TCG Storage Interface Interactions Specification (SIIS)

Version 1.09
Revision 1.16
July 29, 2020

Contact: admin@trustedcomputinggroup.com

PUBLIC REVIEW

Work in Progress

This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.
DISCLAIMERS, NOTICES, AND LICENSE TERMS

THIS SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG specifications or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

Contact the Trusted Computing Group at admin@trustedcomputinggroup.org for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.
# CHANGE HISTORY

<table>
<thead>
<tr>
<th>REVISION</th>
<th>DATE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.09/R1.01</td>
<td>May 13, 2019</td>
<td>Converted Version 1.08/1.00 to the new TCG template</td>
</tr>
<tr>
<td>V1.09/R1.02</td>
<td>May 13, 2019</td>
<td>Updated SCSI EXTENDED COPY</td>
</tr>
</tbody>
</table>
| V1.09/R1.03  | May 21, 2019 | • added ATA cmds: OPEN ZONE EXT, REPORT REALMS EXT, REPORT ZONE DOMAINS EXT, ZONE ACTIVATE EXT, ZONE QUERY EXT, RESTORE ELEMENT AND REPOPULATE  
• added SCSI reset distinction between single port and dual port (SAS only for right now)  
• added NVMe cmds: NVMe-MI Receive and NVMe-MI Send  
• added references under development: ACS-5, ZAC-2, NVMe 1.4 |
| V1.09/R1.04  | July 10, 2019| • added SCSI: Interactions with FORMAT WITH PRESETS  
• added ATA: Interactions with MUTATE EXT |
| V1.09/R1.05  | Jan. 15, 2020| • Incorporated SIIS changes described in document “TCG_Storage-Feature_Set_ShadowMBR_for_Multiple_Namespaces_v1_00_d1_12_20191203_clean”  
• Accepted all previous changes |
| V1.09/R1.06  | Jan 15, 2020 | • Put in details for NVMe-MI Send and NVMe-MI Receive commands (section 7.3)  
• Resolved comments related to ATA depopulation and repopulation  
• Added SCSI repopulation interactions |
| V1.09/R1.07  | Jan. 17, 2020| • Incorporate “TCG_SWG_SIIS_Version_1_08_Revision_1_00_ShadowMBRforMultiNS_20191203_rev1.docx” |
| V1.09/R1.08  | Jan. 23, 2020| • Removed dependency on the “TCG Storage Feature Set ShadowMBR for Multiple Namespaces” for sections 5.5.1.3.4, 5.5.1.4.6, and 5.5.2 |
| V1.09/R1.09  | Jan. 31, 2020| • Added new section 5.5.2 Locking Template interactions with the Namespace Management command  
• Removed all dependencies on the “TCG Storage Feature Set ShadowMBR for Multiple Namespaces” (sections 5.5.1.3.4, 5.5.1.4.6, 5.5.3) |
| V1.09/R1.10  | Feb. 4, 2020  | • The second list in section 5.5.3 started with d), it was changed to start at a) |
| V1.09/R1.11  | Feb. 6, 2020  | • Accepted all changes |
| V1.09/R1.12  | Apr. 8, 2020  | • Review comments from TC review, with replies and corrections |
| V1.09/R1.13  | Apr. 23, 2020 | • Clean version of R1.12, with changes accepted and unaddressed TC comments removed |
| V1.09/R1.14  | June 2, 2020  | • Changed ArialMT fonts to Arial  
• Accepted all changes |
| V1.09/R1.15  | July 14, 2020 | • Addressed comments from TC |
| V1.09/R1.16  | July 29, 2020 | • Fixed the section numbering for what is now 1.4, 1.4.1 and 1.4.2 |
CONTENTS
DISCLAIMERS, NOTICES, AND LICENSE TERMS ................................................................. 1
CHANGE HISTORY .................................................................................................................. 2
1 Introduction ....................................................................................................................... 6
   1.1 Document Purpose ....................................................................................................... 6
   1.2 Scope .......................................................................................................................... 6
   1.3 Intended Audience ...................................................................................................... 6
   1.4 Conventions ................................................................................................................ 6
       1.4.1 Key Words ........................................................................................................... 6
       1.4.2 Statement Type .................................................................................................... 6
   1.5 References to Other Documents ................................................................................ 7
       1.5.1 Document Precedence ....................................................................................... 7
       1.5.2 Approved References ......................................................................................... 7
       1.5.3 References under development ........................................................................ 8
   1.6 Definition of Terms ................................................................................................... 8
2 Overview .......................................................................................................................... 9
   2.1 Summary .................................................................................................................... 9
   2.2 Locking SP Ownership ............................................................................................. 9
   2.3 User data removal method ....................................................................................... 9
   2.4 Additional Status Code ........................................................................................... 9
3 SCSI Interface .................................................................................................................. 10
   3.1 Mapping of Resets .................................................................................................... 10
   3.2 Mapping of IF-SEND and IF-RECV ........................................................................ 17
       3.2.1 IF-SEND ............................................................................................................ 17
       3.2.2 IF-RECV ............................................................................................................ 17
   3.3 Handling Common TPer Errors ................................................................................ 18
   3.4 Discovery of Security Capabilities ............................................................................ 19
       3.4.1 Security Protocol 0x00 ...................................................................................... 19
   3.5 Miscellaneous ............................................................................................................ 19
       3.5.1 Queued Commands .......................................................................................... 19
       3.5.2 MBR Interactions .............................................................................................. 20
       3.5.3 Logical Unit usage ............................................................................................ 20
       3.5.4 Interaction of Opal family with the SANITIZE command ................................. 20
       3.5.5 Interaction of Enterprise SSC with the SANITIZE command ............................ 20
       3.5.6 Special Locking SP command interactions ......................................................... 20
       3.5.7 Interactions with Zoned Block devices ............................................................... 21
3.5.8 Interactions with the FORMAT UNIT command ................................................. 21
3.5.9 Interactions with Verify commands ............................................................... 21
3.5.10 Interactions with Extended Copy Operations ............................................... 21
3.5.11 Interactions with Unmap Operations ............................................................. 21
3.5.12 Interaction of Opal family with the REMOVE ELEMENT AND TRUNCATE command .... 22
3.5.13 Interaction of Enterprise SSC with the REMOVE ELEMENT AND TRUNCATE command .. 22
3.5.14 Interaction of Opal family with the RESTORE ELEMENT AND REBUILD command ........ 22
3.5.15 Interaction of Enterprise SSC with the RESTORE ELEMENT AND REBUILD command .... 22
3.5.16 Interface command interactions with user data removal methods .................. 22
3.5.17 Interactions with the FORMAT WITH PRESET command ............................. 23
3.5.18 Interactions with other SCSI commands ...................................................... 23

4 ATA Interface ........................................................................................................... 24

4.1 Mapping of Resets ................................................................................................. 24
4.2 Mapping of IF-SEND and IF-RECV ..................................................................... 25
  4.2.1 IF-SEND ........................................................................................................ 25
  4.2.2 IF-RECV ........................................................................................................ 25
4.3 Handling Common TPer Errors ........................................................................... 26
4.4 Discovery of Security Capabilities ........................................................................... 27
  4.4.1 IDENTIFY DEVICE .......................................................................................... 27
  4.4.2 Security Protocol 0x00 .................................................................................. 27
4.5 Miscellaneous ........................................................................................................ 27
  4.5.1 Feature set interactions .................................................................................. 27
  4.5.2 Special Locking SP command interactions ................................................... 29
  4.5.3 Interactions with Zoned Block devices ........................................................... 29
  4.5.4 Interactions with SET SECTOR CONFIGURATION EXT. ............................... 29
  4.5.5 Interactions with DATA SET MANAGEMENT commands .............................. 29
  4.5.6 Interaction of Opal family with the REMOVE ELEMENT AND TRUNCATE command .......... 30
  4.5.7 Interaction of Enterprise SSC with the REMOVE ELEMENT AND TRUNCATE command ... 30
  4.5.8 Interaction of Opal family with the RESTORE ELEMENT AND REBUILD command .... 30
  4.5.9 Interaction of Enterprise SSC with the RESTORE ELEMENT AND REBUILD command .... 30
  4.5.10 Interface command interactions with user data removal methods ................... 30
  4.5.11 Interactions with the MUTATE EXT commands ............................................ 31
  4.5.12 Interactions with other ATA commands ...................................................... 31

