (NVM Express)

TPer Error ID	NVMe Status Code Type	NVMe Status Code	NVMe Do Not Retry bit	Comments
Good	Generic Command Status	Successful Completion	0	Normal command completion.
Invalid Security Protocol ID parameter	Generic Command Status	Invalid Field in Command	1	No data SHALL be transferred.
Invalid Transfer Length parameter on IF-SEND	Generic Command Status	Invalid Field in Command	1	No data SHALL be transferred.
Other Invalid Command Parameter	Generic Command Status	Invalid Field in Command	1	No data SHALL be transferred.

TPer Error ID	NVMe Status Code Type	NVMe Status Code	NVMe Do Not Retry bit	Comments
Synchronous Protocol Violation	Generic Command Status	Command Sequence Error	1	No data SHALL be transferred.
Data Protection Error	Media and Data Integrity Errors	Access Denied	1	No user data SHALL be transferred.
Invalid Security State	Command Specific Status	Invalid Format	1	No data SHALL be transferred.
Operation Denied	Generic Command Status	Operation Denied	1	No data SHALL be transferred.

5.5 Discovery of Security Capabilities

5.5.1 Identify Controller Data Structure

The Optional Admin Command Support (OACS) of the Identify Controller Data Structure (see [12]) indicates whether the device has support for the Security Send and Security Receive commands.

5.5.2 Security Protocol 0x00

The Security Receive command (see [12]) describes Security Protocol `0x00`.

5.6 Miscellaneous

5.6.1 Namespaces

5.6.1.1 Overview

An NVM subsystem SHALL have no more than one TPer. The TPer is associated with the NVM subsystem except for namespaces that are permanently write protected (see section 5.1). The TPer is not associated with controllers in the NVM subsystem).

The following requirements apply regardless of the number of existing namespaces:

a) The NVM subsystem SHALL NOT change a namespace ID reported by the NVM Express Identify command and associated with any namespace managed by the TPer as a result of a power cycle or any NVM Express event.
b) When a namespace is created, it becomes associated with the Global Range.

Some namespace and TCG interactions vary depending on the number of existing namespaces (see [12]) in the TPer (see Table 24).

Table 24 – Namespace Management

Number of Existing Namespaces	Reference
0	5.6.1.2
1	5.6.1.3

Number of Existing Namespaces	Reference
Greater than 1	5.6.1.4

5.6.1.2 No Existing Namespace

5.6.1.2.1 Global Range Locking object Interactions

Begin Informative Comment

The Global Range Locking object may be configured even if no namespace exists in the TPer.

End Informative Comment

5.6.1.2.2 Non-Global Range Locking object Interactions

If no namespace exists, then attempts to modify non-Global Range Locking objects SHALL fail with a status of INVALID_PARAMETER. Other operations on non-Global Range Locking objects (e.g., Get, Next) SHALL operate as indicated in the applicable SSC specification.

5.6.1.2.3 Namespace Management

If no namespace exists in the TPer, and:

a) the value of the ReadLockEnabled column of the Global Range Locking object is TRUE and the value of the ReadLocked column of the Global Range Locking object is TRUE; or
b) the value of the WriteLockEnabled column of the Global Range Locking object is TRUE and the value of the WriteLocked column of the Global Range Locking object is TRUE,

then execution of the Namespace Management command with the Select (SEL) field set to Create SHALL fail with a status of Operation Denied.

5.6.1.3 Single Namespace

5.6.1.3.1 Global Range Locking object Interactions

If only one namespace exists in the TPer, then the column values of the Global Range Locking object (e.g., ReadLocked and WriteLocked) apply to all LBAs within that namespace that are not associated with any non-Global Range Locking objects.

Successful execution of any method that results in the cryptographic erasure of the Global Range Locking object SHALL result in the cryptographic erasure of all LBAs within that namespace that are not associated with any non-Global Range Locking objects.

5.6.1.3.2 Non-Global Range Locking Object Interactions

If only one namespace exists in the TPer, then the TPer MAY support configuration of non-Global Range Locking objects.

5.6.1.3.3 Namespace Management

If only one namespace exists in the TPer, and:

a) the value of the ReadLockEnabled column of the Global Range Locking object is TRUE and the value of the ReadLocked column of the Global Range Locking object is TRUE;
b) the value of the WriteLockEnabled column of the Global Range Locking object is TRUE and the value of the WriteLocked column of the Global Range Locking object is TRUE;
c) the value of the RangeStart column of any non-Global Range Locking object is not equal to zero; or
d) the value of the RangeLength column of any non-Global Range Locking object is not equal to zero,

then execution of the Namespace Management command SHALL fail with a status of Operation Denied.

5.6.1.3.4 MBR Shadowing for Single Namespace

If the `Set` method is invoked on the `MBRControlObj` in the `MBRControl` Table, and:

a) the provided Enabled column value is TRUE; and
b) the LBA Format of the `MBR` table is incompatible with the LBA format of the Namespace,

then the `Set` method MAY fail with a Status Code of INCOMPATIBLE_MBR_FORMAT.

5.6.1.4 Multiple Namespaces

5.6.1.4.1 Global Range Locking object Interactions

If more than one namespace exists in the TPer, then the column values of the Global Range Locking object (e.g., ReadLocked and WriteLocked) apply to all existing namespaces in the TPer.

If:

a) the value of the ReadLockEnabled column of the Global Range Locking object is TRUE; and
b) the value of the ReadLocked column of the Global Range Locking object is TRUE,

then all namespaces are read locked, and any command that reads user data or metadata (e.g., Read commands) SHALL fail with a status of Data Protection Error (see section 5.3).

If:

a) the value of the WriteLockEnabled column of the Global Range Locking object is TRUE; and
b) the value of the WriteLocked column of the Global Range Locking object is TRUE,

then all namespaces are write locked and any command that modifies user data or metadata (e.g., Write, Write Zeroes, Write Uncorrectable, or Data Management - Deallocate commands) SHALL fail with a status of Data Protection Error.

A TPer with more than one namespace MAY support a separate media encryption key for each namespace. In this case, the K_AES_* object referenced by the ActiveKey column value of the Global Range Locking object SHALL represent all media encryption keys in use for individual namespace encryption. Successful execution of any method that results in the cryptographic erasure of the Global Range Locking object SHALL result in the cryptographic erasure of all existing namespaces in the TPer.

5.6.1.4.2 Non-Global Range Locking object Interactions

If more than one namespace exists in the TPer, the Global Range Locking object is the only Locking object that is configurable. Attempts to modify other Locking objects SHALL fail with a status of INVALID_PARAMETER. Other operations on non-Global Range Locking objects (e.g., Get, Next) SHALL operate as indicated in the applicable SSC specification.

