

ATA8-ACS Errata

December 4, 2008

Revision 1

Technical Editor:

Jim Hatfield
389 Disc Drive
Longmont, CO 80503
720-684-2120
James.C.Hatfield@Seagate.com

Document Status

Revision History		
Rev	Date	Description
0	Oct. 28, 2006	1) Initial Revision
	Dec. 4, 2006	1) Add specification for TRUSTED NON-DATA in Table 9 "Security Command Actions"

1 Introduction

ATA8-ACS had many, many changes to old material, and included many new features. One of these new features was the TRUSTED NON-DATA command. It was introduced hastily as a response to a letter ballot comment. As a result of the haste, it was not specified well enough to prevent some alternative interpretations.

While ATA8-ACS was being developed, the SATA-IO organization was also developing new features, on its own schedule. SATA-IO recently updated its base T13 reference from ATA/ATAPI-6 to ATA8-ACS. In the process, it introduced a discrepancy with ATA8-ACS.

This proposal seeks to make corrections to ATA8-ACS, and to copy those changes into ACS-2.

2 Scope

Errata to ATA8-ACS and new changes for ACS-2.

It is intended that an ATA8-ACS Erratum project be created and approved by T13 and INCITS.

3 Overview

Regarding the Write-Read-Verify (W-R-V) feature set, ATA8-ACS says that the device shall return to power-on defaults after hardware reset. The author of the Write-Read-Verify proposal later realized that the settings needed to be protected across hardware resets (for SATA) via the Software Settings Preservation (SSP) feature set. Since the SATA-IO organization is the 'owner' of SSP, the change needed to be made there before being done in T13. SATA-IO recently approved the addition of W-R-V to SSP processing, but not until after ATA8-ACS was finalized. In order to remove the discrepancy, this proposal is seeking to add this change to an Erratum for ATA8-ACS.

Regarding the TRUSTED NON-DATA command, there is confusion about how it should behave for security protocols that do not support non-zero data transfers. In particular, the T10 SPC-4 specification allows zero-length data transfer for SECURITY PROTOCOL IN for Security Protocol 00h, but the T13 ATA8-ACS specification does not allow it. There is no specification for the processing of the SP Specific parameter. In addition, the Normal and Error outputs for TRUSTED NON-DATA do not specify what should be returned in the fields which TRUSTED SEND and TRUSTED RECEIVE use for the Transfer Count parameter. Since several security protocols reference ATA8-ACS, it is important to correct that specification. There is no means to determine if the optional TRUSTED NON-DATA command is supported without trial and error. The SAT-2 standard requires it to be implemented, so this proposal makes it a mandatory part of the Trusted Computing feature set.

3.1 Changes to clause 4

(Table 9 - Security Command Actions)

Add a row for TRUSTED NON-DATA:

Table 1 — (Table 9 - Security Command Actions)

Command	Locked	Disabled or Unlocked	Frozen
TRUSTED NON-DATA	Executable	Executable	Executable

4.25 Trusted Computing feature set

The Trusted Computing feature set provides an interface between a horizontal security product embedded in devices whose behavior may be authorized via interaction with a trusted host system.

The following commands are mandatory for devices implementing the Trusted Computing feature set:

- a) TRUSTED SEND;
- b) TRUSTED SEND DMA;
- c) TRUSTED RECEIVE; ~~and~~
- d) TRUSTED RECEIVE DMA; [and](#)
- e) [TRUSTED NON-DATA](#).

~~The following command is optional for devices implementing the Trusted Computing feature set:~~

- ~~a) TRUSTED NON-DATA.~~

TRUSTED SEND and TRUSTED SEND DMA may be used interchangeably. The two commands only differ by the type of data transport protocol used (i.e., PIO Data-Out Command or DMA Command). Similarly, TRUSTED RECEIVE and TRUSTED RECEIVE DMA are interchangeable (i.e., PIO Data-In Command or DMA Command). IDENTIFY DEVICE data word 48 bit 0 indicates whether or not this feature set is supported.