5 NVM Express Interface ............................................................................................. 32
  5.1 Mapping of Resets .............................................................................................. 32
  5.2 Mapping of IF-SEND and IF-RECV ................................................................. 33
5.2.1 IF-SEND ................................................................. 33
5.2.2 IF-RECV ............................................................... 34
5.3 Handling Common TPer Errors ............................................. 34
5.4 Discovery of Security Capabilities ........................................... 35
  5.4.1 Identify Controller Data Structure ..................................... 35
  5.4.2 Security Protocol 0x00 .................................................. 35
5.5 Miscellaneous .................................................................... 35
  5.5.1 Namespaces ............................................................... 35
  5.5.2 Locking Template interactions with the Namespace Management command .................................................. 39
  5.5.3 Locking Template interactions with the Format NVM Command .................................................. 39
  5.5.4 Interaction of Opal Family with the Sanitize command .............. 39
  5.5.5 Locking Template interactions with Dataset Management, Attribute – Deallocate ................................. 39
  5.5.6 Interface command interactions with user data removal methods .................................................. 39
  5.5.7 Locking Template interactions with other NVMe Commands .................................................. 40
6 eMMC Interface .................................................................... 41
  6.1 Mapping of Resets ................................................................ 41
  6.2 Mapping of IF-SEND and IF-RECV ....................................... 42
    6.2.1 IF-SEND .................................................................. 42
    6.2.2 IF-RECV .................................................................. 42
    6.2.3 eMMC Command Structure for TCG IF-SEND and IF-RECV .................................................. 43
  6.3 Handling Common TPer Errors ............................................. 45
  6.4 Discovery of Security Capabilities ........................................... 45
    6.4.1 Discovery of Security Capabilities ..................................... 45
  6.5 Miscellaneous .................................................................... 46
    6.5.1 Partition Management ................................................... 46
7 Appendix: Locking SP Interactions With Other Commands ....................... 47
  7.1 SCSI Command Interactions ................................................ 47
  7.2 ATA Command Interactions ................................................ 55
  7.3 NVMe Command Interactions .............................................. 64
1 Introduction

1.1 Document Purpose
The 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 as a trusted peripheral (TPer). This document also serves as a specification for TPers 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. The command interfaces described are ATA and SCSI. SCSI transports described are SAS, FC, and ATAPI. This document is written from the perspective of the Storage Device, not the host.

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.

1.4 Conventions

1.4.1 Key Words
The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “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.

1.4.2 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
1.5 References to Other Documents

1.5.1 Document Precedence
If there is a conflict between this specification and an approved reference (see 1.5.2) or a reference under development (see 1.5.3), then the precedence shall be:
1. this specification;
2. references under development; and
3. approved references.

1.5.2 Approved References

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

[25] TCG Opal SSC Feature Set: Configurable Namespace Locking version 1.00 revision 1.32
[29] TCG Storage Opal Family Feature Set: Shadow MBR for Multiple Namespaces, Version 1.00, Revision 1.12

1.6 Definition of Terms

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

2.4 Additional 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 follows

<table>
<thead>
<tr>
<th>Table 1 - Additional TPer Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
</tr>
<tr>
<td>-------------------------------------</td>
</tr>
<tr>
<td>INCOMPATIBLE MBR FORMAT</td>
</tr>
</tbody>
</table>
3 SCSI Interface

See [2], [21], [22], [7], [8], [20], and [18] for details on SCSI architecture, commands and transports.


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

See [15] and [24] for details on UFS.

3.1 Mapping of Resets

Table 2 – SAS Resets Mapped to TCG reset_type (single port)

<table>
<thead>
<tr>
<th>SAS Event</th>
<th>Maps to TCG reset_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power on reset</td>
<td>Power cycle</td>
</tr>
<tr>
<td>I-T Nexus Loss</td>
<td>(none)</td>
</tr>
<tr>
<td>ABORT TASK task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>ABORT TASK SET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>CLEAR TASK SET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>CLEAR ACA task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>I_T NEXUS RESET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>LOGICAL UNIT RESET task management function</td>
<td>Hardware Reset</td>
</tr>
<tr>
<td>Link Reset Sequence</td>
<td>(none)</td>
</tr>
<tr>
<td>Link reset sequence with hard reset</td>
<td>Hardware Reset</td>
</tr>
</tbody>
</table>
### Table 3 – SAS Resets Mapped to TCG reset_type (dual port)

<table>
<thead>
<tr>
<th>SAS Event</th>
<th>Maps to TCG reset_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power on reset</td>
<td>Power cycle</td>
</tr>
<tr>
<td>I-T Nexus Loss</td>
<td>(none)</td>
</tr>
<tr>
<td>ABORT TASK task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>ABORT TASK SET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>CLEAR TASK SET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>CLEAR ACA task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>I_T NEXUS RESET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>LOGICAL UNIT RESET task management function</td>
<td>Hardware Reset</td>
</tr>
<tr>
<td>Link Reset Sequence</td>
<td>(none)</td>
</tr>
<tr>
<td>Link reset sequence with hard reset</td>
<td>Hardware Reset</td>
</tr>
<tr>
<td>FC Event</td>
<td>Maps to TCG reset_type</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Power on reset</td>
<td>Power cycle</td>
</tr>
<tr>
<td>I-T Nexus Loss</td>
<td>(none)</td>
</tr>
<tr>
<td>ABORT TASK task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>ABORT TASK SET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>CLEAR TASK SET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>CLEAR ACA task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>I_T NEXUS RESET task management function</td>
<td>(none)</td>
</tr>
<tr>
<td>LOGICAL UNIT RESET task management function</td>
<td>Hardware Reset</td>
</tr>
<tr>
<td>LIP(AL_PD,AL_PS)</td>
<td>Hardware Reset</td>
</tr>
<tr>
<td>LIP(FF,AL_PS)</td>
<td>Hardware Reset</td>
</tr>
<tr>
<td>Port Login</td>
<td>(none)</td>
</tr>
<tr>
<td>Process Login</td>
<td>(none)</td>
</tr>
</tbody>
</table>
## Table 5 – ATAPI Resets Mapped to TCG reset\_type

<table>
<thead>
<tr>
<th>ATAPI Event</th>
<th>Maps to TCG reset_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power on reset</td>
<td>Power cycle</td>
</tr>
<tr>
<td>Hardware reset</td>
<td>PATA: Hardware Reset</td>
</tr>
<tr>
<td></td>
<td>SATA:</td>
</tr>
<tr>
<td></td>
<td>If Software Settings Preservation is enabled, then COMRESET is not a TCG Hardware Reset.</td>
</tr>
<tr>
<td></td>
<td>If Software Settings Preservation is disabled, then COMRESET is a TCG Hardware Reset.</td>
</tr>
<tr>
<td>Software reset</td>
<td>(none)</td>
</tr>
<tr>
<td>DEVICE RESET command</td>
<td>(none)</td>
</tr>
</tbody>
</table>
Table 6 – UAS Events Mapped to TCG reset_type

<table>
<thead>
<tr>
<th>Event</th>
<th>Maps to TCG reset_type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABORT TASK task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>ABORT TASK SET task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>CLEAR TASK SET task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>CLEAR ACA task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>I_T NEXUS RESET task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>LOGICAL UNIT RESET task management function</td>
<td>Hardware Reset</td>
<td>[21]</td>
</tr>
<tr>
<td>USB Port Reset</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Set Configuration with wValue set to zero</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Set Configuration with wValue set to non-zero value that is not equal to the current value of bConfiguration</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Set Configuration with wValue set to non-zero value that is equal to the current value of bConfiguration</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Bulk-Out Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-Out pipe of the Mass Storage Interface)</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Bulk-In Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-In pipe of the Mass Storage Interface)</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Suspend</td>
<td>Hardware Reset</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Resume</td>
<td>Hardware Reset</td>
<td>[11]</td>
</tr>
<tr>
<td>Event</td>
<td>Maps to TCG reset_type</td>
<td>Reference</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>USB Port Reset</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Set Configuration with wValue set to zero</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Set Configuration with wValue set to non-zero value that is not equal to the current value of bConfiguration.</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Set Configuration with wValue set to non-zero value that is equal to the current value of bConfiguration.</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Bulk-Out Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-Out pipe of the Mass Storage Interface)</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Bulk-In Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-In pipe of the Mass Storage Interface)</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>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)</td>
<td>(none)</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Suspend</td>
<td>Hardware Reset</td>
<td>[11]</td>
</tr>
<tr>
<td>USB Resume</td>
<td>Hardware Reset</td>
<td>[11]</td>
</tr>
</tbody>
</table>
### Table 8 – UFS Events Mapped to TCG reset_type

<table>
<thead>
<tr>
<th>Event</th>
<th>Maps to TCG reset_type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power-on</td>
<td>Power cycle</td>
<td>[15]</td>
</tr>
<tr>
<td>HW Pin Reset</td>
<td>Hardware Reset</td>
<td>[15]</td>
</tr>
<tr>
<td>EndPoint Reset</td>
<td>Hardware Reset</td>
<td>[15]</td>
</tr>
<tr>
<td>ABORT TASK task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>ABORT TASK SET task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>CLEAR TASK SET task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>LOGICAL UNIT RESET task management function</td>
<td>(none)</td>
<td>[21]</td>
</tr>
<tr>
<td>Host System UniPro Reset</td>
<td>Hardware Reset</td>
<td>[15]</td>
</tr>
</tbody>
</table>
3.2 Mapping of IF-SEND and IF-RECV

3.2.1 IF-SEND
IF-SEND SHALL be implemented with the SECURITY PROTOCOL OUT [21] command, with additional requirements on the CDB as specified in Table 9.