5.6.1.4.3 Namespace Management

If more than one namespace exists in the TPer, and:

a) the value of the ReadLockEnabled column of the Global Range Locking object is TRUE and the value of the ReadLocked column of the Global Range Locking object is TRUE; or
b) the value of the WriteLockEnabled column of the Global Range Locking object is TRUE and the value of the WriteLocked column of the Global Range Locking object is TRUE,

then execution of the Namespace Management command SHALL fail with a status of Operation Denied.

5.6.1.4.4 Geometry Feature Descriptor with Multiple Namespaces

The host should ignore the Geometry Feature Descriptor.

5.6.1.4.5 LockingInfoTable with Multiple Namespaces

The host should ignore the AlignmentRequired, LogicalBlockSize, Alignment Granularity, and LowestAlignedLBA columns in the `LockingInfo` table. The MaxRanges column of the `LockingInfo` table SHALL operate as indicated in the applicable SSC specification.

5.6.1.4.6 MBR Shadowing for Multiple Namespaces

If MBR shadowing (see [17]) is supported by the TPer, the `MBR` and `MBRControl` tables in the Locking SP are shared by all namespaces and controllers within the TPer.

If the `Set` method is invoked on the `MBRControlObj` in the `MBRControl` table, and:

a) the provided Enabled column value is TRUE; and
b) the LBA Format is incompatible between the content of MBR table and any existing Namespace,

then the `Set` method MAY fail with a Status Code of INCOMPATIBLE_MBR_FORMAT.

The MBR shadow size in logical blocks depends on the specific namespace logical block size.

If MBR shadowing is active, the TPer SHALL respond to LBA requests for any namespace from LBA 0 up to the LBA that maps to the end of the `MBR` table with values from the `MBR` table.

Read commands to the MBR shadow region when MBR shadowing is active SHALL return data from the `MBR` table formatted according to the logical block size of the specified namespace.

Once the Done column of the `MBRControl` table is set to TRUE, MBR shadowing SHALL be disabled for all namespaces.

It is the responsibility of the host to manage `MBR` table content between namespaces within the TPer. LBA format compatibility is not a TPer responsibility.

5.6.2 Locking Template interactions with the Namespace Management command

If:

a) the Locking SP is owned;
b) a controller processes a Namespace Management command;
c) the Enabled column value of the `MBRControl` table is TRUE; and
d) the Namespace Management command specifies the creation of a namespace with an LBA Format (see [12]) that is different from any of the existing Namespaces ,

then the Namespace Management command SHALL fail with a status of Operation Denied.

5.6.3 Locking Template interactions with the Format NVM command

The Format NVM command MAY be supported on a TPer that contains an SP that incorporates the Locking Template.

If:

a) the Locking SP is owned; and:
b) for any Locking object:
    A) the value of the WriteLockEnabled column of the Locking object is TRUE; and
    B) the value of the WriteLocked column of the Locking object is TRUE,

then any Format NVM command SHALL fail with a status of Invalid Security State.

If the TPer supports the Shadow MBR for Multiple Namespaces Feature Set (see [25]), and:

a) the Locking SP is owned;
b) a controller processes a Format NVM command;
c) the Enabled column value of the `MBRControl` table(see [25]) is TRUE; and
d) the Format NVM command specifies changes to an LBA Format of the Namespace corresponding to the value of NamespaceID column of `MBRControl` table (see [25]) from the original LBA Format (see [12])

then the Format NVM command SHALL fail with a status of Invalid Security State.

5.6.4 Interaction of the Opal Family with the Sanitize command

If the Locking SP is not owned (see section 2.2), then the SD MAY support (i.e., the SANICAP field is non-zero) the Sanitize command.

If the Locking SP is owned, then the SD SHALL:

a) report that the Sanitize command is not supported (i.e., the SANICAP field is zero); or
b) perform the following:
    A) report that the Sanitize command is supported (i.e., the SANICAP field is non-zero); and
    B) terminate the Sanitize command with a Data Protection Error (see section 5.4).

5.6.5 Locking Template interactions with Dataset Management, Attribute – Deallocate

The TPer that contains an SP that incorporates the Locking Template MAY support the Dataset Management command with attribute, Deallocate.

The Dataset Management command with Attribute – Deallocate SHALL fail and report Data Protection Error (see section 5.4) if:

a) the command provides an LBA range that is included in one or more Locking objects; and
b) the values of the WriteLockEnabled column and WriteLocked column are TRUE for at least one of the Locking objects that contains at least part of the LBA range specified.

5.6.6 Interactions of the Opal Family with Namespace Write Protection

5.6.6.1 Overview

The NVM subsystem that contains an SP that incorporates the Locking Template MAY support Namespace Write Protection (see [12]). This section describes the interaction of the Opal Family with Namespace Write Protection.

If any namespace with the Permanent Write Protect state exists in the NVM subsystem and the Locking SP is not owned in an Opal family TPer, then the namespace SHALL not be included in the scope of the TPer (see section 5.1) upon successful invocation of the `Activate` method.

Begin Informative Comment

No TCG method affects the configuration of Namespace Write Protection.

Since a namespace with the Permanent Write Protect state is excluded from the scope of the TPer (see section 5.1), the successful invocation of any TCG method has no effect on the namespace. For example, user data in the namespace is not altered by the successful invocation of the `Revert` method. Similarly, the Shadow MBR is not applicable to a Permanent Write Protected Namespace even if the Shadow MBR is enabled.

End Informative Comment

If any namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer and the Locking SP is owned in an Opal family TPer, then the write-locking feature SHALL be applied to the namespace as described in Table 25:

Table 25 - Write Access Restriction

Namespace Write Protection state	Write lock state	Request to write user data
No Write Protect	Write locked	Not allowed
	Write unlocked	Allowed
Write Protect / Write Protect Until Power Cycle	Write locked	Not allowed
	Write unlocked	

5.6.6.2 Interactions of the NVMe Set Features command with Namespace Write Protection Config

If:

a) the Locking SP is owned; and
b) the value of the ReadLockEnabled column of the Global Range Locking object is TRUE or the value of the WriteLockEnabled column of the Global Range Locking object is TRUE,

then the Set Features command with the Feature Identifier set to 0x84 (i.e., Namespace Write Protection Config), and the Write Protection State field set to Permanent Write Protect SHALL fail with a status of Feature Not Changeable.

If the TPer supports the Configurable Namespace Locking Feature Set [30]) and:

a) Locking SP is owned; and
a) the Namespace Global Locking object is assigned to a namespace,

then the Set Features command with the Feature Identifier set to 0x84 (i.e., Namespace Write Protection Config), and the Write Protection State field set to Permanent Write Protect SHALL fail with a status of Feature Not Changeable.

