TCG Storage Interface Interactions Specification (SIIS)

Specification Version 1.02
Revision 1.00

30 December, 2011

TCG

TCG PUBLISHED

Change History

Version	Date	Description
Version 1.00 Rev 1.00	27 Jan 2009	First publication
Version 1.01 Revision 1.00	03 Nov 2011	for all interfaces: a) added specification of Current Maximum LBA b) clarified the specification of behavior when Transfer Length is zero for the SCSI interface a) added mapping of USB and UAS resets b) clarified the use of INC_512 c) Tables 4 and 5: indicated which standard or specification defines the event, and removed the false indication that all of the events were 'resets' d) SCSI: Table 7: changed TRANSFER LENGTH to ALLOCATION LENGTH and noted that the non-zero length requirement is a variance from the definition of the command in SPC-4 for the ATA interface: a) changed the base ATA reference from ATA8-ACS to ACS-2 b) clarified the Locking Template interactions with the ATA Security feature set to include Locking SP activation and revert functions c) clarified the use of the ATA Sense Data Reporting feature set in ATA error reporting d) added specification of interaction of the ATA Sanitize Device feature set with the Locking SP e) Addressed comments received during public review
Version 1.02 Revision 1.00	30 Dec 2011	Added NVM Express support

Table of Contents

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 MAY also serve 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 MAY wish to tie storage devices and peripherals into trusted platforms.

1.4 References to Other Documents

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

[2]. [INCITS T10/1683-D], "Information technology - SCSI Architecture Model - 4 (SAM-4)"

[3]. [INCITS T10/1731-D], "Information technology - SCSI Primary Commands - 4 (SPC-4)"

[4]. [INCITS T10/1799-D], "Information technology - SCSI Block Commands - 3 (SBC-3)"

[5]. [INCITS T13/2015-D], "Information technology - ATA/ATAPI Command Set - 2 (ACS-2)"

[6]. [INCITS T13/1700-D], "Information technology - AT Attachment – 8 ATA/ATAPI Architecture Model (ATA8-AAM)"

[7]. [INCITS T10/1828-D], "Information technology - Fibre Channel Protocol for SCSI, Fourth Version (FCP-4)"

[8]. [ANSI INCITS 417-2006], "Information technology - Serial Attached SCSI - 1.1 (SAS-1.1)

[9]. Information technology - USB Attached SCSI (UAS), T10/2095-D Revision 4, March 9, 2010

[10]. Universal Serial Bus Mass Storage Class USB Attached SCSI Protocol (UASP), Revision 1.0, June 24, 2009

[11]. Universal Serial Bus Mass Storage Class Bulk-Only Transport (USBBOT), Revision 1.0, September 31, 1999

[12]. NVM Express Specification version 1.0. Available from http://www.nvmexpress.org/

1.5 Definition of Terms

Term	Definition
IF-RECV	An interface command used to retrieve security protocol data from the TPer.
IF-SEND	An interface command used to transmit security protocol data to the TPer.
Locking SP	A security provider that incorporates the Locking Template as described in the Core Spec.
SSC	Security Subsystem Class. SSC specifications describe profiled sets of TCG functionality
TCG Reset	A high-level reset type defined in the Core Spec.
TPer	The TCG security subsystem within a storage device.
Trusted Peripheral	A TPer.

.

2 Overview

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 issues

3 SCSI Interface

See [2], [3], [4], [7] and [8] for details on SCSI architecture, commands and transports.

See [5] for details on ATAPI commands.

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

3.1 Mapping of Resets

Table 1 - SAS Resets Mapped to TCG reset_type

SAS Event	Maps to TCG reset_type
Power on reset	Power cycle
I-T Nexus Loss	(none)
Task Management-Abort Task	(none)
Task Management-Abort Task Set	(none)
Task Management-Clear Task Set	(none)
Task Management-Clear ACA	(none)
Task Management-I-T Nexus reset	(none)
Task Management-LUN Reset	Hardware Reset
Link Reset Sequence	(none)
Link reset sequence with hard reset	Hardware Reset

Table 2 - Fibre Channel Resets Mapped to TCG reset_type

FC Event	Maps to TCG reset_type	Other Comments
Power on reset	Power cycle	
I-T Nexus Loss	(none)	
Task Management-Abort Task	(none)	
Task Management-Abort Task Set	(none)	
Task Management-Clear Task Set	(none)	
Task Management-Clear ACA	(none)	
Task Management-I-T Nexus reset	(none)	
Task Management-LUN Reset	Hardware Reset	
Task Management-Target reset	Hardware Reset	
LIP(AL_PD,AL_PS)	Hardware Reset	LIP directed reset
LIP(FF,AL_PS)	Hardware Reset	LIP Global reset
Port Login	(none)	
Process Login	(none)	