Table 9 – IF-SEND CDB field contents (SCSI)

<table>
<thead>
<tr>
<th>SECURITY PROTOCOL</th>
<th>SECURITY PROTOCOL SPECIFIC</th>
<th>INC_512</th>
<th>TRANSFER LENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Security Protocol 0x00 is not defined for IF-SEND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x01</td>
<td>a ComID</td>
<td>1 a</td>
<td>Non-zero b number of 512-byte data units.</td>
</tr>
<tr>
<td>0x02</td>
<td>a ComID</td>
<td>1 a</td>
<td>Non-zero b number of 512-byte data units.</td>
</tr>
<tr>
<td>0x06</td>
<td>a ComID</td>
<td>0</td>
<td>Number of bytes of data.</td>
</tr>
</tbody>
</table>

a If the INC_512 field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3).
b If the TRANSFER LENGTH field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3).

3.2.2 IF-RECV
IF-RECV SHALL be implemented with the SECURITY PROTOCOL IN [21] command, with additional requirements on the CDB as described in Table 10.

Table 10 – IF-RECV CDB field contents (SCSI)

<table>
<thead>
<tr>
<th>SECURITY PROTOCOL</th>
<th>SECURITY PROTOCOL SPECIFIC</th>
<th>INC_512</th>
<th>ALLOCATION LENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>(See [21] for details)</td>
<td>0 or 1</td>
<td>INC_512=0: Number of bytes of data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>INC_512=1: Number of 512-byte data units.</td>
</tr>
<tr>
<td>0x01</td>
<td>a ComID</td>
<td>1 a</td>
<td>Non-zero b number of 512-byte data units.</td>
</tr>
<tr>
<td>0x02</td>
<td>a ComID</td>
<td>1 a</td>
<td>Non-zero b number of 512-byte data units.</td>
</tr>
<tr>
<td>0x06</td>
<td>a ComID</td>
<td>0</td>
<td>Number of bytes of data.</td>
</tr>
</tbody>
</table>

a If the INC_512 field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3).
b If the ALLOCATION LENGTH field in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3), even though SPC-4 allows the ALLOCATION LENGTH field to be zero.
3.3 Handling Common TPer Errors

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

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

3.4.1 Security Protocol 0x00
See the description of SECURITY PROTOCOL IN [21] for information on Security Protocol 0x00.

3.5 Miscellaneous

3.5.1 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 that 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 Content

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 drive. For non-queuing devices, synchronicity is enforced at the time the IF-SEND/RECV 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 drive can only process one IF-SEND/RECV interface command at a time.

End Informative Content
3.5.2 MBR Interactions
The LUN associated with the MBR is the boot LUN.

3.5.3 Logical Unit usage
A target that has multiple logical units MAY have multiple TPers. 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. A logical unit MAY have no TPer.

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

If the Locking SP is owned 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 3.3).

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

If the Locking SP is owned (see 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a SANITIZE command with a Data Protection Error (see 3.3).

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

3.5.6 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. 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. The additional sense code:
   a) SHOULD be set to INVALID FIELD IN CDB; or
   b) MAY be set to INVALID COMMAND OPERATION CODE.

3.5.7 Interactions with Zoned Block devices
For a zoned block device (see [20]), cryptographic erase or key change methods (e.g., Erase or Revert) SHALL NOT change the write pointer of any zone.

3.5.8 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 3.3); 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.

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

3.5.10 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.

3.5.11 Interactions with Unmap Operations
An UNMAP command shall return a Data Protection Error (see 3.3) if:
   a) the parameter list specifies an LBA range that is included in one or more Locking objects; and
   b) the value 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.
3.5.12 Interaction of Opal family with the REMOVE ELEMENT AND TRUNCATE command

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

If the Locking SP is owned 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 3.3).

3.5.13 Interaction of Enterprise SSC with the REMOVE ELEMENT AND TRUNCATE command

If the Locking SP is not owned (see 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 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a REMOVE ELEMENT AND TRUNCATE command with a Data Protection Error (see 3.3).

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

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

If the Locking SP is owned 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 4.3).

3.5.15 Interaction of Enterprise SSC with the RESTORE ELEMENT AND REBUILD command

If the Locking SP is not owned (see 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 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a RESTORE ELEMENT AND REBUILD command with a Data Protection Error (see 4.3).

3.5.16 Interface command interactions with user data removal methods

If a user data removal method (see 2.3) is in process, then the device server shall terminate all supported SCSI commands with a Synchronous Protocol Violation (see 3.3), except for the following:

a) SECURITY PROTOCOL IN commands (see [21]);

b) SECURITY PROTOCOL OUT commands (see [21]);

c) INQUIRY commands (see [21]);

d) LOG SENSE commands that specify the Temperature log page (see [21]);

e) MODE SENSE commands that specify (see [21]):
   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 [21]);

g) REPORT LUNS commands (see [21]);

h) REPORT SUPPORTED OPERATION CODES commands (see [21]);

i) REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS commands (see [21]);

j) REPORT ZONES commands (see [20]) with:
A. the ZONE START LBA field set 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 [21]); and
l) TEST UNIT READY command; and
m) vendor specific commands that do not affect or retrieve user data.

3.5.17 Interactions with the FORMAT WITH PRESET command
If the Locking SP is owned and a FORMAT WITH PRESET command is sent to the device in order to:

a) 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 3.3); or
b) 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.

3.5.18 Interactions with other SCSI commands
Table 29 specifies the interactions of SCSI commands not already described by other subclauses.
4 ATA Interface


4.1 Mapping of Resets

Table 12 – ATA Resets Mapped to TCG reset_type

<table>
<thead>
<tr>
<th>ATA Event</th>
<th>Maps to TCG reset_type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power on reset</td>
<td>Power Cycle</td>
</tr>
<tr>
<td>Software reset</td>
<td>(none)</td>
</tr>
<tr>
<td>Hardware reset</td>
<td>PATA:</td>
</tr>
<tr>
<td></td>
<td>Hardware Reset</td>
</tr>
<tr>
<td></td>
<td>SATA:</td>
</tr>
<tr>
<td></td>
<td>If Software Settings Preservation is enabled, then COMRESET is not a TCG Hardware Reset.</td>
</tr>
<tr>
<td></td>
<td>If Software Settings Preservation is disabled, then COMRESET is a TCG Hardware Reset.</td>
</tr>
</tbody>
</table>
4.2 Mapping of IF-SEND and IF-RECV

4.2.1 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 13:

<table>
<thead>
<tr>
<th>SECURITY PROTOCOL</th>
<th>SP SPECIFIC</th>
<th>TRANSFER LENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Security Protocol 0x00 is not defined for IF-SEND</td>
<td></td>
</tr>
<tr>
<td>0x01</td>
<td>a ComID</td>
<td>Non-zero a number of 512-byte data units.</td>
</tr>
<tr>
<td>0x02</td>
<td>a ComID</td>
<td>Non-zero a number of 512-byte data units.</td>
</tr>
<tr>
<td>0x06</td>
<td>Protocol 0x06 is not defined for ATA.</td>
<td></td>
</tr>
</tbody>
</table>

a If the Transfer Length parameter is zero, then the TPer SHALL report Other Invalid Command Parameter (see 4.3).