If the TPer supports the Shadow MBR for Multiple Namespaces Feature Set (see[25]) and:

b) Locking SP is owned;
c) a controller processes a Set Features command with the Feature Identifier set to 0x84 (i.e., Namespace Write Protection Config), and the Write Protection State field set to Permanent Write Protect; and
d) the value of the Enabled column of the `MBRControl` table is TRUE and the value of the NamespaceID column of the `MBRControl` table is equal to the Namespace Identifier (NSID) field of the Set Features command,

then the Set Features command SHALL fail with a status of Feature Not Changeable.

Any namespace with the Permanent Write Protect state SHALL NOT be included in the scope of the TPer (see section 5.1) upon the successful invocation of the Set Features command.

Begin Informative Comment

The host may invoke the Set Features command with the Write Protection State field set to Write Protect or Write Protect Until Power Cycle on a namespace even if Global Range Locking object is Write Locked or Read Locked.

If the Tper supports the Configurable Namespace Locking Feature Set, then the host may invoke the Set Features command with the Feature Identifier set to 0x84 (i.e., Namespace Write Protection Config), and the Write Protection State field set to Write Protect or Write Protect Until Power Cycle on a namespace even if the Namespace Global Range Locking object is assigned to the namespace and the Namespace Global Range Locking object is Write Locked or Read Locked.

End Informative Comment

5.6.6.3 Interactions with Opal Family TCG Methods

The following sections describes the interactions between the NVMe protocol and the Opal Family TCG methods.

5.6.6.3.1 Interactions with the Set Method

If the TPer supports the Shadow MBR for Multiple Namespaces Feature Set (see [25]) and:

a) the Locking SP is owned; and
b) the `Set` method is invoked on the NamespaceID column of the `MBRControl` table and the value of the NamespaceID column is equal to the Namespace Identifier of a namespace with the Permanent Write Protect state,

then the `Set` Method SHALL fail with a status of INVALID_PARAMETER.

5.6.6.3.2 Interactions with the GenKey Method

If:

a) the Locking SP is owned;
b) a namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer; and
c) the `GenKey` method is invoked on the Global Range Locking object or non-Global Range Locking object,

then the `GenKey` Method:

a) SHALL be applied to namespace(s) with the No Write Protect status;
b) SHALL NOT be applied to namespace(s) with Write Protect Until Power Cycle or Write Protect state; and
c) SHALL fail with a status of WP_DATA_REMAIN.

If the TPer supports the Configurable Namespace Locking Feature Set (see [27]); and:

a) the Locking SP is owned;
b) a Namespace Global Range Locking object is assigned to a namespace;
c) a namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer; and
d) the `GenKey` method is invoked on the Namespace Global Range Locking object,

then the `GenKey` Method SHALL fail with a status of WP_DATA_REMAIN.

5.6.6.3.3 Interactions with the Revert Method

If:

a) the Locking SP is owned; and
b) any namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer,

then the `Revert` Method SHALL fail with a status of WP_DATA_REMAIN.

5.6.6.3.4 Interactions with the RevertSP Method

If:

a) the Locking SP is owned; and
b) any namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer,

then the `RevertSP` Method SHALL fail with a status of WP_DATA_REMAIN.

5.6.6.3.5 Interactions with the Erase Method

If the TPer supports the Single User Mode Feature Set (see [23]) and:

a) Locking SP is owned;
b) any namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer; and
c) the `Erase` method is invoked on the Global Range Locking object or non-Global Range Locking object,

then the `Erase` Method:

a) SHALL be applied to namespace(s) with the No Write Protect status;
b) SHALL NOT be applied to namespace(s) with Write Protect Until Power Cycle or Write Protect state, and
c) SHALL fail with a status of WP_DATA_REMAIN.

If the TPer supports the Single User Mode Feature Set (see [23]) and:

a) the Locking SP is owned;
b) the TPer supports the [30]Configurable Namespace Locking Feature Set (see [28]);
c) a Namespace Global Range Locking object is assigned to a namespace;
d) a namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer; and
e) the `Erase` method is invoked on the Namespace Global Range Locking object,

then the `Erase` Method SHALL fail with a status of WP_DATA_REMAIN.

5.6.6.3.6 Interactions with the Assign Method

If the TPer supports the Configurable Namespace Locking Feature Set (see [30]) and:

a) the Locking SP is owned;
b) a namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer; and
c) a Namespace Global Range Locking object is assigned to a namespace;
d) the `Assign` method is invoked to assign a Locking object to the namespace with the Write Protect Until Power Cycle or Write Protect state,

then the `Assign` Method SHALL fail with a status of INVALID_PARAMETER.

Begin Informative Comment

If the TPer supports TCG Opal SSC Feature Set: Configurable Namespace Locking, then it is allowed to assign the Namespace Global Range on a namespace with the No Write Protect, Write Protect Until Power Cycle, or Write Protect state. It is permitted to assign the Namespace non-global Range for a namespace with the No Write Protect state.

End Informative Comment

5.6.6.3.7 Interactions with the Deassign Method

If the TPer supports the Configurable Namespace Locking Feature Set (see [30]) and:

a) the Locking SP is owned;
b) a namespace with the Write Protect Until Power Cycle or Write Protect state exists in the TPer;
c) the `Deassign` method is invoked without the KeepGlobalRangeKey parameter set to TRUE to deassign a Locking object from the namespace with the Write Protect Until Power Cycle or Write Protect state,

then the `Deassign` Method SHALL fail with a status of INVALID_PARAMETER.

5.6.7 Interface command interactions with user data removal methods

If a user data removal method (see section 2.3) is in progress on an LBA range, then the controller shall terminate all supported NVMe commands affecting that LBA range with a Synchronous Protocol Violation (see section 5.4), except for the following:

a) Security Send command (see [12]);
b) Security Receive command (see [12]);
c) Abort command (see [12]);
d) Asynchronous Event Request command (see [12]);
e) Create I/O Completion Queue command (see [12]);
f) Create I/O Submission Queue command (see [12]);
g) Delete I/O Completion Queue command (see [12]);
h) Delete I/O Submission Queue command (see [12]);
i) Get Features command (see [12]);
j) Get Log Page command (see [12]) for these log pages:
    A) Error Information;
    B) SMART / Health Information;
    C) Changed Namespace List;
    D) Reservation Notification; and
    E) Sanitize Status;
k) Identify command (see [12]);
l) Keep Alive command (see [12]);
m) Set Features command (see [12]);
n) Zone Management Receive (see [12]);
o) Opcode 7Fh for these Fabric commands (see [13]):
    A) Property Set;
    B) Connect;
    C) Property Get;
    D) Authentication Send;
    E) Authentication Receive; and
    F) vendor specific fabric commands that do not affect or retrieve user data;

and

p) vendor specific commands that do not affect or retrieve user data.

5.6.8 Interactions with Zoned Namespaces

If a namespace is not a zoned namespace (see [12]), then this subclause does not apply. This subclause applies to all zoned namespaces.

