TCG Storage Interface Interactions Specification

Specification Version 1.0

January 27, 2009

Contacts:
storagewg@trustedcomputinggroup.org

TCG

Disclaimer, Notices and License Terms

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

[6]. [ANSI INCITS 452-2008], "Information technology – AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS)"

[7]. INCITS T13 proposal E07123R4 “ACS-2: REQUEST SENSE for ATA"

[8]. INCITS T13 proposal E07172R6 “ACS-2 Issues List" (item #18)

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

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

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], [9] and [10] for details on SCSI architecture, commands and transports.

See [6] for details on ATAPI commands.

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)

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 4.

Table 4 - IF-SEND CDB field contents (SCSI)

SECURITY PROTOCOL	SECURITY PROTOCOL SPECIFIC	INC_512	TRANSFER LENGTH
0x01	a ComID	1	Non-zero number of 512-byte data units.
0x02	a ComID	1	Non-zero number of 512-byte data units.
0x06	a ComID	0	Non-zero number of bytes of data.

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 5.

Table 5 - IF-RECV CDB field contents (SCSI)

SECURITY PROTOCOL	SECURITY PROTOCOL SPECIFIC	INC_512	ALLOCATION LENGTH
0x00	(See SPC-4 for details)	0 or 1	INC_512=0: Non-zero number of bytes of data. INC_512=1: Non-zero number of 512-byte data units.
0x01	a ComID	1	Non-zero number of 512-byte data units.
0x02	a ComID	1	Non-zero number of 512-byte data units.
0x06	a ComID	0	Non-zero number of bytes of data.

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 6 - TPer Errors (SCSI)

TPer Error ID	Status	Sense Key	ASC/ASCQ	Comments
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).

> NOTE: 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.