4.2.2 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 14:

<table>
<thead>
<tr>
<th>SECURITY PROTOCOL</th>
<th>SP SPECIFIC</th>
<th>TRANSFER LENGTH</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>(See [5])</td>
<td>Non-zero number of 512-byte data units.</td>
</tr>
<tr>
<td>0x01</td>
<td>a ComID</td>
<td>Non-zero a number of 512-byte data units.</td>
</tr>
<tr>
<td>0x02</td>
<td>a ComID</td>
<td>Non-zero a number of 512-byte data units.</td>
</tr>
<tr>
<td>0x06</td>
<td>Protocol 0x06 is not defined for ATA.</td>
<td></td>
</tr>
</tbody>
</table>

a If the Transfer Length parameter is zero, then the TPer SHALL report Other Invalid Command Parameter (see 4.3).
4.3 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 15 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 is cleared to zero.

Table 16 describes common TPer errors if:

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

Table 15 – TPer Errors (ATA) – Without Sense Data Reporting (SDA=0)

<table>
<thead>
<tr>
<th>TPer Error ID</th>
<th>ATA Status Field</th>
<th>ATA Error Field</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>0x50</td>
<td>0x00</td>
<td>Normal command completion.</td>
</tr>
<tr>
<td>Invalid Security Protocol ID parameter</td>
<td>0x51</td>
<td>0x04</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Invalid Transfer Length parameter on IF-SEND</td>
<td>0x51</td>
<td>0x04</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Other Invalid Command Parameter</td>
<td>0x51</td>
<td>0x04</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Synchronous Protocol Violation</td>
<td>0x51</td>
<td>0x04</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Data Protection Error</td>
<td>0x51</td>
<td>0x04</td>
<td>No user data SHALL be transferred.</td>
</tr>
</tbody>
</table>
Table 16 – TPer Errors (ATA) – With Sense Data Reporting (SDA=1)

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

4.4 Discovery of Security Capabilities

4.4.1 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.

4.4.2 Security Protocol 0x00

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

4.5 Miscellaneous

4.5.1 Feature set interactions

4.5.1.1 Trusted Computing feature set

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

4.5.1.2 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 4.3).

4.5.1.3 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 (a User Password is set), 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.

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

If the Locking SP is not owned in an Opal family TPer (see 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:
   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 4.3):
      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.

4.5.1.5 Interaction of Enterprise SSC with the ATA Sanitize Device feature set

If the Locking SP is owned (see 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate the following commands with a Data Protection Error (see 4.3):

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.

4.5.1.6 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., a User Password is set), then the method invocation SHALL fail with a status of FAIL.

### 4.5.2 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:

- READ LONG;
- WRITE LONG;
- SCT READ LONG; and
- 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:

- READ LONG;
- WRITE LONG;
- SCT READ LONG; and
- SCT WRITE LONG.

### 4.5.3 Interactions with Zoned Block devices

For a zoned block device (see [18]), cryptographic erase or key change methods (e.g., Erase or Revert) SHALL NOT change the write pointer of any zone.

### 4.5.4 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 3.3); 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.

### 4.5.5 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 4.3) 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 value 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.
4.5.6 Interaction of Opal family with the REMOVE ELEMENT AND TRUNCATE command

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

If the Locking SP is owned 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 4.3).

4.5.7 Interaction of Enterprise SSC with the REMOVE ELEMENT AND TRUNCATE command

If the Locking SP is not owned (see 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 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a REMOVE ELEMENT AND TRUNCATE command with a Data Protection Error (see 4.3).

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

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

If the Locking SP is owned 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 4.3).

4.5.9 Interaction of Enterprise SSC with the RESTORE ELEMENT AND REBUILD command

If the Locking SP is not owned (see 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 2.2) in an Enterprise SSC TPer, then the SD SHALL terminate a RESTORE ELEMENT AND REBUILD command with a Data Protection Error (see 4.3).

4.5.10 Interface command interactions with user data removal methods

If a user data removal method (see 2.3) is in process, then the device shall terminate all supported ATA commands with a Synchronous Protocol Violation (see 4.3), 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 (see [18]) command 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 subcommand (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.

4.5.11 Interactions with the MUTATE EXT commands
If the Locking SP is owned and a MUTATE EXT command is sent to the device in order to:
   a) change the number of logical blocks per physical block, then the SD SHALL terminate that MUTATE EXT
      command with a Data Protection Error (see 3.3); or
   b) 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.

4.5.12 Interactions with other ATA commands
Table 30 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 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 17; and

b) set to one (i.e., the NVM subsystem may contain more than one NVM subsystem port), then use Table 18.

Table 17 – NVM Express over PCIe Resets Mapped to TCG reset_type (single port)

<table>
<thead>
<tr>
<th>NVM Express Event</th>
<th>Maps to TCG reset_type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Power loss / PCIe cold reset</td>
<td>Power Cycle</td>
<td>[16]</td>
</tr>
<tr>
<td>PCIe hot reset</td>
<td>None</td>
<td>[16]</td>
</tr>
<tr>
<td>PCIe warm reset</td>
<td>Hardware Reset</td>
<td>[16]</td>
</tr>
<tr>
<td>PCIe transaction layer Data Link Down status</td>
<td>None</td>
<td>[16]</td>
</tr>
<tr>
<td>NVMe subsystem reset</td>
<td>Hardware Reset</td>
<td>[12]</td>
</tr>
<tr>
<td>NVMe Controller reset (CC.EN transitions from 1 to 0)</td>
<td>None</td>
<td>[12]</td>
</tr>
<tr>
<td>NVMe Function level (PCI) reset</td>
<td>None</td>
<td>[12]</td>
</tr>
<tr>
<td>NVMe Queue level reset</td>
<td>None</td>
<td>[12]</td>
</tr>
</tbody>
</table>
Table 18 – NVM Express over PCIe Resets Mapped to TCG reset_type (multiple ports)

<table>
<thead>
<tr>
<th>NVM Express Event</th>
<th>Maps to TCG reset_type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Power loss / PCIe cold reset</td>
<td>Power Cycle</td>
<td>[16]</td>
</tr>
<tr>
<td>PCIe hot reset</td>
<td>None</td>
<td>[16]</td>
</tr>
<tr>
<td>PCIe warm reset</td>
<td>None</td>
<td>[16]</td>
</tr>
<tr>
<td>PCIe transaction layer Data Link Down status</td>
<td>None</td>
<td>[16]</td>
</tr>
<tr>
<td>NVMe subsystem reset</td>
<td>Hardware Reset</td>
<td>[12]</td>
</tr>
<tr>
<td>NVMe Controller reset (CC.EN transitions from 1 to 0)</td>
<td>None</td>
<td>[12]</td>
</tr>
<tr>
<td>NVMe Function level (PCI) reset</td>
<td>None</td>
<td>[12]</td>
</tr>
<tr>
<td>NVMe Queue level reset</td>
<td>None</td>
<td>[12]</td>
</tr>
</tbody>
</table>

5.2 Mapping of IF-SEND and IF-RECV

5.2.1 IF-SEND

IF-SEND SHALL be implemented with the Security Send command, with additional requirements on the inputs as described in Table 19:

Table 19 – IF-SEND command parameters (NVM Express)

<table>
<thead>
<tr>
<th>Security Protocol</th>
<th>SP Specific b</th>
<th>Transfer Length</th>
<th>Namespace Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Security Protocol 0x00 is not defined for IF-SEND</td>
<td>0x00 is not defined for IF-SEND</td>
<td>Is not used a</td>
</tr>
<tr>
<td>0x01</td>
<td>SPSP0 = ComID (7:0)  SPSP1= ComID (15:8)</td>
<td>Number of bytes to transfer.</td>
<td>Is not used a</td>
</tr>
<tr>
<td>0x02</td>
<td>SPSP0 = ComID (7:0)  SPSP1= ComID (15:8)</td>
<td>Number of bytes to transfer.</td>
<td>Is not used a</td>
</tr>
<tr>
<td>0x06</td>
<td>Security Protocol 0x06 is not defined for NVMe.</td>
<td>0x06 is not defined for NVMe.</td>
<td></td>
</tr>
</tbody>
</table>

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).
5.2.2 IF-RECV

IF-RECV SHALL be implemented with the Security Receive command, with additional requirements on the inputs as described in Table 20:

<table>
<thead>
<tr>
<th>Security Protocol</th>
<th>SP Specific</th>
<th>Allocation Length</th>
<th>Namespace Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>See [12]</td>
<td>Number of bytes to transfer.</td>
<td>Is not used a</td>
</tr>
<tr>
<td>0x01</td>
<td>SPSP0= ComID (7:0) SPSP1= ComID (15:8)</td>
<td>Number of bytes to transfer.</td>
<td>Is not used a, except as specified in the Configurable Namespace Locking Feature set (see [25]) for Namespace Level 0 Discovery.</td>
</tr>
<tr>
<td>0x02</td>
<td>SPSP0= ComID (7:0) SPSP1= ComID (15:8)</td>
<td>Number of bytes to transfer.</td>
<td>Is not used a</td>
</tr>
<tr>
<td>0x06</td>
<td>Security Protocol 0x06 is not defined for NVMe.</td>
<td>Is not used a</td>
<td></td>
</tr>
</tbody>
</table>

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 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 21.
### Table 21 – TPer Errors (NVM Express)

<table>
<thead>
<tr>
<th>TPer Error ID</th>
<th>Status Code Type</th>
<th>Status Code</th>
<th>Do Not Retry bit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>Generic Command Status</td>
<td>Successful Completion</td>
<td>0</td>
<td>Normal command completion.</td>
</tr>
<tr>
<td>Invalid Security Protocol ID parameter</td>
<td>Generic Command Status</td>
<td>Invalid Field in Command</td>
<td>1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Invalid Transfer Length parameter on IF-SEND</td>
<td>Generic Command Status</td>
<td>Invalid Field in Command</td>
<td>1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Other Invalid Command Parameter</td>
<td>Generic Command Status</td>
<td>Invalid Field in Command</td>
<td>1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Synchronous Protocol Violation</td>
<td>Generic Command Status</td>
<td>Command Sequence Error</td>
<td>1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Data Protection Error</td>
<td>Media and Data Integrity Errors</td>
<td>Access Denied</td>
<td>1</td>
<td>No user data SHALL be transferred.</td>
</tr>
<tr>
<td>Invalid Security State</td>
<td>Command Specific Status</td>
<td>Invalid Format</td>
<td>1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Operation Denied</td>
<td>Generic Command Status</td>
<td>Operation Denied</td>
<td>1</td>
<td>No data SHALL be transferred.</td>
</tr>
</tbody>
</table>

### 5.4 Discovery of Security Capabilities

#### 5.4.1 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.

#### 5.4.2 Security Protocol 0x00

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

### 5.5 Miscellaneous

#### 5.5.1 Namespaces

##### 5.5.1.1 Overview

An NVM subsystem SHALL have no more than one TPer. The TPer is associated with the NVM subsystem rather than with any controller within the NVM subsystem.

The following items apply regardless of the number of existing namespaces:
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.

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 NVM subsystem (see Table 22).

**Table 22 – Namespace Management**

<table>
<thead>
<tr>
<th>Number of Existing Namespaces</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>5.5.1.2</td>
</tr>
<tr>
<td>1</td>
<td>5.5.1.3</td>
</tr>
<tr>
<td>Greater than 1</td>
<td>5.5.1.4</td>
</tr>
</tbody>
</table>

5.5.1.2  No Existing Namespace

5.5.1.2.1  Global Range Locking object Interactions

*Begin Informative Content*

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

*End Informative Content*

5.5.1.2.2  Non-Global Range Locking object Interactions

If no namespace exists, 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.

5.5.1.2.3  Namespace Management

If no namespace exists in the NVM subsystem, 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.

5.5.1.3  Single Namespace

5.5.1.3.1  Global Range Locking object Interactions

If only one namespace exists in the NVM subsystem, 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 erase of the Global Range Locking object SHALL result in the cryptographic erase of all LBAs within that namespace that are not associated with any non-Global Range Locking objects.
5.5.1.3.2 Non-Global Range Locking Object Interactions
If only one namespace exists in the NVM subsystem, then the device MAY support configuration of non-Global
Range Locking objects.

5.5.1.3.3 Namespace Management
If only one namespace exists in the NVM subsystem, 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.

5.5.1.3.4 MBR Shadowing for Single Namespace
If the Set method is invoked on the MBRC, and:
   a) the provided Enabled column value is TRUE; and
   b) the LBA Format is incompatible with the content of MBR table and the Namespace,
then the Set method MAY fail with a Status Code of INCOMPATIBLE_MBR_FORMAT.

5.5.1.4 Multiple Namespaces

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

An NVM subsystem 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 erase of the Global Range Locking object SHALL result in the
cryptographic erase of all existing namespaces in the NVM subsystem.

5.5.1.4.2 Non-Global Range Locking Object Interactions
If more than one namespace exists in the NVM subsystem, 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.

5.5.1.4.3 Namespace Management
If more than one namespace exists in the NVM subsystem, 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.

5.5.1.4.4 Geometry Feature Descriptor with Multiple Namespaces
The host SHOULD ignore the Geometry Feature Descriptor.

5.5.1.4.5 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.

5.5.1.4.6 MBR Shadowing for Multiple Namespaces
If MBR shadowing (see [17]) is supported by the TPer, the MBR and MBRCntrol tables in the Locking SP are shared by all namespaces and controllers within the NVM subsystem.

If the Set method is invoked on the MBRCntrolObj, and:

a) the provided Enabled column value is TRUE; and
b) the LBA Format is incompatible with 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 MBRCntrol 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 NVM subsystem. LBA format compatibility is not a TPer responsibility.
5.5.2 Locking Template interactions with the Namespace Management command

If the Locking SP is owned, and:
   a) a controller processes a Namespace Management command;
   b) the Enabled column value of the MBRCtrlObj is TRUE; and
   c) the Namespace Management command specifies the creation of a namespace with an LBA Format (see [12]) that is different from one of the existing Namespaces,
then the Namespace Management command SHALL fail with a status of Operation Denied.

5.5.3 Locking Template interactions with the Format NVM Command

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

If the Locking SP is owned and 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 Locking SP is owned, and:
   a) a controller processes a Format NVM command;
   b) the Enabled column value of the MBRCtrlObj [29] is TRUE; and
   c) the Format NVM command specifies changing to an LBA Format of the Namespace corresponding to the value of NamespaceID column of MBRCtrl table from the original LBA Format (see [12]),
then the Format NVM command SHALL fail with a status of Invalid Security State.

5.5.4 Interaction of Opal Family with the Sanitize command

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

If the Locking SP is owned in a TPer, 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 5.3).

5.5.5 Locking Template interactions with Dataset Management, Attribute – Deallocate

The NVM subsystem 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 5.3) if:
   a) the command provides an LBA range that is included in one or more Locking objects; and
   b) the value 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 provided.

5.5.6 Interface command interactions with user data removal methods

If a user data removal method (see 2.3) is in process, then the controller shall terminate all supported NVMe commands with a Synchronous Protocol Violation (see 5.3), 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) 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
   o) vendor specific commands that do not affect or retrieve user data.

5.5.7 **Locking Template interactions with other NVMe Commands**

Table 31 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. Further details relating to the mapping provided below are found in [23].

See [14] for details on e•MMC architecture, commands and transports. Further details relating to the mapping provided below are found in [23].

6.1 Mapping of Resets

Table 23 specifies the e•MMC events that are mapped to TCG resets.

Table 23 – e•MMC Events Mapped to TCG reset_type

<table>
<thead>
<tr>
<th>e•MMC Event</th>
<th>Maps to TCG reset_type</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power On</td>
<td>Power cycle</td>
<td>[14]</td>
</tr>
<tr>
<td>H/W Reset (Pin, Reset Signal)</td>
<td>Hardware Reset</td>
<td>[14]</td>
</tr>
<tr>
<td>GO_IDLE_STATE (CMD0)</td>
<td>Hardware Reset</td>
<td>[14]</td>
</tr>
<tr>
<td>GO_PRE_IDLE_STATE (CMD0)</td>
<td>Hardware Reset</td>
<td>[14]</td>
</tr>
<tr>
<td>GO_INACTIVE_ STATE (CMD15)</td>
<td>Power cycle</td>
<td>[14]</td>
</tr>
<tr>
<td>HPI (High Priority Interrupt)</td>
<td>None</td>
<td>[14]</td>
</tr>
</tbody>
</table>
6.2 Mapping of IF-SEND and IF-RECV

6.2.1 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 24.