If the KEY CHANGE ZONE BEHAVIOR bit (see Table 2) is set to one, then cryptographic erase or key change methods (e.g., `GenKey` or `Revert`) SHALL:

a) reset the write pointer of all zones in the affected range; and
b) change the state of those Zones to Empty state (i.e. ZSE:Empty state).

If the KEY CHANGE ZONE BEHAVIOR bit is cleared to zero: then cryptographic erase or key change methods SHALL NOT:

a) change the write pointer of any zones in the affected range; and
b) change the state of those Zones.

The Geometry Reporting Feature for Multiple Namespaces Descriptor and the fields in the Geometry Reporting Feature Descriptor SHALL be set to the following values:

e) Align field = 1;
f) LogicalBlockSize = LogicalBlockSize;
g) AlignmentGranularity = Zone Size (ZSZE); and
h) LowestAlignedLBA = 0.

5.6.9 Interactions with the Verify command

The Verify command MAY be supported on an NVM subsystem that contains an SP that incorporates the Locking Template.

If the Locking SP is owned, then for any Verify command that targets an LBA Range associated with a Locking Object for which:

a) the value of the ReadLockEnabled column is TRUE; and
b) the value of the ReadLocked column is TRUE,

then the Verify command SHALL fail with a status of Data Protection Error.

5.6.10 Interactions with the Compare command

The Compare command MAY be supported on an NVM subsystem that contains an SP that incorporates the Locking Template.

If

a) MBR shadowing (see [17]) is supported by the TPer;
b) the Locking SP is owned;
c) the `MBRControl` Enable column value is True; and
d) the `MBRControl` Done column value is False,

then any Compare command that targets an LBA Range within the MBR Shadow region SHALL process the command using data from the MBR table.

If the Locking SP is owned, then for any Compare command that targets an LBA Range associated with a Locking Object for which:

a) the value of the ReadLockEnabled column is TRUE; and
b) the value of the ReadLocked column is TRUE,

then the Compare command SHALL fail with a status of Data Protection Error.

5.6.11 Locking Template interactions with the Copy command

The Copy command is both a read command and a write command.

If the Locking SP is owned, then for any Copy command that:

a) targets a source LBA Range associated with a Locking Object for which:
    a. the value of the ReadLockEnabled column is TRUE; and
    b. the value of the ReadLocked column is TRUE;

    or

b) targets a destination LBA Range associated with a Locking Object for which:
    a. the value of the WriteLockEnabled column is TRUE; and
    b. the value of the WriteLocked column is TRUE,

then the Copy command SHALL fail with a status of Data Protection Error.

5.6.12 Locking Template interactions with other NVMe commands

Table 34 specifies the interactions of NVMe commands not already described by other subclauses.

6 *e*•MMC Interface

See [14] for details on *e*•MMC architecture, commands and transports. In addition, details relating to the mapping provided below are found in [28].

6.1 TPer scope

In the context of the *e*•MMC interface, the scope of the TPer is the *e*•MMC device.

6.2 Mapping of Resets

Table 26 specifies the *e*•MMC events that are mapped to TCG resets.

Table 26 – e•MMC Events Mapped to TCG reset_type

***e*•MMC Event**	**Maps to TCG reset_type**	**Reference**
Power On	Power cycle	[14]
H/W Reset (Pin, Reset Signal)	Hardware Reset	[14]
GO_IDLE_STATE (CMD0)	Hardware Reset	[14]
GO_PRE_IDLE_STATE (CMD0)	Hardware Reset	[14]
GO_INACTIVE_ STATE (CMD15)	Power cycle	[14]
HPI (High Priority Interrupt)	None	[14]

6.3 Mapping of IF-SEND and IF-RECV

6.3.1 IF-SEND

IF-SEND is implemented with the combination of a CMD23 (i.e., SET_BLOCK_COUNT), followed by a CMD54 (PROTOCOL_WR), with additional requirements on the inputs as described in Table 27.

CMD23 command is used to set the transfer block count for the CMD54. See [14] for details regarding CMD23 and CMD54.

Table 27 – IF-SEND command parameters (*e*•MMC)

Security Protocol	SP_Specific	Transfer Length
0x00	Security Protocol 0x00 is not defined for IF-SEND	
0x01	a ComID	Non-zero[a] number of 512 byte data units as defined in CMD23
0x02	a ComID	Non-zero[a] number of 512 byte data units as defined in CMD23
0x06	Protocol 0x06 is not defined for *e*•MMC.	
[a] If the Transfer Length parameter ("number of blocks") in CMD23 is zero or if CMD23 was not successfully received, then the e•MMC device SHALL report SEC_INVALID_COMMAND_PARAMETER (see section 6.4).		

6.3.2 IF-RECV

IF-RECV is implemented with the combination of a CMD23 (SET_BLOCK_COUNT), followed by a CMD53 (PROTOCOL_RD), with additional requirements on the inputs as described in Table 28.
CMD23 command is used to set the transfer block count for the CMD53. See [14] for details regarding CMD23 and CMD53.

Table 28 – IF-RECV command parameters (*e*•MMC)

Security Protocol	SP_Specific	Allocation Length
0x00	See [14] [b]	Non-zero[a] number of 512 byte data units as defined in CMD23
0x01	a ComID	Non-zero[a] number of 512 byte data units as defined in CMD23
0x02	a ComID	Non-zero[a] number of 512 byte data units as defined in CMD23
0x06	Protocol 0x06 is not defined for *e*•MMC.	
[a] If the Transfer Length parameter ("number of blocks") in CMD23 is zero or if CMD23 was not successfully received, then the e•MMC device SHALL report SEC_INVALID_COMMAND_PARAMETER (see section 6.4) [b]When receiving CMD53 (PROTOCOL_RD) with Security Protocol value equal to 00h the SD SHALL return the list of supported protocols.		

6.3.3 *e*•MMC Command Structure for TCG IF-SEND and IF-RECV

6.3.3.1 *e*•MMC Block Allocation Overview

The *e*•MMC protocol uses the CMD23 SET_BLOCK_COUNT command (see section 6.3.3.2) to set the block count for the CMD54 command or the CMD53 command (see section 6.3.3.3) that immediately follows it. The block count of the CMD54 command or the CMD53 command is specified in 512-byte blocks (i.e., Allocation Length maps to the number of blocks in the payload multiplied by 512). Payload padding to the specified number of 512 byte blocks SHALL consist of zeros.

For TCG on the *e*•MMC transport, the IF-SEND command consists of the combination of a CMD23, followed by a CMD54.

In TCG on the *e*•MMC transport, the IF-RECV command consists of the combination of a CMD23, followed by a CMD53.