Table 3 - ATAPI Resets Mapped to TCG reset_type

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

Table 4 - UAS Events Mapped to TCG reset_type

Event	Maps to TCG reset_type	Reference
Device Power Cycle	Power cycle	[11]
Task Management-Abort Task	(none)	[3]
Task Management-Abort Task Set	(none)	[3]
Task Management-Clear Task Set	(none)	[3]
Task Management-Clear ACA	(none)	[3]
Task Management-I-T Nexus reset	Hardware Reset	[3]
Task Management-LUN Reset	(none)	[3]
USB VBus Power Cycle	Power cycle	[11]
USB Port Reset	(none)	[11]
USB Set Configuration with wValue set to zero	(none)	[11]
USB Set Configuration with wValue set to non-zero value that is not equal to the current value of bConfiguration.	(none)	[11]
USB Set Configuration with wValue set to non-zero value that is equal to the current value of bConfiguration.	(none)	[11]
USB Bulk-Out Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-Out pipe of the Mass Storage Interface)	(none)	[11]
USB Bulk-In Endpoint Reset (Also known as Clear Feature, Endpoint Halt of the first Bulk-In pipe of the Mass Storage Interface)	(none)	[11]
USB Suspend	Hardware Reset	[11]
USB Resume	Hardware Reset	[11]

Table 5 - USB Events Mapped to TCG reset_type

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

3.2 Mapping of IF-SEND and IF-RECV

3.2.1 IF_SEND

IF_SEND SHALL be implemented with the SECURITY PROTOCOL OUT [3] command, with additional requirements on the CDB as specified in Table 6.

Table 6 - IF-SEND CDB field contents (SCSI)

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

[a] If the INC_512 parameter in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3).

[b] If the TRANSFER LENGTH parameter 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 [3] command, with additional requirements on the CDB as described in Table 7.

Table 7 - IF-RECV CDB field contents (SCSI)

SECURITY PROTOCOL	SECURITY PROTOCOL SPECIFIC	INC_512	ALLOCATION LENGTH
0x00	(See [3] for details)	0 or 1	INC_512=0: Number of bytes of data. INC_512=1: Number of 512-byte data units.
0x01	a ComID	1 [a]	Non-zero [b] number of 512-byte data units.
0x02	a ComID	1 [a]	Non-zero [b] number of 512-byte data units.
0x06	a ComID	0	Number of bytes of data.

[a] If the INC_512 parameter in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3).

[b] If the ALLOCATION LENGTH parameter in the CDB is zero, then the TPer SHALL report Other Invalid Command Parameter (see 3.3), even though SPC-4 allows ALLOCATION LENGTH 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 8 - TPer Errors (SCSI)

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

3.4 Discovery of Security Capabilities

3.4.1 Security Protocol 0x00

See the description of SECURITY PROTOCOL IN [3] for information on Security Protocol `0x00`.