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

Table 24 – IF-SEND command parameters (e•MMC)

<table>
<thead>
<tr>
<th>Security Protocol</th>
<th>SP_Specific</th>
<th>Transfer Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Security Protocol 0x00 is not defined for IF-SEND</td>
<td></td>
</tr>
<tr>
<td>0x01</td>
<td>a ComID</td>
<td>Non-zero(^a) number of 512 byte data units as defined in CMD23</td>
</tr>
<tr>
<td>0x02</td>
<td>a ComID</td>
<td>Non-zero(^a) number of 512 byte data units as defined in CMD23</td>
</tr>
<tr>
<td>0x06</td>
<td>Protocol 0x06 is not defined for e•MMC.</td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) 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 .(6.4)

6.2.2 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 25.

CMD23 command is used to set the transfer block count for the CMD53. See [14] for details regarding CMD23 and CMD53.

Table 25 – IF-RECV command parameters (e•MMC)

<table>
<thead>
<tr>
<th>Security Protocol</th>
<th>SP_Specific</th>
<th>Allocation Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>See [14] (^b)</td>
<td>Non-zero(^a) number of 512 byte data units as defined in CMD23</td>
</tr>
<tr>
<td>0x01</td>
<td>a ComID</td>
<td>Non-zero(^a) number of 512 byte data units as defined in CMD23</td>
</tr>
<tr>
<td>0x02</td>
<td>a ComID</td>
<td>Non-zero(^a) number of 512 byte data units as defined in CMD23</td>
</tr>
<tr>
<td>0x06</td>
<td>Protocol 0x06 is not defined for e•MMC.</td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) 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 .(6.4)

\(^b\)When receiving CMD53 (PROTOCOL_RD) with Security Protocol value equal to 00h the device SHALL return the list of supported protocols.
6.2.3 eMMC Command Structure for TCG IF-SEND and IF-RECV

6.2.3.1 eMMC Block Allocation Overview
The eMMC protocol uses the CMD23 SET_BLOCK_COUNT command (see 6.2.3.2) to set the block count for the CMD54 command or the CMD53 command (see 6.2.3.3) 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 eMMC transport, the IF-SEND command consists of the combination of a CMD23, followed by a CMD54.

For TCG on the eMMC transport, the IF-RECV command consists of the combination of a CMD23, followed by a CMD53.

6.2.3.2 eMMC 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 blocks. See Table 26.

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

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].
6.2.3.3 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 27.

### Table 27 – e•MMC CMD54 and CMD53 Structure

<table>
<thead>
<tr>
<th>Bit Byte</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>[31:24] Security Protocol Specific (7:0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>[15:8] Reserved</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>[7:1] CRC7</td>
<td>[0] Stop Bit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See Table 24 and Table 25 for usage of Bytes 1 and 2, the Security Protocol Specific fields and the Security Protocol field. All other fields are defined in [14].
6.3 Handling Common TPer Errors

Security related errors are detected by the e•MMC interface or by the TPer. This section describes how they are reported by the e•MMC interface.

See [14] for details.

<table>
<thead>
<tr>
<th>TPer Error ID</th>
<th>e•MMC Device Status</th>
<th>EXCEPTION EVENTS STATUS a</th>
<th>EXT SECURITY ERR b</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>No error</td>
<td>No error</td>
<td>No error</td>
<td>Normal command completion.</td>
</tr>
<tr>
<td>Invalid Security Protocol ID parameter</td>
<td>EXCEPTION EVENT=1</td>
<td>EXTENDED SECURITY FAILURE =1</td>
<td>SEC INVALID COMMAND PARAMETER S=1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Invalid Transfer Length parameter on IF-SEND</td>
<td>EXCEPTION EVENT=1</td>
<td>EXTENDED SECURITY FAILURE =1</td>
<td>SEC INVALID COMMAND PARAMETER S=1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Other Invalid Command Parameter</td>
<td>EXCEPTION EVENT=1</td>
<td>EXTENDED SECURITY FAILURE =1</td>
<td>SEC INVALID COMMAND PARAMETER S=1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Synchronou s Protocol Violation</td>
<td>EXCEPTION EVENT=1</td>
<td>EXTENDED SECURITY FAILURE =1</td>
<td>SEC INVALID COMMAND PARAMETER S=1</td>
<td>No data SHALL be transferred.</td>
</tr>
<tr>
<td>Data Protection Error</td>
<td>EXCEPTION EVENT=1</td>
<td>EXTENDED SECURITY FAILURE =1</td>
<td>ACCESS DENIED=1</td>
<td>No user data SHALL be transferred.</td>
</tr>
</tbody>
</table>

a  EXCEPTION_EVENTS_STATUS field of the EXT_CSD register
b  EXT_SECURITY_ERR field of the EXT_CSD register

6.4 Discovery of Security Capabilities

6.4.1 Discovery of Security Capabilities

6.4.1.1 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 device SHALL return the list of supported protocols.
6.5 Miscellaneous

6.5.1 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 29 specifies the interactions of SCSI commands not already described by other subclauses.

The commands in Table 29 MAY be supported on an SD that incorporates the Locking Template. Table 29 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 29 as Read commands SHALL behave as defined in the Interface Read Command Access table (see [17]).

Commands identified in Table 29 as Write commands SHALL behave as defined in the Interface Write Command Access table (see [17]).

<table>
<thead>
<tr>
<th>SCSI Command</th>
<th>Service Action / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKGROUND CONTROL</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BIND</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CHANGE ALIASES</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CLOSE ZONE</td>
<td></td>
<td>ZBC</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>COMPARE AND WRITE</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>COPY OPERATION ABORT</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>EXTENDED COPY</td>
<td></td>
<td>SPC-5</td>
<td></td>
<td>See 3.5.10</td>
</tr>
<tr>
<td>FINISH ZONE</td>
<td></td>
<td>ZBC</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>FORMAT UNIT</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>See 3.5.8</td>
</tr>
<tr>
<td>GET LBA STATUS</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>GET PHYSICAL ELEMENT STATUS</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GET STREAM STATUS</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>INQUIRY</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### SCSI command interactions with the Locking SP

<table>
<thead>
<tr>
<th>SCSI Command</th>
<th>Service Action / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOG SELECT</td>
<td></td>
<td>SPC-5, SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>LOG SENSE</td>
<td></td>
<td>SPC-5, SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MODE SELECT (6/10)</td>
<td></td>
<td>SPC-5, SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MANAGEMENT PROTOCOL IN</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MANAGEMENT PROTOCOL OUT</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MODE SENSE (6)</td>
<td></td>
<td>SPC-5, SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MODE SENSE (10)</td>
<td></td>
<td>SPC-5, SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>OPEN ZONE</td>
<td></td>
<td>ZBC</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ORWRITE (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ORWRITE (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>PERSISTENT RESERVE IN</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>PERSISTENT RESERVE OUT</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>POPULATE TOKEN</td>
<td></td>
<td>SBC-4</td>
<td>See 3.5.10</td>
<td>No</td>
</tr>
<tr>
<td>PRE-FETCH (10)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PRE-FETCH (16)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PREVENT ALLOW MEDIUM REMOVAL</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ (6)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ (10)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### SCSI command interactions with the Locking SP

<table>
<thead>
<tr>
<th>SCSI Command</th>
<th>Service Action / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ (16)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ (32)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ ATTRIBUTE</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ BUFFER (10)</td>
<td>Except modes 0Ah, 0Bh, and 1Ch</td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ BUFFER (16)</td>
<td>Mode 0Ah and 0Bh - Echo Buffer Mode</td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ CAPACITY (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ CAPACITY (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ DEFECT DATA (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ DEFECT DATA (12)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>READ LONG (10)</td>
<td></td>
<td>SBC-4</td>
<td>See 3.5.6</td>
<td></td>
</tr>
<tr>
<td>READ LONG (16)</td>
<td></td>
<td>SBC-4</td>
<td>See 3.5.6</td>
<td></td>
</tr>
<tr>
<td>READ MEDIA SERIAL NUMBER</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REASSIGN BLOCKS</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>RECEIVE COPY DATA</td>
<td></td>
<td>SPC-5</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RECEIVE DIAGNOSTIC RESULTS</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RECEIVE ROD TOKEN INFORMATION</td>
<td></td>
<td>SPC-5, SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>REMOVE ELEMENT AND TRUNCATE</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>See 3.5.12 and 3.5.13</td>
</tr>
<tr>
<td>REMOVE I-T NEXUS</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SCSI Command</td>
<td>Service Action / Special Cases</td>
<td>Reference</td>
<td>Read Command</td>
<td>Write Command</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>RELEASE (6)</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RELEASE (10)</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT ALIASES</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT ALL ROD TOKENS</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT IDENTIFYING INFORMATION</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT LUNS</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT PRIORITY</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT PROVISIONING INITIALIZATION PATTERN</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT REFERRALS</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT SUPPORTED TASK MANAGEMENT FUNCTIONS</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT TARGET PORT</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT TIMESTAMP</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT ZONES</td>
<td></td>
<td>ZBC</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REQUEST SENSE</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RESERVE (6)</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RESERVE (10)</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RESET WRITE POINTER</td>
<td></td>
<td>ZBC</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>REZERO UNIT</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
| SANITIZE              | BLOCK ERASE                    | SBC-4     | See 3.5.4 and 3.5.5 | No
### SCSI command interactions with the Locking SP