6.3.3.2 *e*•MMC CMD23 SET_BLOCK_COUNT command

CMD23 SET_BLOCK_COUNT is sent before CMD54 or CMD53 to set a transfer length of one or more 512-byte block. See Table 29.

Table 29 – e•MMC CMD23 Command Block

Bit Byte	7	6	5	4	3	2	1	0
0	[47] Start Bit	[46] Transition Bit	[45:40] Command Index					
1	[39] Reliable Write Request	[38] ‘0’ non-packed	[37] tag request	[36:33] context ID				[32]: forced programming
2	[31:24] set to 0							
3	[23:16] Number of Blocks (15:8)							
4	[15:8]: Number of Blocks (7:0)							
5	[7:1] CRC7							[0] Stop Bit

The value of Command Index is defined as 23 for this command. See [14] for more information.
The value in the Number of Blocks field specifies how many blocks are to be transferred in the next command. See [14] for more information.

All other fields are defined in [14].

6.3.3.3 *e*•MMC CMD54 PROTOCOL_WR and CMD53 PROTOCOL_RD commands

CMD54 PROTOCOL_WR and CMD53 PROTOCOL_RD commands are used to send the Security Protocol and the Security Protocol Specific parameters of the TCG IF-SEND and IF-RECV commands. See Table 30.

Table 30 – *e*•MMC CMD54 and CMD53 Structure

Bit Byte	7	6	5	4	3	2	1	0
0	[47] Start Bit	[46] Transition Bit	[45:40] Command Index					
1	[39:32] Security Protocol Specific (15:8)							
2	[31:24] Security Protocol Specific (7:0)							
3	[23:16] Security Protocol							
4	[15:8] Reserved							
5	[7:1] CRC7							[0] Stop Bit

See Table 27 and Table 28 for usage of Bytes 1 and 2, the Security Protocol Specific fields and the Security Protocol field.

All other fields are defined in [14].

6.4 Handling Common TPer Errors

Security related errors are detected by the *e*•MMC interface or by the TPer. Table 31 describes how they are reported by the *e*•MMC interface.

See [14] for details.

Table 31 – TPer Errors (*e*•MMC)

TPer Error ID	*e*•MMC Device Status	EXCEPTION EVENTS STATUS [a]	EXT SECURITY ERR [b]	Comments
Good	No error	No error	No error	Normal command completion.
Invalid Security Protocol ID parameter	EXCEPTION EVENT=1	EXTENDED SECURITY FALURE =1	SEC INVALID COMMAND PARAMETERS=1	No data SHALL be transferred.
Invalid Transfer Length parameter on IF-SEND	EXCEPTION EVENT=1	EXTENDED SECURITY FALURE =1	SEC INVALID COMMAND PARAMETERS=1	No data SHALL be transferred.
Other Invalid Command Parameter	EXCEPTION EVENT=1	EXTENDED SECURITY FALURE =1	SEC INVALID COMMAND PARAMETERS=1	No data SHALL be transferred.
Synchronous Protocol Violation	EXCEPTION EVENT=1	EXTENDED SECURITY FALURE =1	SEC INVALID COMMAND PARAMETERS=1	No data SHALL be transferred.
Data Protection Error	EXCEPTION EVENT=1	EXTENDED SECURITY FALURE =1	ACCESS DENIED=1	No user data SHALL be transferred.

[a] EXCEPTION_EVENTS_STATUS field of the EXT_CSD register

[b] EXT_SECURITY_ERR field of the EXT_CSD register

6.5 Discovery of Security Capabilities

6.5.1 Discovery of Security Capabilities

6.5.1.1 Security Protocol Information

In order to discover whether the extended protocol pass through commands are supported, the host should verify that Command Class 10 is supported by the device (in CCC field in CSD Register).

In order to receive and send extended protocol information CMD53 and CMD54 SHALL be used.

Refer to Security Protocol Information (see [14]) for the discovery of which security feature set is supported.

When receiving PROTOCOL_RD (CMD53) with Security Protocol value equal to 00h, the SD SHALL return the list of supported protocols.

6.6 Miscellaneous

6.6.1 Partition Management

The Locking Template SHALL be associated with and manage only the User Data Area partition (see [14]).

7 Appendix: Locking SP Interactions with Other Commands

7.1 SCSI Command Interactions

Table 32 specifies the interactions of SCSI commands not already described by other subclauses.

The commands in Table 32 MAY be supported on an SD that incorporates the Locking Template. Table 32 identifies whether a SCSI command is considered as a Read command or a Write command for the purposes of interactions with ReadLockEnabled, WriteLockEnabled, ReadLocked, and WriteLocked column values in the `Locking` table.

Commands identified in Table 32 as Read commands SHALL behave as defined in the Interface Read Command Access table (see [17]).

Commands identified in Table 32 as Write commands SHALL behave as defined in the Interface Write Command Access table (see [17]).

Table 32 – SCSI command interactions with the Locking SP

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
BACKGROUND CONTROL		SBC-4	No	No
BIND		SPC-5	No	No
CHANGE ALIASES		SPC-5	No	No
CLOSE ZONE		ZBC	No	Yes
COMPARE AND WRITE		SBC-4	Yes	Yes
COPY OPERATION ABORT		SPC-5	No	No
EXTENDED COPY		SPC-5	See section 3.6.10	
FINISH ZONE		ZBC	No	Yes
FORMAT UNIT		SBC-4	No	See section 3.6.8
GET LBA STATUS		SBC-4	Yes	No
GET PHYSICAL ELEMENT STATUS		SBC-4	No	No
GET STREAM STATUS		SBC-4	No	No
INQUIRY		SPC-5	No	No

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
LOG SELECT		SPC-5, SBC-4	No	No
LOG SENSE		SPC-5, SBC-4	No	No
MODE SELECT (6/10)		SPC-5, SBC-4	No	No
MANAGEMENT PROTOCOL IN		SPC-5	No	No
MANAGEMENT PROTOCOL OUT		SPC-5	No	No
MODE SENSE (6)		SPC-5, SBC-4	No	No
MODE SENSE (10)		SPC-5, SBC-4	No	No
OPEN ZONE		ZBC	No	Yes
ORWRITE (16)		SBC-4	No	Yes
ORWRITE (32)		SBC-4	No	Yes
PERSISTENT RESERVE IN		SPC-5	No	No
PERSISTENT RESERVE OUT		SPC-5	No	No
POPULATE TOKEN		SBC-4	See section 3.6.10	No
PRE-FETCH (10)		SBC-4	Yes	No
PRE-FETCH (16)		SBC-4	Yes	No
PREVENT ALLOW MEDIUM REMOVAL		SBC-4	No	No
READ (6)		SBC-4	Yes	No
READ (10)		SBC-4	Yes	No