3.5 Miscellaneous Issues

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

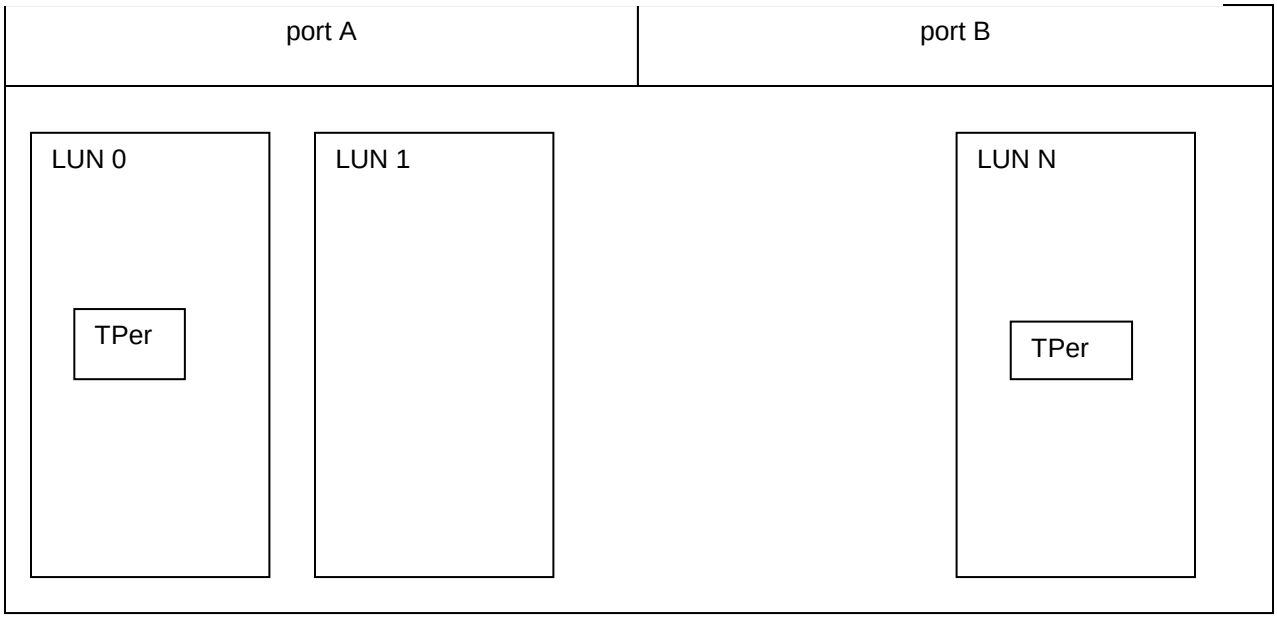
3.5.2 MBR Interactions

The LUN associated with the MBR is the boot LUN.

3.5.3 LUN usage

A target that has multiple LUNs MAY have multiple TPers. Each TPer SHALL be associated with a different LUN. Every LUN on a device is not required to have a TPer, but LUNs that support the TCG Core specification commands and functionality SHALL have a TPer. A TPer SHALL only be associated with exactly one LUN. A LUN MAY have no TPer.

Figure 1 - SCSI target: port, LUN and TPer relationships



3.5.4 Current Maximum LBA

The Current Maximum LBA is the maximum LBA that is permitted at the current time by a normal read or write command.

Table 9 specifies the definition of Current Maximum LBA. Current Maximum LBA is undefined if it is not specified in Table 9.

Table 9 - Current Maximum LBA (SCSI)

READ CAPACITY(10) [1]	**READ CAPACITY(16) [1]**	**Current Maximum LBA**
RETURNED LOGICAL BLOCK ADDRESS < FFFF_FFFFh	CDB not supported	READ CAPACITY(10) RETURNED LOGICAL BLOCK ADDRESS parameter
RETURNED LOGICAL BLOCK ADDRESS <= FFFF_FFFFh	CDB supported and RETURNED LOGICAL BLOCK ADDRESS <= FFFF_FFFF_FFFF_FFFEh	READ CAPACITY(16) RETURNED LOGICAL BLOCK ADDRESS parameter
[1] For this determination, PMI shall be set to zero in the CDB.		

4 ATA Interface

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

4.1 Mapping of Resets

Table 10 - ATA Resets Mapped to TCG reset_type

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

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 11:

Table 11 - IF-SEND command parameters (ATA)

Security Protocol	SP_Specific	Transfer Length
0x00	Security protocol 0x00 is not defined for IF-SEND	
0x01	a ComID	Non-zero [a] number of 512-byte data units.
0x02	a ComID	Non-zero [a] number of 512-byte data units.
0x06	Protocol 0x06 is defined for SCSI only.	
[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 12:

Table 12 - IF-RECV command parameters (ATA)

Security Protocol	SP_Specific	Transfer Length
0x00	(See [5])	Non-zero number of 512-byte data units.
0x01	a ComID	Non-zero [a] number of 512-byte data units.
0x02	a ComID	Non-zero [a] number of 512-byte data units.
0x06	Protocol 0x06 is defined for SCSI only.	
[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. Table 13 describes common TPer errors when SDR is disabled. Table 14 describes common TPer errors when SDR is enabled.

Table 13 - TPer Errors (ATA) – Sense Data Reporting is Disabled

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

Table 14 - TPer Errors (ATA) – Sense Data Reporting is Enabled

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

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 Issues

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 Locking Template interactions with the ATA Sanitize Device feature set

The storage device MAY support (i.e., IDENTIFY DEVICE, word 59, bit 12 = 1) the ATA Sanitize Device feature set when no SP exists that incorporates the Locking Template or when an SP that incorporates the Locking Template is in the Manufactured-Inactive state. In all other cases, the storage device SHALL report that the ATA Sanitize Device feature set is not supported (i.e., IDENTIFY DEVICE, word 59, bit 12 = 0).