<table>
<thead>
<tr>
<th>SCSI Command</th>
<th>Service Action / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRYPTO ERASE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVERWRITE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EXIT FAILURE MODE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SECURITY PROTOCOL IN</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SECURITY PROTOCOL OUT</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SEEK (6)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SEEK (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SEND DIAGNOSTIC</td>
<td></td>
<td>SPC-5</td>
<td>Vendor specific a</td>
<td></td>
</tr>
<tr>
<td>SET AFFILIATION</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET PRIORITY</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET IDENTIFYING INFORMATION</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET TARGET PORT GROUPS</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET TIMESTAMP</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>STREAM CONTROL</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>START STOP UNIT</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SYNCHRONIZE CACHE (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SYNCHRONIZE CACHE (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>TEST UNIT READY</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>UNBIND</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>UNMAP</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>See 3.5.11</td>
</tr>
</tbody>
</table>
## SCSI command interactions with the Locking SP

<table>
<thead>
<tr>
<th>SCSI Command</th>
<th>Service Action / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERIFY (10)</td>
<td>BYTCHK=0</td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>BYTCHK=1</td>
<td>SBC-4</td>
<td>See 3.5.9</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>BYTCHK=0</td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>BYTCHK=1</td>
<td>SBC-4</td>
<td>See 3.5.9</td>
<td>No</td>
</tr>
<tr>
<td>VERIFY (12)</td>
<td>BYTCHK=0</td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>BYTCHK=1</td>
<td>SBC-4</td>
<td>See 3.5.9</td>
<td>No</td>
</tr>
<tr>
<td>VERIFY (16)</td>
<td>BYTCHK=0</td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>BYTCHK=1</td>
<td>SBC-4</td>
<td>See 3.5.9</td>
<td>No</td>
</tr>
<tr>
<td>VERIFY (32)</td>
<td>BYTCHK=0</td>
<td>SBC-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>BYTCHK=1</td>
<td>SBC-4</td>
<td>See 3.5.9</td>
<td>No</td>
</tr>
<tr>
<td>XDWRITEREAD (10)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>XDWRITEREAD (32)</td>
<td></td>
<td>SBC-4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>XPWRITE (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>XPWRITE (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE (6)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE AND VERIFY (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE AND VERIFY (12)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE AND VERIFY (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE AND VERIFY (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Notes:
- BYTCHK=0 indicates the standard behavior.
- BYTCHK=1 indicates a special case where the Locking SP returns a different result.
- SBC-4 refers to the specific section in the TCG Storage Interface Interactions Specification (SIIS).
## SCSI command interactions with the Locking SP

<table>
<thead>
<tr>
<th>SCSI Command</th>
<th>Service Action / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRITE AND VERIFY (32)</td>
<td>BYTCHK=1</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE ATOMIC (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE ATOMIC (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE ATTRIBUTE</td>
<td></td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>WRITE BUFFER</td>
<td>all modes except those modes associated with Download Microcode and the Echo Buffer mode</td>
<td>SPC-5</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>all modes associated with Download Microcode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mode 0Ah - Echo Buffer Mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRITE LONG (10)</td>
<td>WR_UNCOR=0</td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>WR_UNCOR=1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WRITE LONG (16)</td>
<td>WR_UNCOR=0</td>
<td>SBC-4</td>
<td>See 3.5.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WR_UNCOR=1</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE SAME (10)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE SAME (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE SAME (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE STREAM (16)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE STREAM (32)</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE USING TOKEN</td>
<td></td>
<td>SBC-4</td>
<td>No</td>
<td>See 3.5.10</td>
</tr>
<tr>
<td>SCSI Command</td>
<td>Service Action / Special Cases</td>
<td>Reference</td>
<td>Read Command</td>
<td>Write Command</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------</td>
<td>-----------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| 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 30 specifies the interactions of ATA commands not already described by other subclauses.

The commands in Table 30 MAY be supported on an SD that incorporates the Locking Template. Table 30 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 30 as Read commands SHALL behave as defined in the Interface Read Command Access table (see [17]).

Commands identified in Table 30 as Write commands SHALL behave as defined in the Interface Write Command Access table (see [17]).