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
READ (16)		SBC-4	Yes	No
READ (32)		SBC-4	Yes	No
READ ATTRIBUTE		SPC-5	No	No
READ BUFFER (10) READ BUFFER (16)	Except modes 0Ah, 0Bh, and 1Ch	SPC-5	No	No
	Mode 0Ah and 0Bh - Echo Buffer Mode		No	No
	Mode 1Ch - Error Retrieval Mode		No	No
READ CAPACITY (10)		SBC-4	No	No
READ CAPACITY (16)		SBC-4	No	No
READ DEFECT DATA (10)		SBC-4	No	No
READ DEFECT DATA (12)		SBC-4	No	No
READ LONG (10)		SBC-4	See section 3.6.6	
READ LONG (16)		SBC-4	See section 3.6.6	
READ MEDIA SERIAL NUMBER		SPC-5	No	No
REASSIGN BLOCKS		SBC-4	Yes	Yes
RECEIVE COPY DATA		SPC-5	Yes	No
RECEIVE DIAGNOSTIC RESULTS		SPC-5	No	No
RECEIVE ROD TOKEN INFORMATION		SPC-5, SBC-4	Yes	No

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
REMOVE ELEMENT AND TRUNCATE		SBC-4	No	Yes See section 3.6.12 and section 3.6.13
REMOVE I-T NEXUS		SPC-5	No	No
RELEASE (6)		SPC-5	No	No
RELEASE (10)		SPC-5	No	No
REPORT ALIASES		SPC-5	No	No
REPORT ALL ROD TOKENS		SPC-5	No	No
REPORT IDENTIFYING INFORMATION		SPC-5	No	No
REPORT LUNS		SPC-5	No	No
REPORT PRIORITY		SPC-5	No	No
REPORT PROVISIONING INITIALIZATION PATTERN		SBC-4	No	No
REPORT REFERALS		SBC-4	No	No
REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS		SPC-5	No	No
REPORT TARGET PORT		SPC-5	No	No
REPORT TIMESTAMP		SPC-5	No	No
REPORT ZONES		ZBC	No	No
REQUEST SENSE		SPC-5	No	No
RESERVE (6)		SPC-5	No	No

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
RESERVE (10)		SPC-5	No	No
RESET WRITE POINTER		ZBC	No	Yes
REZERO UNIT		SBC-4	No	No
SANITIZE	BLOCK ERASE	SBC-4	See section 3.6.4 and section 3.6.5	
	CRYPTO ERASE			
	OVERWRITE			
	EXIT FAILURE MODE			
SECURITY PROTOCOL IN		SPC-5	No	No
SECURITY PROTOCOL OUT		SPC-5	No	No
SEEK (6)		SBC-4	No	No
SEEK (10)		SBC-4	No	No
SEND DIAGNOSTIC		SPC-5	Vendor specific [a]	
SET AFFILIATION		SPC-5	No	No
SET PRIORITY		SPC-5	No	No
SET IDENTIFYING INFORMATION		SPC-5	No	No
SET TARGET PORT GROUPS		SPC-5	No	No
SET TIMESTAMP		SPC-5	No	No
STREAM CONTROL		SBC-4	No	No
START STOP UNIT		SBC-4	No	No
SYNCHRONIZE CACHE (10)		SBC-4	No	No

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
SYNCHRONIZE CACHE (16)		SBC-4	No	No
TEST UNIT READY		SPC-5	No	No
UNBIND		SPC-5	No	No
UNMAP		SBC-4	No	Yes See section 3.6.11
VERIFY (10)	BYTCHK=0	SBC-4	Yes	No
	BYTCHK=1		Yes See section 3.5.9	No
VERIFY (12)	BYTCHK=0	SBC-4	Yes	No
	BYTCHK=1		Yes See section 3.5.9	No
VERIFY (16)	BYTCHK=0	SBC-4	Yes	No
	BYTCHK=1		Yes See section 3.5.9	No
VERIFY (32)	BYTCHK=0	SBC-4	Yes	No
	BYTCHK=1		Yes See section 3.5.9	No
XDWRITEREAD (10)		SBC-4	Yes	Yes
XDWRITEREAD (32)		SBC-4	Yes	Yes
XPWRITE (10)		SBC-4	No	Yes
XPWRITE (32)		SBC-4	No	Yes

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
WRITE (6)		SBC-4	No	Yes
WRITE (10)		SBC-4	No	Yes
WRITE (16)		SBC-4	No	Yes
WRITE (32)		SBC-4	No	Yes
WRITE AND VERIFY (10)	BYTCHK=0	SBC-4	No	Yes
	BYTCHK=1		No	Yes
WRITE AND VERIFY (12)	BYTCHK=0	SBC-4	No	Yes
	BYTCHK=1		No	Yes
WRITE AND VERIFY (16)	BYTCHK=0	SBC-4	No	Yes
	BYTCHK=1		No	Yes
WRITE AND VERIFY (32)	BYTCHK=0	SBC-4	No	Yes
	BYTCHK=1		No	Yes
WRITE ATOMIC (16)		SBC-4	No	Yes
WRITE ATOMIC (32)		SBC-4	No	Yes
WRITE ATTRIBUTE		SPC-5	No	No
WRITE BUFFER	all modes except those modes associated with Download Microcode and the Echo Buffer mode	SPC-5	No	No
	all modes associated with Download Microcode		No	No
	mode 0Ah - Echo Buffer Mode		No	No
WRITE LONG (10)	WR_UNCOR=0	SBC-4	See section 3.6.6	

SCSI command interactions with the Locking SP				
SCSI Command	**Service Action / Special Cases**	**Reference**	**Read Command**	**Write Command**
	WR_UNCOR=1		No	Yes
WRITE LONG (16)	WR_UNCOR=0	SBC-4	See section 3.6.6	
	WR_UNCOR=1		No	Yes
WRITE SAME (10)		SBC-4	No	Yes
WRITE SAME (16)		SBC-4	No	Yes
WRITE SAME (32)		SBC-4	No	Yes
WRITE STREAM (16)		SBC-4	No	Yes
WRITE STREAM (32)		SBC-4	No	Yes
WRITE USING TOKEN		SBC-4	No	See section 3.6.10

[a] For Vendor Specific commands and for each SCSI command not identified in the table, the command is considered a:

a) Write command, if the command modifies user data; and

b) Read command, if the command accesses user data.

7.2 ATA Command Interactions

Table 33 specifies the interactions of ATA commands not already described by other subclauses.

The commands in Table 33 MAY be supported on an SD that incorporates the Locking Template. Table 33 identifies whether an ATA command is considered as a Read command or a Write command for the purposes of interactions with ReadLockEnabled, WriteLockEnabled, ReadLocked, and WriteLocked column values in the `Locking` table.

Commands identified in Table 33 as Read commands SHALL behave as defined in the Interface Read Command Access table (see [17]).