The DEVICE CONFIGURATION OVERLAY SET command provides a mechanism to remove support for this feature set.

The data streams and subsequent actions resulting from these commands are defined by the security protocol identified in the command parameters. These protocols may be defined by groups outside of this standard. The intent is to standardize the data content so it is identical across both ATA and SCSI interfaces.

3.2 Changes to clause 7

7.48.10 Enable/Disable Write-Read-Verify feature set

Subcommand code 0Bh enables the Write-Read-Verify feature set. Subcommand code 8Bh disables the Write-Read-Verify feature set.

...

Current text:

A device shall set the Write-Read-Verify feature set to its factory default setting after processing of a power-on reset or a hardware reset.

If a device is in the reverting to defaults enabled mode (see 7.48.16), then the device shall set the Write-Read-Verify feature set to its factory default setting after processing of a software reset.

If a device is in the reverting to defaults disabled mode (see 7.48.16), then the device shall not change the settings of the Write-Read-Verify feature set after processing of a software reset.

Proposed text:

A device shall set the Write-Read-Verify feature set to its factory default setting after processing of a power-on reset ~~or hardware reset~~ or if the Software Settings Preservation feature set is disabled and a hardware reset is processed. If the Software Settings Preservation feature set is enabled and a hardware reset is processed, the device shall not change the settings of the Write-Read-Verify feature set.

If a device is in the reverting to defaults enabled mode (see 7.48.16), then the device shall set the Write-Read-Verify feature set to its factory default setting after processing of a software reset.

If a device is in the reverting to defaults disabled mode (see 7.48.16), then the device shall not change the settings of the Write-Read-Verify feature set after processing of a software reset.

7.56 TRUSTED NON-DATA - 5Bh, Non-Data

7.56.1 Feature Set

This 28-bit command is ~~optional~~ **mandatory** for devices implementing the Trusted Computing feature set..

7.56.2 Description

The TRUSTED NON-DATA command delivers the SP Specific field using the specified Security Protocol and transfers no data.

7.56.3 Inputs

Name	Description
Feature	Security Protocol (see 7.57.3.2)
Count	Reserved
LBA	<p>Bit Description</p> <p>27:25 Reserved</p> <p>24 Direction</p> <p>0 - Non-Data TRUSTED SEND, 1 - Non-Data TRUSTED RECEIVE</p> <p>23:8 SP Specific - Security Protocol Specific (see 7.57.6)</p> <p>7:0 Reserved</p>
Device	<p>Bit Description</p> <p>7 Obsolete</p> <p>6 Shall be set to one</p> <p>5 Obsolete</p> <p>4 Transport Dependent - See 6.1.10</p> <p>3:0 Reserved</p>
Command	7:0 5Bh

7.56.3.2 Security Protocol

If Bit 24 is cleared to zero then see 7.59.3.2 ([TRUSTED SEND](#)); otherwise, see 7.57.3.2 ([TRUSTED RECEIVE](#)). The device shall transfer no data, and shall ignore any requirements relating to the Transfer Length field.

7.56.3.3 Operation

Bit 24 selects the operation for which this command is emulating a zero-length transfer.

7.56.3.3 SP Specific

If Bit 24 is cleared to zero then see 7.59.3.2 ([TRUSTED SEND](#)); otherwise, see 7.57.3.2 ([TRUSTED RECEIVE](#)).

7.56.4 Normal Outputs

~~If Bit 24 is cleared to zero then see 7.59.4; otherwise, see 7.57.4.~~

See table 111.

The device shall return command complete without errors if:

- a) the the Security Protocol is supported for the selected Operation; and
- b) the SP Specific field is valid for the given Security Protocol and Operation.

7.56.5 Error Outputs

~~If Bit 24 is cleared to zero then see 7.59.5; otherwise, see 7.57.5.~~

See table 124.

The device shall return command aborted if:

- a) the the Security Protocol is not supported for the selected Operation; or
- b) the SP Specific field is not valid for the given Security Protocol and Operation. . .