### Table 30 – ATA command interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABORT NCQ QUEUE</td>
<td></td>
<td>ACS-4</td>
<td>See NCQ NON-DATA</td>
<td></td>
</tr>
<tr>
<td>BLock ERASE EXT</td>
<td></td>
<td>ACS-4</td>
<td>See 4.5.1.4 and 4.5.1.5</td>
<td></td>
</tr>
<tr>
<td>CHECK POWER MODE</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CLOSE ZONE EXT</td>
<td></td>
<td>ACS-4</td>
<td>See ZAC Management Out</td>
<td>No</td>
</tr>
<tr>
<td>CONFIGURE STREAM</td>
<td></td>
<td>ACS-4, ZAC</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>CRYPTO SCRAMBLE EXT</td>
<td></td>
<td>ACS-4</td>
<td>See 4.5.1.4 and 4.5.1.5</td>
<td>Yes</td>
</tr>
<tr>
<td>DATA SET MANAGEMENT</td>
<td>Trim</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Markup LBA Ranges function</td>
<td>ACS-4</td>
<td>No</td>
<td>See 4.5.5</td>
</tr>
<tr>
<td>DATA SET MANAGEMENT XL</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DEADLINE HANDLING</td>
<td></td>
<td>ACS-4</td>
<td>See NCQ NON-DATA</td>
<td></td>
</tr>
</tbody>
</table>
### ATA Command Interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE CONFIGURATION OVERLAY (DCO)</td>
<td>FREEZE LOCK</td>
<td>ACS-2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>IDENTIFY</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>RESTORE</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>SET</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DOWNLOAD MICROCODE</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DOWNLOAD MICROCODE DMA</td>
<td></td>
<td>ACS-4</td>
<td>See DOWNLOAD MICROCODE</td>
<td></td>
</tr>
<tr>
<td>EXECUTE DEVICE DIAGNOSTIC</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FINISH ZONE EXT</td>
<td>ACS-4, ZAC</td>
<td></td>
<td>See ZAC Management Out</td>
<td></td>
</tr>
<tr>
<td>FLUSH CACHE</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FLUSH CACHE EXT</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>FREEZE ACCESSIBLE MAX ADDRESS EXT</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GET ACCESSIBLE MAX ADDRESS EXT</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GET NATIVE MAX ADDRESS EXT</td>
<td>ACS-2</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GET PHYSICAL ELEMENT STATUS</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IDENTIFY DEVICE</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IDLE</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IDLE IMMEDIATE</td>
<td>ACS-4</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>NCQ NON-DATA</td>
<td>ABORT NCQ QUEUE</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>DEADLINE HANDLING</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
### ATA Command Interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SET FEATURES</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZAC Management Out</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZERO EXT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOP</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>OPEN ZONE EXT</td>
<td>ACS-4, ZAC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVERWRITE EXT</td>
<td>ACS-4</td>
<td>See 4.5.1.4 and 4.5.1.5</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>READ BUFFER</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ BUFFER DMA</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ DMA</td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ DMA EXT</td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ FPDMA QUEUED</td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ LOG DMA EXT</td>
<td>Except Logs E0, E1, Logs E0 &amp; E1</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ LOG EXT</td>
<td>ACS-4</td>
<td>See READ LOG DMA EXT</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ MULTIPLE</td>
<td>ACS-3</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ MULTIPLE EXT</td>
<td>ACS-3</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ NATIVE MAX ADDRESS EXT</td>
<td>ACS-2</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ NATIVE MAX ADDRESS</td>
<td>ACS-2</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>READ SECTOR(S)</td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
## ATA Command Interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ SECTOR(S) EXT</td>
<td></td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ STREAM DMA EXT</td>
<td></td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ STREAM EXT</td>
<td></td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ VERIFY SECTOR(S)</td>
<td></td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>READ VERIFY SECTOR(S) EXT</td>
<td></td>
<td>ACS-4</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>RECEIVE FPDMA QUEUED</td>
<td>READ LOG DMA EXT</td>
<td>ACS-4</td>
<td>See READ LOG DMA EXT</td>
<td>See ZAC Management In</td>
</tr>
<tr>
<td></td>
<td>ZAC Management In</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REMOVE ELEMENT AND TRUNCATE</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>See 4.5.6 and 4.5.7</td>
</tr>
<tr>
<td>REPORT REALMS EXT</td>
<td></td>
<td>ZAC-2</td>
<td>See ZAC Management In</td>
<td></td>
</tr>
<tr>
<td>REPORT ZONE DOMAINS EXT</td>
<td></td>
<td>ZAC-2</td>
<td>See ZAC Management In</td>
<td></td>
</tr>
<tr>
<td>REPORT ZONES EXT</td>
<td></td>
<td>ACS-4, ZAC</td>
<td>See ZAC Management In</td>
<td></td>
</tr>
<tr>
<td>REQUEST SENSE DATA EXT</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>RESET WRITE POINTER EXT</td>
<td></td>
<td>ACS-4, ZAC</td>
<td>See ZAC Management Out</td>
<td></td>
</tr>
<tr>
<td>SANITIZE ANTI-FREEZE LOCK EXT</td>
<td></td>
<td>ACS-4</td>
<td>See 4.5.1.4 and 4.5.1.5</td>
<td>No</td>
</tr>
<tr>
<td>SANITIZE FREEZE LOCK EXT</td>
<td></td>
<td>ACS-4</td>
<td>See 4.5.1.4 and 4.5.1.5</td>
<td>No</td>
</tr>
</tbody>
</table>
### ATA Command Interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANITIZE STATUS EXT</td>
<td>Data Tables</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Error Recovery Control</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Feature Control</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Status</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SCT</td>
<td>Read Long</td>
<td>ATA8-ACS</td>
<td>See 4.5.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Write Long</td>
<td></td>
<td>See 4.5.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Write Same</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SECURITY</td>
<td>DISABLE PASSWORD</td>
<td>ACS-4</td>
<td>See 4.5.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ERASE PREPARE</td>
<td>ACS-4</td>
<td>See 4.5.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ERASE UNIT</td>
<td>ACS-4</td>
<td>See 4.5.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>FREEZE LOCK</td>
<td>ACS-4</td>
<td>See 4.5.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SET PASSWORD</td>
<td>ACS-4</td>
<td>See 4.5.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UNLOCK</td>
<td>ACS-4</td>
<td>See 4.5.1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DATA SET MANAGEMENT XL</td>
<td>ACS-4</td>
<td>See DATA SET MANAGEMENT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZAC Management Out</td>
<td></td>
<td>See ZAC Management Out</td>
<td></td>
</tr>
<tr>
<td>SEND FPDMA QUEUED</td>
<td>SET ACCESSIBLE MAX ADDRESS EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>SET DATE &amp; TIME EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Command</td>
<td>Subcommand / Special Cases</td>
<td>Reference</td>
<td>Read Command</td>
<td>Write Command</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------</td>
<td>-----------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>SET FEATURES</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>ADDRESS</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>ADDRESS EXT</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>FREEZE LOCK</td>
<td>ACS-2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>LOCK</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>SET PASSWORD</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>UNLOCK</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET MAX</td>
<td></td>
<td>ACS-2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET MULTIPLE MODE</td>
<td></td>
<td>ACS-3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SET SECTOR CONFIGURATION EXT</td>
<td></td>
<td>ACS-4</td>
<td>See 4.5.4</td>
<td>Yes</td>
</tr>
<tr>
<td>SLEEP</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SMART</td>
<td>DISABLE OPERATIONS</td>
<td>ACS-3</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>ENABLE OPERATIONS</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>ENABLE/DISABLE AUTOSAVE</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>EXECUTE OFF-LINE IMMEDIATE</td>
<td></td>
<td>Vendor specific a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>READ DATA</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>READ LOG</td>
<td>ACS-4</td>
<td>See READ LOG DMA EXT</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>RETURN STATUS</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>WRITE LOG</td>
<td>ACS-4</td>
<td>See WRITE LOG DMA EXT</td>
<td>No</td>
</tr>
<tr>
<td>STANDBY</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Command</td>
<td>Subcommand / Special Cases</td>
<td>Referenc e</td>
<td>Read Command</td>
<td>Write Command</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------</td>
<td>------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>STANDBY IMMEDIATE</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TRUSTED NON-DATA</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TRUSTED RECEIVE</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TRUSTED RECEIVE DMA</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TRUSTED SEND</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>TRUSTED SEND DMA</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE BUFFER</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE BUFFER DMA</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE DMA</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE DMA FUA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE FPDMA QUEUED</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE LOG DMA EXT</td>
<td>ACS-4</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WRITE MULTIPLE</td>
<td>ACS-3</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE MULTIPLE EXT</td>
<td>ACS-3</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE MULTIPLE FUA EXT</td>
<td>ACS-3</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>WRITE SECTOR(S)</td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### ATA Command Interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRITE SECTOR(S) EXT</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE STREAM DMA EXT</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE STREAM EXT</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WRITE UNCORRECTABLE EXT</td>
<td></td>
<td>ACS-4</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>REPORT REALMS EXT</td>
<td>REPORT ZONE DOMAINS EXT</td>
<td>ZAC-2</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>REPORT ZONES EXT</td>
<td>ZAC-2</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ZONE ACTIVATE EXT</td>
<td>ACS-4, ZAC</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ZONE QUERY EXT</td>
<td>ZAC-2</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>CLOSE ZONE EXT</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FINISH ZONE EXT</td>
<td>ACS-4, ZAC</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>OPEN ZONE EXT</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RESET WRITE POINTER EXT</td>
<td></td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ZERO EXT</td>
<td>SEQUENTIALIZE ZONE EXT</td>
<td>ZAC</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ZONE ACTIVATE EXT</td>
<td></td>
<td>ZAC-2</td>
<td>See ZAC Management In</td>
<td></td>
</tr>
<tr>
<td>ZONE QUERY EXT</td>
<td>ZAC-2</td>
<td>See ZAC Management In</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### ATA Command Interactions with the Locking SP

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand / Special Cases</th>
<th>Reference</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
</table>

*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 31 specifies the interactions of NVMe commands not already described by other subclauses.

The commands in Table 31 MAY be supported on an NVM subsystem that incorporates the Locking Template. Table 31 identifies whether an NVMe Commands 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 31 as Read commands SHALL behave as defined in the Interface Read Command Access table (see [17]).

Commands identified in Table 31 as Write commands SHALL behave as defined in the Interface Write Command Access table (see [17]).

<table>
<thead>
<tr>
<th>Command</th>
<th>Subcommand</th>
<th>Read Command</th>
<th>Write Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Asynchronous Event Request</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Compare</td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Create I/O Completion Queue</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Create I/O Submission Queue</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dataset Management</td>
<td>Attribute – Deallocate</td>
<td>No</td>
<td>See 5.5.5</td>
</tr>
<tr>
<td></td>
<td>Attribute – Integral Dataset for Read</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Attribute – Integral Dataset for Write</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete I/O Completion Queue</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Delete I/O Submission Queue</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Doorbell Buffer Config</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Device Self-Test</td>
<td></td>
<td>Vendor specific a</td>
<td></td>
</tr>
<tr>
<td>Directive Receive</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Directive Send</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Firmware Commit</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Firmware Image Download</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Flush</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Format NVM</td>
<td></td>
<td>No</td>
<td>See 5.5.3</td>
</tr>
<tr>
<td>Get Features</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Get Log Page</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Identify</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Command</td>
<td>Subcommand</td>
<td>Read Command</td>
<td>Write Command</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>--------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Keep Alive</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Namespace Attachment</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Namespace Management</td>
<td></td>
<td></td>
<td>See 5.5.1</td>
</tr>
<tr>
<td>NVMe-MI Receive</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>NVMe-MI Send</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Read</td>
<td></td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Reservation Acquire</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Reservation Register</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Reservation Release</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Reservation Report</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Sanitize</td>
<td></td>
<td></td>
<td>See 5.5.4</td>
</tr>
<tr>
<td>Security Receive</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Security Send</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Set Features</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Write</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Write Uncorrectable</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Write Zeroes</td>
<td></td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtualization Management</td>
<td></td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

*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.*