Commands identified in Table 33 as Write commands SHALL behave as defined in the Interface Write Command Access table (see [17]).

Table 33 – ATA command interactions with the Locking SP

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
ABORT NCQ QUEUE		ACS-4	See NCQ NON-DATA	
BLOCK ERASE EXT		ACS-4	See section 4.6.1.4 and section 4.6.1.5	
			No	Yes
CHECK POWER MODE		ACS-4	No	No
CLOSE ZONE EXT		ACS-4, ZAC	See ZAC Management Out	
CONFIGURE STREAM		ACS-4	No	No
CRYPTO SCRAMBLE EXT		ACS-4	See section 4.6.1.4 and section 4.6.1.5	
			No	Yes
DATA SET MANAGEMENT	Trim	ACS-4	No	Yes See section 4.6.5
	Markup LBA Ranges function		No	No

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
DATA SET MANAGEMENT XL		ACS-4	See DATA SET MANAGEMENT	
DEADLINE HANDLING		ACS-4	See NCQ NON-DATA	
DEVICE CONFIGURATION OVERLAY (DCO)	FREEZE LOCK	ACS-2	No	No
	IDENTIFY		No	No
	RESTORE		No	No
	SET		No	No
DOWNLOAD MICROCODE		ACS-4	No	No
DOWNLOAD MICROCODE DMA		ACS-4	See DOWNLOAD MICROCODE	
EXECUTE DEVICE DIAGNOSTIC		ACS-4	No	No
FINISH ZONE EXT		ACS-4, ZAC	See ZAC Management Out	
FLUSH CACHE		ACS-4	No	No
FLUSH CACHE EXT		ACS-4	No	No
FREEZE ACCESSIBLE MAX ADDRESS EXT		ACS-4	No	No
GET ACCESSIBLE MAX ADDRESS EXT		ACS-4	No	No
GET NATIVE MAX ADDRESS EXT		ACS-2	No	No
GET PHYSICAL ELEMENT STATUS		ACS-4	No	No
IDENTIFY DEVICE		ACS-4	No	No
IDLE		ACS-4	No	No

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
IDLE IMMEDIATE		ACS-4	No	No
NCQ NON-DATA	ABORT NCQ QUEUE	ACS-4	No	No
	DEADLINE HANDLING		No	No
	SET FEATURES		See SET FEATURES	
	ZAC Management Out		See ZAC Management Out	
	ZERO EXT		See ZERO EXT	
NOP		ACS-4	No	No
OPEN ZONE EXT		ACS-4, ZAC	See ZAC Management Out	
OVERWRITE EXT		ACS-4	See section 4.6.1.4 and section 4.6.1.5	
			No	Yes
READ BUFFER		ACS-4	No	No
READ BUFFER DMA		ACS-4	No	No
READ DMA		ACS-4	Yes	No
READ DMA EXT		ACS-4	Yes	No
READ FPDMA QUEUED		ACS-4	Yes	No
READ LOG DMA EXT	Except Logs E0, E1	ACS-4	No	No
	Logs E0 & E1		See SCT	
READ LOG EXT		ACS-4	See READ LOG DMA EXT	
READ MULTIPLE		ACS-3	Yes	No
READ MULTIPLE EXT		ACS-3	Yes	No

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
READ NATIVE MAX ADDRESS EXT		ACS-2	No	No
READ NATIVE MAX ADDRESS		ACS-2	No	No
READ SECTOR(S)		ACS-4	Yes	No
READ SECTOR(S) EXT		ACS-4	Yes	No
READ STREAM DMA EXT		ACS-4	Yes	No
READ STREAM EXT		ACS-4	Yes	No
READ VERIFY SECTOR(S)		ACS-4	Yes	No
READ VERIFY SECTOR(S) EXT		ACS-4	Yes	No
RECEIVE FPDMA QUEUED	READ LOG DMA EXT	ACS-4	See READ LOG DMA EXT	
	ZAC Management In		See ZAC Management In	
REMOVE ELEMENT AND TRUNCATE		ACS-4	No	Yes See section 4.6.6 and section 4.6.7
REPORT REALMS EXT		ZAC-2	See ZAC Management In	
REPORT ZONE DOMAINS EXT		ZAC-2	See ZAC Management In	
REPORT ZONES EXT		ACS-4, ZAC	See ZAC Management In	
REQUEST SENSE DATA EXT		ACS-4	No	No

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
RESET WRITE POINTER EXT		ACS-4, ZAC	See ZAC Management Out	
SANITIZE ANTI-FREEZE LOCK EXT		ACS-4	See section 4.6.1.4 and section 4.6.1.5	
			No	No
SANITIZE FREEZE LOCK EXT		ACS-4	See section 4.6.1.4 and section 4.6.1.5	
			No	No
SANITIZE STATUS EXT		ACS-4	See section 4.6.1.4 and section 4.6.1.5	
			No	No
SCT	Data Tables	ACS-4	No	No
	Error Recovery Control		No	No
	Feature Control		No	No
	Status		No	No
	Read Long	ATA8-ACS	See section 4.6.2	
	Write Long		See section 4.6.2	
	Write Same	ACS-4	No	Yes
SECURITY	DISABLE PASSWORD	ACS-4	See section 4.6.1.3	
	ERASE PREPARE		See section 4.6.1.3	
	ERASE UNIT		See section 4.6.1.3	
	FREEZE LOCK		See section 4.6.1.3	
	SET PASSWORD		See section 4.6.1.3	
	UNLOCK		See section 4.6.1.3	

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
SEND FPDMA QUEUED:	DATA SET MANAGEMENT	ACS-4	See DATA SET MANAGEMENT	
	DATA SET MANAGEMENT XL		See DATA SET MANAGEMENT XL	
	ZAC Management Out		See ZAC Management Out	
SEQUENTIALIZE ZONE EXT		ZAC	See ZAC Management Out	
SET ACCESSIBLE MAX ADDRESS EXT		ACS-4	No	Yes
SET DATE & TIME EXT		ACS-4	No	No
SET FEATURES	many	ACS-4	No	No
SET MAX	ADDRESS	ACS-2	No	No
	ADDRESS EXT		No	No
	FREEZE LOCK		No	No
	LOCK		No	No
	SET PASSWORD		No	No
	UNLOCK		No	No
SET MULTIPLE MODE		ACS-3	No	No
SET SECTOR CONFIGURATION EXT		ACS-4	See section 4.6.4	
			No	Yes
SLEEP		ACS-4	No	No
SMART	DISABLE OPERATIONS	ACS-3	No	No
	ENABLE OPERATIONS		No	No