4.5.2 Current Maximum LBA

The Current Maximum LBA is the maximum LBA that is permitted at the current time by a normal read or write command. Table 15 specifies the definition of Current Maximum LBA.

Table 15 - Current Maximum LBA (ATA)

IDENTIFY DEVICE word 83 bit 10	IDENTIFY DEVICE word 69 bit 3	Current Maximum LBA
0	N/A	(IDENTIFY DEVICE words 60 to 61) minus 1
1	0	(IDENTIFY DEVICE words 100 to 103) minus 1
1	1	(IDENTIFY DEVICE words 230 to 233) minus 1

5 NVM Express Interface

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

5.1 Mapping of Resets

Table 16 – NVM Express Resets Mapped to TCG reset_type

NVM Express Event	**Maps to TCG** reset_type
Power (power-up)	Power Cycle
Power (PCIe link down)	None
Controller reset	None
Function level (PCI) reset	None
Queue level reset	None

5.2 Mapping of IF-SEND and IF-RECV

5.2.1 IF_SEND

IF_SEND shall be implemented with the Security Send command [12], with additional requirements on the inputs as described in Table 17:

Table 17 - IF-SEND command parameters (NVM Express)

Security Protocol	SP_Specific	Transfer Length
0x00	Security protocol 0x00 is not defined for IF-SEND	
0x01	a ComID	Number of bytes to transfer.
0x02	a ComID	Number of bytes to transfer.
0x06	Protocol 0x06 is defined for SCSI only.	

5.2.2 IF_RECV

IF_RECV SHALL be implemented with the Security Receive command [12], with additional requirements on the inputs as described in Table 18:

Table 18 - IF-RECV command parameters (NVM Express)

Security Protocol	SP_Specific	Allocation Length
0x00	(See [12])	Number of bytes to transfer.
0x01	a ComID	Number of bytes to transfer.
0x02	a ComID	Number of bytes to transfer.
0x06	Protocol 0x06 is defined for SCSI only.	

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 and the Status Code (SC) field shall indicate and map the TPer error as in Table 19.

Table 19 - TPer Errors (NVM Express)

TPer Error ID	Status Code Type	Status Code	Comments
Good	Generic Command Status	Successful Completion	Normal command completion
Invalid Security Protocol ID parameter	Generic Command Status	Invalid Field in Command	No data shall be transferred.
Invalid Transfer Length parameter on IF-SEND	Generic Command Status	Invalid Field in Command	No data shall be transferred.
Other Invalid Command Parameter	Generic Command Status	Invalid Field in Command	No data shall be transferred.
Synchronous Protocol Violation	Generic Command Status	Command Sequence Error	No data shall be transferred.
Data Protection Error	Media Errors	Access Denied	No data shall be transferred.

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 Issues

5.5.1 Security Commands

The optional Security Send and Security Receive commands SHALL be implemented by the device.

5.5.2 Namespace

A target that has multiple Namespaces MAY have multiple TPers. Each TPer SHALL be associated with a different Namespace. Every Namespace on a device is not required to have a TPer, but Namespaces that support the TCG Core specification commands and functionality SHALL have a TPer. A TPer SHALL only be associated with exactly one Namespace. A Namespace MAY have no TPer.

5.5.3 Locking Template interactions with the Format NVM Command

5.5.3.1 Format NVM Command Behavior

If the Namespace is not `0xFFFFFFFF` and an SP exists in that Namespace's TPer that incorporates the Locking Template, and the lifecycle state of that SP is not "Manufactured-Inactive", then the Format NVM command SHALL fail with an Invalid Security State condition returned in the Admin Completion Queue, Command Specific Error.

If the Namespace is `0xFFFFFFFF` and if any Namespace's TPer contains an SP that incorporates the Locking Tamplate, and the lifecycle state of any of those SPs is not "Manufactured-Inactive", then the FormatNVM command SHALL fail with an Invalid Security State condition returned in the Admin Completion Queue, Command Specific Error.

If no Namespace contains a TPer that contains an SP that incorporates the Locking Template, or if all SPs that incorporate the Locking Template are in the "Manufactured-Inactive" lifecycle state, then the Identify Controller Data Structure NVM Command Set Attributes Field, Format NVM Attributes (FNA) bit 2 MAY be set to one to indicate cryptographic erase is supported. Otherwise, the Identify Controller Data Structure NVM Command Set Attributes Field, Format NVM Attributes (FNA) bit 2 SHALL be cleared to zero to indicate cryptographic erase is not supported.