

# ATA8-ACS Errata

January 21, 2008

Revision 2

Technical Editor:

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

**Document Status**

<b>Revision History</b>		
<b>Rev</b>	<b>Date</b>	<b>Description</b>
0	Oct. 28, 2008	1) Initial Revision
1	Dec. 4, 2008	1) Add specification for TRUSTED NON-DATA in Table 9 "Security Command Actions"
2	Jan. 21, 2009	1) Changes requested by Dec. 2008 plenary 2) Add TRUSTED NON-DATA to table 9 3) Change behaviour for all trusted commands (while locked) to be 'executable' 4) Added missing Output Data section to SET MAX UNLOCK.

## 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.

This proposal requests a change to allow the execution of all Trusted Computing feature set commands while ATA security is Locked. Some security protocols (e.g. ATA Device Server Password Security) even require the use of trusted commands while locked. Security Protocol 00h) was designed to be useable at all times. It is desirable to use some security protocols (e.g. IEEE 1667) even before the ATA security state of a device is known. Even the TCG security protocols allow some use while ATA security is Locked. The requirement to abort Trusted Computing commands while ATA security is Locked comes from a time early in the development of security protocols when there was much fear and misunderstanding about interactions between ATA security and other security protocols and before security protocols began to mature.. There is no longer any need for this restriction. In fact, the restriction gets in the way of proper use of some security protocols.

The Output Data section was accidentally omitted for the SET MAX UNLOCK command. This proposal adds the missing material.

### 3.1 Changes to clause 4

(Table 9 - Security Command Actions)

Add a row for TRUSTED NON-DATA, and change locked behaviour to 'security protocol specific'

**Table 1 — (Table 9 - Security Command Actions)**

Command	Locked	Disabled or Unlocked	Frozen
<a href="#">TRUSTED NON-DATA</a>	<a href="#">Executable</a>	<a href="#">Executable</a>	<a href="#">Executable</a>
TRUSTED RECEIVE	<del>Command-aborted</del> <a href="#">Executable</a>	Executable	Executable
TRUSTED RECEIVE DMA	<del>Command-aborted</del> <a href="#">Executable</a>	Executable	Executable
TRUSTED SEND	<del>Command-aborted</del> <a href="#">Executable</a>	Executable	Executable
TRUSTED SEND DMA	<del>Command-aborted</del> <a href="#">Executable</a>	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.

### 3.2.1 SET MAX UNLOCK - F9h/03h, PIO Data-Out

#### 3.2.1.1 Feature Set

This 28-bit command is mandatory for devices that implement the HPA Security Extensions.

#### 3.2.1.2 Description

This command requests a transfer of a single 512-byte block of data from the host. Table 59 defines the content of this data.

The password supplied in the data transferred shall be compared with the password set by the SET MAX SET PASSWORD command.

If the device is locked from HPA commands and the password compare fails, then the device shall return command aborted and decrement the HPA Security Extensions unlock counter. This counter shall be decremented for each password mismatch when SET MAX UNLOCK is issued and the device is locked from HPA commands. When this counter reaches zero in a device, then the device shall return command aborted for all subsequent SET MAX UNLOCK commands until after the device has processed a power-on reset.

NOTE 1 — The HPA Security Extensions unlock counter is not related to the Security feature set unlock counter.

If the device is HPA Locked, the HPA Security Extensions unlock counter is not zero, and the password compare matches, then the device is HPA Unlocked and all SET MAX commands shall be accepted.

This command should not be immediately preceded by a READ NATIVE MAX ADDRESS command. If this command is immediately preceded by a READ NATIVE MAX ADDRESS command, it shall be interpreted as a SET MAX ADDRESS command.

#### 3.2.1.3 Inputs

Name	Description
Feature	03h
Count	N/A
LBA	N/A
Device	<p><b>Bit Description</b></p> <p>7 Obsolete</p> <p>6 N/A</p> <p>5 Obsolete</p> <p>4 Transport Dependent - See 6.2.11</p> <p>3:0 Reserved</p>
Command	7:0 F9h

#### 3.2.1.4 Normal Outputs

See table 99.

#### 3.2.1.5 Error Outputs

If a device is not HPA Locked, then the device shall return command aborted. A device may return command completion with the Error bit set to one if an Interface CRC error has occurred. See table 126.

#### [3.2.1.6 Output From the Host to the Device Data Structure](#)

[See Table 59](#)

## 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><b>Bit Description</b></p> <p>27:25 Reserved</p> <p>24 Direction</p> <p>0 - Non-Data TRUSTED SEND (<a href="#">see 7.59</a>)</p> <p>1 - Non-Data TRUSTED RECEIVE (<a href="#">see 7.57</a>)</p> <p>23:8 SP Specific - Security Protocol Specific (see 7.57.6)</p> <p>7:0 Reserved</p>
Device	<p><b>Bit Description</b></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; otherwise, see 7.57.3.2. [The device shall transfer no data, and shall ignore any requirements relating to the Transfer Length field.](#)

#### 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 Direction; and](#)
- [b\) the SP Specific field is valid for the given Security Protocol and Direction.](#)

#### 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.](#)

(Make this modification to section 7.57.6)

### 3.2.2 (7.57.6) Security Protocol 00h Description

#### 3.2.2.1 (7.57.6.1) Overview

The purpose of Security Protocol 00h is to return basic information about the device. A TRUSTED RECEIVE using Security Protocol field set to 00h is not linked to an earlier TRUSTED SEND command.

[When ATA security is Locked, TRUSTED RECEIVE for Security Protocol 00h shall be executable.](#)

The Transfer Length field contains the number of 512-byte blocks of data to be transferred (e.g., one means 512 bytes, two means 1,024 bytes). A transfer length of zero is invalid.

The total data length shall conform to the Transfer Length field requirements (e.g., the total data length shall be a multiple of 512). Pad bytes shall be added as needed to meet this requirement. Pad bytes shall have a value of 00h.

If the length of the TRUSTED RECEIVE parameter data is greater than the Transfer Length, then the device shall return the TRUSTED RECEIVE parameter data truncated to the requested Transfer Length.

When the Security Protocol field is set to 00h, the SP Specific field is shown in table 2.

**Table 2 — Security Protocol 00h - SP Specific field descriptions for Protocol 00h**

SP Specific	Description	Support
0000h	Return supported security protocol list (see 7.57.6.2)	Mandatory
0001h	Return a certificate (see 7.57.6.3)	Mandatory
0002h-FFFFh	Reserved	

If the SP Specific field is set to a reserved value, the command shall be aborted.

Each time a TRUSTED RECEIVE command with Security Protocol field set to 00h is received, the device shall transfer the data starting with byte 0.