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
	ENABLE/DISABLE AUTOSAVE		No	No
	EXECUTE OFF-LINE IMMEDIATE		Vendor specific [a]	
	READ DATA		No	No
	READ LOG	ACS-4	See READ LOG DMA EXT	
	RETURN STATUS		No	No
	WRITE LOG		See WRITE LOG DMA EXT	
STANDBY		ACS-4	No	No
STANDBY IMMEDIATE		ACS-4	No	No
TRUSTED NON-DATA		ACS-4	No	No
TRUSTED RECEIVE		ACS-4	No	No
TRUSTED RECEIVE DMA		ACS-4	No	No
TRUSTED SEND		ACS-4	No	No
TRUSTED SEND DMA		ACS-4	No	No
WRITE BUFFER		ACS-4	No	No
WRITE BUFFER DMA		ACS-4	No	No
WRITE DMA		ACS-4	No	Yes
WRITE DMA EXT		ACS-4	No	Yes
WRITE DMA FUA EXT		ACS-4	No	Yes
WRITE FPDMA QUEUED		ACS-4	No	Yes

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
WRITE LOG DMA EXT	Except Logs E0, E1	ACS-4	No	No
	Logs E0 & E1		See SCT	
WRITE LOG EXT		ACS-4	See WRITE LOG DMA EXT	
WRITE MULTIPLE		ACS-3	No	Yes
WRITE MULTIPLE EXT		ACS-3	No	Yes
WRITE MULTIPLE FUA EXT		ACS-3	No	Yes
WRITE SECTOR(S)		ACS-4	No	Yes
WRITE SECTOR(S) EXT		ACS-4	No	Yes
WRITE STREAM DMA EXT		ACS-4	No	Yes
WRITE STREAM EXT		ACS-4	No	Yes
WRITE UNCORRECTABLE EXT		ACS-4	No	Yes
ZAC Management In	REPORT REALMS EXT	ZAC-2	No	No
	REPORT ZONE DOMAINS EXT	ZAC-2	No	No
	REPORT ZONES EXT	ACS-4, ZAC	No	No
	ZONE ACTIVATE EXT	ZAC-2	Yes	Yes
	ZONE QUERY EXT	ZAC-2	No	No
ZAC Management Out	CLOSE ZONE EXT	ACS-4, ZAC	No	Yes
	FINISH ZONE EXT		No	Yes

ATA Command Interactions with the Locking SP				
Command	**Subcommand / Special Cases**	**Reference**	**Read Command**	**Write Command**
	OPEN ZONE EXT		No	Yes
	RESET WRITE POINTER EXT		No	Yes
	SEQUENTIALIZE ZONE EXT	ZAC	No	Yes
ZERO EXT		ACS-4	No	Yes
ZONE ACTIVATE EXT		ZAC-2	See ZAC Management In	
ZONE QUERY EXT		ZAC-2	See ZAC Management In	

[a] For Vendor Specific commands and for each ATA command not identified in the table, the command is considered a:

a) Write command, if the command modifies user data; and

b) Read command, if the command accesses user data.

7.3 NVMe Command Interactions

Table 34 specifies the interactions of NVMe commands not already described by other subclauses.

The commands in Table 34 MAY be supported on the TPer that incorporates the Locking Template. Table 34 identifies whether an NVMe command is considered as a Read command or a Write command for the purposes of interactions with ReadLockEnabled, WriteLockEnabled, ReadLocked, and WriteLocked column values in the `Locking` table.

Commands identified in Table 34 as Read commands SHALL behave as defined in the Interface Read Command Access table (see [17]).

Commands identified in Table 34 as Write commands SHALL behave as defined in the Interface Write Command Access table (see [17]).

Table 34 – NVMe command interactions with the Locking SP

Command [b]	Subcommand	Read Command	Write Command
Abort		No	No
Asynchronous Event Request		No	No
Compare		See section 5.6.10	
Copy		See section 5.6.11	
Create I/O Completion Queue		No	No
Create I/O Submission Queue		No	No
Dataset Management	Attribute – Deallocate	See section 5.6.5	
	Attribute – Integral Dataset for Read	No	No
	Attribute – Integral Dataset for Write	No	No
Delete I/O Completion Queue		No	No
Delete I/O Submission Queue		No	No
Doorbell Buffer Config		No	No
Device Self-Test		Vendor specific [a]	
Directive Receive		No	No
Directive Send		No	No
Firmware Commit		No	No
Firmware Image Download		No	No
Flush		No	No
Format NVM		See section 5.6.3	
Get Features		No	No
Get LBA Status		No	No

Command [b]	Subcommand	Read Command	Write Command
Get Log Page		No	No
Identify		No	No
Keep Alive		No	No
Lockdown		No	No
Namespace Attachment		No	No
Namespace Management		See section 5.6.1	
NVMe-MI Receive		See Table 35	
NVMe-MI Send		See Table 35	
Read		Yes	No
Reservation Acquire		No	No
Reservation Register		No	No
Reservation Release		No	No
Reservation Report		No	No
Sanitize		See section 5.6.4	
Security Receive		No	No
Security Send		No	No
Set Features		No	No
Verify		See section 5.6.9	
Write		No	Yes
Write Uncorrectable		No	Yes
Write Zeroes		No	Yes
Virtualization Management		No	No
Zone Append		No	Yes
Zone Management Receive	Report Zones	No	No
	Extended Report Zones	Yes	No
	All other Zone Receive Action values	Note [a]	Note [a]
Zone Management Send	Close Zone	No	Yes
	Finish Zone	No	Yes
	Open Zone	No	Yes
	Reset Zone	No	Yes
	Offline Zone	No	Yes

Command [b]	Subcommand	Read Command	Write Command
	Set Zone Descriptor Extension	No	Yes

[a] For Vendor Specific commands and for each NVMe command not identified in the table, the command is considered a:

a) Write, if command modifies user data; and

b) Read, if command accesses user data.

[b] References the transported NVMe commands (regardless of delivery path)

Table 35 - NVMe-MI command interactions with the Locking SP

Command [b]	**Read Command** [a]	**Write Command** [a]
Read NVMe-MI Data Structure	No	No
NVM Subsystem Health Status Poll	No	No
Controller Health Status Poll	No	No
Configuration Get	No	No
Configuration Set	No	No
VPD Read	No	No
VPD Write	No	No
Reset	No	No
SES Receive	No	No
SES Send	No	No
Management Endpoint Buffer Read	No	No
Management Endpoint Buffer Write	No	No
PCIe Configuration Read	No	No
PCIe Configuration Write	No	No
PCIe Memory Read	No	No
PCIe Memory Write	No	No
PCIe I/O Read	No	No
PCIe I/O Write	No	No
NVMe-MI Send/NVMe-MI Receive	See Table 34 for the transported NVMe command	

[a] For Vendor Specific commands and for each command not identified in the table, the command is considered a:

a) Write, if command modifies user data; and

b) Read, if command accesses user data.

[b] Regardless of delivery path (e.g., in band or out of band)