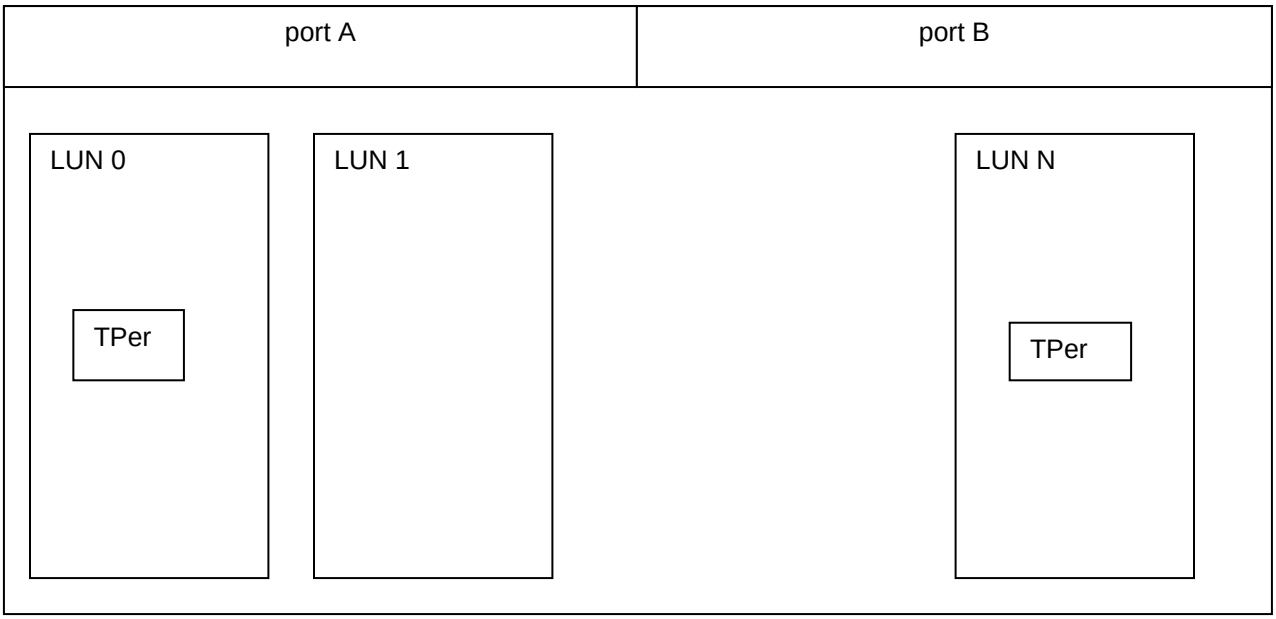
3.5.2 MBR Interactions

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



4 ATA Interface

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

See [7] and [8] for details on the optional Enhanced Status Reporting feature set. This has been accepted by T13 for inclusion in a new draft standard (ACS-2).

4.1 Mapping of Resets

Table 7 - 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 8:

Table 8 - IF-SEND command parameters (ATA)

Security Protocol	SP_Specific	Transfer Length
0x01	a ComID	Non-zero number of 512-byte data units.
0x02	a ComID	Non-zero number of 512-byte data units.
0x06	N/A	Protocol 0x06 is defined for SCSI only.

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 9:

Table 9 - IF-RECV command parameters (ATA)

Security Protocol	SP_Specific	Transfer Length
0x00	(See [6])	Non-zero number of 512-byte data units.
0x01	a ComID	Non-zero number of 512-byte data units.
0x02	a ComID	Non-zero number of 512-byte data units.
0x06	N/A	Protocol 0x06 is defined for SCSI only.

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 [7] and [8] for information about the Enhanced Status Reporting (ESR) feature set. The error reporting method is different when ESR is supported and enabled than otherwise.

Table 10 - TPer Errors (ATA) – Enhanced Status Reporting is Enabled

TPer Error ID	ESR Supported and Enabled	ATA Status Field	ATA Error Field	Sense Key	ASC/ASCQ	Comments
Invalid Security Protocol ID parameter	No	0x51	0x04	N/A	N/A	No data shall be transferred
	Yes	0x51	0x7F	ILLEGAL REQUEST	INVALID FIELD IN CDB	
Invalid Transfer Length parameter on IF-SEND	No	0x51	0x04	N/A	N/A	No data shall be transferred.
	Yes	0x51	0x7F	ILLEGAL REQUEST	INVALID FIELD IN CDB	
Other Invalid Command Parameter	No	0x51	0x04	N/A	N/A	No data shall be transferred.
	Yes	0x51	0x7F	ILLEGAL REQUEST	INVALID FIELD IN CDB	
Synchronous Protocol Violation	No	0x51	0x04	N/A	N/A	No data shall be transferred.
	Yes	0x51	0x7F	ILLEGAL REQUEST	COMMAND SEQUENCE ERROR	
Data Protection Error	No	0x51	0x04	N/A	N/A	No data shall be transferred.
	Yes	0x51	0x7F	DATA PROTECT	ACCESS DENIED– NO ACCESS RIGHTS	

4.4 Discovery of Security Capabilities

4.4.1 IDENTIFY DEVICE

The IDENTIFY DEVICE command (see [6]) 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 [6]) 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 Extended Status Reporting feature

The ACS-2 Extended Status Reporting feature SHOULD be supported by the device. It is automatically disabled by a power on reset. If it is supported, it MAY be enabled via the SET FEATURES command after every power on reset

4.5.1.3 Locking SP Life Cycle interactions with the ATA Security feature set

The storage device MAY support the ATA Security feature set when the Locking SP is in the "Nonexistent" state (for TPers that support issuance of the Locking SP) or the "Manufactured-Inactive" state (for TPers that contain a manufactured Locking SP). In all other life cycle states for the Locking SP, the storage device SHALL report that the ATA Security feature set is "not supported" (IDENTIFY DEVICE, word 82, bit 1 = 0).

When ATA Security is Enabled (a User Password is set), the TPer SHALL prohibit issuance of the Locking SP, and SHALL prohibit a manufactured Locking SP from transitioning out of the "Manufactured-Inactive" state.